88

PROPOZYCJE I MATERIAŁY

Łukasz Kołodziejczyk

Prywatność w Internecie

Nagroda Młodych SBP

WYDAWNICTWO SBP

Prywatność w Internecie: postawy i zachowania dotyczące ujawniania danych prywatnych w mediach społecznych

Stowarzyszenie Bibliotekarzy Polskich

88

Propozycje i Materiały

Łukasz Kołodziejczyk

Prywatność w Internecie: postawy i zachowania dotyczące ujawniania danych prywatnych w mediach społecznych

Wydawnictwo SBP

Warszawa 2014

Recenzja: prof. dr hab. Barbara Sosińska-Kalata

Redaktor prowadzący: Marta Lach

Projekt okładki: Studio Kałamarnica

Redakcja techniczna i korekta: Patrycja Lewandowska

ISBN: 978-83-64203-20-6

CIP – Biblioteka Narodowa
Kołodziejczyk, Łukasz
Prywatność w Internecie : postawy i zachowania dotyczące
ujawniania danych prywatnych w mediach społecznych /
Łukasz Kołodziejczyk. - Warszawa : Wydawnictwo
Stowarzyszenia Bibliotekarzy Polskich, 2014. -
(Propozycje i Materiały / Stowarzyszenie
Bibliotekarzy Polskich ; 88)

Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich
00-335 Warszawa, ul. Konopczyńskiego 5/7, tel. 22 827 52 96
www.sbp.pl
Warszawa 2014. Wyd. I. Ark. wyd. 9,0. Ark. druk. 9,5
Łamanie: Studio Kałamarnica (http://www.studiokalamarnica.pl)
Druk i oprawa: Fabryka Druku sp. z o.o., ul. Zgrupowania AK „Kampinos" 6,
01-943 Warszawa / fabrykadruku@fabrykadruku.pl

STRESZCZENIE

W niniejszej pracy przedstawiono wyniki badań dotyczących prywatności w internetowych mediach społecznych. W pierwszej części opisano różne ujęcia prywatności, m.in. Warrena i Brandeisa, Westina i Altmana; a także dwie współczesne teorie: Petronio i Nissenbaum. W dalszej części pracy omówiona jest specyfika prywatności w cyfrowym środowisku Internetu i mediów społecznych oraz dwa duże raporty z badań na ten temat przeprowadzone przez Microsoft oraz Komisję Europejską. W ostatniej części pracy przedstawione zostały wyniki badań własnych autora przeprowadzonych wśród studentów kierunku *Informacja naukowa i bibliotekoznawstwo*. Do badań wykorzystano metodę pogłębionych wywiadów z listą poszukiwanych informacji. Badania wykazały, że zachowanie prywatności w komunikacji internetowej jest dla badanych ważne. Jednak większość z nich świadomie rezygnuje z dużej jej części. Zwykle starają się oni równocześnie unikać udostępnienia takich danych o sobie, które mogłyby doprowadzić do poważnych naruszeń ich prywatności.

Dziękuję Kalinie, bez której ta praca by nie powstała
Autor

SPIS TREŚCI

Wstęp 9

1. Prywatność i prawo do prywatności 13
   1.1. Definicje i wymiary prywatności 13
      1.1.1. Pierwsze definicje prawa do prywatności 14
      1.1.2. Rozwój teorii Alana Westina i Irwina Altmana 15
      1.1.3. Prywatność jako stan 17
      1.1.4. Wymiary prywatności 18
      1.1.5. Współczesne ujęcia prywatności 19
         1.1.5.1. Prywatność jako integralność kontekstowa informacji 20
         1.1.5.2. Teoria zarządzania prywatnością komunikacji 21
   1.2. Krytyka prawa do prywatności 24
   1.3. Typy postaw w stosunku do prywatności 26

2. Prywatność *online* 29
   2.1. Czym są media społeczne 32
   2.2. Strukturalne cechy Internetu 35
   2.3. Zmiana trybu dostępu do informacji 37
   2.4. Media społeczne – problemy z prywatnością 39
      2.4.1. Niejednorodna publiczność 40
      2.4.2. Niewidzialna publiczność 45
   2.5. Paradoksy prywatności 47
      2.5.1. Beztroska młodzież, zmartwieni rodzice 47
      2.5.2. Niezgodność postaw i zachowań 49
   2.6. Kapitał społeczny a prywatność *online* 53

3. Ochrona prywatności w Internecie 59
   3.1. Prawo 59
      3.1.1. Polityki prywatności 62
   3.2. *Think before you post* – strategie samodzielnej ochrony użytkowników 66
      3.2.1. Ustawienia prywatności 68
   3.3. Rynkowa samoregulacja 71

4. Przegląd badań 77
   4.1. Specjalny Eurobarometr 77
      4.1.1. Cyfrowi tubylcy 78
      4.1.2. Postawy i zachowania dotyczące ujawniania informacji prywatnych 79

4.1.3. Bezpieczeństwo i ochrona prywatności ... 80
4.1.4. Ocena ryzyka ... 81
4.1.5. Personalizacja ... 82
4.1.6. Zaufanie ... 82
4.1.7. Troski ... 83
4.1.8. Prawo ... 84
4.2. Badanie Microsoft „Online Profile & Reputation Perceptions Study" ... 84
4.2.1. Profil *online* ... 85
4.2.2. Kontrola nad profilem ... 88
4.2.3. Konsekwencje korzystania z Internetu ... 89

5. Badanie postaw dotyczących prywatności użytkowników mediów społecznych ... 95
5.1. Projekt i założenia badania ... 95
5.1.1. Wstęp ... 95
5.1.2. Grupa badanych ... 96
5.1.3. Ograniczenia badania ... 96
5.1.4. Pytania badawcze ... 97
5.2. Etap I – ankieta ... 97
5.2.1. Metodologia ... 97
5.2.2. Wyniki ankiety ... 99
5.3. Etap II – pogłębione wywiady indywidualne ... 104
5.3.1. Metodologia ... 104
5.3.2. Etyka badania ... 105
5.3.3. Omówienie wyników ... 105
5.3.3.1. Definiowanie i funkcje prywatności ... 106
5.3.3.2. Pozbywanie się prywatności i całkowita z niej rezygnacja ... 108
5.3.3.3. Funkcje prywatności ... 112
5.3.3.4. Zarządzanie prywatnością w Internecie ... 114
5.3.3.5. Obawy – publikowanie przez osoby trzecie ... 116
5.3.3.6. Obawy – techniczne bezpieczeństwo informacji ... 119
5.3.3.7. Opinie – obowiązek korzystania z prawdziwej tożsamości ... 120
5.3.3.8. Opinie – wykorzystanie mediów społecznych przez pracodawców i rekruterów ... 121
5.3.3.9. Polityki prywatności i ustawienia prywatności ... 123
5.3.3.10. Zachowania, publikowanie ... 125
5.4. Etap III – weryfikacja ... 127
5.5. Podsumowanie badania ... 130

6. Podsumowanie ... 135

Bibliografia ... 141

If you have something that you don't want anyone to know,
maybe you shouldn't be doing it in the first place?

Eric Schmidt (CEO Google) o prywatności w Internecie (2009)

WSTĘP

W ostatnich kilku latach, zarówno w mediach, jak i w dyskursie naukowym, zagadnienie prywatności w Sieci pojawia ze wzrastającą częstotliwością. Wszystkie strony w dyskusji, niezależnie od zajmowanego stanowiska, zgadzają się, że zbieranie i przetwarzanie danych o użytkownikach Internetu jest coraz powszechniejsze, łatwiejsze, tańsze i stwarza coraz większe możliwości dla podmiotów zarządzających tymi danymi. Zjawisko to jest pogłębiane przez zachowanie użytkowników, którzy dobrowolnie zamieszczają prywatne informacje w Internecie, często nie zdając sobie sprawy z konsekwencji. W rezultacie za pomocą wyszukiwarki internetowej można odnaleźć takie informacje jak imię i nazwisko, fotografie, ukończone szkoły, adres zamieszkania czy numer telefonu komórkowego. Osoby, które bardzo aktywnie korzystają z różnych narzędzi w Internecie, pozostawiają po sobie ślady, pozwalające wręcz na odtworzenie ich aktywności na przestrzeni wielu miesięcy, zainteresowań, poglądów – praktycznie kompletnego profilu psychologicznego.

W związku z tym ukuto termin *Prywatność 2.0* (nawiązujący do popularnego *Web 2.0* Tima O'Reilly'ego), który wskazuje na konieczność ponownego określenia znaczenia prywatności w społeczeństwie podłączonym stale do Sieci. W społeczeństwie, w którym życie jednostek jest *transmitowane* na żywo w interneto-

wych mediach społecznych, wiele z tych informacji jest dostępnych publicznie. Pozostałe, ograniczane ustawieniami prywatności serwisów społecznościowych, trafiają do różnorodnego i czasem nieznanego audytorium, które ma możliwość skopiowania i ponownego udostępnienia tych informacji. Wielu internautów nie zdaje sobie sprawy z zachodzących procesów, a nawet jeśli tak jest, to nie potrafi tego procesu kontrolować. Rezygnacja z części własnej prywatności jest w wielu przypadkach pomocna – ludzie korzystają z mediów społecznych po to, żeby się socjalizować i wzbogacać komunikację ze swoimi znajomymi; dane prywatne są wykorzystywane przez firmy internetowe, aby oferować doskonalsze i lepiej spersonalizowane produkty; branża marketingowa otrzymuje możliwość precyzyjnego kierowania reklam, co również może być postrzegane jako korzyść dla ich odbiorców. Media społeczne *żywią się* treściami generowanymi przez użytkowników, co w wielu przypadkach równa się prywatnym informacjom.

Dwaj giganci branży internetowej, firmy Google i Facebook, zbudowali swoją potęgę na podstawie danych zdobytych od użytkowników, którzy często nie mają pełnej wiedzy o zasadach ich gromadzenia, przetwarzania i ponownego wykorzystania. Praktyki tych firm związane z zarządzaniem danymi prywatnymi były wielokrotnie krytykowane w mediach, przez organizacje broniące praw konsumenckich i obywatelskich, a także przez samych użytkowników.

Zacytowane na początku pracy słowa padły podczas udzielonego w 2009 roku wywiadu dla telewizji CNBC w programie „Inside the Mind of Google" (CNBC, 2009) w odpowiedzi na pytanie, czy użytkownicy produktów Google powinni obawiać się o informacje, które ich dotyczą, i są zbierane i przechowywane przez internetowego giganta. Opinia publiczna odczytała wypowiedź Erica Schmidta jako sugestię, że pożądanym standardem jest pełna swoboda w zarządzaniu danymi dotyczącymi osób, a powodem, dla którego ludzie chcą kontrolować informacje o sobie, są wyłącznie zachowania niemoralne czy wręcz kryminalne. Google oskarżono o kolejny atak na prawo do prywatności, którego koncepcja była rozwijana od przeszło stu lat. Prawo to, uznane jest za jedno z podstawowych praw człowieka, a sama prywatność, za jeden ze składników niezbędnych do prawidłowego rozwoju psychologicznego. Dyrektor wykonawczy Facebooka, Mark Zuckerberg, stwierdził, że „prywatność jako społeczna norma przepływu informacji osobistych została zastąpiona przez otwartość" (Kirkpatrick, 2010).

Aktualność, dynamika zagadnienia oraz niewielka liczba opracowań w języku polskim spowodowana niemal całkowitym brakiem badań na polskim gruncie, stały się główną motywacją do podjęcia tematu prywatności w mediach społecznych. Z drugiej strony aktywny dyskurs w nauce międzynarodowej oraz zainte-

resowanie środowiska profesjonalistów zajmujących się nowymi technologiami gwarantuje solidne podstawy teoretyczne, możliwość zaproponowania weryfikowalnych hipotez i przygotowania metodologii badania. Prywatność, jej ochrona, oraz waga, jaką przywiązują do niej użytkownicy Internetu, a więc także cena, za jaką są w stanie się z nią rozstać – to wciąż niezbadane zagadnienia, które mają duży wpływ na kształtowanie się Internetu.

Ze względu na bardzo szeroki zakres problemu prywatności w Internecie, autor zdecydował ograniczyć tematykę pracy do środowiska mediów społecznych, czyli serwisów społecznościowych, a także stron internetowych umożliwiających dzielenie się treściami. Teoretyczna część pracy obejmuje wyjaśnienie istotnych zagadnień związanych z prywatnością w tego rodzaju serwisach.

Rozdział pierwszy zawiera omówienie teoretycznych koncepcji prywatności, prawa do prywatności oraz funkcji, jaką spełnia. Przede wszystkim podjęto próbę uchwycenia różnic pomiędzy rozumieniem prywatności w środowisku *offline* i *online*. Zamieszczono w nim również prezentację kilku ujęć krytycznych prawa do prywatności, w tym stanowiska radykalnej transparencji reprezentowanego między innymi przez Google i Facebooka.

Rozdział drugi zawiera obszerny opis środowiska Internetu i samych mediów społecznych, z uwzględnieniem specyficznych cech dla tych środowisk, które wpływają na problemy związane z prywatnością, a zwłaszcza na zaistnienie zjawisk niejednorodnej i niewidzialnej publiczności.

W **rozdziale trzecim** opisuję sposoby ochrony prywatności w Internecie, wyodrębniając trzy kategorie: regulacje prawne, pasywne i aktywne sposoby samodzielnej ochrony oraz rynkową samoregulację.

Rozdział czwarty zawiera podsumowanie dwóch najbardziej kompleksowych raportów na temat prywatności w Internecie, które są publicznie dostępne: (1) specjalny raport Eurobarometru na temat postaw Europejczyków dotyczących prywatności, ochrony danych i zarządzania elektroniczną tożsamością oraz (2) badanie Microsoftu na temat profili i reputacji w Sieci.

Wyniki badania zostały przedstawione w **rozdziale piątym**. Zawiera on opis pogłębionych wywiadów przeprowadzonych na wyselekcjonowanej grupie aktywnych użytkowników mediów społecznych. Badanie miało na celu ustalić wagę, jaką respondenci przywiązują do prywatności w Internecie, świadomość zagrożeń oraz zdefiniować postawy i zachowania, jakie charakteryzują ich aktywność w mediach społecznych.

Przygotowując się do napisania pracy, poszukiwałem naukowej literatury poświęconej zagadnieniu prywatności w Internecie, a zwłaszcza w mediach społecz-

nych, w różnych ujęciach: społecznym, psychologicznym, filozoficznym, a także – w podstawowym zakresie – prawniczym.

Niewiele uwagi poświęciłem na opisanie faktycznego stanu prawa. Po pierwsze, kompleksowe analizy prawne w tym temacie już istnieją, także w języku i na gruncie polskim. Przykładem może być analiza Barty i Markiewicza (2009). Po drugie dostępny jest również doskonały i często aktualizowany blog Piotra „VaGla" Waglowskiego opisujący „prawne aspekty społeczeństwa informacyjnego". Ponadto, prawo obowiązujące w Polsce, Unii Europejskiej i Stanach Zjednoczonych – *ojczyźnie* większości portali mediów społecznych – okazuje się być niedostatecznie dostosowane do dynamicznie zmieniających się warunków Internetu. Obowiązujące prawo, które może być zastosowane do przypadków naruszenia prywatności w Internecie, jest często martwe. Działania organów ścigania i sądów są ograniczone przez specyfikę technologii, wymagają dużego nakładu specjalistycznej pracy, podczas gdy szkodliwość popełnianych czynów uznawana jest za względnie niską.

Bogatym źródłem informacji są organizacje zajmujące się ochroną prawa do prywatności w Internecie. Do najważniejszych należą Electronic Frontier Foundation (EFF) oraz Electronic Privacy Information Center (EPIC). Prowadzą one działalność badawczą, organizują konferencje, włączają się do debaty publicznej, wydają informatory, aktywnie występują w obronie praw np. poprzez interwencje w instytucjach rządowych, lobbowanie zmian w prawie. Od niedawna istnieje także polska organizacja, Fundacja Panoptykon, której celem jest obrona wolności i praw obywateli (ze szczególnym uwzględnieniem prawa do prywatności), które są zagrożone przez ekspansję nowych technologii.

1. PRYWATNOŚĆ I PRAWO DO PRYWATNOŚCI

Termin *prywatność* jest często używany w różnych kontekstach zarówno w mowie potocznej, jak i w dyskursie naukowym. Mówiąc o *prywatnych sprawach*, myślimy o tych elementach naszego życia, które chcemy pozostawić dla nas samych i dla tych, z którymi łączą nas najbliższe relacje. Każdy zakwalifikuje do tej kategorii informacje innego typu. Dla jednych będą to niemal wszystkie szczegóły z życia, także zawodowego, inni zaliczą do swojej sfery prywatnej życie rodzinne. Jeszcze inni – tylko sekrety, które wolą pozostawić w sypialni. Zdarzają się też osoby, które nie tylko nie widzą potrzeby utrzymywania pewnych informacji w sekrecie, ale wręcz odnajdują przyjemność w eksponowaniu całego swojego życia – czy to w rozmowach, czy w bardzo popularnych swego czasu programach *reality-show*, czy na swoim internetowym blogu. Zgoda, co do tego, że każdy ma prawo decydować o ujawnieniu lub nie takich informacji, jest powszechna. Aby zagwarantować prawo do samodzielnego podejmowania decyzji dotyczących sfery prywatnej, potrzebne było precyzyjne zdefiniowanie pojęcia prywatności i prawa do prywatności.

1.1. Definicje i wymiary prywatności

Za twórcę pojęcia sfery prywatnej uznaje się Arystotelesa, który rozgraniczył publiczną aktywność polityczną, *polis*, od sfery prywatnej, rodzinnej zwanej *oikos*. Takie dychotomiczne rozróżnienie było obecne także w pracach Johna Locka i Johna Stuarta Milla. Rozważając zagadnienia indywidualizmu i prawa do własności, uznali, że każdy powinien mieć prawo dysponowania nie tylko swoim majątkiem, ale także informacjami dotyczącymi samego siebie – informacjami prywatnymi (DeCew i Zalta, 2008).

1.1.1. Pierwsze definicje prawa do prywatności

Za twórców nowoczesnej koncepcji prawa do prywatności uważa się Samuela Warrena i Louisa Brandeisa, którzy w 1890 roku opublikowali w Harvard Law Review esej „The Right to Privacy". Podczas analizy wyroków wydawanych przez amerykańskie sądy w sprawach o naruszenie własności prywatnej, zniesławienie czy nadużycie zaufania zidentyfikowali ogólniejsze *prawo do bycia pozostawionym w spokoju* (w oryginale – ang. *the right to be let alone*). Zaproponowali wydzielenie tej zasady, aby lepiej chronić prawa jednostki. Prawo do prywatności gwarantuje samodzielne ustalanie zakresu, w jakim informacje są rozpowszechniane publicznie, ze szczególnym uwzględnieniem myśli, uczuć i emocji, których ujawnienie narusza *prawo do osobowości* jednostki. Jednym z argumentów przemawiających za potrzebą zaistnienia takiej ochrony był rozwój technologii komunikacyjnych i coraz większa popularyzacja prasy i fotografii, co otworzyło nowe możliwości naruszenia prywatności poprzez masowe rozpowszechnianie szczegółów dotyczących czyjegoś życia prywatnego. Warren i Brandeis wyznaczają granice prawa do prywatności poprzez analogię do istniejących praw dotyczących oszczerstwa i zniesławienia. Przede wszystkim prawo do prywatności nie może ograniczać prawa do komentowania i uzasadnionej krytyki, co byłoby występowaniem przeciwko interesowi publicznemu. Wyraźnie oddzielają obszary życia prywatnego i publicznego, a także wyłączają spod ochrony informacje, które zostały samodzielnie opublikowane przez jednostkę (Brandeis i Warren, 1890).

Choć prawo do prywatności zostało zaakceptowane w literaturze prawniczej, to nie miało początkowo dużego wpływu na decyzje zapadające w sądach. Z czasem zostało uznane przez amerykańską jurysdykaturę, o czym ze szczegółami pisze William Prosser. Rozwija on pojęcie prywatności do wielopłaszczyznowego konstruktu, który może zostać naruszony na cztery sposoby:

1. Wtargnięcie w czyjąś izolację, odosobnienie lub w jego prywatne sprawy (*intrusion upon solitude or seclusion*) – fizyczne lub podobnego gatunku (np. optyczne, akustyczne – z pomocą aparatu fotograficznego, kamery, dyktafonu itp.), wtargnięcie w odosobnienie lub separację albo w sprawy prywatne innej osoby, jeżeli wtargnięcie jest z punktu widzenia roztropnej osoby wysoce naganne.
2. Publiczne ujawnienie kompromitujących prywatnych treści o jednostce (*public disclosure of private facts*) – naganne publiczne ujawnienie spraw prywatnych, jeśli nie jest ono usprawiedliwione interesem społecznym.

3. Przywłaszczenie czyjegoś nazwiska lub wizerunku (*appropriation of name or likeness*) – przywłaszczenie nazwiska lub wizerunku innej osoby dla własnego użytku lub korzyści.
4. Postawienie w fałszywym świetle (*false right*) – naganne, umyślne lub wynikające z zaniedbania, publikowanie błędnych informacji, które osobę trzecią stawiają w złym świetle.

Prywatność w rozumieniu Warrena i Brandeisa koncentrowała się wokół drugiego prawa do prywatności według Prossera. Sam Prosser twierdzi, że powodem takiego zogniskowania uwagi u poprzedzających go badaczy są osobiste motywy Warrena, którego ceremonia weselna córki została ze szczegółami opisana w prasie brukowej (Prosser, 1960).

1.1.2. Rozwój teorii Alana Westina i Irwina Altmana

Alan Westin definiuje prywatność jako roszczenie jednostek, grup czy instytucji, aby móc decydować kiedy, jak i w jakim zakresie informacja o nich jest komunikowana do innych. Wymienia cztery wymiary prywatności: odosobnienie (wolność od bycia obserwowanym przez innych), intymność (bycie na osobności z jedną lub większą ilością innych osób), anonimowość (bycie w otoczeniu społecznym, ale przy zachowaniu prywatności) i rezerwę (nieujawnianie osobistych informacji o sobie) (Pedersen, 1997). Warto zwrócić uwagę, że Westin, w przeciwieństwie do Prossera, był psychologiem. Kolejni badacze na ogół potwierdzali słuszność definiowania prywatności poprzez wskazanie jej aspektów. Pedersen potwierdził empirycznie istnienie czterech wymiarów prywatności wskazanych przez Westina, identyfikując jednak dwa dodatkowe. Rozróżnił dwa rodzaje intymności – z rodziną i przyjaciółmi, a także zasugerował istnienie kolejnego stanu – izolacji, czyli skrajnej odmiany odosobnienia, przebywania z dala od innych ludzi. Zakładając jednocześnie, że osoba przebywająca w odosobnieniu nie jest przez nikogo widziana ani słyszana, Pedersen uważa odosobnienie za najpełniejszy stan prywatności, jaki można osiągnąć (Pedersen, 1997).

Podobnie jak w przypadku samych definicji, istnieje wiele teorii mówiących o znaczeniu, jakie ma prywatność dla ludzkiej osobowości. Westin wyodrębnił cztery funkcje, jakie spełnia prywatność. Pedersen rozszerzył katalog funkcji prywatności o jedną dodatkową:

1. Prywatność pozwala utrzymać *autonomię osobistą*, co należy rozumieć jako możliwość uniknięcia zdominowania lub zmanipulowania przez inne osoby.

2. Dzięki prywatności jednostka może odpocząć od napięć życia społecznego, ról i wymagań, jakie są przed nią stawiane (funkcja *ulgi emocjonalnej*).
3. Umożliwia *ograniczenie i chronienie komunikacji*, czyli zapewnia prywatność informacyjną. Dzięki niej jednostka może ustalać granice interpersonalne i decydować o udostępnieniu informacji osobistych, np. wyłącznie dla osób zaufanych.
4. Umożliwia eksperymentowanie i odkrywanie własnej tożsamości oraz ukrywanie przed innymi jej niepożądanych części (*samoocena*).
5. Pederson uważa, że prywatność wyzwala *kreatywność* – jednostka może pełniej angażować się w kreatywne doświadczenia, rozwój idei oraz rozwiązywanie problemów, jeżeli jej proces twórczy jest nieskrępowany obserwacją i krytyką innych osób (Pedersen, 1997).

Altman definiuje prywatność na gruncie swojej *regulacyjnej teorii prywatności*, która miała duży wpływ na późniejsze badania nad tym zagadnieniem (Margulis, 2003). Nazywa prywatność *selektywną kontrolą jednostki nad dostępem do niej samej*. W jego ujęciu prywatność jest dobrowolnym, fizycznym lub psychicznym, wycofaniem się jednostki ze społeczeństwa. Zauważa, że sam fakt istnienia prywatności jest uniwersalny, tj. ponadkulturowy, niezależny od społeczeństwa, ale już mechanizmy jej zapewniania są unikalne w zależności od fizycznych, psychologicznych i socjologicznych aspektów danej kultury. Altman uznaje dynamiczną i dialektyczną perspektywę regulacji prywatności jednostki zaproponowaną przez Westina. Zgodnie z nią prywatność jest zmienna w czasie i regulowana w zależności od stanu wewnętrznego (potrzeb) i uwarunkowań zewnętrznych (wymagań roli społecznej). Jednostka reguluje okresową zmianę w określaniu własnej potrzeby prywatności. Są chwile, kiedy potrzebujemy kontaktu z innymi osobami, ujawnienia swoich głęboko osobistych myśli czy uczuć, zaś innym razem potrzebujemy odosobnienia, bycia sam na sam ze sobą. To dwubiegunowe zachowanie wywodzi się według Altmana z potrzeby osiągnięcia *tymczasowo optymalnego* stanu jednostki, osiągnięcia homeostazy. Wykres funkcji takiej zmiany w czasie przypomina sinusoidę. Po osiągnięciu jednego bieguna rozpoczyna się kierowanie ku stanowi przeciwnemu. Zbyt duży poziom dostępu do jednostki powoduje odczucie przez nią naruszenia jej prywatności, zbyt niski skutkuje poczuciem alienacji i osamotnienia (Margulis, 2003).

Altman uważa również, że prywatność istnieje w kontekście kulturowym. Co prawda potrzeba prywatności jest kulturowo uniwersalna, ale konkretne przejawy prywatności są już różne w różnych kulturach, tak jak zmieniają się normy społeczne. W jego teorii rozróżnia się pożądany i faktyczny poziom prywatności.

Zmienność utrudnia ustalenie pożądanego stopnia prywatności, zarówno podczas badań naukowych, jak i przez samą jednostkę. W przypadku prywatności *online* ma to konsekwencje między innymi w konieczności posiadania możliwości rezygnacji, co w przypadku wielu aktywności nie jest gwarantowane (Margulis, 2003). Kwestia ta została szeroko omówiona w odpowiedniej części pracy.

Altman i Taylor (1973) zaproponowali termin *otwierania się* (ang. *self-disclosure*) oznaczający proces przekazywania informacji prywatnych innym osobom i światu, który pozwala nam regulować własną prywatność. Ma on trzy wymiary: szerokość, głębokość oraz czas trwania. Szerokość oznacza ilość informacji, które są ujawniane. Głębokość opisuje stopień intymności informacji, gdzie *płytkie otwieranie się* oznacza ujawnianie powierzchownych faktów, głębokie – najbardziej intymnych. Trzeci wymiar opisuje po prostu czas od rozpoczęcia do zakończenia ujawniania informacji.

1.1.3. Prywatność jako stan

William Parent, w odróżnieniu od większości autorów, opisuje prywatność jako stan, w jakim może znaleźć się jednostka. Według niego prywatność to „stan, w którym jednostka zachowuje jako poufne pewne nieopublikowane informacje osobiste". Jest to definicja deskryptywna (nienormatywna), w przeciwieństwie do definicji określających prywatność jako moralną lub prawną zasadę, które są definicjami normatywnymi. Takie ujęcie jest interesujące z językowego punktu widzenia – pozwala mówić o zmniejszaniu lub zwiększaniu się prywatności nie jako zmiany stopnia kontroli, a zmiany stanu, w jakim znajduje się jednostka. W rozumieniu Parenta rozpowszechnianie informacji już opublikowanych np. w czasopiśmie, publicznych dokumentach (także w Internecie) nie jest naruszeniem prywatności, gdyż przestały one należeć do strefy prywatności jednostki już podczas pierwszej publikacji. Parent odrzuca także obserwację czy wkroczenie na czyjś teren jako ingerencję w prywatność, sugerując, że te czyny ograniczają czyjąś anonimowość lub powinny być kwalifikowane jako naruszenie własności prywatnej. Utrata prywatności zachodzi wyłącznie w wypadku wejścia w posiadanie niepublicznych informacji osobistych o jednostce (Parent, 1983).

1.1.4. Wymiary prywatności

Burgoon definiuje prywatność jako możliwość kontrolowania i ograniczania dostępu do jednostki (lub grupy, do której należy jednostka) w jednym z czterech wymiarów:

1. Wymiar fizyczny – stopień, do jakiego jednostka jest fizycznie dostępna innym. Bazuje na biologicznej potrzebie przestrzeni osobistej, może być naruszona m.in. poprzez obserwację, wkroczenie w przestrzeń osobistą lub bezpośredni kontakt.
2. Wymiar interakcyjny – zwany również społecznym lub komunikacyjnym. Określany przez możliwość i wysiłek, jaki jest niezbędny do kontrolowania kontaktów społecznych, tj. ich uczestników, częstotliwości, długości trwania oraz treści komunikatów i oddziaływań. Przykładami werbalnego naruszenia prywatności społecznej mogą być np. nietaktowne komentowanie, niedyskretne pytanie czy rozpoczynanie niechcianej rozmowy. Do niewerbalnych naruszeń zaliczyć można np. nieodpowiednie miejsce konwersacji.
3. Wymiar psychologiczny – kontrola racjonalnych i emocjonalnych bodźców człowieka, możliwość autonomicznego wartościowania, a także określania czy, z kim i w jakich warunkach odbędzie się dzielenie poufnymi i intymnymi informacjami. Może zostać naruszone np. przez próbę przekonywania kogoś lub obniżania jego wartości.
4. Wymiar informacyjny – określa prawo jednostki do określania jak, kiedy, i do jakiego stopnia informacja o jednostce zostanie przekazana innym. Od prywatności psychologicznej różni się tym, że ujawnienie informacji odbywa się całkowicie poza kontrolą jednostki, np. podczas czytania cudzej korespondencji czy przekazywania detali czyjegoś życia osobistego innej osobie (Joinson, Paine, 2007).

DeCew (1997), powołując się na teksty Schoemana i Allena, proponuje model składający się z trzech wymiarów: informacyjnego, dostępności (ang. *accesibility dimension*) oraz ekspresji. Prywatność informacyjna dotyczy ochrony wszelkich informacji o jednostce, umożliwia jej decydowanie kto, kiedy, w jakim zakresie, i w jakim celu ma do nich dostęp. Jeśli informacje te są w posiadaniu innych osób (lub instytucji), mają one obowiązek chronić je przed dalszym rozpowszechnianiem, pozostawiając pod kontrolą jednostki, której dotyczą. Wymiar dostępności powinien być rozumiany jako kontrola nad fizycznym i zmysłowym dostępem do osoby. Może być naruszony nie tylko przez kontakt cielesny, ale także poprzez wtargnięcie w czyjeś sąsiedztwo niepożądanym dźwiękiem czy zapachem. Pry-

watność ekspresyjna chroni obszar do wyrażania tożsamości i osobowości jednostki poprzez słowa lub aktywność. Pozostawia jej kontrolę nad kontynuowaniem lub zaprzestaniem zachowania bez względu na interferencję innych osób czy organizacji – w tym znaczeniu słusznie jest kojarzona z wolnością.

W wielu definicjach granice pomiędzy wymiarami prywatności są nieostre, a często zakres znaczeniowy jednego wymiaru zawiera się częściowo w drugim. Cechą tą obarczona jest zwłaszcza typologia zaproponowana przez Burgoona, u którego wymiary psychologiczny i informacyjny mają duży obszar wspólny (DeCew, 1997). Mimo różnic pomiędzy konstruktami, należy zwrócić uwagę, że autorzy zgodnie definiują prywatność poprzez kilka jej wymiarów, co pokazuje złożoność tego pojęcia.

Moore twierdzi, że poprawną definicję można skonstruować jedynie za pomocą normatywnej definicji, tj. wskazując powody, dla których identyfikacja prawa do prywatności jako oddzielnego od innych praw podstawowych jest ważna, i czym to prawo się charakteryzuje. Poddaje silnej krytyce definicję deskryptywną Parenta, wymieniając przykłady sytuacji, które nie mieszczą się w jego zawężonym znaczeniu sfery prywatności, a które intuicyjnie zdecydowana większość ludzi uzna za prywatne. Przykładem może być sekret dwojga kochanków. Jego ujawnienie przez jedną osobę nie spowodowałoby naruszenie prywatności w definicji Parenta. Moore proponuje zaakceptowanie równoległego istnienia dwóch definicji prywatności: normatywnej i deklaratywnej, argumentując, że nie są one wzajemnie wykluczające. Są one różnym ujęciem tej samej kwestii – prywatność może być rozumiana zarówno jako stan, jak i jako prawo. Koncentrując się na tym zagadnieniu, Moore używa co prawda pojęć wymiarów prywatności, nie angażując się w sformułowanie swojej oceny. Stwierdza również, że niemożliwe jest sformułowanie definicji prywatności w sposób, który nie może zostać zakwestionowany. Proponuje własną definicję (na podstawie Burgoon et. al., 1989), zastrzegając, że jest ona niedoskonała i ostatecznie nie rozstrzyga problemu (Moore, 2008).

1.1.5. Współczesne ujęcia prywatności

Na szczególną uwagę zasługują dwie teorie, które powstały już w XXI wieku, po tym jak Internet i media społeczne stały się nierozerwalną częścią rzeczywistości społecznej: teoria integralności kontekstowej Nissenbaum i częściowo opierająca się na niej teoria zarządzania prywatnością komunikacji Petronio.

1.1.5.1. Prywatność jako integralność kontekstowa informacji

Nissenbaum (2004) wychodzi od konceptu kontroli dostępu do własnych informacji prywatnych i rozwija go poprzez wprowadzenie trzech cech, którymi charakteryzuje się każda sytuacja związana z ujawnianiem własnych danych. Te cechy to aktorzy, którzy biorą udział w sytuacji, przestrzeń, w której jest osadzona, i informacje osobiste, które mają zostać ujawnione. Aktorzy i sytuacja tworzą kontekst, w którym zachodzi przepływ informacji osobistych. Prywatność pełni funkcję zaworu, który reguluje przepływ informacji w każdym konkretnym kontekście. Jeżeli spełnia ona swoją funkcję zgodnie intencjami osoby, której dotyczą informacje, to zachowana jest integralność kontekstu tejże informacji. Prywatność nie jest więc pełną kontrolą przepływu informacji osobistej, a jedynie stosowną do danego kontekstu społecznego.

Nissenbaum proponuje, aby kontrolę przepływu informacji prywatnej rozumieć jako możliwość zróżnicowanego dzielenia się lub zatrzymywania informacji osobistej zależnie od jej znaczenia i wrażliwości w danym kontekście. Naruszenie prywatności zachodzi, gdy nie są przestrzegane społeczne i indywidualne normy stosowności i dystrybucji informacji przez jednostki, które posiadają lub którym powierzona została informacja. Normy stosowności oznaczają, jakie informacje mogą być w danej sytuacji przekazane dalej, a normy dystrybucji – komu i w jakim czasie. Większość ludzi nie czuje się zagrożona w trakcie rozmowy z lekarzem o własnym stanie fizycznym, z nauczycielem o problemach wychowawczych z dzieckiem czy z pracownikiem banku o sytuacji finansowej. Dla wielu takich sytuacji posiadamy społeczne i indywidualne zestawy norm stosowności i dystrybucji, określających ilość i typ informacji, jakie są przekazywane w tych specyficznych kontekstach.

Nissenbaum twierdzi, że takie sytuacyjne podejście umożliwia szczegółową analizę opisową prywatności, a ponadto dostarcza mocną podstawę dla normatywnej krytyki tak rozumianych naruszeń prywatności (Barth, Datta, Nissenbaum et al., 2006). Nissenbaum operuje na pograniczu filozofii i prawa, ale jej teoria doskonale tłumaczy problemy wynikające z dynamiki Internetu i mediów społecznych. Peterson (2010), analizując teorię integralności kontekstowej i cechy przestrzeni cyfrowej serwisu społecznościowego (na przykładzie Facebooka), zwraca uwagę, że większość naruszeń prywatności, które tam zachodzą, wynikają z naruszenia kontekstu informacji. Środowisko serwisu społecznościowego jest fundamentalnie różne od rzeczywistości realnej (cechy charakterystyczne usieciowionego środowiska cyfrowego opisano w kolejnym rozdziale). W ekosystemie

Facebooka, którego prawa często stoją w sprzeczności z intuicyjnym rozumieniem świata rzeczywistego, korzystanie z wcześniejszego doświadczenia sprawia, że doświadczenia i spodziewane rezultaty interakcji są inne niż faktyczne. Kwestia integralności kontekstowej informacji zostanie szerzej opisana w części pracy dotyczącej niejednorodności publiczności w mediach społecznych.

1.1.5.2. Teoria zarządzania prywatnością komunikacji

Petronio, proponując teorię zarządzania prywatnością komunikacji, nie nawiązuje bezpośrednio do teorii integralności kontekstowej informacji, ale teorie te są względem siebie komplementarne. Petronio dostarcza kompleksowe narzędzie do opisu przepływu informacji prywatnej, a Nissenbaum oferuje narzędzie do krytyki naruszeń prywatności. W dalszej części pracy używam rozpowszechnionego w literaturze obcojęzycznej akronimu CPM (*Communication Privacy Management Theory*). Jest to systemowa teoria opisująca proces ujawniania informacji prywatnych. Koncentruje się ona na regułach ustalonych przez jednostkę i negocjowanych z innymi (Griffin, 2011). Reguły te mają na celu ustanowienie tymczasowej równowagi pomiędzy procesem ujawniania informacji osobistych, a zachowaniem potrzeby prywatności jednostki lub grupy osób. Odniesienie się do zbioru reguł pozwala na zastosowanie teorii w interpretacji wyborów dotyczących ujawniania lub ukrywania informacji prywatnych.

Teoria opiera się na kartograficznej metaforze granic, które otaczają indywidualną lub kolektywną sferę prywatności. Informacje osobiste, które nie są z nikim dzielone, znajdują się wewnątrz indywidualnych granic. Po podzieleniu się informacją, powstaje kolektywna granica. Cezury każdego rodzaju określają, jakie informacje mogą zostać ujawnione, komu oraz w jakiej sytuacji. Tak jak u Altmana i Westina proces wyznaczania granic jest dynamiczny, zaś poziomy prywatności są nieustannie dostosowywane do warunków zewnętrznych i stanu wewnętrznego jednostki/grupy. Mechanizm ten również u Petronio jest dialektyczny – jednocześnie potrzebujemy być otwarci na społeczeństwo, aby w nim właściwie funkcjonować i czerpać z tego korzyści oraz zachować prywatność i autonomię osobistą. Te dwa przeciwieństwa nieustannie się ścierają, determinując poziom otwarcia granic. Nowym elementem wprowadzonym przez Petronio jest stworzenie systemu opartego na regułach prywatności. Aby podjąć decyzję o udostępnieniu prywatnej informacji, odwołujemy się do własnego systemu zarządzania prywatnością opartego na trzech rodzajach reguł. Reguły przepuszczalności (ang. *permeability*), które opisują szerokość, głębokość oraz liczbę przekazywa-

nych informacji; reguły połączeń (ang. *linkages*) określające kto, poza obecnymi właścicielami, może poznać informacje; oraz reguły współposiadania (ang. *shared ownership*) określające, do czego mają prawo osoby będące w grupie posiadającej informację (Child, Pearson i Petronio, 2009).

Fundament dla CPM stanowi pięć twierdzeń. Po pierwsze, prywatność informacji wynika z faktu jej posiadania. Jeżeli osoba lub grupa osób uważa, że informacja należy do nich, wtedy jest prywatna niezależnie od tego czy pogląd ten jest zgodny z prawdą, czy nie. Posiadanie prywatnych informacji pociąga za sobą korzyści, jak również obowiązki – do tych drugich należy odpowiedzialność za zarządzanie informacją. Stad wynika potrzeba tworzenia granic i kontroli, które informacje są dzielone, z kim oraz w jaki sposób.

Posiadanie informacji na własność umacnia przekonanie o uprawnieniu do sprawowania kontroli. W tym celu, tak mówi drugie twierdzenie, właściciel informacji uznanej za prywatną, tworzy i stosuje reguły prywatności, aby kontrolować przepływ prywatnej informacji. Reguły te powstają na podstawie indywidualnych kryteriów w oparciu o pięć czynników: płeć, kontekst, kulturę, motywację oraz bilans zysków i strat. Po trzecie, gdy prywatna informacja staje się współdzielona z innymi osobami, te stają się *powiernikami*, a tym samym współwłaścicielami informacji. Jednocześnie zostaje utworzona grupowa granica prywatności. Współwłaściciele informacji mają zwykle poczucie odpowiedzialności za kontrolę nad dalszym rozprzestrzenianiem się informacji, nie jest ono jednak równe odpowiedzialności pierwotnego właściciela. Czwarte twierdzenie CPM opisuje konieczność koordynacji grupowych granic prywatności. Każdy członek grupy, właściciel i współwłaściciele informacji, mogą chcieć wyznaczyć inne granice wspólnego terytorium informacyjnego.

Proces negocjacji wspólnych granic nie jest zatem prosty, a koncentruje się na ustaleniu trzech rodzajów zasad: przepuszczalności, połączeń oraz własności. Przepuszczalność granicy określa, które informacje mogą zostać ujawnione przez grupę. *W pełni przepuszczalna*, *otwarta* lub *cienka* granica oznacza sytuację, gdy grupa chce umożliwić dostęp do prywatnej informacji lub zgadza się na dostęp do takiej informacji. *Nieprzepuszczalna*, *zamknięta* lub *gruba* granica oznacza sytuację, w której informacja, zgodnie z wolą jej posiadacza/posiadaczy jest chroniona, a więc niedostępna lub dostęp do niej jest ograniczony. Przepuszczalność może mieć wiele stopni pośrednich. Wtedy granica zachowuje się jak filtr, który przepuszcza część informacji, pozostałe pozostawiając pod ścisłą ochroną. Zasady połączeń określają kto, poza obecnymi współwłaścicielami, może mieć dostęp do prywatnej informacji. Ujawnienie informacji nowej osobie pociąga za sobą

dołączenie do grupy kolejnego współwłaściciela. Głównym kryterium w umożliwieniu dostępu jest rodzaj relacji łączących potencjalnego nowego powiernika z jednostką/grupą. Bliska, intymna relacja zwiększa prawdopodobieństwo, że uszanuje on już istniejące zasady.

Jak już wcześniej wspominano, nie wszyscy współposiadacze informacji czują taki sam obowiązek ochrony dzielonej informacji. Jedna osoba może mieć najwięcej do stracenia w przypadku utracenia kontroli nad prywatną informacją, albo wręcz uważać, że tylko ona powinna ustalać reguły jej przepływu. W wielu przypadkach taką osobą jest pierwotny właściciel. Jeżeli powiernik zgadza się na wskazaną *dyktaturę* i zachowuje się zgodnie z wolą pierwotnego właściciela, Petronio nazywa go *udziałowcem*. Przynależność do jednego z dwóch pozostałych typów powierników zależy od sposobu, w jaki poznali informację. W przypadku aktywnego poszukiwania dostępu do prywatnej informacji nowy współwłaściciel jest *rozmyślnym powiernikiem*. Na drugim biegunie jest osoba, która nie chce poznawać informacji, nie spodziewa się jej poznać, a nawet może uważać, że nowa wiedza stanowi zbędny ciężar – *niechętny powiernik*. Dobrym przykładem *rozmyślnego powiernika* jest osoba, która chce wykorzystać prywatną informację do zaoferowania pomocy – jest to działanie typowe dla takich profesji jak lekarz, adwokat, doradca czy spowiednik.

Zasady mogą być niewypowiedziane (oparte na przypuszczeniach, przeszłych doświadczeniach) lub wypowiedziane (np. gdy zachodzi potrzeba uściślenia, modyfikacji lub wprowadzenia nowej zasady) i mogą zmieniać się w czasie. Petronio zaznacza, że zasady mogą nie zadziałać poprawnie np. gdy współwłaściciel nie czuje się w obowiązku chronić ujawnionej mu prywatnej informacji. Aby wzmocnić skuteczność ochrony informacji, właściciel może stosować sankcje. Często stosowane reguły stają się rutyną i mogą stanowić podstawę dla kształtowania się postaw dotyczących prywatności. Piąte twierdzenie dotyczy możliwości *zawirowania granicy* (ang. *boundary turbulence*), gdy zasady dotyczące zarządzania informacją prywatną nie zostały dostatecznie skoordynowane w grupie, zrozumiane lub nie są respektowane przez współwłaścicieli. Samo zawirowanie następuje, gdy grupa nie jest w stanie efektywnie kontrolować przepływu informacji poza jej obrębem (Griffin, 2011).

Podsumowując, warto zwrócić uwagę na cechy odróżniające CPM od wcześniejszych teorii dotyczących prywatności. Petronio mówi nie o popularnym wśród innych badaczy *otwieraniu się* (*self-disclosure*), ale o *ujawnianiu prywatnej informacji* (*disclosure of private information*). Po pierwsze dlatego, że dzielenie się prywatną informacją nie zawsze dotyczy informacji dotyczącej nas samych.

Po drugie *otwieranie się* jest kojarzone z intymnymi relacjami z innymi osobami, u których wspomaga budowanie więzi. Nie jest to jednak jedyny motyw, dla którego ujawniamy prywatne informacje. Możliwą korzyścią może być również ulga, wsparcie emocjonalne, uzyskanie wpływu na inne osoby, wywarcie wrażenia czy czysta ekspresja samego siebie. Ponadto otwieranie się jest według Petronio jednostronnym aktem, nieuwzględniającym sposobu, w jaki zarządza informacją jej powiernik (Griffin, 2011).

1.2. Krytyka prawa do prywatności

Równolegle do prób zdefiniowania pojęcia prywatności rozwijał się naukowy dyskurs, w którym wysuwano argumenty przeciwko potrzebie sublimowania generalnego prawa z innych praw, jakie przypisywane są człowiekowi. Można wymienić trzy główne kierunki, w których rozwijała się krytyka prawa do prywatności – na gruncie prawa, ekonomii i teorii feministycznych wraz z późniejszym rozwinięciem tych ostatnich jako tzw. *nothing to hide argument*.

Tak zwana redukcjonistyczna krytyka prawa do prywatności została zaproponowana przez prawnik Judith Jarvic Thomson. Zastosowała ona podobną metodologię jak *ojcowie* prawa do prywatności, Warren i Brandeis, to znaczy analizę spraw sądowych w amerykańskim wymiarze sprawiedliwości. Thomson otrzymała jednak zgoła odmienny wynik – według niej prawo do prywatności jest klastrem już istniejących unormowań, a więc jest gwarantowane na podstawie innych praw i nie ma potrzeby *mnożenia bytów więcej niż to konieczne*. Według Thomson wartości przypisywane do sfery prywatności są wystarczająco chronione przez przepisy, z których się ona wywodzi – prawa ochrony własności prywatnej i nietykalności cielesnej. Dodatkowo są one tam precyzyjniej sformułowane, przez co łatwiejsze do stosowania w sądownictwie (Thomson, 1975).

Krytyka Richarda Posnera opiera się przedstawieniu konceptu prywatności, który jest nieusprawiedliwiony ekonomicznie. Uważa on, że prywatność, rozumiana jako kontrola i ograniczanie dostępu do informacji, powinna mieć zastosowanie wyłącznie wtedy, kiedy ma ona sens z punktu widzenia ekonomii, tj. nieograniczony dostęp do informacji zmniejszy jej wartość. Posner powołuje się na przykłady utajania lub selektywnego udostępnianie informacji o sobie w celu zdezinformowania lub manipulacji innych osób dla osiągnięcia osobistej lub ekonomicznej korzyści. Tak rozumiana prywatność nie przyczynia się do powiększania bogactwa. Przykładowo pracownik może chcieć ukryć pewne kompromitujące fakty o nim przed swoim pracodawcą, co może mieć negatyw-

ny wpływ na funkcjonowanie przedsiębiorstwa. W swojej krytyce autor neguje istnienie psychologicznej potrzeby prywatności, uważając wręcz, że dzielenie się (pozytywnymi) informacjami osobistymi z obcymi osobami jest naturalne i często spotykane, np. podczas rozmów ze współpasażerami w samolocie czy w pociągu (Posner, 1983). Teoria Posnera jest często cytowana przez zwolenników braku potrzeby ochrony prywatności w Internecie. W przypadku handlu elektronicznego czy innych usług świadczonych *online* otwarty dostęp do danych o użytkowniku stwarza wiele nowych możliwości. Wiedza o zainteresowaniach i potrzebach kupującego pozwala zaoferować mu dobra, które z dużym prawdopodobieństwem spełnią jego wymagania – w takiej sytuacji obie strony transakcji korzystają ekonomicznie. Dodatkowym argumentem jest kosztowna (w sensie ekonomicznym, funkcjonalności lub jakości usługi) implementacja tzw. *Privacy Enhanced Technology*, czyli funkcji systemów gwarantujących prywatność użytkownikom, którzy z nich korzystają (Price, Adam, Nuseibeh, 2005).

Trzeci nurt krytyki prawa do prywatności wywodzi się ze środowisk feministycznych. Nie jest to jedno, wspólne stanowisko, a raczej kilka, różniących się stopniem radykalizmu proponowanych rozwiązań. Podstawą rozumowania jest zauważenie, że prywatność może mieć również negatywny wpływ na funkcjonowanie społeczeństwa, tj. może być używana jako tarcza zezwalająca na dominację, degradację oraz przemoc względem kobiet. Rozróżnienie sfery publicznej i prywatnej zezwala jednostce na pozostawienie wszystkiego, co złe i poniżające w tej drugiej, sprawiając, że takie zachowania pozostają wolne od napiętnowania. MacKinnon (1989) uważa, że najlepszym sposobem rozwiązania tego problemu jest połączenie publicznej i prywatnej sfery życia, pełna transparencja i otwartość tego, co do tej pory znajdowało się poza zasięgiem wzroku społeczeństwa oraz poza interwencją władz państwowych. Wielu autorów odrzuca to rozwiązanie jako zbyt radykalne. Allen zgadza się z MacKinnon, co do zakresu szkód, jakie może wyrządzić prywatność, stosowana do ukrycia przemocy w relacjach intymnych (domowych, partnerskich), a także negatywnego wpływu, jaki ma ona na postrzeganie przemocy domowej jako mniej godnej potępienia. Zwraca jednak uwagę, że skutkiem całkowitego upublicznienia wszelkich informacji pozostających dotąd w domenie prywatnej byłaby zupełna bezbronność przed atakiem ze strony państwa, argumentując ją przykładami obowiązkowej sterylizacji kobiet w niektórych państwach czy informowanie policji o wynikach testów na obecność narkotyków wykonywanych podczas okresu ciąży. Za skuteczniejsze od zlikwidowania sfery prywatnej (które nazywa *wylewaniem dziecka z kąpielą*) uważa ona działania nakierowane na zmiany prawa czy społeczne pojmowanie tematu

przemocy domowej, a przede wszystkim zrównanie korzyści, jakie przysługują kobietom i mężczyznom dzięki prywatności (Allen, 2000).

W zacytowanej na początku pracy wypowiedzi Erica Schmidta wielu komentatorów tak odczytało stanowisko zbliżone do MacKinnon. Propozycja autorki feministycznej była odbierana jako utopijna (a może dystopijna?), natomiast dyrektor Google odpowiadał w ten sposób na zarzuty o niewystarczającą troskę o prywatne dane użytkowników usług świadczonych przez firmę, która ma realną możliwość upublicznienia ogromu informacji o setkach milionów swoich użytkowników. To skutek rewolucji, jaka nastąpiła wraz z rozwojem globalnej Sieci, i przeniesienia wielu aktywności z świata realnego do Internetu. Kolejnym etapem rewolucji jest przeniesienie oprogramowania i danych z komputera do *przetwarzania w chmurze* – np. oprogramowania do zarządzania pocztą e-mail w komputerze do usługi w przeglądarce internetowej (takiej jak Gmail) czy kopii dokumentów do usług synchronizacji i przechowywania danych *online*, w zastępstwie wymiennych nośników pamięci.

Stanowisko Schmidta nazywa się *radykalną transparencją*, na podobieństwo transparencji instytucji publicznych. Opiera się ono na dwóch kluczowych założeniach: otwartość i transparentność są pozytywnymi siłami w społeczeństwie; otwartość jest pozytywną wartością w relacjach międzyludzkich. Przejrzyste i jasne funkcjonowanie organów, które wykonują publiczny mandat i sprawują władzę nad obywatelami, jest korzystne dla demokracji (Joinson, Houghton, Vasalou i in., 2011). Na pytanie, czy zastosowanie zasad transparencji w społeczeństwie przyniesie pozytywne zmiany, nie znamy jeszcze odpowiedzi.

1.3. Typy postaw w stosunku do prywatności

Wiemy już, że prywatność jest kwestią indywidualną. Warto przytoczyć badania, w których spróbowano empirycznie ustalić, jak bardzo ludzie przejmują się swoją prywatnością, ściślej – jej informacyjnym wymiarem.

Alan Westin (1996) zauważył i wyodrębnił trzy rodzaje postaw w stosunku do ochrony własnej prywatności. Na podstawie badań empirycznych w środowisku *tradycyjnego* rynku konsumenckiego w USA zauważył, że mniej więcej połowa osób charakteryzuje się postawą pragmatyczną, tj. kalkuluje potencjalne korzyści i ryzyko przed podjęciem decyzji o udostępnieniu swoich danych prywatnych. Druga połowa dzieli się na kolejne dwie grupy o skrajnych poglądach. Mniej więcej 25% ogółu społeczeństwa stanowią *fundamentaliści*, czyli osoby broniące swojej prywatności, niechętne umożliwieniu dostępu do swoich prywatnych

danych niezależnie od możliwych korzyści. Dla przykładu taka osoba nie zgodzi się na założenie karty lojalnościowej w supermarkecie, która uprawnia do rabatów – *fundamentalista* nie zgodzi się na gromadzenie i przetwarzanie danych osobowych oraz informacji o zakupach. Sklep korzysta bowiem z danych socjodemograficznych oraz z danych o zakupach do analizy zachowań konsumentów, a także do profilowania klientów i personalizacji reklam. Kolejne 25% stanowią *beztroscy*, którzy cechują się niskim poziomem obaw o prywatność, chętnie udostępniają informacje o sobie, nawet jeśli potencjalne korzyści są niewielkie, a podmiot, który jest zainteresowany prywatnymi danymi, nie jest znany i nie jest obdarzony zaufaniem.

Proporcje pragmatyków do fundamentalistów i beztroskich nie są stałe i inni badacze raportują odmienne wyniki niż Westin. Sheehan (2002) powołuje się na raport ze zogniskowanego wywiadu grupowego na temat prywatności przeprowadzonego przez Smitha (1994), w którym proporcje osób o różnych postawach w stosunku do prywatności są zgoła odmienne. Przed prowadzeniem wywiadu aż 72% zostało sklasyfikowanych jako pragmatycy, 17% stanowili fundamentaliści, a 11% beztroscy. Okazało się jednak, że większość badanych miała niewielką wiedzę na temat praktyk gromadzenia i przetwarzania danych o konsumentach. Przykładowo żaden z badanych nie miał świadomości kategoryzacji klientów na podstawie zakupów za pomocą kart kredytowych. Po ponownym sklasyfikowaniu badanych po dyskusji okazało się, że znaczna część pragmatyków zmieniła swe poglądy i została przeniesiona do kategorii fundamentalistów. Dodatkowo, ci *nowi fundamentaliści* charakteryzowali się najbardziej skrajnymi poglądami i byli wzburzeni sposobami przetwarzania ich prywatnych danych.

Sam Sheehan (2002) przeprowadził podobne badanie, tym razem analizując postawy użytkowników Internetu. Opierając się na typologii Westina, zaliczył zdecydowaną większość (81%) badanych do kategorii pragmatycznych, przy 16% beztroskich i tylko 3% fundamentalistów. Sheehan zaproponował więc rozbicie kategorii pragmatyków na dwie podkategorie: osoby o niskim do średniego stopnia obawy o naruszenie ich prywatności – *rozważni*, stanowiący 38% ogółu respondentów oraz *nieufni*, których byli co prawda skłonni pozbawić się części kontroli nad swoimi danymi prywatnymi, ale wymagali wyraźnej zachęty lub zapewnienia o bezpieczeństwie przetwarzania ich danych – 43% respondentów. Badacz zauważył również, że wśród młodych osób (w wieku 18–24 lat) jest wyższy odsetek skrajnych postaw – co trzeciego zaliczył do beztroskich, a 18% do fundamentalistów (których nazywa *zaalarmowanymi*). Odsetek najbardziej dbających o swoją prywatność respondentów okazał się bardzo wysoki w grupie osób

w wieku 65 i więcej lat – ponad połowa badanych. Również wyższe wykształcenie (tytuł magistra lub wyższy) miało wpływ na wzrost liczby osób o surowym podejściu do ochrony swoich danych prywatnych – co trzeci badany z wyższym wykształceniem został zaliczony do grupy zaalarmowanych. Nie zauważono natomiast wyraźnych korelacji pomiędzy intensywnością i stażem korzystania z Sieci z poziomem dbałości o własną prywatność. Podsumowanie przytoczonych badań obrazuje tabela 1.

Badanie	**Westin (1996)**		**Smith (1994)**		**Sheehan (2002)**	
Kontekst	Rynek konsumencki (nieinternetowy)		Ogólny (nieinternetowy)		Korzystanie z usług internetowych	
Stopień troski o prywatność						
Niewielka	Beztroscy	25%	Beztroscy	11%	Beztroscy	16%
Średnia	Pragmatycy	50%	Pragmatycy	72%	Rozważni	38%
					Nieufni	42%
Wysoka	Fundamentaliści	25%	Fundamentaliści	17%	Zaalarmowani	3%

Tabela 1. Opracowanie własne na podstawie: Westin (1996); Smith (1994); Sheehan (2002)

Wyniki otrzymane przez Sheehana potwierdzają silny związek prywatności z kontekstem, w jakim może zostać ona naruszona. Większość badanych spontanicznie podejmuje decyzje związane z udostępnianiem swoich danych, zgodnie ze swoim systemem przekonań i przy kalkulacji możliwych zysków i strat. Sheehan, przypominając badanie Smitha, zwraca uwagę na fakt, że wiele osób ze środkowych kategorii może w przyszłości wzmóc lub osłabić stopień troski o swoje dane prywatne. Zwiększanie świadomości przez edukację, sposób formułowania polityki prywatności przez serwisy internetowe, a także doświadczenia wynikające z korzystania z różnego rodzaju usług internetowych, mogą różnie wpływać na obawy o naruszenie prywatności, a w rezultacie – na zachowania związane z dzieleniem się informacjami o sobie. Praktyczną implikacją badania jest fakt, że większość osób można przekonać do podawania informacji prywatnych poprzez rozmaite zachęty (finansowe, lepsze usługi) oraz klarowne i uczciwe zasady gromadzenia oraz przetwarzania danych osobowych.

2. PRYWATNOŚĆ ONLINE

Prywatność w Internecie, w prasie popularnej, a także w opinii wielu osób to oksymoron. Argumentacją za takim stanowiskiem jest następująca teza: jeżeli coś prywatnego jest zamieszczane w Internecie, to jest potencjalnie dostępne dla wszystkich ludzi, którzy mają dostęp do Internetu, a tym samym przestaje być prywatne. Nawet przy korzystaniu z teoretycznie prywatnych narzędzi komunikacji, takich jak komunikatory internetowe czy e-mail, cyfrowy przekaz informacji powoduje, że jest wiele miejsc, w których mogą być one przechwycone – począwszy od złośliwego oprogramowania zainstalowanego na komputerze, z którego wysyłane są dane, przez włamanie do Sieci, do której jest podłączony komputer, dostawcę Internetu (ISP), różnego rodzaju służby, które filtrują ruch w Sieci i w końcu operatora usługi internetowej.

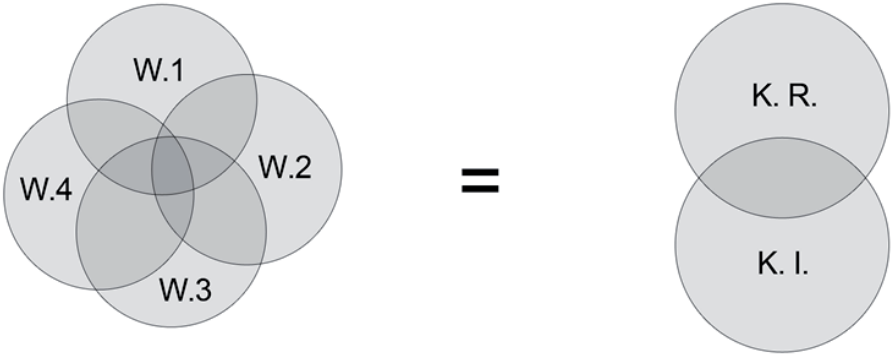
Spróbuję przyjrzeć się temu zjawisku bliżej, nie skupiając się jednak na wirusach komputerowych, cyberprzestępcach, działalności policji czy służb specjalnych. Zagadnienia związane z bezpieczeństwem danych są z przyjętego przeze mnie punktu widzenia mniej interesujące, gdyż na poziomie jednostki wystarczające rozwiązania polegają na korzystaniu z aktualnego oprogramowania antywirusowego i szyfrowania danych, obecnie powszechnie stosowanego w Internecie. Załóżmy dodatkowo, że nie żyjemy w świecie, w którym wszyscy dookoła czyhają w przestępczym celu na każdy skrawek naszej prywatnej informacji. Warto zadać sobie pytanie, jaką korzyść może mieć przestępca lub policjant z przechwycenia naszej konwersacji przez komunikator internetowy. Tym, co interesuje mnie najbardziej, jest społeczny kontekst prywatności. Sposób, w jaki użytkownicy Internetu, a zwłaszcza mediów społecznych, sprawują kontrolę nad dostępem do swoich prywatnych informacji przez inne osoby – przyjaciół, rodziców, nauczycieli, współpracowników itp.

Autorzy opisujący zagadnienie prywatności w Internecie zazwyczaj ograniczają się do przytoczenia istniejących już definicji, osadzając je w nowym kontekście. Wyjątkiem od tej reguły jest próba zdefiniowania *prywatności wirtualnej* przez Annę Mazur (2004, s. 8–9):

> Wydaje się, że konstrukcja prywatności powinna obejmować także nowy wyłaniający się wymiar, tj. prywatność wirtualną. Prywatność wirtualna to zachowanie odrębności w sensie wirtualnym. W wirtualnym świecie prywatność może być naruszona ichronią w sposób wirtualny (…). Prywatność ujmowana jest nie tylko jako kontrola informacji, ale także kontrola interakcji (…), która dotyczy prywatności poczty elektronicznej i innych form komunikacji wirtualnej. (…) Stąd prywatność może być rozumiana jako proces kontroli interakcji, który regulują jednostki: z kim nawiązać kontakt oraz jak częsta i jakiego rodzaju powinna być interakcja.

Wnioskowanie, że *prywatność wirtualna* powinna być zidentyfikowana jako kolejny, czwarty wymiar prywatności (Mazur skłania się ku trójwymiarowej koncepcji DeCew i innych) wydaje się niewystarczająco uzasadnione. Przede wszystkim brak badań, które sugerowałyby istnienie kolejnego wymiaru. Także na płaszczyźnie teoretycznej wydaje się, że prywatność wirtualna nakłada się w dużym stopniu na pozostałe wymiary zaproponowane przez DeCew i poprzedników. Prywatność fizyczna, po uwzględnieniu możliwości naruszenia fonicznego, również może być zagrożona podczas korzystania z Internetu (np. przez agresywne, dźwiękowe reklamy). Naruszenie takie nie jest jednak możliwe zawsze (wystarczy wyłączyć dźwięk w komputerze), natomiast w przypadku informacyjnego wymiaru prywatności – jego naruszenie *online* może nastąpić nawet wtedy, kiedy jesteśmy *offline*. Prywatność wirtualna jest więc osadzeniem wymiarów prywatności znanych z epoki przedinternetowej w nowym, wirtualnym kontekście. Jak suma zazębiających się wymiarów prywatności oddaje znaczenie całego pojęcia, tak samo oddaje ją suma przecinających się semantycznie pojęć prywatności *online* i *offline*. Ilustruje to Schemat 1.

Internet przejmuje lub uzupełnia coraz większą liczbę aktywności, które ludzie zwykli wykonywać *offline*, w wyznaczonych do tego miejscach lub domu. Zakupy, kontakty z rodziną i znajomymi, transakcje finansowe, konsumpcja dóbr kultury, poszukiwanie pracy, a nawet sama praca – wszystko to może odbywać się przez Internet, w pełnym lub ograniczonym wymiarze. W związku z tym możliwość kontroli, rozumiana jako prawo do utrzymania w tajemnicy lub dzielenia się informacjami o tych aktywnościach, a także samych działań, zależy między innymi



Oznaczenia:
W.x – jeden z wymiarów prywatności
K.R. – kontekst rzeczywisty
K.I. – kontekst internetowy

Schemat 1: Wymiary prywatności, a jej konteksty. Opracowanie własne

od struktury rzeczywistości, w której się one odbywają. Problem z prywatnością *online* wynika właśnie ze zgoła odmiennych cech strukturalnych Internetu, do których wiele osób zdążyło przywyknąć. Osoba korzystająca w przeszłości z usług nieskomputeryzowanego banku zrozumiała, że wszelkie transakcje są zapisywane i pracownicy banku mają do nich dostęp, ale jednocześnie miała też świadomość ograniczeń w cyrkulacji dokumentów ich dotyczących. Po wprowadzeniu elektronicznego obiegu dokumentów w bankach, dane te zaczęły być znacznie łatwiejsze do gromadzenia, kopiowania czy analizy. W dalszym ciągu jednak klient takiego banku mógł zakładać, że prywatność jego danych jest strzeżona tajemnicą i nikt spoza kręgu pracowników banku nie będzie miał do nich dostępu. W przypadku usług bankowych dostępnych przez Internet, powstaje problem utrzymania w tajemnicy danych przesyłanych pomiędzy bankiem a klientem. Przesyłane przez Sieć dane mogą być przechwycone przez osoby postronne – usługodawcy dostępu do Internetu czy *złodzieja* korzystającego z elektronicznego podsłuchu (np. podsłuchującego sieć lokalną, tzw. *sniffing*). Samo urządzenie, z którego osoba korzystająca z bankowości *online*, również jest podatne na ataki (np. hackerów, wirusów, oprogramowania szpiegowskiego), a odpowiedzialność za odpowiednie zabezpieczenia jest po stronie użytkownika.

2.1. Czym są media społeczne

Serwis społecznościowy (ang. *social network site*, SNS) to oparta na Sieci WWW usługa, która umożliwia jednostkom: (1) stworzenie publicznego lub częściowo publicznego profilu w ramach systemu, (2) utworzenie listy użytkowników, z którymi związani są różnego rodzaju relacjami oraz (3) przeglądanie profilów i list użytkowników innych osób (boyd i Ellison, 2007). Podstawową funkcją serwisu społecznościowego jest odtworzenie w sieci społecznej jednostki z rzeczywistości *offline* w Internecie, i w ramach tej sieci, podtrzymywanie i rozwijanie relacji. Powszechny niegdyś pogląd, że portale społecznościowe służą przede wszystkim do nawiązywania nowych znajomości, nie jest już prawdziwy – wykazało to m.in. polskie badanie etnograficzne „Młodzi i media": „najwięcej czasu i energii poświęca się na kontakt i budowanie relacji z grupą najbliższych znajomych" (Filiciak, Danielewicz, Halawa i in., 2010, s. 29). Na podobne obserwacje wskazują również inni badacze (boyd i Ellison, 2007; Mayer i Puller, 2008).

Profil w portalu społecznościowym składa się z informacji zamieszczonych przez jego właściciela – zwykle jest to imię i nazwisko (lub pseudonim), wiek, miejsce zamieszkania, zainteresowania, fotografia, dane kontaktowe (np. e-mail, telefon, komunikator internetowy), swobodna sekcja „o mnie" itp. Poprzez profil można również zwykle przeglądać aktywność użytkownika w serwisie: zamieszczone multimedia, odnośniki do stron internetowych, aktualizacje statusu, posty i inne. Niektóre serwisy społecznościowe, w tym najbardziej popularne: Facebook, Google+, wymagają podania prawdziwego imienia i nazwiska. Widoczność profilu i jego elementów zależy od serwisu oraz decyzji podejmowanych przez użytkowników, a wyrażanych przez tzw. *ustawienia prywatności*. Niektóre serwisy społecznościowe umożliwiają bardzo precyzyjną kontrolę nad tym, kto może zobaczyć poszczególne elementy profilu i aktywności użytkownika – od publicznej dostępności, aż po jednego tylko *znajomego* (m.in. Facebook i Google+). Inne, jak rodzima Nasza-Klasa.pl, pozwalają jedynie na określenie widoczności całego profilu: np. dla wszystkich, zarejestrowanych użytkowników serwisu lub osób z sieci kontaktów.

Drugim rodzajem serwisów, który zaliczam do mediów społecznych, są serwisy z treściami tworzonymi przez użytkowników (ang. *user generated content*, UGC lub *user created content*, UCC). To bardzo szeroka kategoria, w której zawierają się wszystkie strony internetowe, umożliwiające zamieszczanie własne treści – fotografii, materiałów wideo, tekstów, komentarzy itp. Wiele serwisów UGC udostępnia funkcje, które definiują serwisy społecznościowe – założenie własnego konta,

uzupełnienie podstawowych informacji profilowych i tworzenie sieci kontaktów. W porównaniu z serwisami społecznościowymi, nacisk jest jednak przesunięty z użytkownika i społecznych relacji, jakie tworzy, na treść, którą zamieścił. Wielokrotnie pojedynczy użytkownik w serwisie UGC jest niemal niewidoczny dla przeciętnego odbiorcy. Doskonałym przykładem takiego serwisu jest Wikipedia. Użytkownicy zamieszczają treści poprzez edycję artykułów internetowej encyklopedii, ale dla zwykłego użytkownika efekt pracy wielu osób jest widoczny jako jeden artykuł. Istnieje co prawda możliwość sprawdzenia, kto wprowadził zmiany w artykule, ale ta funkcja jest przydatna raczej pozostałym *Wikipedystom*, a nie osobie zainteresowanej wyłącznie treścią prezentowaną w serwisie. Dla mnie szczególnie ciekawy jest fakt wykorzystania serwisów UGC do zamieszczania treści osobistych, np. filmów przedstawiających wydarzenia rodzinne czy towarzyskie.

W literaturze oraz języku potocznym spotyka się dwa tłumaczenia angielskiego zwrotu *social media*, które opisuję w pracy: *media społecznościowe i media społeczne*. Za Dominikiem Kaznowskim (2010) zdecydowałem się używać terminu *media społeczne*, gdyż opisując media, jako całość, niepoprawne wydaje się użycie słowa *społeczność*, określającego część. „Społeczność to nie to samo co społeczeństwo", a to właśnie społeczeństwo kontroluje nowy rodzaj mediów za pomocą narzędzi dostarczonych przez twórców serwisów społecznościowych i serwisów UGC. Analogicznie, zwrot *serwis społeczny*, byłby niepoprawny, gdyż nie tworzy go *społeczeństwo*, a tylko *społeczność* użytkowników.

Oferta wielu stron internetowych na czele z serwisami społecznościowymi takimi jak Facebook, istnieje wyłącznie dzięki treściom udostępnianym przez użytkowników. Im bardziej użytkownicy otwierają się, tym więcej korzyści odnoszą z działania systemu, a system z zamieszczanych przez nich danych. Zakres udostępnianych informacji z jednej strony jest ograniczany przez pragnienie ochrony prywatności użytkowników, a z drugiej przez architekturę prywatności serwisu (Burke, Marlow i Lento, 2009). Wymiana informacji służąca utrzymywaniu i nawiązywaniu nowych więzi społecznych leży w samej istocie sieci społecznościowych. Zmiana statusu, napisanie kilku zdań na tak zwanej *ścianie* znajomego, zamieszczenie fotografii pozwalają na utrzymanie dużej ilości społecznych interakcji przy stosunkowo niewielkim wysiłku, przy czym więzi te, mimo satysfakcji, którą przynoszą, są słabe i sztuczne, choć pragmatycznie użyteczne. Mogą na przykład zaowocować dostępem do przydatnych informacji lub otwarciem się nowych możliwości. Zjawisko to nazwane jest *słabymi więzami w przepływie informacji* (Gross and Acquisti 2005; Ellison, Lampe i Steinfield, 2007). Jednocześnie popularność sieci społecznościowych oraz starania ich twórców o łatwiejszą i szybszą komuni-

kację między użytkownikami są czynnikami motywującymi częste zamieszczanie informacji. W efekcie użytkownicy dobrowolnie ujawniają dużą ilość informacji osobistych, przyczyniając się do rozwoju tzw. efektu śnieżnej kuli. Ściślej ujmując, normy dotyczące rozpowszechniania informacji, które wyłaniają się na portalach społecznościowych, mogą spowodować, że niewielka aktywność jest postrzegana negatywnie. Mianowicie użytkownicy, którzy zamieszczają niewiele informacji osobistych, spotykają się z krytyką w postaci usunięcia z kręgu znajomych przez inne osoby (Belleghem, Marloes i Veris 2011). Badania pokazują, że użytkownicy portali społecznościowych, których znajomi ze światów: internetowego i fizycznego, mają restrykcyjne ustawienia prywatności, modyfikują swoje zachowania dotyczące udostępniania danych i ich profile również często są prywatne. Wpływ presji rówieśników na zachowania związane z prywatnością jest wysoki zwłaszcza wśród młodych ludzi (Lewis, Kaufman, Christakis i in., 2008; Lewis 2011).

Właściciele i administratorzy portali społecznościowych muszą uwzględniać potrzeby swoich użytkowników, także te dotyczące ochrony prywatności. Media społeczne funkcjonują dzięki treściom zamieszczonym przez użytkowników, to oni tworzą całą ich wartość. Architektura serwisu, która usprawnia dzielenie się treściami, domyślnie zakładająca dzielenie się ze wszystkimi wydaje się być czynnikiem zwiększającym wartość serwisu, co przekłada się na jego popularność. Peterson (2010) uważa, że w rzeczywistości takie intuicyjne rozumienie procesu dzielenia się nie jest prawdziwe. Błąd leży w przyjęciu założenia „im łatwiejsze będzie dzielenie się informacjami, tym chętniej ludzie będą z tego korzystali". To prawda, ale tylko do momentu wystąpienia naruszenia prywatności, po którym użytkownik rozpocznie wycofywanie się: ograniczy liczbę zamieszczanych informacji, zastosuje bardziej restrykcyjne ustawienia prywatności, a w skrajnym wypadku usunie konto z serwisu. Długoterminowo optymalnym rozwiązaniem jest więc zaproponowanie skutecznych narzędzi kontroli dostępu do tych treści, a także uświadamianie użytkownikom ryzyka, jakie może wiązać się z nadmiernym odkrywaniem swojej prywatności. Internauci, którzy publikując informacje o sobie będą potrafili ograniczyć ich zasięg do wybranego kontekstu zgodnego z ich intencjami (np. kilku przyjaciół), będą mieli większe zaufanie do serwisu i w rezultacie chętniej będą z niego korzystali. Peterson (2010, s. 21) pisze:

> Im lepsza architektura prywatności tym bezpieczniej czują się użytkownicy; im bezpieczniej czują się użytkownicy tym bardziej ufają Facebook`owi; im bardziej użytkownicy ufają Facebookowi, tym więcej się dzielą i w ten sposób obie strony wygrywają.

Należy zaznaczyć, że opisanie norm określających właściwy sposób zachowania na portalach społecznościowych jest bardzo trudne lub wręcz niemożliwe. Media społeczne, po błyskawicznym okresie wzrostu, dopiero zaczynają wchodzić w fazę dojrzałości, debata na temat prywatności w Internecie ciągle się toczy, a użytkownicy uczą się funkcjonować z pożytkiem i bezpiecznie w nowym otoczeniu. Ponadto Internet, mimo szybkości przepływu informacji i swojej bezterytorialności, nie jest przecież środowiskiem homogenicznym i normy zachowań mogą się różnić nie tylko w różnych kulturach czy otoczeniu prawnym, ale także w zależności od charakteru usługi internetowej czy nawet w obrębie mniejszych grup znajomych. Tak zwana netykieta, czyli niepisany zbiór norm zachowań funkcjonujących w Internecie (etykieta w necie, czyli Sieci), funkcjonuje raczej w narzędziach komunikacji internetowej, które powstały jeszcze przed powstaniem Sieci WWW i z początkiem XXI wieku straciły na znaczeniu na rzecz sieci społecznościowych i innych stron internetowych (np. listy dyskusyjne, IRC). Co więcej nie reguluje ona kwestii związanych z prywatnością, poza krytyką nadmiernego rozprzestrzeniania bezwartościowej informacji (np. spamming), która jest rozumiana jako wtargnięcie w sferę prywatną (Hampridge, 1995). Normy zachowań, które funkcjonują obecnie w Internecie, są kompozycją skodyfikowanych regulaminów poszczególnych serwisów i wypadkowej zachowania samych użytkowników. Te z kolei są skrajnie odmienne w zawodowym portalu społecznościowym typu LinkedIn, Facebooku czy gwarantującym anonimowość użytkowników i obrazoburczym 4chanie.

2.2. Strukturalne cechy Internetu

Wielu badaczy twierdzi, że zachowania użytkowników związane z udostępnianiem własnych informacji prywatnych są przeniesieniem przez analogię tradycyjnych sposobów komunikowania się na grunt nowoczesnych technologii informacyjno-komunikacyjnych (Walther, 2011). Ulotność rozmowy w cztery oczy, telefonicznej czy nawet rozmowy lub zachowania w większym gronie nie ma jednak swojego odpowiednika w środowisku *online*, gdzie może być ona łatwo przechwycona, zapisana, kopiowana i transmitowana bez ograniczeń.

Dodatkowo fakt pośredniczenia mechanicznych, bezosobowych urządzeń w komunikacji internetowej, prowadzi do autentycznej prywatności psychologicznej, która wytwarza, już iluzoryczne, poczucie prywatności informacyjnej (Trepte i Reinecke, 2011). Podobny mechanizm funkcjonuje w przypadku rozmów telefonicznych czy korespondencji pocztowej, które również mogą być przechwy-

cone. Jednak w odróżnieniu od tradycyjnych form komunikacji, fundamentalną zasadą funkcjonowania Internetu jest zapisywanie i przesyłanie dalej kopii, a nie oryginału danych. Walther (2002) zauważa dwie istotne dla prywatności implikacje tej zasady. Po pierwsze, oczekiwanie zachowania kontroli nad jakąkolwiek informacją zamieszczoną w Internecie nie może być uzasadnione (z wyjątkiem szczególnie silnego szyfrowania) i niezależnie od wysiłków osoby, która ją zamieściła, pozostaje dostępna *online*. Ta sama cecha Internetu zachęca do udostępniania, przesyłania dalej wszelkich danych, a więc jednej z podstawowych funkcji portali społecznościowych (Papacharissi i Gibson, 2011).

Jedną ze specyficznych cech technologii cyfrowej jest to, że wszelkiego rodzaju dane mogą być łatwo skopiowane, zapisane, edytowane i przetwarzane. Te same cechy charakteryzują również środowisko Internetu. Boyd (2010b) wskazuje na cztery immanentne cechy światowej Sieci, które wpływają na prywatność użytkowników Internetu. Po pierwsze, każda treść zamieszczona w Internecie jest automatycznie zapisywana i archiwizowana (*trwałość*), a ponadto jest bardzo łatwa do skopiowania (*replikowalność*). Informacje można szybko odnaleźć dzięki wyszukiwarkom internetowym (*wyszukiwalność*), a teoretyczny ich zasięg jest niemal nieograniczony (*skalowalność*). Papacharissi i Gibson (2011) wyróżniają jeszcze jedną cechę wynikającą z „usieciowienia przestrzeni cyfrowej", określoną trudnym do przetłumaczenia zwrotem *shareability*. Internet nie tylko umożliwia dzielenie się informacjami, ale jego struktura wręcz przedkłada to zachowanie ponad chęć utrzymania informacji w tajemnicy. Swobodny przepływ informacji pomiędzy węzłami sieci jest przecież głównym założeniem przyświecającym stworzeniu globalnej Sieci. W przypadku korzystania z mediów społecznych strukturalne cechy Internetu mają jeszcze większy wpływ na wzrost prawdopodobieństwa niekontrolowanego wycieku danych prywatnych. Istnienie serwisu społecznościowego bez przepływu informacji pomiędzy osobami z niego korzystającymi (węzłami) nie ma sensu, gdyż nie spełnia on swojego podstawowego założenia. Im większy przepływ, tym sieci społecznościowe są bardziej społeczne, im są bardziej społeczne, tym większą przynoszą korzyść jej użytkownikom. Osoba, który pragnie aktywnie udzielać się w Internecie, a jednocześnie zachować prywatność, musi osiągnąć wysoki stopień umiejętności dystrybucji informacjami o sobie. Z opublikowanych w ciągu kilku ostatnich lat raportów badań nad użytkownikami sieci społecznościowych wynika, że stopień cyfrowej edukacji i biegłości w zarządzaniu swoją prywatnością w Internecie systematycznie wzrasta, choć czynniki socjodemograficzne mają istotny wpływ na szybkość tej zmiany – przyspieszają ją młody

wiek, wyższe wykształcenie, zamieszkanie w mieście oraz średni lub wyższy poziom dochodów (Zukowski, 2007; Marwick, Diaz i Palfrey, 2010). Z drugiej strony warto odnotować, że nasza aktywność *online* jest coraz mocniej związana z naszą tożsamością, a stopień wpływu informacji zamieszczonych w Internecie coraz bardziej oddziałowuje na reputację osobistą. Jak twierdzą Schneider i Zimmer (2006), jesteśmy świadkami konwergencji pomiędzy dwoma aspektami tożsamości: *offline* i *online*. Nie wygląda więc na to, aby zbliżał się schyłek ery problemów z prywatnością w Internecie.

2.3. Zmiana trybu dostępu do informacji

Jedną z właściwości świata fizycznego jest fakt, że przepływ informacji wymaga podjęcia pewnego wysiłku związanego z jej transportem. Informacja w formie tekstu narzuca konieczność zapisania go na papierze lub innym medium, co wymaga nakładów pracy i finansowych. Tak przygotowane informacje mają swoją wagę, należy je przetransportować do odbiorców. Odległości do pokonania są zatem kolejną barierą. W świecie cyfrowym nakład pracy przy powielaniu i dystrybucji treści zmalał niemal do minimum, jednak w dalszym ciągu przepływ informacji wymagał wykonania podstawowych czynności pozwalających na jej przesłanie i odbiór. Wraz z wprowadzeniem usług WWW sytuacja nie zmieniła się diametralnie – aby uzyskać informacje ze strony internetowej, należało odnaleźć ją z pomocą wyszukiwarki internetowej lub odwiedzić ją bezpośrednio, wpisując adres w przeglądarce. Podobnie było w portalach społecznościowych – aby zobaczyć profil, posty czy zdjęcia innego użytkownika, należało odwiedzić jego stronę.

News Feed i *Mini Feed* wprowadzone przez Facebooka w 2006 roku (Saghvi, 2006) zainicjowały rewolucję w przepływie informacji w sieciach społecznościowych w podobny sposób jak kanały RSS w przypadku stron WWW. *News Feed*, lub w polskiej wersji serwisu po prostu *aktualności*, agregują i wyświetlają najnowsze bądź najczęściej komentowane aktualizacje i zmiany informacji profilowych znajomych, a następnie publikują je na głównej stronie serwisu. *Mini Feed* jest fragmentem profilu, który chronologicznie wyświetla aktualizacje tylko jednego użytkownika. *News Feed* wydaje się być wzorowany na podobnej funkcji Twittera, który został opublikowany zaledwie kilka miesięcy wcześniej. Twitter to platforma mikroblogowa: służy do publikowania krótkich wiadomości, które są następnie wysyłane do użytkowników, którzy zdecydowali się *śledzić* nadawcę. Dzięki *News Feed* jakiekolwiek zmiany w treści profilu, a także zamieszczone posty, zdjęcia

i inne treści zamieszczone w portalu, są dostępne natychmiast na stronach głównych znajomych użytkownika. Ta funkcja powoduje, że nie ma potrzeby podjęcia wysiłku w celu odnalezienia ich w profilu użytkownika. Początkowo zarejestrowani w serwisie internauci wyrażali głęboką dezaprobatę dla wprowadzenia tej zmiany. Poza poczuciem złej organizacji aktualności zamieszczonych w *News Feed*, użytkownicy zwracali uwagę na zbyt wielkie ułatwienie śledzenia takich aktywności użytkownika jak zmiany w związku, udział w wydarzeniach czy dyskusji z innymi użytkownikami, np.:

> Nie potrafię zrozumieć, czemu ktokolwiek miałby chcieć oglądać każdy krok swoich przyjaciół? […] Nie chcę, aby wszyscy moi przyjaciele mogli zobaczyć wszystko co robię (Venice, 2006).

Ogromna liczba osób wyraziła swój brak akceptacji, dołączając do utworzonej w serwisie grupy „Students Against Facebook News Feed"(Schmidt, 2006). Hoadley, Xu, Lee i inni (2010) zapytali użytkowników Facebooka o reakcję na wprowadzoną zmianę. Wyraźna większość (68%) w różnym stopniu odnosiła się do niej negatywnie (29% ogółu badanych bardzo negatywnie), a tylko niecałe 8% mniej lub bardziej pozytywnie. Blisko połowa (49%) czuła się „niekomfortowo", korzystając z odmienionego Facebooka. Sprawdzono, czy na negatywną opinię o *News Feed* i *Mini Feed* mogła mieć medialna dyskusja o zmianach: aż 71% badanych potwierdziło, że dzięki mediom wzrosła ich świadomość zagrożenia prywatności, ale zdecydowana większość (80% ogółu badanych) nie zgodziła się ze stwierdzeniem: „Moja dezaprobata wynika z tego, że innym ta zmiana się nie podoba". Na tej podstawie autorzy uważają, że negatywna opinia o zmianach nie powinna być łączona z ich powszechną krytyką w mediach. Co ciekawe, powodem niechęci użytkowników do nowych funkcji portalu nie była (i nie mogła być) zmiana możliwości dostępu do informacji zamieszczonych przez nich samych na Facebooku – ingerując we własną architekturę Facebook pozostawił wszystkie ustawienia prywatności bez zmian. Tym, co rozzłościło dużą liczbę użytkowników, była jedynie zmiana trybu dostępu do niej. Dwie trzecie badanych zgodziło się ze stwierdzeniem: „Ta sama ilość informacji była dostępna wcześniej, ale teraz jest łatwiej do niej dotrzeć".

Według badaczy rezygnacja z poprzedniego interfejsu wymagającego *wyciągania* informacji z systemu (ang. *pull-based information delivery*), sprawiła, że spadł postrzegany poziom kontroli nad informacjami prywatnymi. Nowy system, *pchający* informację do użytkowników serwisu (ang. *push-based informa-*

tion delivery), nie zmienił nic w kontroli dostępu do danych prywatnych w ujęciu zero-jedynkowym (dane dostępne lub nie) (boyd, 2008). Doprowadził on jednak do zwiększenia możliwości zaistnienia naruszeń prywatności. Informacja opublikowana przez użytkownika (lub informacja o użytkowniku, ale opublikowana przez innych) stała się efektywniej dostępna, szybciej i z większą niż wcześniej łatwością dociera do publiczności. Publiczności, która jest dla użytkownika częściowo *niewidzialna*, a przede wszystkim *niejednorodna*. Może zatem trafić do osób, które nie były zamierzonym audytorium. Zgodnie z teorią integralności kontekstowej Nissenbaum to przyczynia się do zapaści kontekstu. Zjawiska niewidzialnej i niejednorodnej publiczności zostały szerzej opisane w kolejnym rozdziale.

Po kontrowersjach wokół *News Feed* i *Mini Feed* założyciel Facebooka wystosował list otwarty do użytkowników, przepraszając za zmiany (Zuckerberg, 2006). Nie wycofano się jednak z ich wprowadzenia, a jedynie udostępniono użytkownikom większy zakres narzędzi do kontroli prywatności. Mechanizmy podobne do *News Feed* funkcjonują we wszystkich większych portalach społecznościowych, także na Google+ (*strumień*), czy polskiej Naszej Klasie (*śledzik*).

2.4. Media społeczne – problemy z prywatnością

Wraz z bardzo dużym wzrostem liczby użytkowników internetowych serwisów społecznościowych, początkowo MySpace i Friendster, a potem serwisu mikroblogowego Twitter i portalu Facebook, badacze prywatności przenieśli swoją uwagę z zachowań związanych z handlem elektronicznym, szkodliwym oprogramowaniem i niechcianą korespondencją elektroniczną na nowy fenomenem. Użytkownicy serwisów społecznościowych, zachęcani przez administratorów możliwością kontaktowania się ze znajomymi, dobrowolnie upubliczniali swoje imię i nazwisko, wiek, zainteresowania, listy znajomych, a nawet dane teleadresowe. Facebook stał się kopalnią danych prywatnych nie tylko dla rzeszy zwyczajnych użytkowników portalu, ale również dla marketerów, policji, napastników seksualnych i innego rodzaju przestępców. Rosnąca liczba osób ujawniających w ten sposób swoje dane, przy jednocześnie malejących kosztach infrastruktury IT umożliwiającej ich pobieranie, przetwarzanie, łączenie i analizę, sprawiły, że każdy podmiot zainteresowany dostępem do wielkiej osobowej bazy danych uzyskał nielimitowane i niemal bezpłatne źródło cennych informacji. W mediach zaczęły pojawiać się anegdotyczne informacje o różnego rodzaju problemach pojedynczych osób, wynikających z wykorzystania informacji zamieszczonych w portalach społeczno-

ściowych – często przez samych zainteresowanych. Powszechniało twierdzenie, że młodzież, która korzysta z serwisów społecznościowych, niefrasobliwie traktuje swoją prywatność.

Raynes-Goldie (2010) obaliła tę hipotezę poprzez badanie etnograficzne na niewielkiej grupie młodych Kanadyjczyków. Zauważyła, że prywatność, rozumiana jako pełna kontrola nad informacjami prywatnymi, które są przetwarzane przez instytucje takie jak firmy, banki czy rządy, jest dla młodych badanych mniej ważna niż kontrola dostępu do ich prywatnych informacji dla osób z ich otoczenia społecznego: kto, kiedy i w jaki sposób może zobaczyć ich prywatne treści. Raynes-Goldie nazywa to rozróżnienie *społecznym kontekstem prywatności*. Aby skuteczniej zarządzać dostępem do własnych danych w portalach społecznościowych, badani podawali czasem fałszywe dane osobowe (np. nazwisko) i w ten sposób utrudniali ich odszukanie i identyfikację przez osoby niebędące ich bliskimi znajomymi. Ponadto badani regularnie przeglądali posty i zdjęcia, w których ich oznaczono, komentarze pod ich własnymi aktualizacjami i usuwali te, które były dostępne publicznie. Aktywnie zarządzali swoją prywatnością, odnosząc sukcesy i narażając się na porażki. Podobne zachowania zauważyła w swoim badaniu boyd (2008). Sugeruje ona, że młodzież chroni w ten sposób swoją prywatność w sieciach społecznościowych nie przed instytucjami, ale przed rodzicami, nauczycielami i innymi osobami, które mogą mieć na ich życie bezpośredni wpływ (boyd, 2008).

2.4.1. Niejednorodna publiczność

Portale społecznościowe przez długi czas zdawały się ignorować fakt, że w prywatność jest silnie kontekstowa, tj. to, co w jednym kontekście (np. rodzinie czy grupie znajomych) jest komunikowane otwarcie, w innym jest okryte tajemnicą (np. w pracy czy w szkole). W rzeczywistości dostosowujemy nasze zachowanie i przekazywane informacje do odpowiedniego kontekstu. Inny stopień otwartości cechuje rozmowa z wykładowcą akademickim, a inny z najlepszym przyjacielem. W ten sposób tworzymy wiele różnych aspektów naszej tożsamości i podczas komunikacji ze światem prezentujemy wybrane, inne – czasowo ukrywając. W rzeczywistości *offline* sytuacje społeczne są oddzielone granicami przestrzennymi, czasowymi i społecznymi. W Internecie brak tych granic doprowadza do tzw. *zapaści kontekstu* (ang. *collapsed context*) (Nissenbaum, 2004; boyd, 2008). Wiele homogenicznych środowisk, które są publicznością naszych społecznych zachowań w świecie realnym, zapadają się w Internecie w jedną *niejednorodną*

publiczność. Ta kolizja wytwarza wiele napięć i jest jednym z najczęściej występujących zagrożeń dla prywatności w Internecie.

W internetowych sieciach społecznościowych najczęściej spotykana jest prosta koncepcja *znajomych*. W terminologii anglojęzycznej stosuje się termin *friends* oznaczający przyjaciół. W języku polskim *przyjaciel* ma węższe znaczenie i odnosi się tylko do najbliższych osób. Słowo *znajomi* jest zresztą powszechnie używane w polskich wersjach językowych międzynarodowych portali społecznościowych. W literaturze stosowany jest też anglojęzyczny zwrot *friending* oznaczający akt zaproszenia osoby do własnej sieci kontaktów. Związanym terminem jest *friending behaviour*, czyli zachowania dotyczące rozszerzenia sieci kontaktów. W najprostszej wersji tego konceptu użytkownik może wysłać innemu użytkownikowi zaproszenie do swojej sieci kontaktów. Gdy zaproszenie jest zaakceptowane, użytkownicy stają się *znajomymi*, co domyślnie wiąże się z umożliwieniem pełnego dostępu do informacji profilowych oraz aktualizacji. Technologiczna fikcja nieistniejących w rzeczywistości *płaskich przyjaźni* (Peterson, 2010) wymuszona przez cyfrową architekturę skłania użytkownika sieci społecznościowej do zero-jedynkowej kategoryzacji osób: dzieli ich na znajomych i nie-znajomych (wszystkich użytkowników spoza własnej sieci kontaktów). Nie uwzględnia zatem ani różnic w sile relacji wiążących dwie osoby, ani wspominanego wcześniej kontekstu, które w rzeczywistości *offline* oczywiście istnieją pomiędzy tymi osobami (Lewis, Kaufman, Christakis i in., 2008). O ile użytkownik nie ma bardzo restrykcyjnego *friending behaviour* (np. wysyła i przyjmuje zaproszenia jedynie od najbliższych przyjaciół), a sieć społecznościowa nie umożliwia łączenia znajomych we własne podgrupy, to istnieje duża szansa wystąpienia problemu niejednorodnej publiczności (boyd, 2008). Pojawia się on, gdy w sieci kontaktów, a więc wśród osób mających dostęp do profilu i informacji zamieszczanych przez użytkownika, są osoby z różnych kontekstów społecznych. W takiej sytuacji użytkownik nie ma wystarczającej kontroli nad tym, kto ma dostęp do danej części jego profilu, z kim dzieli się informacjami o sobie. *Oversharing* zachodzi, gdy komunikat dociera do zbyt dużej liczby osób. W ten sposób można łatwo utracić kontrolę nad prywatnymi informacjami. *Undersharing* powstaje, gdy na skutek świadomości, że nie mamy kontroli nad audytorium, do którego się zwracamy, całkowicie rezygnujemy z zamieszczenia jakiegoś komunikatu lub udostępniamy go tylko częściowo (Peterson, 2010). Prowadzi to do zaprzepaszczenia potencjalnych korzyści wynikających z dzielenia się informacjami, np. ograniczenia kontaktu czy rozwoju kapitału społecznego (zob. sekcję *Kapitał społeczny a prywatność online*).

Peterson (2010, s. 15–16) cytuje za Mayrowitzem bardzo obrazowy przykład takiej sytuacji, często zachodzącej w portalach społecznościowych:

> Po powrocie z wakacji w Europie dzieliłem się spostrzeżeniami z moimi przyjaciółmi, rodziną i innymi znajomymi. Rozmawiając z nimi, nie opisywałem dokładnie tych samych doświadczeń. Rodzice usłyszeli o bezpiecznych i czystych hotelach, w których nocowałem i o tym, w jaki sposób podróż sprawiła, że stałem się mniej wybredny kulinarnie. Z drugiej strony, moi przyjaciele usłyszeli o doświadczeniach wypełnionych przygodą, niebezpieczeństwem a także romansem. Znajomym profesorom opowiedziałem o edukacyjnych aspektach wycieczki… każdy z różnych typów moich słuchaczy usłyszał inną relację. Czy opowiadając o wyjeździe w ten sposób, skłamałem komukolwiek? W zasadzie nie. Ale opowiedziałem im inne prawdy. Zastanówmy się, co by się stało z odmiennymi relacjami z wycieczki, gdyby po moim powrocie rodzice postanowili zorganizować przywitalną imprezę-niespodziankę, na którą zaprosiliby moich przyjaciół, krewnych, profesorów i sąsiadów. Co by się stało z moimi spostrzeżeniami, gdyby słuchacze nie byli od siebie oddzieleni?… Niemal każdy opis przeznaczony właściwemu audytorium składałby się z części, które albo by znudziły, albo zgorszyły część połączonej publiczności… Mógłbym szybko dostosować się i do nietypowej sytuacji i opowiedzieć coś wystarczająco mdłego, żeby nie urazić nikogo. Najważniejszą kwestią jest to, że kiedy odmienne otoczenia społeczne są połączone, nasze poprawne zachowanie może nagle stać się niepoprawne.

Dodatkowym problemem jest wcześniej opisany język. *Friending* w portalu społecznościowym językowo przypomina zaprzyjaźnienie się, ale rzeczywistość jest odmienna. Badania pokazują, że zdecydowana większość relacji między użytkownikami sieci społecznościowych ma swoje korzenie w świecie rzeczywistym (Mayer i Puller 2008; boyd i Ellison, 2007; Filiciak, Danielewicz, Halawa i in., 2010), ale w jednym przypadku podstawą internetowej relacji jest zażyła, długoletnia przyjaźń, a w innym zupełnie pobieżna znajomość. Architektura sieci społecznościowych niesłusznie zakłada, że zasady przyjaźni stosują się także do znajomości potwierdzonej przyjęciem zaproszenia w SNS.

Facebook był początkowo portalem umożliwiającym rejestrację wyłącznie studentom amerykańskich uczelni wyższych i zezwalał na komunikację jedynie pomiędzy studentami jednej uczelni, tworząc nie jedną, ale wiele sieci społecznościowych. Otwierając się we wrześniu 2005 roku dla liceów zastosował poważne ograniczenia: uczniowie, przed umożliwieniem rejestracji w portalu, musieli być zweryfikowani przez studenta wyższej uczelni, który ukończył tę samą szkołę.

Studenci nie mieli dostępu do sieci licealnych i odwrotnie. Według współtwórcy Facebooka, Chrisa Hughesa, taka architektura była wzorowana na faktycznych warunkach społecznych, w których licealiści rzadko mają kontakt ze studentami. Facebook miał ułatwić i rozszerzyć możliwości codziennej komunikacji, a także zapoznawania się z innymi uczniami tej samej szkoły czy uczelni. Rok później Facebook pozwolił na otwartą rejestrację, umożliwiając założenie konta każdej osobie, która posiada adres e-mail. Jednocześnie zniesiono ograniczenia komunikacji pomiędzy wieloma homogenicznymi Sieciami, tworząc jedną sieć społecznościową. Dotychczasowi użytkownicy utracili jednolitą studencką społeczność, bezpieczne miejsce do kontaktów z rówieśnikami, gdzie mogli zamieszczać fotografie z zakrapianych alkoholem imprez i dzielić się wrażeniami z korzystania z narkotyków. Młodzi użytkownicy Facebooka z przerażeniem otrzymywali zaproszenia do sieci kontaktów od swoich rodziców, wykładowców czy babć (Peterson, 2010).

W odpowiedzi na narastające niezadowolenie użytkowników, Facebook umożliwił w 2007 roku tworzenie różnych kontekstów w trakcie dzielenia się informacjami (blog na Facebooku, 2007). Nowe funkcje pozwalają na stworzenie własnych list znajomych i takie zarządzanie ustawieniami prywatności profilu, w tym także widocznością pojedynczego elementu profilu (np. pojedynczego zdjęcia czy aktualizacji statusu), że można w niemal dowolny sposób ograniczyć widoczność każdego elementu. Można na przykład zamieścić na swoim profilu status widoczny tylko dla jednej osoby lub album ze zdjęciami widoczny dla wszystkich znajomych poza grupą dalszych znajomych. Domyślnie, każda nowa osoba w sieci kontaktów trafia jednak do ogólnej sieci kontaktów.

Google, prezentując w 2011 roku serwis Google+ (czyt. *Googleplus*), zaproponował nieco inny model rozszerzenia własnej sieci kontaktów. Każdą nową osobę dodaje się do jednej lub kilku z predefiniowanych bądź własnych grup, tzw. kręgów. Podobnie jak w życiu realnym, gdzie kręgi społeczne zachodzą na siebie, jedna osoba może należeć do kilku kręgów. W Google+ nie ma możliwości dodania osoby do własnej sieci kontaktów bez wskazania przynajmniej jednej grupy, do której będzie przynależeć. Łatwe przenoszenie znajomych między grupami za pomocą techniki *przeciągnij i upuść* oraz możliwość publikowania informacji tylko dla wybranych kręgów, faktycznie zachęcają użytkowników do aktywnego zarządzania listą znajomych i osadzania komunikatów w odpowiednich dla nich kontekstach. Jednocześnie Google umożliwił tworzenie jednostronnych relacji – osoba dodana do kręgu nie otrzymuje zaproszenia do sieci kontaktów, ale jedynie powiadomienie o wykonaniu takiej czynności przez innego użytkownika. Dzięki temu można otrzymywać we własnym *strumieniu* informacje udostępnio-

ne publicznie przez daną osobę lub instytucję, analogicznie jak odbywa się obserwowanie w portalu Twitter. Klasyczne, dwustronne dodanie do sieci kontaktów zachodzi przy wzajemnym dodaniu się do kręgów.

Kręgi i jednostronne obserwowanie użytkowników miały być elementami odróżniającymi portal społecznościowy Google od lidera tej branży – Facebooka. Niedługo później podobne funkcje zostały wprowadzone przez giganta. Opracowano system *inteligentnych* list znajomych i umożliwiono tworzenie jednostronnych relacji (subskrypcję informacji dostępnych publicznie) podobnie jak w Google+. U wszystkich użytkowników pojawiły się automatycznie listy znajomych takie jak „Rodzina", „Bliżsi znajomi", „Dalsi znajomi" oraz listy związane z edukacją, miejscem zamieszkania czy pracą. Decyzja o dodaniu nowego znajomego do grupy bliskich czy dalekich znajomych podejmowana jest za każdym razem przez użytkownika, w każdej chwili można też przenieść osobę do odpowiedniejszej grupy. Pozostałe grupy są tworzone całkowicie automatycznie na podstawie pasujących pól w informacjach profilowych. Dzięki temu można zamieścić post tylko dla rodziny, dla wszystkich znajomych z wyjątkiem znajdujących się w grupie „Dalsi znajomi", czy tylko dla znajomych, którzy zamieścili na Facebooku informację, że mieszkają Warszawie. To znaczne udogodnienie w zarządzaniu listami znajomych, ustępujące jednak łatwością tworzenia i edytowania kręgów w Google+. Wybór odpowiedniej grupy dla nowych znajomych nie jest centralnym punktem procesu *zaprzyjaźniania się*, ale pojawia się jako propozycja po wcześniejszym dodaniu osoby do sieci kontaktów (Ross, 2011). Domyślnie, nowe kontakty pozostają zapisane bez żadnej grupy, co jest niemożliwe w Google+. Twórcy Facebooka zyskali w ten sposób argumenty w konkurencji z Google+, nie zmieniając jednak swojej filozofii dzielenia się wszystkim ze wszystkimi i zasady *radykalnej transparencji* wyłożonej w zasadach Facebooka.

Część komentatorów z branży internetowej zwróciła uwagę na to, że tworzenie zabezpieczeń i ograniczeń w dostępie do internetowego profilu pozwala uzyskać niecałkiem uzasadnione wrażenie bezpieczeństwa informacyjnego. „Ściany są iluzoryczne", zabezpieczenia są tylko techniczne i mogą zawieść. Jeszcze bardziej prawdopodobne jest, że informacja, zamieszczona dla wąskiej grupy osób, zostanie udostępniona dalej. Poczucie pełnej kontroli, jakie mogą dać narzędzia do zarządzania własną prywatnością w sieciach społecznościowych, zachęca do szerszego i głębszego otwierania się, przez co ewentualny wyciek informacji prywatnych może wyrządzić poważne szkody. Niektórzy komentatorzy uważają, że w związku z tym znacznie bezpieczniejszym rozwiązaniem jest kontrolowany *undersharing* (Ulanoff, 2011).

Kolejnym minusem kręgów jest uciążliwość zarządzania grupami znajomych. Gwarantem dużego sukcesu usługi w Internecie jest prostota jej obsługi. Pionierem takiego podejścia jest zresztą Google. Strona główna wyszukiwarki internetowej składająca się z paska, w którym można wpisać treść zapytania, i dwóch przycisków, jest symbolem minimalizmu w projektowaniu aplikacji internetowych i receptą na sukces. System zarządzania kręgami nie jest skomplikowany, ale konieczność przyporządkowania do kręgów kilkudziesięciu czy kilkuset znajomych wymaga od użytkownika pewnego nakładu pracy. Jeszcze bardziej uciążliwe jest przenoszenie zmian z rzeczywistej sieci kontaktów do aplikacji internetowej. Relacje międzyludzkie są dynamiczne, dalsi znajomi stają się przyjaciółmi, poznajemy nowe osoby, tracimy kontakt z innymi – wymaganie od użytkownika ciągłego wprowadzania zmian w kręgach Google+ jest mało realistyczne, a pomyłki mogą skutkować naruszeniami prywatności (Pachal, 2011).

Google+, mimo bardzo szybkiego wzrostu liczby użytkowników, ciągle pozostaje daleko w tyle z Facebookiem, przyciągając głównie mężczyzn (blisko 70%), często inżynierów, osoby interesujące się nowinkami technicznymi (FindPeopleonPlus, 2012, Google+ SocialStatistics, 2012). Według portalu comScore blisko 100 milionów użytkowników spędza w portalu średnio 3 minuty miesięcznie (Google Investor Relations 2012). Dla porównania: przeciętny użytkownik Facebooka spędza w serwisie aż 405 minut miesięczne (Efrati, 2012). Trudno wyrokować, czy to funkcja kręgów jest powodem małej aktywności użytkowników Google+. Bardziej prawdopodobne, że jego użytkownicy są wystarczająco zadowoleni z innych serwisów społecznościowych, a wirtualna *przeprowadzka* na nowy serwis nie jest dla nich atrakcyjna. Duża liczba użytkowników Google+ wynika między innymi z intensywnego reklamowania własnej usługi społecznościowej. Poza tym Google *zmusza* użytkowników innych swoich serwisów do założenia konta w Google+. Na przykład utworzenie nowego konta Gmail było uzależnione od rejestracji w Google+ (Brian, 2012). Dzięki temu tempo wzrostu liczby użytkowników jest rekordowe w porównaniu do rozwoju innych stron internetowych, ale proces ten generuje również wiele nieaktywnych kont.

2.4.2. Niewidzialna publiczność

Kolejnym problemem związanym z prywatnością komunikatów nadawanych przez Internet jest brak jednoczesnej fizycznej obecności nadawcy i odbiorcy. W rzeczywistości niewirtualnej, np. w czasie rozmowy, informując kogoś o swoich prywatnych sprawach, bierzemy pod uwagę, kto nas słucha oraz kto poten-

cjalnie może nas usłyszeć – jakie jest prawdopodobieństwo, że w pobliżu jest niepożądany słuchacz, osoba, która nie powinna mieć dostępu do przekazywanych i odbieranych przez nas informacji. Takie wnioskowanie nazywamy heurystyką społeczną (Grimmelmann, 2009). Istnieje również heurystyka architektoniczna, która pomaga w odnalezieniu odpowiedzi na pytanie, czy obiektywne warunki środowiskowe pozwalają podsłuchującemu przechwycić komunikat. Znamy właściwości świata fizycznego, wiemy, jak nasz głos rozchodzi się w powietrzu, bezwiednie oceniamy warunki zewnętrzne, regulując siłę głosu. Rozmawiając na głośnej ulicy, możemy domniemywać, że uliczny zgiełk zagłuszy treść rozmowy dla potencjalnego podsłuchiwacza.

Przyzwyczajeni do właściwości świata rzeczywistego mamy problemy z heurystyką architektoniczną w świecie cyfrowym, gdyż jego właściwości są skuteczniej przed nami ukryte. Audytorium nie jest fizycznie widzialne, a większość serwisów społecznościowych nie wyświetla listy osób, która zobaczy nasz komunikat. W przypadku osób, które świadomie lub z powodu budowy portalu społecznościowego, decydują się na otwarte profile, niewidoczna publiczność jest ogromna, ale przynajmniej znana: jest nią cały Internet, czyli kilka miliardów użytkowników i jeszcze większa liczba urządzeń podłączonych do Sieci, które mają możliwość zapisania, magazynowania, przetwarzania i udostępniania danych. W przypadku profili o większym stopniu zamkniętości, dostępnych tylko dla sieci kontaktów lub tzw. rozszerzonej sieci kontaktów (*znajomych znajomych*), niewidzialna publiczność również istnieje. Po pierwsze, jak już wspomniano, większość użytkowników ma średnio od 130 do 180 znajomych, co przekłada się na nawet kilkadziesiąt tysięcy *znajomych znajomych* (Ugander, Karrer, Backstrom i in., 2011). Są to osoby, z którymi łączą nas relacje o różnym natężeniu – najbliżsi przyjaciele, osoby znane z różnych kontekstów społecznych (szkoły, pracy), po osoby zupełnie nieznane. Ponadto wszyscy *powiernicy* mają możliwość skopiowania i udostępnienia treści dalej, przez co publiczność może się błyskawicznie rozszerzyć o nowe grono osób, które nie były pierwotnie docelowymi odbiorcami. W takiej komunikacji nie istnieje warunek jednoczesności. Informacje, które kilka lat temu uważaliśmy za stosowne do komunikowania ówczesnym znajomym, dziś mogą być nieodpowiednie choćby dlatego, że zmienia się audytorium. W sieciach społecznościowych użytkownik, mając świadomość, że inni ludzie mają dostęp do jego danych, może żmudnie ustalać reguły tego dostępu, ale prawie nigdy nie wie, kto finalnie uzyskał dostęp i do jakich danych, a także kiedy i co z nimi zrobił. W mediach społecznych są od tej zasady wyjątki, chociażby popularna zawodowa sieć społecznościowa LinkedIn. W takiej sytuacji trudne jest uszanowanie norm

stosowności. Obrazowo opisuje to Peterson (2010): „Jak podejrzany w pokoju przesłuchań, użytkownik wie, że ktoś stoi za lustrem weneckim, ale nie wie dokładnie, kto i w związku z tym, jaką rolę powinien odgrywać". Nawet, jeżeli wiemy, kto potencjalnie może mieć dostęp do naszego profilu i aktualności, to przy zamieszczaniu treści nie wizualizujemy sobie obrazu całej publiczności, nie widzimy wszystkich odbiorców wyraźnie. Przy braku tej świadomości łatwo o niezgodne z intencjami udostępnienie informacji.

2.5. Paradoksy prywatności

Badacze Internetu, mediów społecznych i prywatności w środowisku *online* zwrócili uwagę w połowie pierwszej dekady XXI wieku na dwa fenomeny, które powodują wiele napięć związanych z ujawnianiem prywatnych danych w Internecie. Opinia publiczna zaczęła interesować się mediami społecznymi i kwestiami dotyczącymi prywatności. Najczęściej reprezentowano uproszczone stanowisko, zakładając, że ludzie korzystający z serwisów społecznościowych, zazwyczaj młodzież, po prostu nie dbają o swoją prywatność. Charakteryzuje je zdanie Roberta Samuelsona (2006) z artykułu dla Washington Post:

> Wygląda na to, że [użytkownicy serwisów społecznościowych – przyp. autora] błagają o popularność i sławę bardziej niż obawiają się utraty prywatności.

Naukowcy zwrócili swoją uwagę na ten problem, a przeprowadzone badania wykazały, że sytuacja jest zgoła odmienna.

2.5.1. Beztroska młodzież, zmartwieni rodzice

Barnes (2006) zauważyła, że wraz z rozwojem i gwałtownym wzrostem popularności sieci społecznościowych zwiększała się różnica pomiędzy obawą dorosłych Amerykanów o prywatność swoją oraz swoich dzieci, a udostępnianiem przez dzieci i młodzież coraz większej ilości informacji *online*. Badaczka nazwała ten problem paradoksem prywatności. Młode osoby, *early adopters*, czyli pierwsi użytkownicy MySpace, Friendstera czy Facebooka, nie zostały uświadomione przez rodziców, wychowawców, nauczycieli, media o możliwych negatywnych konsekwencjach ujawniania swoich danych prywatnych. Osoby, na barkach których powinien spocząć ten obowiązek, w 2006 roku często nie wiedziały o istnieniu serwisów społecznościowych, a prawie nigdy z nich nie korzystały. W związku

z tym zachowania użytkowników serwisów społecznościowych zostały wykształcone przez interakcję z innymi użytkownikami, a także samodzielne eksperymenty związane z odkrywaniem i budowaniem własnej tożsamości *online*. Chęć przedłużenia i rozszerzenia komunikacji z rówieśnikami, poznawania nowych osób, wyrażania siebie poprzez zamieszczanie zdjęć, obrazów wideo stanowi dużą zachętę do publikowania informacji prywatnych w takich portalach.

Jako podstawowy powód powstania paradoksu Barnes zidentyfikowała brak jasno wytyczonych granic pomiędzy tym, co publiczne a tym, co prywatne w Internecie. Jest wiele argumentów popierających stwierdzenie, że w Internecie nic nie jest prywatne: najczęściej „prywatność" w Sieci oznacza takie ograniczenie dostępu do danych, że są one widoczne tylko dla wybranej grupy osób lub nawet wyłącznie dla jej posiadacza. Jednak mechanizmy zabezpieczenia dostępu do danych są zawodne, a użytkownicy nie zawsze potrafią z nich odpowiednio korzystać. Dodatkowo użytkownicy portali społecznościowych mogą mieć wrażenie, że ich profil *online* to przestrzeń prywatna. Możliwość ograniczenia widoczności profilu oraz fakt pojawiania się na *ścianie* informacji pochodzących od bliskich znajomych powodują poczucie zachowania prywatności komunikacji w sieci społecznościowej. Sullivan (2010) zwraca uwagę na kolejny element potęgujący to wrażenie – wymóg rejestracji, a także jej ograniczenie, np. wymóg posiadania zaproszenia czy adresu internetowego w domenie uczelni wyższej lub liceum. Takie ograniczenie utrzymywał do września 2006 roku Facebook (Abram 2006, Lacy 2006). Wcześniej, w 2005 roku, 33% badanych zgodziło się ze stwierdzeniem: „Dostęp do Facebooka jest niemożliwy lub prawie niemożliwy dla osób, które nie są studentami uniwersytetu" (Gross i Acquisti 2005).

W praktyce są dwa główne powody, dla których poczucie prywatności komunikacji na stronach wymagających rejestracji jest złudne. Po pierwsze, rejestracja wymaga zwykle zaledwie aktywnego adresu e-mail oraz wypełnienia kilku pól z danymi osobowymi, których prawdziwość nie jest weryfikowana. Zdobycie zaproszenia do sieci, która tego wymaga lub wykorzystanie adresu e-mail w odpowiedniej domenie również nie jest barierą nie do ominięcia. Po drugie – nawet jeżeli dane, które zamieszczamy w sieci społecznościowej, są początkowo dostępne tylko dla wąskiej grupy osób, to w dalszym ciągu istnieje możliwość łatwego ich skopiowania i dalszego udostępnienia, często za pomocą funkcji wbudowanych w portal społecznościowy.

2.5.2. Niezgodność postaw i zachowań

Barnes zdefiniowała paradoks prywatności jako rozbieżność pomiędzy liberalnym ujawnianiem danych prywatnych przez nastolatków, a obawami ich rodziców. Inne badania (m.in. Gross i Acquisti, 2005; Jensen, Potts i Jensen, 2005; Stutzman, 2006; Norberg, Horne oraz Horne, 2007; Lewis, Kaufman, Christakis i in., 2008; boyd i Hargittai, 2010) sugerują, że istnieje również drugi paradoks – wielu internautów uważa prywatność za ważne dobro osobiste i wykazuje dużą troskę o jej zachowanie, ale ich postępowanie zdaje się temu przeczyć. Mimo wysokiego deklarowanego poziomu troski o prywatność, wielu internautów udostępnia komplet własnych danych prywatnych na portalach społecznościowych, nie poświęca czasu na zapoznanie się i dostosowanie ustawień prywatności czy akceptuje zaproszenia do grona znajomych od obcych osób.

Gross i Acquisti (2006) przeprowadzili dwuetapowe badanie wśród studentów i wykładowców akademickich na jednej z uczelni w USA, składające się z ankiety oraz analizy danych uzyskanych dzięki data miningowi informacji profilowych na Facebooku. Badacze chcieli uzyskać odpowiedź na pytanie, czy stopień troski o ochronę własnych danych prywatnych jest dobrym wskaźnikiem prawdopodobieństwa posiadania konta na Facebooku oraz czy wiąże się on ze stopniem upublicznienia profilu. Badacze wykazali niewielkie, ale statystycznie istotne różnice pomiędzy użytkownikami Facebooka, a osobami z niego niekorzystającymi. Osoby niezarejestrowane na Facebooku: (1) przypisywały wyższą wagę konieczności uchwalenia regulacji dotyczących ochrony danych prywatnych w USA, (2) wyrażały wyższy stopień troski o własną prywatność oraz (3) wyrażały wyższy stopień obaw przy hipotetycznych scenariuszach, w których mogło dojść do naruszenia ich prywatności. Autorzy nie odnaleźli jednak jednoznacznego poparcia dla hipotezy, że wysoki poziom obawy o własną prywatność może skłonić ludzi do rezygnacji z korzystania z portali społecznościowych. Przeciwnie, np. w przypadku studentów studiów licencjackich blisko 90% respondentów, którzy wyrażali najwyższy stopień troski o własną prywatność, była użytkownikami Facebooka (przy średniej dla tej grupy studentów równej 93%).

Zdecydowana większość badanych zgadzała się ze stwierdzeniem, że prywatność oraz legislacja z nią związana, to kwestia ważniejsza nawet od bezpieczeństwa czy zagrożeń terrorystycznych, a nieco mniej istotna tylko od polityki gospodarczej i edukacyjnej. Dane te zaprzeczały stawianej przez opinię publiczną tezie o zupełnym braku zainteresowania ochroną prywatności przez użytkowników portali społecznościowych.

Wysoki poziom troski o prywatność nie wpływał jednak ani na rezygnację z korzystania z Facebooka, ani na rodzaj oraz ilość danych prywatnych zamieszczanych tam publicznie. Autorzy wskazują na niespójności pomiędzy wyrażanymi postawami i obawami, a rzeczywistym zachowaniem. Przykładowo, 22% osób, które były bardzo zaniepokojone scenariuszem, w którym „obca osoba zna twój rozkład zajęć oraz wie, gdzie mieszkasz", zamieściło na FB swój adres domowy, 40% rozkład zajęć, a 16% oba powyższe. Podobne zjawisko pojawiło się w przypadku osób najbardziej zaniepokojonych następującym scenariuszem: „Ktoś za pięć lat będzie mógł poznać twoje obecne poglądy polityczne, orientację seksualną i nazwisko partnera". Wśród osób, które tak stwierdziły, 16% udostępniało wszystkie powyższe dane publicznie na Facebooku.

Wielu badanych, którzy nigdy nie zmieniali ustawień prywatności swojego profilu, miało błędne przekonania na temat faktycznej publicznej widoczności swoich danych prywatnych. Jedna czwarta niesłusznie uważała, że ich profil nie jest możliwy do odnalezienia za pomocą wbudowanej wyszukiwarki. Takie było wtedy domyślne ustawienie w portalu Facebook, tak też jest obecnie. Respondentów, których profile były publiczne, zapytano o ocenę liczby osób, które teoretycznie mogą mieć do nich dostęp (ze skali: kilkaset, kilka tysięcy, kilkadziesiąt tysięcy, kilkaset tysięcy, miliony). Najwięcej osób wskazało *miliony*, jednak więcej niż połowa stwierdziła, że może to być kilkaset tysięcy i mniej.

Podsumowując: blisko trzy czwarte użytkowników Facebooka uważało, że prywatność ich danych to ważna kwestia i ma świadomość, na ile ich profil w portalu społecznościowym jest widoczny, ale jednocześnie nie zawsze ogranicza w istotny sposób dostęp do niego. Mniejszość osób znacząco zaniża widoczność swoich danych profilowych oraz ich potencjalny zasięg.

Gross i Acquisti (2006) uważają, że jednym z najbardziej prawdopodobnych wytłumaczeń dla tego paradoksu jest sama idea serwisu społecznościowego. Jego budowa z założenia powinna unikać silnych mechanizmów kontroli dostępu, bezpieczeństwa oraz ochrony prywatności i w taki też sposób konstruuje tego typu serwisy. Im łatwiej nowym osobom dołączyć do Sieci i odnaleźć swoich znajomych z rzeczywistości offline, a następnie odnaleźć wspólne płaszczyzny kontaktu z nimi oraz innymi użytkownikami – tym większą wartość funkcjonalną dla użytkownika stanowi serwis społecznościowy. Popularność serwisu przekłada się na atrakcyjność dla reklamodawców i dochodowość serwisu dla firmy nim zarządzającej.

Inne wytłumaczenie dla wyników uzyskanych przez Gross i Acquisti zakłada, że opisywany paradoks wcale nie istnieje, a jego pozorna realność wynika z wiary

w teorię racjonalnego wyboru, którą wielu badaczy próbuje zastosować do przestrzeni cyfrowej. Nie potrafi ona odpowiedzieć na pytanie, czemu ludzie, którzy szczerze troszczą się o własną prywatność, narażają ją poprzez udostępnianie własnych danych w Sieci. Klasyczna ekonomia zakłada, że ludzie podejmują decyzje zgodnie z ich racjonalnym interesem. Oceniają, jak ich zachowanie wpłynie na przyszły dobrobyt i wybierają te możliwości, które według nich przybliżą osiągnięcie pożądanego celu. Zachowania związane z prywatnością są dla klasycznych ekonomistów zwykłą transakcją, w której jednostki, kierując się zimną analizą zysków i strat, dążą do maksymalizacji korzyści w zgodzie z własnymi preferencjami. Opierając się na tej teorii, należałoby przyjąć założenie, że jednostki są w stanie w pełni przewidzieć skutki własnych działań w Internecie na ich teraźniejszą i przyszłą prywatność.

Konfrontując teorię racjonalnego wyboru z głęboką troską o prywatność internautów korzystających z portali społecznościowych, musimy natknąć się na paradoks prywatności: czemu internauci, którzy twierdzą, że dbają o swoją prywatność, tak często zachowują się przeciwstawnie do swojej postawy? Czemu nie rezygnują z korzystania z portalu społecznościowego lub przynajmniej nie ograniczają dostępu do swojego profilu poprzez korzystanie z ustawień prywatności? Czemu użytkownicy Facebooka nie przenoszą się do portalu, który bardziej szanuje ich prywatność i umożliwia łatwiejsze zarządzanie prywatnością? Klasyczna ekonomia odpowiada – użytkownicy portali społecznościowych wysoko cenią korzyści wynikające z publikowania prywatnych informacji w mediach społecznych, a mało obawiają się ryzyka naruszenia prywatności. Takie wytłumaczenie nie jest zgodne z danymi zebranymi w wielu badaniach. Acquisti (2004), analizując zachowania internautów w środowisku handlu elektronicznego, oparł się na ekonomii behawioralnej i zaproponował uwzględnienie dodatkowych czynników i psychologicznych błędów poznawczych, które wpływają na decyzje podejmowane przez użytkowników. Te błędy są systemowe, czyli zarówno powtarzalne, jak i przewidywalne. Jak twierdzi Peterson (2010), decyzje podejmowane przez użytkowników są *przewidywalnie irracjonalne*. Acquisti zauważył, że jednostka, która podejmuje decyzję związaną z udostępnieniem (bądź nie) swoich informacji w Sieci, staje przed typowym problemem związanym z transakcją ekonomiczną – posiada *niekompletne informacje*. W jaki sposób może ocenić precyzyjnie bilans ekonomiczny ochrony bądź udostępnienia swoich danych prywatnych? Koszty i korzyści mogą być materialne (np. straty wynikające z kradzieży tożsamości, zniżka na zakupy uzyskana w konkursie na portalu społecznościowym), jak i niematerialne (np. czas spędzony na dostosowaniu ustawień prywatności

w portalu społecznościowym po stronie kosztów, a po stronie korzyści – utrzymywanie kontaktu z przyjaciółmi). Większość kosztów związanych z racjonalną oceną możliwości jest istotna i natychmiastowa (np. czas spędzony na tworzenie list znajomych), natomiast korzyści są odsunięte w czasie i często niewidoczne (np. brak naruszenia prywatności).

Kolejną niewiadomą w równaniu zysków i strat jest trudna ocena prawdopodobieństwa wystąpienia zdarzeń w dynamicznym środowisku cyfrowym, zwłaszcza, że dane prywatne zamieszczone dzisiaj mogą zostać wykorzystane niezgodnie z naszą wolą dopiero za kilka lat. Ludzkie jednostki mają *ograniczoną racjonalność*, gdyż niezależnie od kompletności posiadanych informacji, nie są w stanie przetworzyć ich wszystkich. Wysiłek intelektualny, który musiałby zostać poniesiony, aby wybrać optymalną strategię, może być tak wysoki, że jednostka zdecyduje się pominąć racjonalny proces i skorzysta z metod heurystycznych. W przypadku portali społecznościowych efektem ograniczonej racjonalności może być korzystanie z ustawień domyślnych (zob. sekcję *3.3. Rynkowa samoregulacja*).

Hiperboliczne obniżenie wartości to kolejny błąd poznawczy, który może mieć wpływ na decyzje związane z ochroną prywatności. Występuje, gdy osobiste preferencje nie są stałe w czasie – wydarzenia bliskie w czasie (lub natychmiastowe) są bardziej wartościowe od tych samych wydarzeń w przyszłości. Użytkownicy sieci społecznościowych zdają się obniżać prawdopodobieństwo ryzyka utraty kontroli nad swoimi danymi prywatnymi w przyszłości. Takie zachowanie jest potęgowane przez kolejny błąd poznawczy – *nierealistyczny optymizm*. To nastawienie można streścić zdaniem: „Wypadki zdarzają się innym, nie mnie". Jako punkt odniesienia Peterson (2010) podaje za Thaler i Sunstein (2008) kilka przykładów przekonań wynikających z tego błędu: 95% studentów uważa, że ich ocena z testu będzie wyższa niż mediana ocen; 90% kierowców uważa, że prowadzi samochód lepiej niż przeciętny kierowca; mimo że wiele małżeństw kończy się rozwodami, ludzie pobierają się, wierząc, że im się to nie przydarzy. Jednostki mają również problem z oszacowaniem *skumulowanego ryzyka*. W kontekście prywatności oznacza on brak pełnego zrozumienia, że całe ryzyko związane z regularnym ujawnianiem niewielkich fragmentów informacji prywatnej jest większe niż suma pojedynczych zagrożeń. Ostatnim problemem, na który zwraca uwagę Acquisti (2004), jest problem z samokontrolą. Nawet jeżeli szczerą intencją jednostki jest ochrona swoich danych prywatnych, może odkładać wysiłek związany z zarządzaniem nimi w nieokreśloną przyszłość, tak jak osoba paląca papierosy, która planuje rzucenie palenia *od przyszłego tygodnia*. Odsuwanie w czasie ochrony własnej prywatności powoduje, że więcej danych

jest już udostępnionych i wysiłek związany z ich zarządzaniem wzrasta, podobnie jak ryzyko utraty kontroli nad nimi.

Acquisti (2004, s. 4) podsumowuje:

> Gdy podejmujemy decyzje związane z prywatnością, prawie nigdy nie mamy wystarczającej ilości danych niezbędnych dla dobrze poinformowanego wyboru. Ale nawet jeśli byśmy je mieli, nie jesteśmy w stanie ich przetworzyć. I jeśli nawet moglibyśmy to zrobić, w dalszym ciągu możemy zachować się niezgodnie z naszym racjonalnym osądem.

Peterson (2010) zwraca uwagę na to, że opisane zniekształcenia w racjonalnym podejmowaniu decyzji, znane z ekonomii behawioralnej, mają istotny wpływ na jednostki w dobrze im znanym świecie rzeczywistym. Internet, cyfrowe media społeczne pełne *technologicznych fikcji*, nie są takim środowiskiem, więc uprzedzenia i problemy oddziałują na ich użytkowników jeszcze silniej. Peterson (2010, s. 22) uważa, że decyzje użytkowników sieci społecznościowych dotyczące prywatności prawie nigdy nie są motywowane racjonalną oceną, a „niechlujną mieszanką norm i oczekiwań społecznych oraz błędów poznawczych". Według niego użytkownicy stale i przewidywalnie zaniżają szacunek ryzyka zagrożenia prywatności i niewystarczająco zabezpieczają się przed nim, zdając sobie sprawę z pomyłek dopiero po fakcie. Nissenbaum (2010, s. 178) z kolei uważa, że „nie ma sprzeczności w jednoczesnej głębokiej trosce o prywatność i ochoczym dzieleniu się informacjami, dopóki dzielenie się i wstrzymywanie się od dzielenia podporządkowane jest zasadniczym warunkom nałożonym przez kontekstowe normy zarządzania dystrybucją informacji" (zob. sekcję *1.1.5.1. Prywatność jako integralność kontekstowa informacji*).

2.6. Kapitał społeczny a prywatność *online*

Część badaczy sieci społecznościowych, czy ogólniej Internetu, zwraca uwagę na rozwój kapitału społecznego jako na istotną wartość, która może być rozwijana poprzez korzystanie z mediów społecznych. Zważywszy na możliwości komunikacyjne, jakie oferuje Internet, oczywiste jest, że nowe medium wymaga przewartościowania dotychczasowej wiedzy na ten temat.

Życie w społeczeństwie zawsze wymagało dobrowolnego zrzeczenia się pewnej części swojej prywatności. Aby stać się osobą społeczną, jednostka musi podzielić się częścią swojego czasu, prywatnej przestrzeni i informacjami o so-

bie. Teoria kapitału społecznego przynosi nowe możliwości interpretacyjne dla skrzyżowania wątków prywatności i Internetu. Koncept ten dotyczy szeroko rozumianych rzeczywistych lub potencjalnych zasobów, powstałych ze związków między ludźmi w specyficznym kontekście sieci społecznej (Ellison, Steinfield i Lampe, 2007). Teoria kapitału społecznego opisuje mechanizmy, które generują wartościowe zasoby (np. zaufanie, umiejętność współpracy), a także same zasoby powstałe ze związków międzyludzkich (np. inicjatywa obywatelska, dzielenie się użytecznymi informacjami). Putnam (2008) wyróżnia dwa typy kapitału społecznego – wiążący (ang. *bonding*) i pomostowy (ang. *bridging*). Wiążący wywodzi się z silnych lub intymnych więzi takich jak związek rodzinny czy przyjaźń, natomiast pomostowy opiera się na słabych więziach międzyludzkich. Wiążący kapitał społeczny łączony jest z cennymi wartościami takimi jak zaufanie, wzajemność, wsparcie emocjonalne czy udzielanie rzeczywistej pomocy. Relacje występujące w silnych związkach są zwykle wzajemnie połączone, tworząc gęsty splot, a wiele informacji przezeń przepływających się powtarza. Szeroka sieć słabych więzi sprzyja natomiast rozprzestrzenianiu się unikalnej informacji – jest to główna korzyść wynikająca z pomostowego kapitału społecznego. Ellison, Steinfield i Lampe (2007) zaproponowali trzeci koncept, którym jest tak zwany *utrzymany kapitał społeczny* (ang. *maintaned social capital*), odnoszący się do umiejętności utrzymania wartościowych relacji społecznych. Miał on posłużyć do zbadania, czy narzędzia internetowe umożliwiają utrzymanie relacji zbudowanych w rzeczywistości offline, po utraceniu kontaktu fizycznego. Jest to zatem koncept operacyjny, choć obrazujące ważne, opisywane już w pracy zjawisko – sieci społecznościowe częściej służą podtrzymaniu istniejących w świecie realnym kontaktów, niż zawieraniu nowych znajomości.

Zawieranie i rozwijanie znajomości są jednymi z najważniejszych celów, dla których ludzie korzystają z sieci społecznościowych. Przebywanie w sieci relacji międzyludzkich jest niezbędnym elementem poprzedzającym wytwarzanie kapitału społecznego. Połączenia między ludźmi wymagają komunikacji i otwierania się na innych. Słabe relacje, pozwalające budować pomostowy kapitał społeczny, wymagają mniejszego i węższego otwierania się niż silne, niezbędne do wytworzenia wiążącego kapitału społecznego.

Ellison (2011), podsumowując badania wpływu Internetu na umiejętność formowania i utrzymywania kapitału społecznego, wyodrębniła trzy grupy rezultatów: (1) korzystanie z Internetu zmniejsza wielkość kapitału społecznego; (2) Internet umożliwia tworzenie nowego kapitału społecznego; (3) Internet pomaga wzmacniać relacje *offline* i uzupełnia rozwój kapitału społecznego. Informacje o możli-

wym negatywnym wpływie Internetu na interakcje i zachowania społeczne pojawiły się na początku XXI wieku, między innymi dzięki artykułowi Normana Nie (2001), który przewidywał, że komunikacja zdalna będzie w przyszłości zastępować komunikację bezpośrednią zamiast ją uzupełniać, a to może doprowadzić do osłabienia więzi społecznych i spadku kapitału społecznego. Wyniki jego badania wskazywały na fakt, że internauci spędzają mniej czasu ze swoimi bliskimi niż osoby niekorzystające z Internetu. Bargh i McKenna (2004) zauważyli jednak, że to nie Internet jest narzędziem tak zajmującym czas badanych, ale tak zwane media tradycyjne, a zwłaszcza czasopisma i telewizja. Większość późniejszych badań wykazała istnienie pozytywnej korelacji pomiędzy wykorzystaniem Internetu i rozwojem kapitału społecznego. Przykładowo Donath i boyd (2004) wskazały na portale społecznościowe, jako doskonałe narzędzie do łatwego i wydajnego (w sensie ekonomicznym) tworzenia i zarządzania siecią słabych połączeń. Inne badania (m.in. Ellison, Steinfield i Lampe, 2007; Ellison, Steinfield i Lampe, 2008; Steinfield, DiMicco, Ellison i in., 2009; Burke, Marlow i Lento 2010) wykazały wyraźne zależności pomiędzy intensywnym korzystaniem z Facebooka i innych sieci społecznościowych, a wysokim poziomem kapitału społecznego pomostowego i wiążącego. Według niedawnego badania Ellison (2011) aktywnością, która wpływa pozytywnie na wzrost kapitału społecznego, jest poszukiwanie i dzielenie się informacjami, zwłaszcza dotyczącymi osób związanych z jakiegoś rodzaju relacjami w rzeczywistości *offline*.

Informacje opublikowane na osobistym profilu w serwisie społecznościowym sprzyjają nawiązywaniu nowych kontaktów (Ellison, 2010). Przykładowo, jeśli student uczelni odnajdzie na portalu społecznościowym profil kolegi z roku, którego nie znał osobiście, to dzięki publicznej widoczności jego profilu dowie się o wspólnych zainteresowaniach. Dzięki temu będzie mógł łatwiej nawiązać pierwszy kontakt i w przyszłości skorzystać z tej znajomości. Im więcej informacji znajdzie się na profilu, tym większe prawdopodobieństwo skutecznej identyfikacji ciekawego tematu do rozpoczęcia dyskusji. Przeglądanie informacji profilowych spełnia ważną rolę w procesie tworzenia spójnych obrazów innych osób, osadzania ich w odpowiednim kontekście, nadawania sensu (ang. *people sense-making*). DiMicco, Geyer, Millen i inni (2009) zaproponowali taki wniosek, badając użytkowników aplikacji intranetowej, zawierającej między innymi informacje o pracownikach organizacji – oprogramowania klasy ERP ze zintegrowanymi funkcjami społecznościowymi.

Ważny czynnik poprzedzający powstawanie kapitału społecznego – zaufanie – jest wyższy, gdy operatorzy sieci społecznościowej wymagają podawania praw-

dziwego imienia i nazwiska (Dwyer, Hiltz i Passerini, 2007). Rośnie on również wraz z większą ilością informacji zamieszczanych na profilu w sieci społecznościowej (Mazer, Murphy i Simonds, 2009). Ellison, Steinfield i Lampe (2007) wskazali na powiązanie pomiędzy wysoką liczbą wirtualnych znajomych a kompletnością podstawowych informacji profilowych w serwisach społecznościowych. Opierając się na teorii wspólnych cech (ang. *common grounds*) Clarka i Brennan (1991), badacze wyjaśnili korelację poprzez możliwość natychmiastowego odnalezienia wspólnych płaszczyzn porozumienia. Publiczna widoczność informacji profilowych, sieci kontaktów czy aktywności na portalu społecznościowym są zatem czynnikami, które sprzyjają budowie kapitału społecznego.

Najnowsze badania biorą pod uwagę również dynamiczne aspekty korzystania z sieci społecznościowych – interakcje między użytkownikami. W badaniu dużej grupy użytkowników Facebooka z wykorzystaniem ankiety i data miningu ustalono, że aktywna, ukierunkowana komunikacja z innymi użytkownikami sprzyja rozwijaniu wiążącego kapitału społecznego. Ma ona również pozytywny wpływ na samopoczucie użytkowników serwisu. Zmiany własnego statusu, zamieszczanie wiadomości na *ścianie* znajomego, komentowanie i ocenianie wpisów występuje w korelacji z wysokim poziomem samooceny, satysfakcji z życia oraz niskim poziomem postrzeganej samotności. W przypadku użytkowników serwisów społecznościowych, którzy jedynie konsumują treści zamieszczone przez inne osoby i nie angażują się w komunikację, kapitał społeczny nie wzrastał, podnosił się natomiast poziom odczuwanej samotności (Burke, Marlow i Lento, 2010).

Czerpanie zysków z kapitału społecznego w sieci społecznościowej wymaga od użytkownika ujawnienia pewnej liczby informacji osobistych, rezygnacji z części prywatności. Zachowania związane z jej ochroną ograniczają zatem potencjalny kapitał społeczny. Restrykcyjne kryteria przyjmowania nowych znajomych mogą uniemożliwić rozwój pomostowego kapitału społecznego związanego z siecią słabych relacji. Niewielka liczba interakcji ze znajomymi może natomiast ograniczyć możliwość skorzystania z dobrodziejstw wiążącego kapitału społecznego.

Związek pomiędzy prywatnością *online* a kapitałem społecznym, mimo swojej złożoności, rzadko pojawia się jako główny temat badań. Ellison, Vitak, Steinfield i inni (2011) opisali zależności pomiędzy sposobami kontroli osobistych informacji w Sieci, a postrzeganym poziomem kapitału społecznego. Badanie przeprowadzono na blisko trzystu studentach korzystających z Facebooka. Określono proste wyznaczniki zachowań chroniących prywatności *online* opierające się na strategii *budowania płotów* – dodawania znajomych (ang. *friending behaviour*) oraz dosto-

sowaniu ustawień prywatności (zob. sekcję *3.2. Think before you post – strategie samodzielnej ochrony użytkowników*).

Badacze założyli, że wykorzystanie zaawansowanych narzędzi ochrony prywatności, takich jak ograniczanie dostępu dla wybranych znajomych lub grup znajomych, może prowadzić do pełniejszej wymiany informacji, co w konsekwencji może skutkować rozwojem kapitału społecznego. Wyniki badania pozwoliły na podtrzymanie tej hipotezy – studenci, którzy zgłaszali wykorzystanie zaawansowanych ustawień prywatności, mieli wyższe poziomy postrzeganego wiążącego i pomostowego kapitału społecznego. Jeszcze wyraźniejszą korelację zaobserwowano pomiędzy liczbą znajomych a postrzeganym kapitałem społecznym. Im więcej znajomych w serwisie społecznościowym miał badany, tym wyższy zgłaszał poziom obu form kapitału społecznego. Zależność ta była prawdziwa zarówno dla ogólnej liczby osób dodanych do sieci kontaktów, jak i dla liczby osób, które są znajomymi również w rzeczywistości. Próba włączenia do badania trzeciego rodzaju strategii chroniącej prywatność, czyli zwyczajów publikowania (ang. *disclosure habits*), została odrzucona ze względu na trudności w stworzeniu odpowiedniego narzędzia pomiaru zachowań badanych. Pytania zadane użytkownikom dotyczyły ograniczonego kontekstu (dzielenia się swoimi pozytywnymi i negatywnymi odczuciami za pomocą aktualizacji statusu), podczas gdy publikowanie informacji i interakcja z innymi użytkownikami może się odbywać na wiele innych sposobów. Poza publikowaniem własnych aktualizacji, użytkownicy mogą między innymi *lubić* i komentować aktualizacje innych osób, zamieszczać i oznaczać zdjęcia, zamieszczać hiperłącza do innych stron internetowych, dyskutować na forach zintegrowanych z serwisem, korzystać z aplikacji, grać w gry wieloosobowe itd.

Według autorów wyniki badania podpierają hipotezę, że postawy oraz działania użytkowników serwisów społecznościowych związane z ochroną prywatności pozostają w pozytywnej korelacji z rozwojem kapitału społecznego. Przykładowo, jeśli użytkownik ma dużą liczbę internetowych znajomych, z dużym prawdopodobieństwem są wśród nich osoby z różnych sfer (zawodowa, prywatna, rodzinna itp.), wymaga on łatwych w użyciu narzędzi do skutecznego kontrolowania dostępu. Dzięki temu jego publiczność przestaje być *niejednorodna*. Świadomość, że komunikat dotrze wyłącznie do właściwych adresatów, pozwala na większą otwartość i szczerość, skutkując rozwojem wiążącego kapitału społecznego. I odwrotnie, osoba korzystająca z zaawansowanych ustawień prywatności może pozwolić sobie na dodawanie do znajomych bardziej przypadkowych osób i tym samym pełniej korzystać z sieci słabych połączeń tworzących pomostowy kapitał społeczny.

Jeżeli serwis społecznościowy nie umożliwia tworzenia list znajomych i ograniczania dostępu do informacji osobistych lub użytkownicy z różnych powodów z nich nie korzystają (niewiedza, skomplikowanie narzędzia), to użytkownicy będą chronili swoją prywatność, używając jednej z dwóch pozostałych strategii ochronnych: stosowanie rygorystycznych kryteriów akceptowania znajomych (ang. *limited friending*) lub zamykanie się, ograniczanie liczby i istotności publikowanych informacji (ang. *undersharing*). Obie metody wiążą się z utratą przynajmniej części potencjalnych zysków, które może przynieść korzystanie z portalu społecznościowego, w tym ograniczenie rozwoju kapitału społecznego.

Dodatkową rolę spełnia w tym procesie przejrzystość zasad dotyczących prywatności w serwisie społecznościowym, jak również stopień świadomości użytkowników w kwestii zagrożeń prywatności i możliwości kontroli informacji osobistych. Użytkownik musi mieć możliwość wyboru, co i z kim chce dzielić, a także pewność, że jego kontrola jest efektywna, aby osiągnąć maksimum korzyści z aktywności na mediach społecznych, jednocześnie minimalizując możliwości naruszenia prywatności, wynikające z niewłaściwego rozprzestrzeniania opublikowanych informacji.

3. OCHRONA PRYWATNOŚCI W INTERNECIE

Prywatność może być chroniona w Internecie poprzez trzy główne mechanizmy: regulacje prawne, samodzielną ochronę użytkowników oraz rynkową samoregulację.

3.1. Prawo

Współcześnie w większości społeczeństw prywatność jest chroniona przez prawo, choć zakres jej ochrony jest różny w różnych państwach. W wielu gwarantuje je konstytucja. Również w Konstytucji Rzeczpospolitej Polskiej znalazł się artykuł dotyczący prywatności. Wyjątkiem od tej reguły są Stany Zjednoczone, których konstytucja nie ustanawia bezpośredniej ochrony prywatności, a jedynie powiązane prawa w postaci kolejnych poprawek do konstytucji. Gwarantują one między innymi ochronę osobistych przekonań, nietykalność osobistą, ochronę własności prywatnej w tym ograniczenie możliwości przeszukania. USA przyjęły z czasem pakiet kilku ustaw gwarantujących prywatność informacji zdrowotnej i prywatność osób niepełnoletnich, które jednak są krytykowane ze względu na słabą skuteczność (Debatin, 2011).

Zasadniczy problem z zastosowaniem dotychczasowego porządku prawnego w Internecie polega na trudności w ustaleniu, co jest prywatne, a co publiczne, oraz w zdefiniowaniu, co oznacza fakt publikacji. Warren i Braindeis (1890), którzy jako pierwsi sformułowali prawo do prywatności, piszą: „Jednostka zrzeka się prawa do prywatności wraz z publikacją faktów". W tym stwierdzeniu ukryte jest założenie, że akt publikacji poprzedzony jest wolą upublicznienia informacji, które do tej pory były prywatne. Kiedy publikowanie było czasochłonne i kosztowne, takie ujęcie miało sens, gdyż osoba, która podjęła wysiłek publikacji, z pewnością chcia-

łaby rozpowszechnić informacje dla jak najszerszego grona odbiorców. Obecnie, w dobie powszechnie dostępnego Internetu i wszechobecnych mediów społecznych, takie rozumowanie jest błędem. Shirky (2008, s. 79) uważa, że „w świecie, w którym publikowanie nie wymaga najmniejszego wysiłku, decyzja o publikacji nie jest czymś wyjątkowo doniosłym". W Internecie, a zwłaszcza w mediach społecznych, prawdziwe jest twierdzenie odwrotne – akt publikowania jest łatwy, zaś ograniczenie przepływu informacji wymaga wysiłku. Legislatorzy muszą rozumieć, że w kontekście cyfrowych mediów społecznych nie sprawdza się dychotomia publiczne-prywatne. Użytkownicy Facebooka korzystają z niego właśnie po to, aby publikować, dzielić się faktami ze swojego życia prywatnego, zainteresowaniami itp., ale w większości nie chcą, aby wszystkie te dane były całkowicie publiczne. Bez uwzględnienia sposobu, w jaki ludzie korzystają z technologii, nie da się stworzyć skutecznego prawa chroniącego dobra osobiste w tym obszarze (Grimmelmann, 2009).

Grimmelmann (2009) proponuje szereg rozwiązań prawnych, które według niego mogą sprawdzić się w dynamicznym środowisku cyfrowych mediów społecznych. Pierwsze z nich, *odpowiedzialność za publiczne ujawnienie prywatnych informacji*, powstało w oparciu o sieciową teorię prywatności Strahilevitza (2005). Grimmelmann proponuje, aby prawo uwzględniało wypowiedziane intencje i oczekiwania dotyczące prywatności osób, które zamieszczają informacje w Internecie, a które później rozprzestrzeniają się niezgodnie z ich wolą. Gdy powierzamy informację prywatną kilku osobom, możemy oczekiwać, że uszanują naszą prywatność i nie opowiedzą naszej historii innym. Nasza informacja nie jest już trzymana w sekrecie, ale dopóki nie jest znana osobom spoza wąskiego kręgu powierników, pozostaje *efektywnie prywatna*. W świecie cyfrowym tego rodzaju relacje i oczekiwania również istnieją. Co więcej, o ile w rzeczywistości struktura sieci społecznej i zasady rozprzestrzeniania informacji prywatnej są trudne do opisania i zweryfikowania (np. przez sąd), tak w mediach społecznych sieć kontaktów i ustawienia prywatności profilu czy pojedynczej aktualizacji są wyrażone *explicite*. Dzięki temu można poznać intencje osoby zamieszczającej informacje, jej faktyczny zasięg przed dalszym, nieuprawnionym rozpowszechnieniem. Prawo powinno również regulować dostęp organów ścigania do danych użytkowników, które nie są zamieszczone publicznie. Jeżeli użytkownik zamieści w serwisie społecznościowym informację widoczną tylko dla wąskiej grupy znajomych, policja powinna być zobligowana do uzyskania zgody sądu na otrzymanie do niej dostępu od administratora serwisu, analogicznie jak przy przeszukania mieszkania.

Kolejnym problemem, które prawo mogłoby rozwiązać, jest wykorzystanie danych o użytkownikach do celów komercyjnych, np. personalizacji reklam. Grimmelmann (2009) uważa, że serwisy internetowe nie mają prawa do domniemania zgody użytkownika, a więc powinny uzyskiwać świadomą zgodę, bez sugerowania zalecanych ustawień. Użytkownicy powinni też mieć możliwość łatwej rezygnacji z korzystania z usług, a także permanentnego usunięcia własnych danych i treści zamieszczonych w mediach społecznych. Negatywnym przykładem może być tutaj Facebook – do 2008 roku usunięcie konta z tego serwisu było praktycznie niemożliwe. Użytkownik mógł je tylko *dezaktywować*. Dezaktywacja powodowała, że jego profil i wszystkie aktywności stawały się niewidoczne, ale dane w dalszym ciągu pozostawały na serwerze. Blogger Steven Mansour, który chciał usunąć własne konto z serwisu, otrzymał zalecenie ręcznego usunięcia wszystkich aktywności – kontaktów, wiadomości, aktualizacji statusu, fotografii itp., razem ponad 2500 danych (Mansour, 2007). Facebook gromadzi również dane na temat osób, które nie mają założonego konta w portalu – np. poprzez oznaczenie ich na zdjęciach przez zarejestrowane osoby (Grimmelmann, 2009).

Kontrowersje związane ze zmianami w architekturze serwisów i wprowadzaniu nowych funkcji, takich jak *News Feed* w portalu Facebook (zob. sekcję *2.3. Zmiana trybu dostępu do informacji*), wskazują kolejny kierunek zmian w prawie, który mógłby przynieść pozytywny efekt dla ochrony prywatności. Podmioty przetwarzające dane osobowe mają w niektórych krajach (w tym w Polsce) obowiązek uzyskania zgody od osób, których te dane dotyczą. Są również zobligowane do poinformowania o zakresie i celu gromadzenia oraz przetwarzania tych danych. W przypadku zmiany zakresu lub celu przetwarzania, podmiot ma obowiązek uzyskać ponowną zgodę. Grimmelmann postuluje, aby podobnie interpretować wprowadzenie poważnych zmian w serwisach internetowych. Jeżeli serwis społecznościowy planuje wprowadzić nową funkcję, która w istotny sposób wpłynie na sposób wyświetlania danych prywatnych użytkowników, to może tym samym spowodować naruszenie ich prywatności. W związku z tym powinien odpowiednio wcześnie poinformować o niej użytkowników, wprowadzać zmiany stopniowo, z umożliwieniem wcześniejszego, dokładnego, bezpiecznego zapoznania się z nowymi możliwościami i zagrożeniami. Zmiany, które z dużym prawdopodobieństwem uderzą w prywatność, powinny być oferowane dobrowolnie, poprzez umożliwienie użytkownikom podjęcia decyzji. Priorytetem powinno być oferowanie usługi, której konsekwencje są przewidywalne, a nie mylące dla użytkownika.

Podobne wnioski wyciągnęli administratorzy serwisu Facebook i zastosowali je przy wprowadzaniu *osi czasu*. To nowy wygląd profilu użytkownika, w którym

niemal wszystkie dotychczasowe aktualizacje widoczne są chronologicznie na jednej stronie. Pozwala ona na szybsze przeglądanie i nawigowanie po historii aktywności użytkownika czy łatwe przejście do aktualizacji z określonego czasu. Zmiana, choć poważna i krytykowana przez wielu użytkowników, nie wzbudziła aż takich kontrowersji jak *News Feed*. Po pierwsze, zapowiedziano ją kilka miesięcy wcześniej, a po drugie użytkownicy mogli skorzystać z *jazdy próbnej*. Facebook umożliwił tymczasowe włączenie *osi czasu*, podczas którego użytkownik mógł zapoznać się z nową funkcją i dostosować widoczność i wyróżnienie poszczególnych elementów. W tym czasie profil użytkownika widoczny dla innych osób wyglądał jak dawniej. Po personalizacji *osi* można było zatwierdzić zmiany i opublikować nowy wygląd profilu. Gdy nową funkcję uruchomiono dla wszystkich profili, każdy użytkownik Facebooka miał 7 dni na dostosowanie własnej *osi czasu* przed jej publikacją (Lessin, 2011; McDonald, 2011).

Prawo może rozwiązać część, ale nie wszystkie problemy związane z ochroną prywatności w Internecie. Głównymi winowajcami naruszeń prywatności związanych z Internetem i mediami społecznymi nie są ich twórcy, ale użytkownicy. Serwis społecznościowy jest narzędziem pozwalającym wyrażać siebie, tworzyć i rozwijać relacje społeczne i jak każde inne narzędzie może wyrządzić krzywdę, jeśli jest niewłaściwie użyte. Prawo może wyznaczyć bezpieczne standardy konstrukcji narzędzia i nakazać jego twórcom czytelne informowanie konsumentów o możliwych zagrożeniach związanych z jego użytkowaniem, nie może natomiast zmusić obywateli do korzystania z narzędzia w jedyny właściwy sposób. Prawo działa głównie *post hoc*, nie rozwiązuje natomiast problemów z oceną *ex ante* użytkowników (Grimmelmann, 2009).

3.1.1. Polityki prywatności

Niektóre propozycje zmian prawnych proponują wprowadzenie obowiązkowej publikacji polityki prywatności przez podmioty gromadzące i przetwarzające prywatne informacje użytkowników. Polityka prywatności to oświadczenie lub dokument prawny stworzony i opublikowany przez władze podmiotu, który gromadzi, przechowuje i przetwarza dane osobowe. Opisuje się w nim praktyki związane z administracją danymi osobowymi. W Sieci polityka prywatności przybiera najczęściej formę specjalnej podstrony serwisu internetowego.

Koncept internetowej polityki prywatności opiera się na założeniu, że firmy stosują się do sformułowanych przez siebie zasad zarządzania danymi prywatnymi, a odbiorcy usług – użytkownicy serwisów internetowych – dokładnie czytają

i rozumieją jej postanowienia oraz implikacje i podejmują decyzję o skorzystaniu z usługi oraz powierzeniu swoich danych, bądź rezygnują z tej możliwości. Poinformowani obywatele powinni podejmować wybory zgodne ze swoimi preferencjami. W przypadku niespełnienia postanowień polityku prywatności przez firmę administrującą ich danymi, można traktować ją jako umowę między klientem a usługodawcą, a więc podstawę do jakichkolwiek roszczeń (Ciocchetti, 2007).

Niestety teoria nie zawsze przekłada się na praktykę. Takie rozwiązanie ma kilka podstawowych wad ograniczających jego skuteczność: (1) skomplikowany, prawniczy język polityki prywatności zniechęca użytkowników do jej przeczytania, a nawet jeśli to zrobią, niekoniecznie zrozumieją znaczenie jej postanowień; (2) postanowienia polityk prywatności są często ogólnikowe i zwykle nie chronią prywatnych danych użytkownika, ani nie ograniczają w istotny sposób możliwości przekazania danych podmiotom zewnętrznym; (3) prawo rzadko wymaga włączenia polityki prywatności do regulaminu serwisu internetowego, przez co firmy często nie widzą potrzeby, aby formułować jej zasady, publikować i zwiększać wśród użytkowników świadomość istnienia takiego dokumentu (Ciocchetti, 2007).

Świadomość istnienia polityk prywatności wśród użytkowników serwisów internetowych w ciągu ostatnich lat wyraźnie się zwiększyła. W ankiecie z 2002 roku przeprowadzonej wśród amerykańskich internautów jedynie 3% respondentów przyznało, że zwykle uważnie czyta polityki prywatności stron, które odwiedza (Harris Interactive, 2002). W 2007 roku w podobnym badaniu takie zdanie wyraziło 32% badanych (IBOPE, 2007). Tak samo odpowiedziało 58% Europejczyków korzystających z Internetu w badaniu przeprowadzonym przez Komisję Europejską w 2011 roku. Dodatkowo 25% stwierdziło, że zapoznaje się z zasadami polityki prywatności przynajmniej okazjonalnie. Istotnym czynnikiem socjodemograficznym wpływającym na zwiększoną częstość udzielania pozytywnej odpowiedzi jest wiek – w badaniu Eurobarometru młodsi badani (15–24) wyraźnie częściej niż starsi (55+) uważali, że zwykle są wystarczająco dobrze poinformowani po przeczytaniu polityki prywatności (odpowiednio 54 i 37%). Zaobserwowano również korelację pomiędzy wyższym poziomem zgody z powyższym stwierdzeniem, a zaufaniem do portali internetowych oraz firm telekomunikacyjnych świadczących usługi internetowe. Wśród 21% respondentów, którzy nie czytają polityk prywatności, czterech na dziesięciu stwierdziło, że sam fakt, że administratorzy strony internetowej opublikowali taki dokument, jest wystarczającą formą ochrony przed nieprawidłowym użyciem ich informacji osobistych. W sumie połowa badanych, która nie czyta polityk prywatności, jest zdania, że nie mają one zna-

czenia. Połowa tej grupy uważa, że w przypadku narażenia ich prywatności, może liczyć na prawodawstwo, a druga, że polityka prywatności nie musi być realizowana w praktyce przez administratorów strony internetowej.

Wzrost liczby internautów czytających polityki prywatności nie idzie w parze z wysokim poziomem zrozumienia zawartych w nich sformułowań. Czterech na dziesięciu respondentów Eurobarometru, którzy czytają polityki prywatności stron internetowych uważa, że nie jest w stanie zrozumieć wszystkich postanowień opisanych w dokumencie. Znajomość polityki prywatności nie ma też wielkiego wpływu na decyzje internautów: co trzeci respondent w żaden sposób nie ogranicza ujawniania swoich danych prywatnych po jej lekturze. Podobna liczba przyznała, że co najmniej raz zrezygnowała ze skorzystania z usług z powodu niewystarczającego zapewnienia o ochronie ich danych osobowych (Komisja Europejska, 2011).

Grimmelmann (2009) uważa, że polityki prywatności serwisów społecznościowych to „piękna błahostka", nic nieznaczący dokument, który nie jest czytany, nie jest zrozumiany, a przede wszystkim nie chroni w żaden sposób prywatnych danych. Powodem, dla którego internauci nie czytają polityk, jest „boleśnie wysoki stosunek sygnału do szumu". Pod wieloma ogólnikowymi i standardowymi zwrotami administratorzy stron internetowych maskują zaskakujące, niekorzystne dla użytkowników postanowienia. Przykładem niech będzie polityka prywatności Facebooka. Ewoluowała ona w czasie, zmieniając również język z prawniczego żargonu na bardziej zrozumiały dla przeciętnej osoby. To jednak w dalszym ciągu blisko 10 stron druku w języku angielskim. Polska edycja Facebooka, mimo zaleceń Generalnego Inspektora Ochrony Danych Osobowych (Zespół Rzecznika Prasowego Biura GIODO, 2012), nie oferuje pełnej wersji polityki prywatności, a jedynie trochę skrócony i w żaden sposób nieobligujący prawnie dokument o nazwie „Zasady wykorzystania danych" (Facebook, 2012).

Mimo że Facebook ma bardzo precyzyjne narzędzia kontroli dostępu do danych użytkowników i pozwala na ograniczenie wyświetlania całego profilu w swojej witrynie, to uważa takie dane jak imię i nazwisko, główne zdjęcie profilowe, identyfikator użytkownika za *zawsze publiczne*. Dane, które są *publiczne*, mogą być pobierane m.in. przez wyszukiwarki internetowe, twórców aplikacji i stron internetowych korzystających z platformy programistycznej Facebooka. Pośrednio są więc dostępne potencjalnie dla każdej osoby korzystającej z Sieci WWW, nawet jeżeli nie są widoczne bezpośrednio w serwisie. Dodatkowo fakt indeksacji przez wyszukiwarki internetowe jest gwarancją wieloletniej archiwizacji tych danych.

Niektórzy operatorzy stron internetowych starają się za pomocą polityki prywatności zwiększyć świadomość użytkowników o możliwych negatywnych skutkach udostępniania prywatnych danych w Sieci. W badaniu Eurobarometru połowa użytkowników mediów społecznych twierdzi, że dołączając do nich, została wystarczająco poinformowana o możliwych negatywnych konsekwencjach ich aktywności w tych serwisach – dokładnie 49%. Niemal tyle samo respondentów (46%) nigdy nie spotkało się z podobną praktyką. Facebook informuje użytkowników o ryzyku nadmiernego i nieuprawnionego wykorzystania danych prywatnych w swojej polityce prywatności (ale nie w polskojęzycznej wersji serwisu): „Nie możemy zagwarantować, że treści, które zamieszczasz w Serwisie, będą dostępne tylko autoryzowanym osobom, ani zapewnić, że nie staną się publicznie dostępne" (Facebook, 2009, tłum. własne). Facebook nie bierze tym samym odpowiedzialności za naruszenia prywatności związane z użyciem danych prywatnych przez innych użytkowników serwisu, ale także twórców aplikacji wykorzystujących architekturę Facebooka (Grimmelmann, 2009).

W Stanach Zjednoczonych i w Polsce publikacja polityki prywatności nie jest generalnie wymagana, choć bywają wyjątki od tej zasady: władze Kalifornii wymagają publikacji tego dokumentu przez administratorów stron internetowych, którzy przetwarzają dane finansowe lub zdrowotne obywateli tego stanu (Ciocchetti, 2007). Ponadto Federalna Komisja Handlu Stanów Zjednoczonych udostępnia wytyczne, w jaki sposób firmy powinny chronić dane osobowe, które gromadzą i wykorzystują w dokumencie „Fair Information Practice Principles" (Federal Trade Commission, 2007). Legislatura Unii Europejskiej w dyrektywie 95/46/EC dotyczącej ochrony danych osobowych (Dz.U. L 281 z 23.11.1995) nie wymaga formułowania polityki prywatności, a jedynie wyrażenia zgody na przetwarzanie danych przez osobę, której te dane dotyczą. Polska implementacja dyrektywy, Ustawa o Ochronie Danych Osobowych (Dz.U. 1997 nr 133 poz. 883 z poźn. zm.), jest nieco bardziej restrykcyjna. Poza koniecznością uzyskania zgody na przetwarzanie danych osobowych ustawa wymaga podania przez administratora danych w celu ich gromadzenia i przetwarzania (w tym możliwości przekazania danych podmiotom zewnętrznym) oraz poinformowania o prawie do zażądania dostępu do danych oraz ich poprawienia.

Unijna Komisarz ds. Sprawiedliwości, Viviane Reding, zainicjowała w 2010 roku rewizję istniejącej dyrektywy. Unia Europejska planuje zastąpić ją rozporządzeniem, a więc prawem obowiązującym bezpośrednio na terenie państw członkowskich UE, a nie tylko pośrednio, zgodnie z obowiązującą dyrektywą. Obecnie nie są znane szczegóły rozporządzenia, a jedynie wstępne założenia. Przede wszyst-

kim planowane jest dostosowanie go do realiów współczesnego świata cyfrowego. Jednym z nich jest zwiększenie stopnia poinformowania obywateli o prawach kontroli ich danych osobistych w Internecie, w tym: łatwym dostępie do swoich danych osobowych, możliwości przeniesienia danych do innego serwisu, a także trwałego usunięcia danych (tzw. *prawo do bycia zapomnianym*). Nowe prawo ma obowiązywać wszystkie podmioty prowadzące działalność na terenie Unii Europejskiej, niezależnie od ich prawnej siedziby (EUROPA. Press releases RAPID, 2010).

3.2. *Think before you post* – strategie samodzielnej ochrony użytkowników

Najlepszą ochroną prywatności *online* jednostki jest oczywiście samodzielne zabieganie o kontrolę nad przepływem informacji prywatnych. Pasywne strategie ochrony prywatności to takie, w którym jednostka zdaje się na czynniki zewnętrzne takie jak prawo, inne osoby albo technologie chroniące prywatność. Taka ochrona jest poza bezpośrednią kontrolą jednostki lub jest pod jej kontrolą tylko przez ograniczony czas (Yao, 2011). Do pasywnych strategii zalicza się: korzystanie z oprogramowania antywirusowego, antyspamowego, tworzenie bezpiecznych haseł, ochrona dostępu do nich itp. Pasywnym sposobem jest również ograniczenie ujawniania danych prywatnych, a nawet całkowita rezygnacja z ujawniania ich w Internecie. To rozwiązanie jest najprostsze i pozornie najskuteczniejsze – jeśli nasze dane prywatne nie pojawią się w Internecie, to nie musimy martwić się o ich zabezpieczenie. Ta strategia ma dwie zasadnicze wady. Po pierwsze, wynika z niej konieczność rezygnacji z przynajmniej części możliwości, jakie oferuje Internet. Dla młodych *digital natives* całkowita zaprzestanie korzystania z serwisów społecznościowych jest jednak społecznie nieakceptowalne (boyd, 2010b). Po drugie, w dalszym ciągu możemy być narażeni na naruszenia prywatności, gdyż poza naszą kontrolą pozostają informacje na nasz temat zamieszczone w Internecie przez inne osoby. Paradoksalnie obecność w serwisie społecznościowym zmniejsza ryzyko wystąpienia takiej sytuacji. Utrudnia bowiem utworzenie fikcyjnego profilu naszej osoby, założonego przez kogoś innego – internetowej kradzieży tożsamości.

Kolejne pasywne sposoby ochrony prywatności w Sieci to strategie rozszerzania sieci kontaktów oraz regulacji kontroli dostępu. Te dwie strategie nazywane są przez niektórych badaczy *budowaniem płotów* (Debatin, 2011). Wiele elementów tych strategii zostało opisane już w pracy. Budowanie płotów funkcjonuje zwłaszcza w serwisach społecznościowych, gdzie decydując się (bądź nie) na przyjęcie osoby do grupy znajomych, oraz odpowiednio dostosowując ustawie-

nia prywatności, można kontrolować widoczność elementów własnego profilu, aktualizacji statusu itp. Najczęstszym sposobem realizacji tej strategii jest ograniczanie widoczności zamieszczanych treści do kręgu znajomych w serwisach społecznościowych. Jednak nawet ta prosta strategia nie jest szczególnie rozpowszechniona, do jej stosowania przyznaje się, wedle różnych badań, od 30% do 50% użytkowników portali społecznościowych (Ellison, Steinfield i Lampe, 2007; Debatin, Lovejoy, Horn i in., 2009). Częsty jest brak rozróżnienia między najbliższymi przyjaciółmi i pobieżnymi znajomymi (zob. sekcję *2.4.1. Niejednorodna publiczność*), a także dodawanie do sieci kontaktów osób ledwie znanych czy wręcz obcych. Sophos opublikował raport z eksperymentu przeprowadzonego w 2007 roku, w którym stworzono 2 fikcyjne profile i wysłano po 100 zaproszeń do kręgu znajomych do losowej próby osób. Aż 43% zaproszeń zostało przyjętych. Sophos przeanalizował także dane, do których uzyskano dostęp. Okazało się, że niemal wszystkie osoby akceptujące zaproszenia udostępniły w ten sposób swój adres e-mail oraz datę urodzenia, a blisko połowa nazwę szkoły, uczelni lub miejsca pracy i miasta, w którym żyją. Blisko 15% osób udostępniło w ten sposób swój pełny adres, a 5% numer telefonu komórkowego (Ducklin, 2009).

Poprzez stosowanie pasywnych strategii ochrony ograniczamy możliwość wywarcia wrażenia na potencjalnie interesujących osobach (Krämer, Haferkamp 2011), a także ograniczamy rozwój słabych więzi społecznych, choć możemy wzmocnić silne (Ellison, Vitak, Steinfield i in., 2011). Możliwe jest również ponowne udostępnienie informacji, które w intencji pierwszego twórcy, zastrzeżone były tylko dla małej grupy znajomych.

Strategia budowania płotów jest przez niektórych badaczy krytykowana ze względu na ograniczoną skuteczność, jako strategia ochrony prywatności (Stutzman i Kramer-Duffield, 2010). Po pierwsze – opiera się ona na technologii opracowanej przez twórców stron internetowych. Programiści popełniają błędy i mogą pozostawić luki w zabezpieczeniach, które narażone są na wykorzystanie przez osoby o wysokich umiejętnościach technicznych. Drugi problem wymaga szerszego wyjaśnienia. Zagadnienia związane z zagrożeniem prywatności w sieciach społecznościowych można przedstawić na dwóch osiach – widocznej dla użytkownika osi poziomej i pionowej – niewidocznej. Na osi poziomej znajdują się interakcje z innymi użytkownikami, podczas których wymieniają się oni informacjami przez zamieszczenie ich na profilu osobistym, czy procesy komunikacyjne takie jak wymiana wiadomości, dyskusje itp. Oś pionowa to systematyczne zbieranie, łączenie i przetwarzanie danych przez operatorów (np. sieci społecznościowej, dostępu internetowych itp.). Choć wielu użytkowników nie zdaje so-

bie z tego sprawy, widoczna oś pozioma jest tylko wierzchołkiem góry lodowej. Liczba i waga możliwych naruszeń prywatności związanych z przetwarzaniem danych przez operatorów w celach komercyjnych czy kryminalnych, jest znacznie większa. Sytuację pogłębiają również działania samych operatorów, od dawna krytykowane za niejasne polityki prywatności i mylące ustawienia prywatności. Dane, które posiadają operatorzy, są z oczywistych powodów o wiele bardziej wrażliwe i jest ich znacznie więcej, niż tych zamieszczanych publicznie przez użytkowników. Kwestie ich przetwarzania, a także udostępniania osobom trzecim, nie zawsze są jasno chronione przez prawo. Strategia budowania płotów funkcjonuje jedynie na osi poziomej, w interakcji między użytkownikami, nie mając najmniejszego wpływu na zagrożenia na osi pionowej – operatora i osób trzecich, którym informacje mogą zostać udostępnione. Niektórzy badacze twierdzą, że z tego powodu nie można jej nazwać prawdziwą strategią ochrony prywatności, gdyż stwarza fałszywe poczucie bezpieczeństwa prywatności informacyjnej.

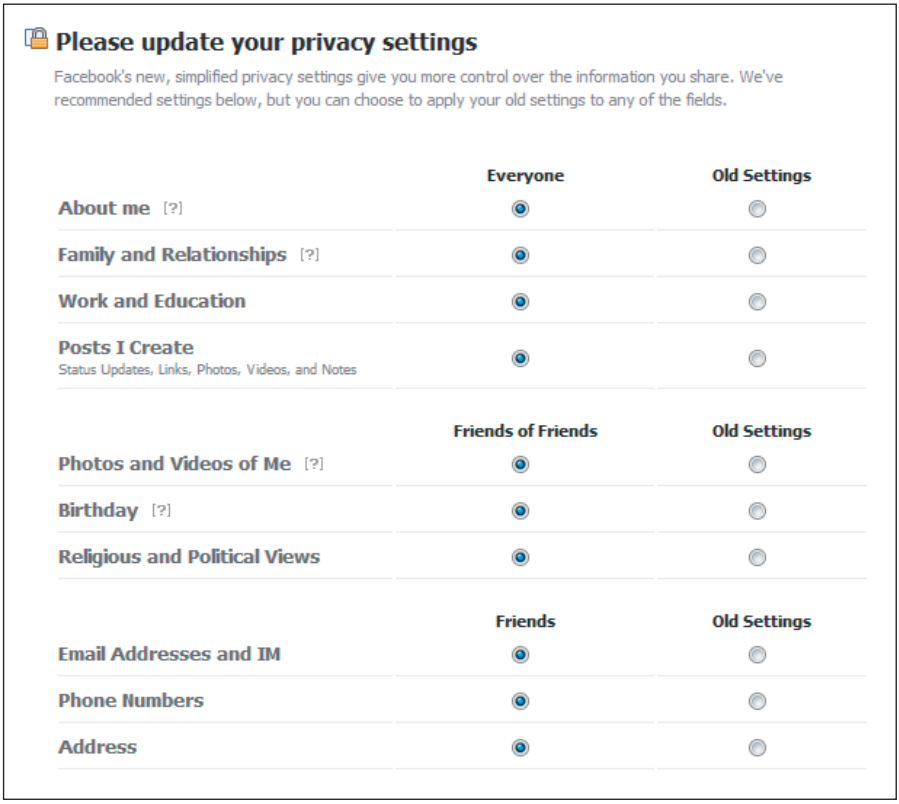
3.2.1. Ustawienia prywatności

Facebook był jednym z pierwszych portali społecznościowych, który umożliwił użytkownikom indywidualne dostosowanie ustawień prywatności profilu o bardzo dużej ziarnistości. Każdy element profilu, np. imię, nazwisko, wiek, data urodzin, numer telefonu, adres, zainteresowania itp. mógł otrzymać jeden z kilku stopni widoczności: wszyscy internauci, zarejestrowani użytkownicy serwisu Facebook, znajomi znajomych, znajomi oraz niewidoczny. Obecnie Facebook pozwala również na udostępnianie informacji dla dowolnej grupy użytkowników portalu, pojedynczej osoby, a także zablokowanie widoczności informacji dla grupy osób lub pojedynczej osoby.

Domyślne ustawienia dla nowo założonego profilu są jednak bardzo otwarte. Dodatkowo, w toku ewolucji ustawień prywatności Facebooka, każda zmiana architektury prywatności wiązała się ze zwiększeniem liczby informacji domyślnie dostępnych dla wszystkich. Aktualnie domyślne ustawienia prywatności umożliwiają całkowicie publiczną widoczność wszystkich danych o użytkowniku poza telefonem i adresem zamieszkania (domyślnie widoczne dla znajomych) oraz datą urodzin, poglądami politycznymi i wyznaniem (domyślnie widoczne dla znajomych znajomych) (McKeon, 2010).

W grudniu 2009 roku inżynierowie Facebooka zaprojektowali od nowa system zmiany ustawień widoczności wszystkich informacji profilowych oraz innych zamieszczonych przez użytkownika (aktualizacji statusu, fotografii itp.). Założyciel

i dyrektor wykonawczy Facebooka, Mark Zuckerberg, w liście otwartym do użytkowników tłumaczył, że nowy menedżer prywatności pozwala na znacznie łatwiejszą kontrolę nad udostępnianiem informacji osobistych i poprawia prywatność użytkowników (Zuckerberg, 2009). Każdy użytkownik po zalogowaniu się otrzymywał komunikat, w którym potwierdzał zrozumienie nowych zasad i przy każdym rodzaju zamieszczanych informacji mógł wybrać jedną z dwóch opcji widoczności: *dotychczasowe ustawienia* lub nowe *zalecane*. Domyślnie wszystkie opcje zaznaczone były nie jako *dotychczasowe ustawienia*, ale jako nowe *zalecane*, bardzo otwarte. Aby uzyskać dostęp do Facebooka, każdy użytkownik musiał zaakceptować zmiany i potwierdzić ustawienia prywatności.



Ryc.1. Zrzut ekranu z ustawień prywatności Facebooka po zmianach w 2009 roku
Źródło: boyd i Hargittai, 2010

Nie ma dostępnych danych świadczących o liczbie użytkowników, którzy zaakceptowali zmiany i nowe *zalecane* ustawienia bez ich uprzedniego przeczytania, jednak zmiany te były często komentowane i krytykowane w mediach. Głównym zarzutem postawionym Facebookowi była manipulacja i narzucanie użytkownikom zmiany ich spersonalizowanych ustawień prywatności (o sile domyślnych ustawień piszę szerzej w kolejnym podrozdziale). Organizacja pozarządowa stojąca na straży prywatności elektronicznej – The Electronic Privacy Information Center (EPIC) – złożyła m.in. z tego powodu skargę na Facebooka do Federalnej Komisji Handlu w USA (EPIC, 2010). Wykorzystanie ustawień prywatności w portalach społecznościowych przyciągnęło uwagę kilku badaczy (Ellison, Steinfield i Lampe, 2007; Stutzman i Kramer-Duffield 2010, Lewis, Kaufman, Christakis i in., 2008), którzy badali czynniki wpływające na ich zmianę, a przede wszystkim – na tworzenie profili całkowicie lub w dużym stopniu prywatnych, tzn. takich, w których informacje profilowe są wyświetlane jedynie znajomym lub nikomu. Lewis, Kaufman, Christakis i in. (2008) wyróżnili cztery zmienne, które wpływają na zwiększenie prawdopodobieństwa wykorzystania restrykcyjnych ustawień prywatności wśród studentów korzystających z Facebooka, gdy: (1) jego lub jej przyjaciele, a zwłaszcza współlokatorzy, również mają prywatne profile; (2) jest aktywnym użytkownikiem Facebooka; (3) jest kobietą; (4) słucha muzyki, która jest relatywnie popularna.

Ankieta przeprowadzona przez boyd i Hargittai (2010) w 2009 roku i powtórzona w 2010 roku wykazała interesujące trendy w wykorzystaniu Facebooka przez studentów pierwszego roku. Po pierwsze, odsetek osób posiadających konto w tym portalu wzrósł w ciągu roku z 87% do 90%. Wzrosła również aktywność zarejestrowanych osób: w 2009 roku częstym użytkownikiem określało się 76% studentów, a w rok później o 5 punktów procentowych więcej. Najwyraźniejszy wzrost widoczny był w odpowiedziach dotyczących częstotliwości zmiany ustawień prywatności: tylko 2% ze wszystkich badanych w 2010 roku nigdy nie edytowała tych ustawień (w 2009 było to 9%), 9% raz (28% w 2009), 39% dwa-trzy razy (28% w 2009), a 51% cztery i więcej razy (24% w 2009).

Hargittai i boyd (2010) wskazują na trzy czynniki, które mogą mieć wpływ na tę zmianę: (1) trwającą publiczną debatę na temat prywatności *online*; (2) kontrowersyjne zmiany w systemie ustawień prywatności Facebooka (opisane wcześniej w tym podrozdziale), a także (3) powiadomienia na Facebooku zachęcające użytkowników do edycji ustawień. Najbardziej aktywni użytkow-

nicy portalu społecznościowego byli jednocześnie osobami, które najczęściej korzystały z możliwości zmiany ustawień prywatności. Ta charakterystyczna zależność uprawdopodobnia tezę Petronio o konieczności harmonizowania dzielenia się treściami i ograniczenia dostępu do nich, inaczej mówiąc – regulacji pomiędzy otwarciem, a zamknięciem (Griffin, 2011). Im więcej prywatnych informacji jest publikowanych, tym większa zachodzi potrzeba ich kontroli. I przeciwnie, im większą postrzeganą kontrolę posiada użytkownik, tym bezpieczniej się czuje, korzystając z portalu, i chętniej dzieli się treściami.

W badaniu boyd i Hargittai (2010) studenci z wyższym postrzeganym poziomem umiejętności korzystania z komputerów i Internetu częściej korzystali z tej możliwości niż ci, którzy byli mniej pewni swoich umiejętności. Edycja ustawień prywatności była przy tym uznawana za łatwą czynność przez obie płcie (średnio 4,3 w 5-stopniowej skali Likerta, gdzie 5 to „bardzo łatwa"), chociaż kobiety raportowały niższy poziom pozostałych umiejętności korzystania z Internetu (np. zamieszczania materiałów wideo w Sieci, korzystania z systemów ocen i recenzji czy edycji stron wiki). Badaczki tłumaczą ten fakt wyższą dbałością kobiet o swoje dane prywatne, co może wynikać z dużej ilości programów edukacyjnych w Stanach Zjednoczonych, które mają na celu uświadomienie zagrożeń ze strony napastników internetowych. Badanie nie zawierało pytań o strach przed różnego rodzaju zagrożeniami, ale boyd i Hargittai argumentują, że to właśnie na strachu opiera się dbałość kobiet o swoją prywatność. To z kolei może ograniczać ich udział w tworzeniu i promowaniu treści w Internecie oraz autoprezentacji np. na profesjonalnych portalach społecznościowych takich jak LinkedIn czy GoldenLine. Skupianie się na jednowymiarowym zagrożeniu ze strony napastników pomija także inne korzyści wynikające z umiejętnego zarządzania swoją prywatnością w Internecie.

3.3. Rynkowa samoregulacja

Ostatnim z ujęć stosowanych przy ocenie rozwiązań wzmacniających stopień ochrony prawa do prywatności w Internecie jest wiara w regulującą siłę wolnego rynku. Opiera się ona na trzech założeniach wynikających z klasycznej ekonomii: (1) każdy internauta, jako osoba racjonalna, dba o swoje dobro, a więc jeżeli zależy mu na własnej prywatności, to będzie roztropnie dzielił się swoimi danymi prywatnymi; (2) jeżeli internauta uzna, że firma świadcząca usługi w Internecie nie zadba wystarczająco o powierzone przez niego dane prywatne, to z niej nie skorzysta – wybierze konkurencję lub zrezygnu-

je z usługi; (3) firmy świadczące usługi muszą dostosować się do wymagań swoich klientów, aby spełnić swoje biznesowe cele, a internauci będą mogli podjąć najlepszą decyzję (Grimmelmann, 2009).

Warto jednak zastanowić się, czy te założenia faktycznie są prawdziwe w Internecie. Wiele wskazuje na to, że nie. Po pierwsze, internauci zwykle nie mają pełnej świadomości tego, jak gromadzi i przetwarza się ich dane prywatne. Specyfika środowiska cyfrowego pozwala na łatwe gromadzenie i operowanie danymi takimi jak *logi* (rejestry zdarzeń systemu), np. historia dostępu do stron internetowych, historia wyszukiwania itp. W zasadzie każda czynność wykonywania w Internecie może być zarejestrowana. Takie zestawy danych są bardzo atrakcyjne np. dla marketerów, umożliwiając im tworzenie spersonalizowanych, a przez to skuteczniejszych reklam. Co więcej, całe zestawy identyfikowalnych danych są udostępniane dobrowolnie przez użytkowników portali społecznościowych, którzy często są zbyt leniwi lub brakuje im umiejętności, aby ograniczyć dostęp do nich za pomocą narzędzi udostępnionych przez administratorów portali (zob. sekcję *2.5. Paradoksy prywatności*).

Problemem jest również możliwość korzystania z konkurencyjnych usług. Rynek usług internetowych jest opanowany w dużej części przez dwóch graczy – Google i Facebooka. Jeszcze kilka lat temu obie firmy koncentrowały się na wyspecjalizowanej działalności, dzięki której zdobyły popularność, a więc odpowiednio na wyszukiwaniu i serwisach społecznościowych. Obecnie obserwujemy coraz większą integrację i przenikanie się ich usług. Google oferuje dostęp do kilkudziesięciu usług i aplikacji, w tym ogromnie popularną pocztę elektroniczną Gmail, wiele z nich o charakterze społecznościowym (m.in. YouTube, Google+). Ponadto ma własną przeglądarkę internetową (Chrome) oraz system operacyjny dla telefonów komórkowych (Android). Facebook natomiast, dzięki rozbudowanej platformie programistycznej (API), jest zintegrowany z ponad 7 milionami stron internetowych i aplikacji (Facebook Newsroom, 2011). Wtyczka (*plug-in*), którą każdy może bezpłatnie zainstalować na własnej stronie internetowej, umożliwia publikację komentarzy, *lubienie* artykułów czy rejestrację i logowanie się w innych portalach poprzez powiązanie konta z Facebookiem. Umożliwia się w ten sposób łatwe dzielenie się wartościowymi stronami ze znajomymi, wygodne logowanie się i komentowanie, bez konieczności zapamiętywania nowych nazw użytkownika i haseł. Dla Facebooka to prawdziwa kopalnia danych o preferencjach i aktywnościach jego użytkowników. Należy dodać, że są to bardzo wartościowe dane, bo przypisane do konkretnego profilu, z całą jego historią i aktywnością.

W sytuacji opisanego oligopolu bardzo trudno o całkowitą rezygnację usług choćby jednej z powyższych firm. Google i Facebook są praktycznie wszechobecne. Ponadto dane o internaucie, który nie jest zalogowany ani w Google, ani na Facebooku, zostaną wielokrotnie zapisane przez ich serwery, nawet podczas zwykłego przeglądania stron internetowych. Informacje zapisane w ciasteczkach (*cookies*), a także unikalne dane konfiguracyjne przeglądarki internetowej i systemu (Eckersley, 2010), pozwalają na powiązanie ze sobą aktywności tej samej osoby, nawet jeżeli świadomie nie podaje ona żadnych danych pozwalających na identyfikację.

W przypadku mediów społecznych, a zwłaszcza serwisów społecznościowych, polityka prywatności czy jakość technologii chroniących prywatność zwykle nie jest podstawowym kryterium wyboru serwisu. Internauci nie korzystają z *najlepszych* serwisów społecznościowych, ale z tych, w których są ich znajomi (boyd, 2008). Kluczowe momenty rozwoju portali społecznościowych następują nie wtedy, gdy administratorzy wprowadzają nowe funkcje, ale gdy osiągnięta zostaje krytyczna liczba użytkowników, dzięki której warto dołączyć do portalu (Peterson, 2010).

Kolejnym problemem utrudniającym zaistnienie realnej konkurencji na rynku usług internetowych oferowanych przez Google i Facebooka jest przenośność danych. Gdy internauta rozpocznie korzystanie z portalu społecznościowego, uzupełni swoje informacje profilowe, połączy się ze znajomymi, zamieści aktualizacje statusu – zostanie *zamknięty* w tym ekosystemie. Wysiłek niezbędny do przeniesienia swoich danych oraz do odtworzenia sieci kontaktów jest dla większości użytkowników niewspółmierny do możliwych korzyści. Dodatkowo użytkownicy zwykle korzystają z jednego portalu społecznościowego, który spełnia różne zadania, rzadko z kilku portali o odmiennym przeznaczeniu. Duże serwisy społecznościowe pozwalają nie tylko na dzielenie się informacjami ze znajomymi, ale także na zamieszczanie zdjęć, wideo, uruchamianie gier *online*, przeprowadzanie wideorozmów itp. Dzieje się tak, ponieważ zakładając konto w innym portalu (np. tylko do udostępniania fotografii), użytkownik każdorazowo musi uzupełnić swoje dane, odszukać znajomych itp. Kumulacja danych prywatnych w jednym miejscu podwyższa ryzyko związane z naruszeniem prywatności, jest jednak wygodna dla użytkowników.

Odpowiedzią internauty na problemy związane z prywatnością w mediach społecznych może być oczywiście całkowite usunięcie profilu. Jednak niewielu użytkowników decyduje się na ten krok. Inicjatywa „Quit Facebook Day"

zachęcająca do usunięcia konta z serwisu Facebook, m.in. z powodu związanych z nim zagrożeń prywatności, spotkała się z umiarkowanym odzewem. Według Kiss (2010) około 33 tysiące osób usunęło swoje konta 30 maja 2010 (data wybrana przez organizatorów inicjatywy). W badaniu Grossa i Acquisti (2006) ok. 2,5% badanych określiło się jako „były użytkownik Facebooka".

Dla wielu *cyfrowych tubylców* profil na serwisie społecznościowym jest równie niezbędny jak telefon czy e-mail do komunikacji z rówieśnikami i budowania kapitału społecznego. Cyfrowa przestrzeń pozwala użytkownikom na dość swobodny wybór metod korzystania z mediów społecznych. Pod koniec 2013 roku prywatna firma badawcza GlobalWebIndex opublikowała raport, w którym wskazała na interesujący trend – spadek liczby młodych użytkowników portalu Facebook. W czwartym kwartale 2012 roku aż 79% amerykańskich nastolatków (w wieku od 16 do 19 lat) oraz 75% na świecie (pomijając Chiny) zadeklarowało korzystanie z portalu Facebook w ciągu ostatniego miesiąca. Zaledwie kilka miesięcy później, w drugim kwartale 2013, udziały te spadły odpowiednio do 61% w USA (spadek o 23%) oraz do 51% (spadek o 32%). Rekordowo duży spadek liczby aktywnych użytkowników odnotowano w takich krajach jak Holandia (o ponad 50%) czy Francja (o 44%), stosunkowo mały m.in. w Polsce czy Rosji (o 6–7%) (GlobaWebIndex, 2013). W raporcie opublikowanym przez iStrategyLabs (2014) widać, jak zmienia się struktura użytkowników Facebooka. Przez 3 lata, od 2011 do 2014, liczba użytkowników Facebooka w Stanach Zjednoczonych wzrosła o 22%, ale jednocześnie aż o 25% spadła liczba użytkowników w wieku 13–17 lat.

Ten trend nie oznacza odwrócenia się młodzieży od mediów społecznych, ale jedynie zmianę nawyków ich wykorzystywania. W przytaczanym wcześniej raporcie GlobalWebIndex (2013) informuje o dużym wzroście liczby użytkowników aplikacji mobilnych należących do dwóch kategorii: programy pozwalające na dzielenie się multimediami (m.in. Instagram, Flickr, SnapChat czy Vine) oraz komunikatory do wysyłania wiadomości tekstowych (WeChat, WhatsApp, Skype). Chrys Bader (2014) uważa, że Facebook nie jest dla młodych osób przestrzenią, w której mogą się swobodnie komunikować z rówieśnikami, jak robiła to kilka lat wcześniej poprzednia generacja użytkowników. Młodzież korzystająca z Facebooka „nie chce przesiadywać ze swoimi rodzicami", więc aby wyrazić siebie, szuka schronienia w tych miejscach w Sieci, w których ich działanie nie jest obserwowane przez bliskich. Zmiana sposobu korzystania z mediów społecznych może wynikać z problemów opisanych w sekcji *2.4.1. Niejednorodna publiczność*. Nie należy przy tym upatrywać bli-

skiego końca popularności portalu, wręcz przeciwnie – obserwujemy w tej chwili stabilizację tej platformy, przyjęcie jej przez zdecydowaną większość użytkowników Internetu. Odpływ młodych użytkowników jest skutkiem ubocznym tego zjawiska. Poszukujący i eksperymentujący z nowymi formami komunikacji, są pierwszymi użytkownikami nowych form mediów społecznościowych, ale także jako pierwsi opuszczają odnalezione przez nich portale. Facebook staje się dla nich tym, czym niegdyś LinkedIn dla osób kilka lat od nich starszych – miejscem w Sieci, w którym jest się dostępnym dla szerokiej publiczności i w którym należy uważnie budować swój wizerunek, a nie wyrażać siebie i budować szczere relacje ze znajomymi.

Kolejną barierą dla regulującej siły wolnego rynku są trudne do uchwycenia pragnienia ochrony prywatności użytkowników mediów społecznościowych. Projektując architekturę serwisu społecznościowego, jego twórcy potrzebują informacji zwrotnej od użytkowników. Uzyskanie dokładnej i odpowiadającej rzeczywistym postawom informacji zwrotnej bywa dużym problemem, ponieważ nie tylko użytkownicy mają wpływ na ustawienia prywatności, ale i ustawienia mają wpływ na użytkowników. Wiele osób nie zadaje sobie trudu, żeby dokładnie poznać ustawienia prywatności w serwisie społecznościowym i dostosować je do własnych wymagań. Dlatego właśnie zdają się na ustawienia domyślne. Aby dobrze zobrazować, jak duża jest ich siła (ang. *power of the default*), warto omówić przykład z innej dziedziny. W Niemczech i Austrii, krajach bardzo do siebie podobnych kulturowo, liczba kierowców, którzy wyrazili zgodę na pobranie organów do przeszczepu, gdyby zginęli w wypadku samochodowym, wynosi odpowiednio 12% i 99%. Ta różnica wynika z faktu, że w niemieckim wniosku o wydanie prawa jazdy obywatele wyrażają zgodę na pobranie organów (procedura *opt-in*), a w austriackim mogą wyrazić swój sprzeciw (procedura *opt-out*). Zmiana formularza wniosku zapewne wystarczyłaby, aby odwrócić tendencję (Thaler i Sunstein, 2008). Problem polega na tym, że ludzie nie zawsze mają jasno określone preferencje oraz często nie zależy im, aby ponieść koszty związane ze zrozumieniem zagadnienia i podjęciem świadomej decyzji. Można założyć, że twórcy Facebooka, wprowadzając zmiany w architekturze prywatności w portalu, mieli na celu spełnienie wymagań użytkowników i dostarczenie im efektywnych narzędzi kontroli dostępu do ich informacji osobistych. Jak pokazują badania opisane powyżej, wielu użytkowników nigdy nie podjęła wysiłku związanego z personalizacją tych ustawień a ci, którzy to zrobili, nie wykorzystali nawet ułamka możliwości oferowanych przez bardzo precyzyjne narzędzia. Jeżeli użytkownicy nie wyrażają

swoich faktycznych preferencji dotyczących prywatności, to administratorzy Facebooka nie mogą ich wysłuchać. Brak informacji zwrotnej tworzy lukę w komunikacji i zmusza portal społecznościowy do oparcia się na opinii tylko części użytkowników, komentarzy prasy oraz tzw. adwokatów prywatności, czyli organizacji i autorytetów w dziedzinie ochrony prywatności (Grimmelmann, 2009). Stworzenie równowagi pomiędzy łatwością i szybkością dzielenia się informacjami, a ochroną prywatności użytkowników w sieciach społecznościowych, jest niezmiernie wymagającym wyzwaniem.

4. PRZEGLĄD BADAŃ

Poprzednie rozdziały pracy zawierały przegląd modeli teoretycznych związanych z problemem prywatności ogólnie oraz prywatności w internetowych mediach społecznych. Część analiz została zweryfikowana lub sfalsyfikowana przez badania empiryczne. W tym rozdziale przedstawiam streszczenie dwóch najbardziej obszernych i aktualnych raportów, które dotyczą problemu prywatności w Internecie. Wiele zagadnień poruszonych w omówionych badaniach stało się inspiracją i wskazówką dla przeprowadzenia pogłębionych wywiadów w badaniach autorskich, które zostały przedstawione w rozdziale 5.

4.1. Specjalny Eurobarometr

W 2011 roku Komisja Europejska zaprezentowała przygotowaną przez TNS Opinion and Social specjalną edycję Eurobarometru. Zbadano postawy Europejczyków dotyczące prywatności, ochrony danych oraz zarządzania elektroniczną tożsamością. Badanie przeprowadzone zostało na próbie blisko 27 tysięcy obywateli wszystkich krajów członkowskich Unii Europejskiej na przełomie listopada i grudnia 2010 roku.

Według badania 66% Europejczyków korzysta z Internetu (44% codziennie lub prawie codziennie), 39% korzysta z e-commerce, 34% z sieci społecznościowych, a 29% zamieszcza w Internecie zdjęcia i/lub filmy. Wśród użytkowników Internetu 44% osób korzysta z bankowości elektronicznej, 24% korzysta z tzw. *przetwarzania w chmurze* (ang. *cloud computing*).

4.1.1. Cyfrowi tubylcy

Raport z badania opisuje szczegółowo postawę osób w wieku 15–24 lata, których nazywa zapożyczonym od Marka Prenskiego (2001) terminem *digital natives*, czyli cyfrowi tubylcy. Określa się tak młode osoby urodzone w trakcie lub po rozpowszechnieniu się nowoczesnych technologii informacyjnych, zwłaszcza Internetu. Osoby, które nie zostały wychowane w kontakcie ze światem cyfrowym to *digital immigrants* – imigranci lub *initiates* – nowicjusze. Rozbieżne postawy i zachowania w stosunku do nowych technologii tubylców i imigrantów wynikają z innych przyzwyczajeń, a może nawet, jak sugerują niektórzy badacze, z odmiennie ukształtowanego w procesie dojrzewania mózgu. Imigranci mają w zwyczaju bezpośrednio przenosić modele zachowań ze świata rzeczywistego do cyfrowego, w którym nie rządzą przecież takie same prawa.

Aż 94% Europejczyków w wieku 15–24 lat korzysta z Internetu, 84% jest zarejestrowanych jako użytkownicy sieci społecznościowych, a 73% korzysta ze stron umożliwiających oglądanie i publikowanie zdjęć, fotografii i muzyki. Wśród wszystkich obywateli UE *online* jest zaledwie 2/3 osób, a nieco ponad połowa korzysta z sieci społecznościowych. Większa aktywność młodych osób w Internecie jest związana z mniejszym poszanowaniem własnego prawa do prywatności. 43% *tubylców* uważa, że podawanie danych osobowych i innych danych prywatnych nie jest dla nich ważną sprawą (średnia UE 33%). To z kolei owocuje większą skłonnością do otwierania się w Internecie, m.in. podawania swoich danych osobowych serwisom oferującym różnego rodzaju usługi w Internecie, np. pocztę e-mail (48%, średnia UE 29%) czy upubliczniania prywatnych informacji w sieciach społecznościowych wyłącznie dla zabawy (26%, średnia UE 22%). Młodzi ludzie, częściej od starszych, zmieniają ustawienia prywatności swojego profilu w portalu społecznościowym (62%, średnia UE 51%) i czują się dobrze poinformowani o sposobie wykorzystania ich prywatnych danych podczas rejestracji w nowej usłudze (64%, średnia UE 54%), mimo że jednocześnie nieco rzadziej czytają dokumenty i deklaracje usługodawców dotyczących tej kwestii (69%, średnia UE 75%). Młodzież częściej uważa, że kontroluje informacje na swój temat zamieszczone w sieciach społecznościowych czy innych stronach z treścią generowaną przez użytkowników (84%, średnia UE 78%) oraz w sklepach internetowych (80%, średnia UE 68%). *Natives* są bardziej beztroscy – rzadziej martwią się o spam (24%, średnia UE 28%), nieprzestrzeganie polityki prywatności (20, średnia UE 24%), a także o to, że informacje o nich mogą być używane w innym celu niż podano (63%, średnia UE 70%).

4.1.2. Postawy i zachowania dotyczące ujawniania informacji prywatnych

74% badanych uważa, że dzielenie się informacjami prywatnymi ma coraz większe znaczenie w życiu nowoczesnego człowieka, a jednocześnie tylko dla 33% upublicznianie tego rodzaju informacji nie jest ważną kwestią (Polacy 48%). Większość Europejczyków nie zgadza się na wykorzystanie ich danych prywatnych w zamian za dostęp do bezpłatnych usług np. e-maila (51%) oraz nie czuje się zobowiązana do podawania ich w Internecie (49%). Mimo niechęci, 58% zgadza się, że aby korzystać ze specyficznych usług i kupować produkty (nie tylko w Internecie) muszą podawać swoje dane osobiste. Dodatkowo, częściej zgadzają się z tym stwierdzeniem osoby, które korzystają z e-commerce (71%) niż Europejczycy, którzy nie robią zakupów *online* (59%).

Wśród osób, które korzystają z sieci społecznościowych, niemal 80% zamieściło na jednej z nich swoje prawdziwe imię i nazwisko, a około połowa dołączyła fotografie (51%) oraz informacje o swojej narodowości (47%). Czterech na dziesięciu określiło *rzeczy, które robi*, własny adres domowy oraz upubliczniło listę swoich znajomych. Jedna trzecia badanych informuje w Internecie o swoich gustach i opiniach, a 23% zamieściło swój numer telefonu komórkowego. Badani rzadziej przyznają się do publikowania ich historii zatrudnienia (18%), odwiedzanych stron internetowych (14%), numerów osobistych (np. numer dowodu, paszportu, PESEL – 13%) czy danych finansowych (10%). Nieliczna grupa badanych wskazała na informacje medyczne (5%) oraz odciski palców (3%), jako udostępnione *online*. 8% stwierdziło, że nie udostępniło w sieciach społecznościowych żadnych danych osobistych.

Badani z Polski wykazali się jednym z niższych poziomów udostępniania powyższych informacji z trzema wyjątkami: prawdziwe imię i nazwisko, adres domowy oraz numer telefonu komórkowego udostępniono częściej niż średnio w całym badaniu (o odpowiednio 5, 13 oraz 11 pkt. procentowych więcej).

Dwie najczęściej wskazywane w badaniu motywacje dla zamieszczania danych prywatnych w mediach społecznych to umożliwienie dostępu do usługi (61% wskazań) oraz możliwość utrzymywania kontaktu z innymi ludźmi (52%). Co piąty Europejczyk podaje swoje dane prywatne *dla zabawy* (22%), w celu otrzymania bezpłatnej usługi lub lepiej spersonalizowanej usługi (po 18%). Co dziesiąty robi to celem oszczędzenia czasu przy kolejnej wizycie (12%), czerpania korzyści ze spersonalizowanych reklam oraz otrzymania rabatów czy nagród (po 8%). Ciekawe, że w przypadku Polaków motywacja rozrywkowa (odpowiedź *dla zabawy*) jest zdecydowanie rzadsza, niż w innych krajach (8%, przy średniej 22%).

W przypadku zakupów *online* zdecydowana większość (79%) osób korzystających z tego rodzaju usług podaje swoje dane prywatne, aby móc skorzystać z usługi. Pozostałe motywacje mają mniejsze znaczenie: co czwarty badany podaje swoje dane, aby móc skorzystać z usług bardziej dopasowanych do jego potrzeb; co piąty, aby oszczędzić czas przy kolejnej wizycie, a co dziesiąty, aby otrzymać korzystniejszą finansowo ofertę.

4.1.3. Bezpieczeństwo i ochrona prywatności

Większość obywateli krajów członkowskich UE dba o bezpieczeństwo swoich danych prywatnych w życiu osobistym. 62% badanych twierdzi, że zawsze podaje tylko minimalną ilość wymaganych przez różne podmioty informacji osobistych (w Polsce – tylko 45%), a 7% umyślnie podaje fałszywe informacje, aby chronić swoją prywatność. Trochę ponad połowa badanych nie podaje nikomu swoich danych finansowych oraz numerów PIN do płatności elektronicznych (56%, Polacy 34%), a nieco mniej trzyma w tajemnicy swoje dane do logowania się w różnych serwisach (45%). Podobna liczba osób nie ujawnia swoich informacji prywatnych osobom i organizacjom, którym nie ufa (45%, Polacy 34%). Niemal co trzeci Europejczyk używa gotówki zamiast kart płatniczych, aby mieć pewność, że zakupy, które robi, nie zostaną przypisane do jego osoby (30%, Polacy 44%). Podobna liczba osób nie korzysta z kart kredytowych w Internecie. Osoby, które robią zakupy w Sieci, są bardziej rozważne, jeśli chodzi o podawanie danych dostępowych (loginów, haseł i numerów PIN) – blisko 70% badanych nigdy nie ich nie podaje.

W badaniu zapytano respondentów korzystających z Internetu, czy i jak często wymagano od nich podania większej liczby informacji prywatnych niż było to konieczne dla skorzystania z usługi. 38% uważa, że zdarza się to często, a 5% – zawsze. Z drugiej strony, 21% spotyka się z taką sytuacją rzadko, a 32% – nigdy. Dla 27% badanych tego typu sytuacje nie mają większego lub żadnego znaczenia, natomiast aż 72% uważa, że nie powinno do nich dochodzić.

Większość Europejczyków nie korzysta z technicznych sposobów ochrony swojej prywatności w Internecie – jedynie czterech na dziesięciu internautów korzysta z narzędzi antyspamowych oraz oprogramowania antywirusowego. Podobna liczba zwraca uwagę, czy strony, z których korzysta, mają aktualne certyfikaty bezpieczeństwa przesyłanych danych w Internecie. Co piąty dostosowuje ustawienia prywatności swojej przeglądarki internetowej. Tyle samo unika podawania tych samych informacji różnym stronom internetowym. Według Eurobaro-

metru aktywne sposoby ochrony swojej tożsamości w Internecie są stosowane przez bardzo niewielki odsetek badanych. Tylko 14% z nich korzysta z wyszukiwarek internetowych, aby ustalić, jakie informacje o nich dostępne są w Internecie, a 8% twierdzi, że zażądało od administratorów strony internetowej usunięcia lub zaktualizowania danych osobowych. Osoby często i aktywnie korzystające z Internetu częściej adoptują każdą z powyższych strategii ochrony swoich danych niż mniej zaangażowani internauci.

Niemal 80% respondentów uważa, że ma kontrolę nad przepływem własnych informacji osobistych opublikowanych w sieciach społecznościowych i stronach umożliwiających dzielenie się treściami (26% pełna kontrola, 52% częściowa). Kontrola jest rozumiana, jako możliwość zmiany, usunięcia oraz poprawienia tych informacji.

4.1.4. Ocena ryzyka

Osoby, które korzystają z serwisów społecznościowych oraz robią zakupy *online* zapytano o ryzyko, które wiąże się z podawaniem swoich informacji *online*. Jako najpoważniejsze ryzyko wskazano wykorzystanie prywatnych informacji bez wiedzy użytkowników (44% wskazań przez korzystających z serwisów społecznościowych i 43% korzystających z e-commerce), bycie ofiarą oszustwa (odpowiednio 41% i 55%), przekazanie danych podmiotom zewnętrznym (odpowiednio 38% i 43%), bycie ofiarą kradzieży tożsamości (odpowiednio 32% i 35%), wysyłanie niechcianych ofert reklamowych (28% i 34%), użycie informacji w innych kontekstach niż konieczny dla usługi (25% i 27%). Użytkownicy serwisów społecznościowych obawiają się również o możliwość naruszenia ich bezpieczeństwa (20%), naruszenia reputacji (12%), nieprawidłowego zrozumienia ich postaw i opinii (11%) oraz dyskryminacji, w różnych kontekstach, m.in. podczas ubiegania się o stanowisko pracy czy miejsce na uczelni (7%).

Kolejne pytanie dotyczyło elektronicznej rejestracji zachowań badanych, także w nie-internetowym kontekście. Najwięcej respondentów obawia się rejestracji danych dotyczących zakupów kartami płatniczymi i kredytowymi (54%), a także lokalizacji ich położenia przy korzystaniu z telefonów komórkowych i mobilnego Internetu (49%). 40% wszystkich badanych obawia się, że rzeczy, które robi w Internecie, mogą być rejestrowane (historia przeglądania stron internetowych, pobieranie plików). Wśród korzystających z Internetu odsetek ten wzrasta do 51%.

4.1.5. Personalizacja

Fakt, że firmy świadczące usługi w Internecie personalizują doświadczenia internetowe użytkowników na podstawie ich wcześniejszej aktywności jest kontrowersyjny dla 54% użytkowników z Internetu. Z drugiej strony, 39% czuje się komfortowo z taką sytuacją. Wśród badanych z Polski tendencja się odwraca – przeciwnych profilowaniu Internetu jest 34% badanych, a aż 57% nie widzi w tym nic złego. Akceptacja dla tego zjawiska jest wyższa także wśród badanych, korzystających z Sieci społecznościowych (60% czuje się komfortowo).

Niemal połowa badanych nigdy nie słyszała o przypadkach strat związanych z kradzieżą tożsamości lub o wyciekach danych prywatnych (44%), a większość pozostałej grupy dowiedziała się o nich poprzez media (42%). Tylko 2% badanych ma osobiste doświadczenia tego typu, a niewiele więcej wskazało, że dotknęło to ich znajomych (7%) lub członków rodziny (3%).

4.1.6. Zaufanie

Europejscy Internauci mają niewielkie zaufanie do firm związanych z Internetem w kwestii ochrony ich danych prywatnych. Tylko aż 62% z nich nie ufa ani operatorom stron internetowych (portali społecznościowych, wyszukiwarek internetowych itp.), ani firmom telekomunikacyjnym, także tym świadczącym usługi dostępu do Internetu. Wyraźnie wyższy stopień zaufania charakteryzuje osoby młode, studentów oraz osoby aktywnie korzystające z Internetu. Zauważono również pozytywną korelację pomiędzy niższym poziomem nieufności do firm internetowych (50%), a poczuciem dobrego zrozumienia zasad gromadzenia i przetwarzania danych osobowych.

Inne badania potwierdzają, że uczciwe i otwarte przedstawienie polityki prywatności zwiększa poziom zaufania do strony internetowej, co przekłada się na większą ilość zarejestrowanych użytkowników, a także większą chęć dzielenia się danymi prywatnymi. W przypadku serwisów e-commerce przekłada się to bezpośrednio na większą sprzedaż, a w przypadku portali społecznościowych i stron umożliwiających dzielenie się treściami na większą aktywność użytkowników, co skutkuje zwiększoną popularnością i atrakcyjnością serwisu, a to też może się przełożyć na przychody strony internetowej (np. dzięki reklamom).

4.1.7. Troski

Zdecydowana większość badanych martwi się, że ich prywatne dane mogą zostać wykorzystane w innych celach niż uzgodniono (70%), a tylko 5% uważa, że nikt nie może gromadzić i przetwarzać ich danych bez wyrażonej przez nich zgody. Większość uważa, że taka zgoda powinna być udzielona w każdym przypadku (74%), a tylko 8% – w przypadku gromadzenia i przetwarzania danych uznawanych za wrażliwe, np. dotyczących informacji zdrowotnych, wyznania, preferencji seksualnych itp. Niemal 90% uważa, że powinna zostać poinformowana, gdy informacje o nich zostaną wykradzione lub ich integralność zostanie w jakiś sposób naruszona w bazie danych jakiejkolwiek organizacji.

Trzy czwarte osób, które korzystają z Internetu, chce mieć prawo do usunięcia informacji prywatnych gromadzonych przez firmy internetowe w dowolnej chwili i bez podawania powodu. Jedna czwarta uważa, że takie prawo powinno przysługiwać w przypadku zaprzestania korzystania z usługi lub strony internetowej.

Nieco ponad połowa badanych, którzy korzystają z portali społecznościowych i stron umożliwiających dzielenie się treściami, kiedykolwiek *spróbowała* zmienić ustawienia prywatności, a 46% nie. Znacznie częściej robiły to osoby młode (15–24 – 62%), niż starsze (55+, tylko 24%). Pozytywna korelacja związana była również z wysokim wykształceniem. Aż 82% uważa, że zmiana ustawień prywatności profilu jest łatwa (18% przeciwnie). Ponownie wiek jest czynnikiem wpływającym na odpowiedź – starsze osoby wyraźnie rzadziej uznawały tę czynność za łatwą, ale ciągle trzem czwartym osób z tej grupy zmiana ustawień prywatności nie sprawiła problemu. Odpowiedź na to pytanie jest związana również ze stopniem postrzeganej kontroli nad danymi prywatnymi. Tylko 67% osób, które twierdzi, że nie ma kontroli nad swoimi danymi, uważa zmianę ustawień prywatności za łatwą. Podobne zdanie ma 91% chwalących się pełną kontrolą nad swoimi danymi.

Osoby, które nigdy nie próbowały zmieniać ustawień prywatności swojego profilu, wskazywały różne powody dla braku tego działania. Najwięcej, bo 28%, wierzy, że ustawienia domyślne są wystarczające. Co piąty badany nie wiedział, że taka możliwość istnieje. Również blisko 20% nie potrafiła ich zmienić. Podobna liczba osób wskazała, że nie martwi się o swoje dane prywatne zamieszczone na portalach społecznościowych i innych stronach umożliwiających dzielenie się treściami. 12% uznało, że nie ma czasu, aby zająć się zmianą widoczności swojego profilu, co można interpretować jako obawę przed zbytnim skomplikowaniem ustawień oraz przywiązywaniem niewielkiej wagi do tego zagadnienia.

4.1.8. Prawo

W specjalnym raporcie Eurobarometru zapytano badanych o kwestie związane z prawną ochroną ich prawa do prywatności w prawodawstwie krajowym i europejskim. Jedynie jedna trzecia badanych słyszała o krajowej instytucji chroniącej dane obywateli. W Polsce do znajomości Generalnego Inspektoratu Ochrony Danych Osobowych przyznało się 40% badanych. Trzy czwarte użytkowników stron społecznościowych uważa jednak, że odpowiedzialność za naruszenia prywatności związane z korzystaniem z tychże stron spada na samych użytkowników (49% jako pierwsze wskazanie, 26% jako drugie). Niemal tyle samo respondentów stwierdziło, że administratorzy *social media*, którzy przetwarzają dane użytkowników, powinni zadbać o prawidłową ich ochronę (33% jako pierwsze wskazanie, 41% jako drugie). 45% wskazało instytucje władzy jako stronę odpowiedzialną za ochronę danych prywatnych – z czego tylko 16% wybrało tę odpowiedź jako pierwszą. Podobne odpowiedziano na pytanie o dane przetwarzane przez sklepy internetowe. Mimo to, zdecydowana większość badanych opowiedziała się za harmonizacją ustawodawstwa w tej materii na terenie Unii Europejskiej (90%). Blisko dwie trzecie badanych uważa, że duże firmy lepiej chroniłyby dane prywatne, gdyby były zobowiązane do utworzenia stanowiska oficera ochrony danych osobowych. 27% respondentów jest przeciwnego zdania.

W badaniu zapytano o uprawnienia organów ścigania do zdobywania danych prywatnych. Najczęściej wskazywanym rozwiązaniem jest ograniczenie możliwości uzyskania danych prywatnych – 37% respondentów uważa, że policja powinna mieć dostęp jedynie do takich danych, które są niezbędne dla konkretnego śledztwa. Co czwarty twierdzi, że takie uprawnienia mogą być nadane jedynie przez władze sądownicze. Z drugiej strony – jedna trzecia respondentów uważa, że dostęp policji do danych prywatnych nie powinien być ograniczany, aby móc skuteczniej zapobiegać wszelkiego rodzaju przestępstwom.

4.2. Badanie Microsoft „Online Profile & Reputation Perceptions Study"

W styczniu 2012 roku opublikowane zostało badanie Microsoftu (Brackenbury, Wong, 2012) dotyczące postrzegania profili oraz reputacji *online*. Przeprowadzono je na dużej grupie 5 tysięcy internautów z pięciu wysoko rozwiniętych krajów – Stanów Zjednoczonych, Kanady, Irlandii, Hiszpanii oraz Niemiec. Połowę ankietowanych z każdego z wymienionych krajów stanowili dorośli (w wieku od 18 do

74 lat), a połowę dzieci i młodzież, czyli *digital natives* (w wieku od 8 do 17 lat). Według autorów badania, na profil *online* składają się trzy typy danych: (1) logi o użytkowniku Internetu, np. wyciągi bankowe, historia zakupów, bilingi telefoniczne, historia przeglądania stron internetowych itp.; (2) treści stworzone przez użytkownika, np. e-maile, wiadomości SMS i MMS, obrazy, dźwięki i materiały wideo zamieszczone *online*, a także aktywność w portalach społecznościowych itp.; (3) treści o użytkowniku zamieszczone przez innych np. otagowana fotografia, wszelkiego rodzaju posty i komentarze dotyczące użytkownika itp.

Profil jest zatem sumą wszystkich interakcji w świecie *online*, włączając w to używanie Sieci WWW, telefonów komórkowych, konsol do gier, telewizorów z obsługą Internetu oraz wszelkich innych urządzeń łączących się ze światową Siecią. Reputacja *online* to wizerunek internauty stworzony na podstawie informacji, które zostały zamieszczone w Internecie na jego lub jej temat, niezależnie od tego, kto je rozpowszechnił. Profil można traktować jako sumę informacji o użytkowniku, a reputację jako ich pochodną.

4.2.1. Profil *online*

Badacze wyodrębnili 22 kategorie czynności, które składają się na tworzenie profilu *online* i zapytali ankietowanych o partycypację w owych czynnościach, a także o wybranie trzech, które w największym stopniu przyczyniają się do kreacji ich profilu. Zarówno wśród dorosłych, jak i ankietowanych w wieku poniżej 18 lat, najbardziej rozpowszechnione było korzystanie z poczty elektronicznej (odpowiednio 93% i 85%), przeglądanie Sieci WWW, w tym korzystanie z wyszukiwarek internetowych (82% i 75%) oraz sieci społecznościowych (68% i 78%). Wśród dorosłych częste było również korzystanie z zakupów oraz bankowości *online* (74% i 68%), z oczywistych względów rzadziej wskazywanych przez młodszych badanych (48% i 32%). Dorośli, rzadziej niż dzieci i młodzież, odtwarzają muzykę i materiały wideo w Sieci (odpowiednio 62% i 79%), zamieszczają zdjęcia w Internecie (60% i 70%) oraz grają w gry *online* (58% i 76%).

Znaczne rozbieżności zaobserwowano przy porównaniu postrzeganego wpływu tych czynności na kreację profilu. Dorośli znacznie większą wagę niż młodzież i dzieci przywiązywali do poczty elektronicznej (odpowiednio 72% i 48% wskazań), a wyraźnie rzadziej uznają za istotne dla kreacji ich profilu korzystanie z sieci społecznościowych (31% dorośli, 42% dzieci i młodzież), a także granie w gry *online* (odpowiednio 23% i 42%) i korzystanie z materiałów audiowizualnych w Sieci (17% i 42%).

W tabeli 2 przedstawiono pełny zestaw odpowiedzi na pytania: (1) proszę wybrać trzy aktywności *online*, które w największym stopniu wpływają na twój profil *online*; (2) proszę wybrać wszystkie aktywności *online*, z których korzystasz w celach osobistych.

	Dorośli		Dzieci i młodzież	
Aktywność	**Uczestnictwo**	**Wpływ na profil *online***	**Uczestnictwo**	**Wpływ na profil *online***
Wysyłanie i odbieranie e-maili	93%	72%	85%	48%
Wyszukiwanie / przeglądanie WWW (komputer i urządzenia mobilne)	82%	28%	75%	22%
Zakupy w Internecie	74%	32%	48%	16%
Media społeczne (zamieszczanie treści – blogi, tweety, zdjęcia i wideo itp.)	68%	31%	78%	42%
Bankowość elektroniczna	65%	31%	32%	9%
Wysyłanie i odbieranie wiadomości tekstowych	62%	10%	72%	15%
Pobieranie lub odtwarzanie muzyki, wideo i filmów	62%	17%	79%	41%
Zamieszczanie zdjęć na stronie internetowej z aparatu lub telefonu komórkowego	60%	6%	70%	12%
Granie w gry *online* (włączając światy wirtualne)	58%	23%	76%	42%
Korzystanie z portali aukcyjnych i ogłoszeniowych	58%	5%	42%	3%
Korzystanie z forów internetowych	53%	9%	53%	9%
Pisanie bloga lub komentowanie na blogu	43%	4%	53%	6%

	Dorośli		Dzieci i młodzież	
Aktywność	**Uczestnictwo**	**Wpływ na profil *online***	**Uczestnictwo**	**Wpływ na profil *online***
Telefonia przez Internet (np. Skype)	43%	8%	52%	11%
Korzystanie z aplikacji na smartphony i tablety	43%	3%	54%	6%
Korzystanie z zakupów grupowych	41%	3%	–	–
Informowanie o swojej lokalizacji rodzinę i znajomych	41%	4%	47%	5%
Korzystanie z serwisów mikroblogowych	36%	4%	51%	6%
Tworzenie własnej strony internetowej	28%	4%	39%	4%
Korzystanie z systemów e-health	25%	1%	–	–
Korzystanie z zawodowego serwisu społecznościowego (np. LinkedIn)	23%	3%	–	–
Publiczne informowanie o swojej lokalizacji	23%	1%	27%	2%
Informowanie biznesu o swojej lokalizacji	20%	2%	24%	2%

Tabela 2. Źródło: Brackenbury, Wong, 2012

Autorzy badania zwracają uwagę na fakt niedoceniania wpływu na profil *online* niektórych czynności – dotyczy to zwłaszcza korzystania z sieci społecznościowych, które są dopiero na czwartej pozycji pod względem postrzeganego wpływu na profil. Podobna sytuacja dotyczy zamieszczania zdjęć w Internecie – jedynie 6% dorosłych i 12% wskazało na nie, jako ważny składnik ich profilu *online*.

4.2.2. Kontrola nad profilem

Wyniki badania udzielają też odpowiedzi na pytanie, czy internauci uważają, że mają kontrolę nad swoimi profilami *online*. Aż 67% dorosłych i 73% *digital natives* odpowiedziało pozytywnie. Dodatkowo 17% ogółu badanych twierdzi, że ma pełną kontrolę nad swoim profilem, przy jedynie 4% twierdzących zupełnie przeciwnie. Interesująco przedstawia się zależność pomiędzy postrzeganą kontrolą nad profilem, a stopniem niepokoju o reputację *online*. Badani, którzy stwierdzili, że mają pełną kontrolę, najczęściej udzielali skrajnych odpowiedzi, mianowicie: „Zupełnie nie niepokoję się o swoją reputację *online*" (28%) oraz „Bardzo niepokoję się o swoją reputację *online*" (25%). Ta rozbieżność jest tłumaczona przez badaczy dwoma przeciwstawnymi postawami użytkowników Internetu: (1) „Nie muszę się martwić o swoją reputację, skoro mam pełną kontrolę nad swoim profilem *online*"; (2) „Bardzo martwię się o swoją reputację, gdyż mój profil *online* jest poza moją kontrolą".

Ponad 90% badanych podjęło przynajmniej jedną czynność w celu kontroli swojego profilu. Najczęściej było to wpisanie swojego imienia i nazwiska w wyszukiwarce internetowej (62% wskazań), dostosowanie ustawień prywatności w portalu społecznościowym (53%) oraz podjęcie decyzji o niepublikowaniu komentarza, filmu czy zdjęcia (48%). Młodsi ankietowani wyraźnie częściej od dorosłych sprawdzali, co inni napisali o nich w Sieci (odpowiednio 45% i 32%) oraz prosili o usunięcie materiałów dotyczących ich samych, np. zdjęcia w sieci społecznościowej (34% i 21%). Ankietowani, którzy we wcześniejszym pytaniu o stopień posiadanej kontroli nad swoim profilem wskazali pełną kontrolę lub całkowity jej brak, rzadziej niż osoby udzielające odpowiedzi ze środka skali (*raczej mam dużą kontrolę*, *raczej mam niewielką kontrolę*), próbowali aktywnie nim zarządzać. W pierwszym przypadku można to interpretować fałszywym poczuciem bezpieczeństwa, opisywanym już wcześniej w pracy (zob. sekcję *2.4 Media społeczne – problemy z prywatnością*). Aż 20% badanych, którzy uważali, że nie mają kontroli nad własnym profilem *online*, nie podjęło jednocześnie żadnych czynności, dzięki którym mogliby tę kontrolę uzyskać. Tę korelację można wytłumaczyć na dwa sposoby – brak kontroli wynika z bierności lub bierność wynika z fatalistycznej postawy: „Co bym nie zrobił, i tak nie jestem w stanie zadbać o ochronę prywatności moich informacji w Internecie".

4.2.3. Konsekwencje korzystania z Internetu

Ankietowani zostali zapytani o częstość myślenia o konsekwencjach ich aktywności *online*. Ponad połowa wszystkich badanych zawsze lub często myśli o informacjach, które mogą zostać ujawnione publicznie podczas wykonywania różnych czynności *online* – to najczęściej wskazywana odpowiedź. Nieco mniej niż 45% ankietowanych aktywnie myśli o długofalowym wpływie ich aktywności *online* na osobistą reputację. Niewiele niższy jest odsetek Internautów świadomych, że zamieszczone przez nich informacje mogą wpływać na reputację innych osób (39%). Ogólnie odsetek osób biorących pod uwagę reputację czy wizerunek innych osób, jest średnio o 5 punktów procentowych niższy niż osób biorących pod uwagę swoje dobra osobiste. W badaniu zaobserwowano również pozytywną korelację pomiędzy częstością myślenia o konsekwencjach aktywności *online* i podjętych próbach zarządzania swoim profilem. Przykładowo: 57% osób myślących o bezpieczeństwie swoich prywatnych informacji dostosowało ustawienia prywatności w portalu społecznościowym. Podobna czynność została podjęta jedynie przez 45% osób rzadziej troszczących się o ochronę własnych informacji.

Mimo niewielkiej świadomości internautów tego, jakie konsekwencje dla innych osób mogą przynieść ich działania w Sieci, stosunkowo mało osób przyznało się do zamieszczenia *online* informacji, które były krzywdzące dla innych. Zrobiło tak 12% dorosłych oraz 18% dzieci i młodzieży, przy czym około trzy czwarte przypadków nie było celowym działaniem na czyjąś szkodę. W rezultacie jedynie nieco ponad 4% wszystkich badanych przyznało się do świadomego podjęcia jakiegoś działania w Sieci, mającego na celu wyrządzenie komuś krzywdy. Jako przykłady nieumyślnych krzywdzących działań badani podali, m.in.: zamieszczenie niechcianych fotografii, naruszenie poufności informacji czy zamieszczenie agresywnego żartu. Wśród krzywd intencjonalnych przytaczano, m.in.: rozpowszechnianie krzywdzących plotek o innych osobach, publikowanie informacji z życia prywatnego, bezpośrednie ataki osobiste czy zamieszczanie zawstydzających fotografii.

Z drugiej strony, spośród ankietowanych aż 15% dorosłych i 22% dzieci i młodzieży doświadczyło poważnych negatywnych konsekwencji działań *online* ze strony innych osób. Najczęściej wskazywano na utratę przyjaciela (znajomego?; ang. *friend*) – 43% wszystkich negatywnych konsekwencji. Niewiele mniej osób zostało postawionych w społecznie kłopotliwej sytuacji (39%). Warto odnotować także, że wśród badanych, którzy doznali negatywnych następstw aktywności innych osób w Sieci: 24% stało się ofiarą kradzieży tożsamości, 20% dorosłych utra-

ciło pracę, 19% rozwiodło się, 15% utraciło prawo do opieki nad dziećmi, 18% straciło szansę na otrzymanie posady, a 16% nie dostało się do wybranej uczelni.

Neutralne i pozytywne konsekwencje korzystania z Internetu dla osobistego wizerunku wskazywane są na szczęście znacznie częściej niż negatywne. Wśród dorosłych stosunek wskazań pozytywnych do negatywnych doświadczeń związanych z różnymi aktywnościami *online* wynosi średnio 5:0, a dla dzieci i młodzieży – aż 7:4. Najwięcej pozytywnych efektów wiąże się z wysyłaniem i odbieraniem poczty e-mail (47% badanych zauważa pozytywny wpływ na ich reputację, tylko 2% – negatywny) i wiadomości tekstowych, przeglądania stron www, korzystania z wyszukiwarek internetowych oraz dzielenia się fotografiami w Sieci. Najwięcej negatywnych efektów było związanych z wszelkiego rodzaju usługami geolokalizacyjnymi, czyli takimi, które pozwalają dzielić się obecnym położeniem ze znajomymi, biznesem lub szeroką publicznością. Jednak tylko w tym ostatnim przypadku, i to wyłącznie wśród dorosłych, negatywne konsekwencje były wskazywane częściej niż pozytywne – odpowiednio 20% i 18%, przy 41% osób wskazujących na brak lub neutralne konsekwencje dla reputacji osobistej.

W tabelach 3 i 4 przedstawiam pełne zestawienie odpowiedzi na pytanie: Jak bardzo poszczególne aktywności wpływają na twoją reputację *online*. Jeśli nie korzystasz ze specyficznej aktywności, spróbuj określić potencjalny wpływ na Twoją reputację *online*?

Dorośli	Pozytywny wpływ	Negatywny wpływ	Stosunek pozytywny/negatywny	Brak wpływu	Różnica pozytywny – negatywny
Wysyłanie i odbieranie e-maili	47%	2%	24	34%	45%
Zakupy w Internecie	31%	4%	8	44%	27%
Bankowość elektroniczna	27%	5%	5	49%	22%
Wyszukiwanie/przeglądanie www (komputer i urządzenia mobilne)	31%	3%	10	42%	28%
Pobieranie lub odtwarzanie muzyki, wideo i filmów	23%	7%	3	45%	16%
Informowanie o swojej lokalizacji rodzinę i znajomych	23%	12%	2	39%	11%
Informowanie biznesu o swojej lokalizacji	19%	15%	1	44%	4%

Dorośli	Pozytywny wpływ	Negatywny wpływ	Stosunek pozytywny/negatywny	Brak wpływu	Różnica pozytywny – negatywny
Publiczne informowanie o swojej lokalizacji	18%	20%	1	41%	-2%
Telefonia przez Internet (np. Skype)	28%	6%	5	48%	22%
Korzystanie z aplikacji na smartphony i tablety	23%	6%	4	51%	17%
Zamieszczanie zdjęć na stronie internetowej z aparatu lub telefonu komórkowego	29%	7%	4	34%	22%
Wysyłanie i odbieranie wiadomości tekstowych	29%	4%	7	45%	25%
Serwisy społecznościowe (zamieszczanie treści – blogi, tweety, zdjęcia i wideo itp.)	32%	9%	4	31%	23%
Korzystanie z zawodowego serwisu społecznościowego (np. LinkedIn)	25%	7%	4	47%	18%
Tworzenie własnej strony internetowej	27%	7%	4	44%	20%
Pisanie bloga lub komentowanie na blogu	28%	8%	4	38%	20%
Granie w gry *online* (włączając światy wirtualne)	26%	7%	4	41%	19%
Korzystanie z serwisów mikroblogowych	25%	8%	3	41%	17%
Korzystanie z portali aukcyjnych i ogłoszeniowych	23%	6%	4	46%	17%
Korzystanie z forów internetowych	29%	6%	5	37%	23%
Korzystanie z zakupów grupowych	20%	7%	3	51%	13%
Korzystanie z systemów e-health	24%	6%	4	49%	18%
Średnia	**27%**	**7%**	**5,0**	**42%**	**19%**

Tabela 3. Źródło: Brackenbury, Wong, 2012

Dorośli	Pozytywny wpływ	Negatywny wpływ	Stosunek pozytywny/ negatywny	Brak wpływu	Różnica pozytywny – negatywny
Wysyłanie i odbieranie e-maili	47%	2%	24	31%	45%
Zakupy w Internecie	27%	4%	7	51%	23%
Bankowość elektroniczna	23%	4%	6	55%	19%
Wyszukiwanie / przeglądanie WWW (komputer i urządzenia mobilne)	35%	2%	18	36%	33%
Pobieranie lub odtwarzanie muzyki, wideo i filmów	35%	4%	9	32%	31%
Informowanie o swojej lokalizacji rodzinę i znajomych	30%	11%	3	30%	19%
Informowanie biznesu o swojej lokalizacji	21%	14%	2	39%	7%
Publiczne informowanie o swojej lokalizacji	22%	16%	1	36%	6%
Telefonia przez Internet (np. Skype)	31%	5%	6	39%	26%
Korzystanie z aplikacji na smartphony i tablety	29%	5%	6	43%	24%
Zamieszczanie zdjęć na stronie internetowej z aparatu lub telefonu komórkowego	41%	6%	7	21%	35%
Wysyłanie i odbieranie wiadomości tekstowych	39%	3%	13	32%	36%
Serwisy społecznościowe (zamieszczanie treści – blogi, tweety, zdjęcia i wideo itp.)	42%	6%	7	20%	36%
Tworzenie własnej strony internetowej	32%	5%	6	38%	27%
Pisanie bloga lub komentowanie na blogu	35%	5%	7	30%	30%
Granie w gry *online* (włączając światy wirtualne)	34%	6%	6	31%	28%

Dorośli	Pozytywny wpływ	Negatywny wpływ	Stosunek pozytywny/ negatywny	Brak wpływu	Różnica pozytywny – negatywny
Korzystanie z serwisów mikroblogowych	31%	6%	5	33%	25%
Korzystanie z portali aukcyjnych i ogłoszeniowych	23%	6%	4	47%	17%
Korzystanie z forów internetowych	30%	6%	5	33%	24%
Średnia	**32%**	**6%**	**7.4**	**36%**	**26%**

Tabela 4. Źródło: Brackenbury, Wong, 2012

Jak wcześniej wspominano, badanie przeprowadzone było na ankietowanych w 5 krajach – Kanadzie, Niemczech, Irlandii, Hiszpanii i USA. Analiza odpowiedzi pozwala zauważyć znaczące różnice kulturowe. Przykładowo – stosunkowo niewielu badanych dorosłych ze Stanów Zjednoczonych przywiązuje dużą lub bardzo dużą wagę do swojej internetowej reputacji (49%, przy np. 69% wskazań przez badanych z Hiszpanii), natomiast aż 15% z nich nie podjęło żadnych kroków, aby kontrolować swój profil *online* (średnia w badaniu to 5%). Jednocześnie dorośli Amerykanie najrzadziej zgłaszali pozytywny lub negatywny wpływ Sieci na ich realne życie. Wydaje się to sprzeczne z obrazem Stanów Zjednoczonych jako kraju innowacji, Doliny Krzemowej, jednego z najbardziej rozwiniętych technologicznie krajów świata. Przykład USA jest bardzo ciekawy również dlatego, że tamtejsi *digital natives* prezentują całkowicie przeciwne stanowisko niż ich rodzice. Wraz z niższym wiekiem znaczenie Internetu i jego wpływ na życie osobiste młodych użytkowników silnie wzrasta i jest najwyższy wśród badanych krajów.

5. BADANIE POSTAW DOTYCZĄCYCH PRYWATNOŚCI UŻYTKOWNIKÓW MEDIÓW SPOŁECZNYCH

5.1. Projekt i założenia badania

5.1.1. Wstęp

Celem badania przeprowadzonego w ramach niniejszej pracy, było sprawdzenie, jak aktywni użytkownicy Internetu, w szczególności mediów społecznych, traktują kwestie zamieszczania informacji osobistych w Sieci. Do szerokiego pojęcia *informacji osobistych* zaliczono, tak jak w całej pracy, nie tylko dane osobowe, ale również opinie, informacje o upodobaniach, aktywnościach *online* (np. odwiedzanych stronach internetowych) i *offline* (np. fizycznej lokalizacji, udziału w wydarzeniach) oraz materiały multimedialne tj. fotografie czy filmy dotyczące badanych.

Autor spróbował również odkryć, w jaki sposób badani internauci interpretują znaczenia ukryte za trudnymi do określenia terminami: prywatności i informacji prywatnych, zwłaszcza w kontekście Internetu i mediów społecznych. Zbadano stopień świadomości dotyczącej publicznej dostępności informacji osobistych dla pozostałych użytkowników Internetu oraz postrzeganego wpływu, jaki internetowy wizerunek badanych może mieć na ich życie poza Siecią.

W badaniu poruszona została również kwestia motywacji, która prowadzi do zwiększania lub ograniczania dostępności informacji prywatnych, zarówno ich szerokości (czyli zakresu), jak i głębokości (czyli stopnia intymności, zob. sekcję *1.1.2. Rozwój teorii Alana Westina i Irwina Altmana*). Podjęto próbę rozpoznania

deklarowanych postaw oraz faktycznych zwyczajów publikowania prywatnych treści w Sieci. W świetle przedstawionych w niniejszej pracy teorii oraz badań spodziewano się, że przynajmniej część badanych zadeklaruje obawy związane z możliwym naruszeniem ich prywatności, ale jednocześnie nie potrafi lub nie chce zadbać o *integralność kontekstową* informacji prywatnych (zob. sekcję *1.1.5.1. Prywatność jako integralność kontekstowa informacji*).

Badanie zostało przeprowadzono w trzech etapach. Pierwszy etap to ankieta, w której zidentyfikowano aktywnych użytkowników Internetu wśród studentów. W drugim, zasadniczym etapie badania, przeprowadzono pogłębione wywiady indywidualne z dwunastoma osobami z grupy wyselekcjonowanej w pierwszym etapie. Trzeci etap to próba weryfikacji faktycznej dostępności danych prywatnych w Internecie osób, z którymi przeprowadzono wywiady, a także skonfrontowanie otrzymanych wyników z informacjami uzyskanymi w trakcie wywiadów.

5.1.2. Grupa badanych

Badanie zostało przeprowadzone wśród studentów pierwszego roku studiów stacjonarnych i niestacjonarnych Instytutu Informacji Naukowej i Studiów Bibliologicznych Uniwersytetu Warszawskiego. Fakt niedawnego rozpoczęcia studiów przez badanych pozwala ograniczyć wpływ specyficznego wykształcenia, związanego z zarządzaniem informacją. Studenci studiów niestacjonarnych są zazwyczaj starsi od słuchaczy studiów dziennych, częściej też pracują, co ma dwojakie konsekwencje. Po pierwsze, autor założył, że kompetencje w dziedzinie obsługi mediów społecznych mogą w ich przypadku być niższe od kompetencji młodszych studentów studiów dziennych, którzy wzrastali w otoczeniu komputerów i technik informacyjno-komunikacyjnych (*digital natives*). Po drugie, wraz z wiekiem oraz faktem rozpoczęcia pracy zawodowej, zazwyczaj wzrasta dbałość o własny wizerunek oraz bardziej ceniona jest prywatność. Oparcie się w badaniu na dwóch, różnych pod wieloma względami grupach studentów, miało umożliwić zróżnicowanie grupy badanych oraz zidentyfikowanie ewentualnych różnic zależnych od wspomnianych czynników.

5.1.3. Ograniczenia badania

Ze względu na jakościowy charakter badania, jego wyniki nie umożliwiają generalizacji wniosków na szerszą zbiorowość, jak również na pełną charakterystykę badanej grupy. Celem przedstawionego tu materiału jest możliwie dokładne opi-

sanie i skategoryzowanie różnych postaw i zachowań dotyczących prywatności w mediach społecznych.

5.1.4. Pytania badawcze

W badaniu postawiono szereg pytań badawczych:

1. Jak badani rozumieją prywatność?
2. Czy prywatność w Internecie znaczy dla nich co innego niż prywatność ogólnie?
3. Jakie funkcje spełnia dla badanych prywatność?
4. W jaki sposób badani korzystają ze stron internetowych umożliwiających zamieszczanie treści, w tym:
   4.1. Jakie i jak wiele treści zamieszczają?
   4.2. W jakim stopniu ograniczają dostęp do informacji o sobie w Internecie?
   4.3. Czemu zamieszczają w Internecie informacje o sobie oraz własne opinie i komentarze?
5. Czy badani znają zasady polityki prywatności serwisów internetowych, z których korzystają oraz czy rozumieją sposoby wykorzystania ich informacji prywatnych (np. dla optymalizacji wyników wyszukiwania, wyświetlania spersonalizowanych reklam)?
6. Jaki stosunek mają badani do kontrowersyjnych tematów związanych z prywatnością? Poruszone tematy to: personalizacja reklam, wykorzystanie mediów społecznych w procesach rekrutacyjnych, stanowisko *radykalnej transparencji* oraz polityczne inicjatywy zmierzające do wprowadzenia zakazu anonimowego łączenia się z Internetem?

5.2. Etap I – ankieta

5.2.1. Metodologia

W pierwszym etapie badania przeprowadzono ankietę, której celem było wyłonienie grupy aktywnych użytkowników Internetu wśród badanych studentów. Sama ankieta nie przedstawia dużej wartości dla podstawowych zagadnień badawczych. Ze względu na możliwość przybliżenia charakterystyki badanej grupy wyniki zostały zaprezentowane i omówione w dalszej części pracy.

Kwestionariusze zostały rozdane studentom podczas zajęć, na których spodziewano się najwyższej frekwencji – obowiązkowe ćwiczenia. Na studiach stacjonarnych były to dwie grupy studentów, na niestacjonarnych – jedna. Na zajęcia

w każdej z grup zapisanych było około 30 studentów, faktycznie uczestniczyło w nich o kilka osób mniej. W sumie zebrano 81 wypełnionych kwestionariuszy. Dane zostały ręcznie wprowadzone do arkusza kalkulacyjnego, gdzie zostały poddane analizie.

Poza pytaniami metrykalnymi, które pozwoliły na ogólne opisanie grupy studentów pierwszego roku studiów (wiek, płeć, obecny poziom wykształcenia, miejsce zamieszkania, zatrudnienie), pytania kwestionariusza dotyczyły:

1. Częstotliwości korzystania z Internetu.
2. Sposobów łączenia się z Internetem.
3. Stażu internetowego.
4. Częstotliwości i sposobów korzystania z:
   a) wyszukiwarek internetowych,
   b) poczty e-mail,
   c) for internetowych (grup dyskusyjnych),
   d) portali informacyjnych,
   e) blogów i mikroblogów,
   f) portali społecznościowych,
   g) innych serwisów internetowych umożliwiających publikowanie treści (np. filmowych, fotograficznych czy przeznaczonych do prezentowania opinii i recenzowania).

Sposoby korzystania z usług i portali internetowych zostały tak opisane, aby możliwe było późniejsze przeanalizowanie ich ze względu na kryterium publikowania treści tworzonych przez użytkownika, czyli aktywności. Aktywne sposoby korzystania z Internetu, wymagają utworzenia lub przetwarzania treści oraz ich opublikowania, np. prowadzenie bloga, zamieszczanie fotografii w portalu społecznościowym czy też komentowanie artykułów w portalu informacyjnym. Do pasywnych sposobów korzystania z Sieci zaliczono konsumpcję mediów społecznych (przeglądanie portali społecznościowych, oglądanie materiałów multimedialnych na stronach typu YouTube), ale także korzystanie z wyszukiwarek internetowych czy poczty e-mail. Wysyłanie e-maili również polega na tworzeniu treści, które jednak pozostają formą komunikacji prywatnej.

We wszystkich pytaniach o częstotliwość korzystano z jednolitej, pięciostopniowej skali Likerta o następujących wartościach:

1) wcale,
2) okazjonalnie (kilka razy w roku),
3) rzadko (kilka razy w miesiącu),

4) często (kilka razy w tygodniu),
5) codziennie.

Odpowiedzi na te pytania zostały przekonwertowane na wartości liczbowe (wcale = 1, codziennie = 5), celem obliczenia średnich arytmetycznych i odchyleń standardowych (dalej stosowana jest abrewiacja SD, ang. *standard deviation*). Brak odpowiedzi na pytanie nie był uwzględniany w obliczeniach.

W celu uproszczenia analizy otrzymanych wyników kilkukrotnie korzystano z grupowania odpowiedzi. W przypadku pytań o częstotliwość używania poszczególnych portali internetowych łącznie omówiono odpowiedzi *okazjonalnie* i *rzadko* (rozumiane odpowiednio jako kilka razy w roku lub kilka razy w miesiącu) oraz *często* i *codziennie* (rozumiane odpowiednio jako kilka razy w tygodniu lub częściej). W kwestionariuszu zostały one zaproponowane oddzielnie, aby dać ankietowanym możliwość wyboru, jednak przy analizie ankiety rozróżnienie to zwykle nie miało większego znaczenia. Od tej zasady odstąpiono w niektórych przypadkach, np. gdy obie odpowiedzi występowały w danym pytaniu często lub zauważono korelację z odpowiedziami na inne pytanie lub pytania.

Zgrupowano również wyniki dla pytań metrykalnych dotyczących:

- Wieku: zgrupowano kategorie wiekowe *35–45 lat* i *ponad 45 lat*. Wśród badanych były tylko 2 osoby, które wybrały najwyższą kategorię wiekową, zastosowano więc wspólną kategorię *ponad 35 lat*.
- Miejsca zamieszkania: zgrupowano odpowiedzi *wieś* i *miasto do 10 tysięcy mieszkańców*. Powód jest analogiczny jak powyżej, jedynie 3 osoby zaznaczyły odpowiedź *miasto do 10 tysięcy mieszkańców* w pytaniu o miejsce zamieszkania.
- Stażu internetowego: zgrupowano odpowiedzi *nie dłużej niż 1 rok*, *od 1–2 lat* i *od 2–5 lat*, w związku z czym powstały tylko dwie kategorie – *krócej niż 5 lat* i *ponad 5 lat*. Jedynie 4 respondentów korzysta z Internetu krócej niż 2 lata, dlatego nieuzasadnione jest analizowanie każdego przypadku oddzielnie.

5.2.2. Wyniki ankiety

Zdecydowana większość badanych korzysta z Internetu kilka razy w tygodniu lub częściej. Tylko 3% ankietowanych odpowiedziało inaczej, a jedna osoba stwierdziła, że nie korzysta z Internetu wcale. Badani studenci studiów niestacjonarnych korzystają z Internetu nieco rzadziej niż studenci studiów dziennych. Łączących się z Siecią codziennie w pierwszej grupie jest 61%, a w drugiej aż 88% pytanych. Dla wszystkich badanych odsetek ten wyniósł 80%. Ponadto przeprowadzone badania wykazały, że kobiety z tej grupy korzystają z Internetu nieco rzadziej niż

mężczyźni – 78% kobiet i 88% mężczyzn korzysta z Internetu codziennie. Wśród badanych, którzy mieszkają na wsiach i w małych miasteczkach, zauważono wyraźnie mniejszy odsetek osób korzystających z Internetu codziennie – 60%.

Większość badanych korzysta z Internetu od dłuższego czasu – aż 95% dłużej niż 2 lata, a blisko 68% dłużej niż 5 lat. Wszystkie osoby, które zadeklarowały krótszy okres korzystania z Internetu, są w najniższej kategorii wiekowej (do 24 lat). Po raz kolejny mężczyźni deklarują nieco większe doświadczenie internetowe, blisko 88% z nich korzysta z Internetu dłużej niż 5 lat, przy 68% kobiet w tej kategorii.

Poczta elektroniczna i wyszukiwarki internetowe okazały się najczęstszymi zastosowaniami, do jakich badani wykorzystują Internet. Kilka razy w tygodniu lub częściej korzysta z nich odpowiednio 86% i aż 98% badanych. Poczta elektroniczna jest nieznacznie częściej używana przez kobiety (60% codziennie, przy 50% mężczyzn). Również wśród osób pracujących częstotliwość korzystania z poczty elektronicznej jest o kilka punktów procentowych wyższa niż w przypadku niezatrudnionych, jednak badanie nie wykazało istotnej zależności pomiędzy wykorzystaniem poczty elektronicznej, a łączeniem się z Internetem z miejsca zatrudnienia. Częstsze korzystanie z poczty e-mail nie jest zatem bezpośrednio związane z wykonywaną pracą.

Komunikatory internetowe cieszą się wśród badanych mniejszą popularnością niż poczta elektroniczna, jednak blisko 50% badanych korzysta z nich codziennie lub prawie codziennie. Najczęściej aktywność tę deklarują najmłodsi badani: w grupie do 24 lat komunikatory internetowe są narzędziem codziennego użytku dla 31% badanych, natomiast w grupie ponad 35 lat zaledwie dla 8%.

Portale informacyjne są czytane kilka razy w tygodniu lub częściej przez 66% badanych, nieco częściej przez mieszkańców dużych (ponad 50 tys. mieszkańców) i największych (ponad 200 tys.) miast. Mniejszą popularnością cieszą się komentarze. Wśród badanych nie było osoby, która zamieszczałaby swoje opinie na portalach informacyjnych codziennie, jedynie 6% ogółu robiło to kilka razy w tygodniu, a aż 43% – wcale. Dodatkowo żaden z badanych mężczyzn nie zadeklarował komentowania artykułów częściej niż kilka razy w miesiącu.

Blogi cieszą się mniejszą popularnością wśród badanych niż portale informacyjne, zaledwie 5% przegląda je codziennie. Kilka razy w tygodniu blogi są odwiedzane przez około 10% badanych. Połowa badanych mężczyzn nie odwiedza blogów w ogóle, przy 31% kobiet (ogółem 35% badanych). Pozostała połowa respondentów odwiedza blogosferę kilka do kilkunastu razy w roku. Co może być zaskakujące, ankieta pokazuje, że najmniejszy odsetek osób nieczytających blogów jest wśród osób starszych (35 lat i więcej) – jedynie 7,5%, podczas gdy

wśród młodszych ankietowanych aż 40% nie jest zainteresowana ich czytaniem. Blogi i mikroblogi są medium, z którego chętnie korzystają młodzi. Prawdopodobnie wiek nie jest najważniejszym czynnikiem wpływającym na czytelnictwo blogów – bardziej może wpływać na nie na przykład rodzaj wykonywanej pracy czy zainteresowania (blogi specjalistyczne). Blisko dwie trzecie badanych nigdy nie komentuje blogowych wpisów, częściej ten sposób wypowiadania się wybierają mężczyźni niż kobiety. Jedynie 6 badanych prowadzi własnego bloga – pięć kobiet i jeden mężczyzna, wszyscy w wieku do 34 lat.

Jeszcze mniej badanych korzysta z mikroblogów – 9% korzysta z nich kilka razy w tygodniu lub częściej, natomiast aż 70% nie zagląda na serwisy typu Twitter w ogóle. Ten typ komunikacji w Internecie najmniej przemawia do badanych w wieku 25–34 lat. Tak jak w przypadku blogów, najniższy odsetek osób z nich niekorzystających odnotowano w kategorii wiekowej ponad 35 lat, około 62%. Siedem osób badanych, tj. blisko 9%, prowadzi własnego mikrobloga, z różną częstotliwością. Tylko dwoje badanych prowadzi zarówno bloga, jak i mikrobloga.

Analiza wykorzystania portali społecznościowych pokazuje duże zainteresowanie tym medium. Tylko 6% nie korzysta z nich w ogóle, natomiast codziennie lub kilka razy w tygodniu przegląda je 73% badanych. Nieco większy odsetek kobiet niż mężczyzn czyni to codziennie, jak również młodzi nieco częściej niż starsi, a niezatrudnieni częściej niż pracujący. Dwie ostatnie zależności dotyczą również komentowania aktywności innych na portalach społecznościowych, jednak ogólny odsetek komentujących jest niższy: 20% badanych nigdy nie zamieszcza swoich opinii, 33% czyni to kilka do kilkunastu razy do roku, częściej – 46% ankietowanych. Odsetek mężczyzn, którzy niechętnie dyskutują, korzystając z portali społecznościowych, jest wyraźnie wyższy niż kobiet – 31% badanych mężczyzn i 17% kobiet nigdy nie zamieszcza komentarzy do publikowanych treści. Ciekawie prezentują się odpowiedzi na pytanie dotyczące publikowania własnych treści w sieciach społecznościowych. Wynika z nich, że badani z niewiele niższą częstotliwością publikują niż komentują – 21% nie czyni tego w ogóle, około 38% kilka razy w tygodniu i częściej. W przypadku mężczyzn ten ostatni odsetek wynosi 50%. Jest to aktywność zdecydowanie najbardziej powszechna wśród badanych w wieku 18–24 lat. Codziennie różnego rodzaju materiały w sieciach społecznościowych publikuje 17% najmłodszych badanych, natomiast wśród pozostałych kategorii wiekowych nie było ani jednej takiej odpowiedzi.

Portale pozwalające zamieszczać materiały fotograficzne lub wideo są chętnie przeglądane wśród badanych. Ponad 60% czyni to codziennie lub kilka razy w ty-

godniu, przy 5% ankietowanych niekorzystających z nich w ogóle. Nie znalazła się też ani jedna osoba, która zamieszczałaby swoje treści codziennie, co wydaje się zrozumiałe ze względu na czas i wysiłek potrzebny do ich przygotowania. Niecałe 10% deklaruje umieszczanie własnych plików kilka razy w tygodniu, 38% od czasu do czasu, natomiast nieco ponad połowa nigdy nie zamieszcza własnych materiałów fotograficznych czy wideo na przeznaczonych do tego portalach. Postawa ta jest wyraźnie związana z płcią, 31% mężczyzn przy niecałych 56% kobiet nigdy nie korzysta z możliwości publikowania na portalach typu YouTube czy Flickr. Podobną odpowiedź częściej udzielały osoby w wieku ponad 35 lat niż młodsi badani.

Kolejne pytanie kwestionariusza odnoszące się do częstotliwości wykorzystania portali internetowych, dotyczyło dość szeroko rozumianej kategorii pozostałych portali pozwalających na przeglądanie i zamieszczanie ocen, recenzji oraz rekomendacji, czy to dotyczących handlu elektronicznego czy wytworów kultury takich jak książki, filmy i muzyka. Niemal 24% badanych korzysta z tego typu portali kilka razy w tygodniu lub codziennie, około 21% zaś nigdy. Cieszą się one większą popularnością wśród mężczyzn, młodszych badanych oraz wśród osób mieszkających w dużych miastach.

Ostatnie pytanie zawierało dwa stwierdzenia, a badanych poproszono o wybranie z pięcioelementowej skali stopnia, w jakim się z nimi zgadzają. Pierwsze brzmiało: *Moja prywatność i mój wizerunek w Internecie są dla mnie ważne*. Blisko 61% badanych odpowiedziało *zdecydowanie tak*, a niemal 30% *raczej tak*. Na drugim biegunie skali znalazła się tylko jedna odpowiedź – *zdecydowanie nie*. Pozostałe 11% osób zaznaczyło odpowiedź na środku skali *nie mam zdania*. Średnia wszystkich odpowiedzi, przy założeniu, że *zdecydowanie tak* = 5, a *zdecydowanie nie* = 1, wyniosła 4,5 (SD = 0,74). Prywatność i wizerunek w Internecie jako bardzo ważną wybierały nieco częściej kobiety niż mężczyźni oraz osoby w wieku ponad 25 lat niż młodsze. Ujawniła się również zależność pomiędzy odpowiedzią na to pytanie, a doświadczeniem internetowym – wśród osób korzystających z Internetu dłużej niż 5 lat ponad 64% deklarowało najwyższą zgodność ze stwierdzeniem przy 53% osób z internetowym stażem krótszym niż 5 lat.

Drugie stwierdzenie brzmiało *Posiadam pełną kontrolę nad informacjami dotyczącymi mojej osoby, jakie znajdują się w Internecie*. Średnia odpowiedzi dla tego pytania wyniosła 3,7. Rozbieżność odpowiedzi okazała się nieco większa – SD wyniosło 1,09. Odpowiedzi *raczej nie* lub *zdecydowanie nie* udzieliło 16% badanych (w porównaniu do 1,2% analogicznych odpowiedzi przy poprzednim stwierdzeniu). I tutaj ciekawą zmienną niezależną jest czas, w którym badana osoba korzysta z Internetu: osoby z długim stażem rzadziej udzielały odpowiedzi ze środka

skali – 6% zaznaczyło odpowiedź *nie mam zdania*, w stosunku do 17% mniej doświadczonych internautów. Osoby korzystające z Internetu dłużej niż 5 lat częściej odpowiadały negatywnie – niecałe 22%, przy 4,5% podobnych odpowiedzi w grupie osób krótszym stażem.

Jeden z badanych, którego obie odpowiedzi o zgodność ze stwierdzeniami brzmiały *zdecydowanie tak*, ręcznie dopisał: „Mój wizerunek ani faktyczne nazwisko nie istnieją w Internecie", sugerując w ten sposób nie tylko wyjątkową ostrożność w podawaniu informacji osobistych w Internecie, ale także systematyczną kontrolę, czy ktoś inny nie zamieścił ich bez jego zgody. Co ciekawe, osoba ta w pytaniu o miejsce zatrudnienia podała „tworzenie stron internetowych (freelancing)". Osobom pracującym w ten sposób może zależeć na promocji oraz tworzeniu własnej marki w Internecie i pozyskiwaniu w ten sposób zleceniodawców. Z drugiej strony, jako internauta prawdopodobnie o wysokich kompetencjach technicznych, osoba ta może lepiej zdawać sobie sprawę z zagrożeń, jakie niesie utrata kontroli nad informacjami osobistymi w Internecie i z tego powodu bardziej zabiegać o ich bezpieczeństwo.

W związku z drugim etapem badania polegającym na przeprowadzeniu wywiadów z wybranymi respondentami, aktywnymi internautami, kwestionariusz ankiety został zakończony prośbą o pozostawienie swoich danych kontaktowych. Wyraźnie zaznaczono, że podanie tych informacji jest nieobowiązkowe i zostaną one wykorzystane jedynie w celu nawiązania kontaktu z badanym i ustalenia terminu spotkania. Prawie 41% badanych zdecydowało się pozostawić adres e-mail lub numer telefonu, a tym samym wyraziło zgodę na drugi etap badania. Wśród studentów studiów niestacjonarnych było to zaledwie około 17%, przy 50% studentów studiów dziennych. Tę rozbieżność można interpretować różnicami w rozkładzie zajęć obu programów studiów – na studiach niestacjonarnych zajęcia odbywają się raz na dwa tygodnie i trwają zwykle od rana do wieczora, z bardzo krótkimi przerwami między zajęciami. Studenci studiów dziennych mają mniej napięty harmonogram, często również tzw. *okienka*, czyli przerwy między zajęciami trwające jedną czy dwie godziny wykładowe. Poza tym wielu studentów studiów niestacjonarnych mieszka poza Warszawą i odwiedza ją jedynie w terminach zjazdów, co utrudnia zorganizowanie wywiadu. Wyraźnie wyższy odsetek osób, które nie pozostawiły swoich danych kontaktowych, jest również wśród osób pracujących niż niezatrudnionych – odpowiednio 73% i 60%. Z otrzymanych danych trudno wyczytać zależność pomiędzy deklarowanym stopniem dbałości o prywatność, a pozostawieniem danych do kontaktu. Około 30% osób, dla których prywatność jest ważna lub bardzo waż-

na zdecydowało się zapisać na kwestionariuszu swój adres e-mail bądź numer telefonu kontaktowego. W przypadku osób, które wybrały odpowiedź *nie mam zdania* proporcja wzrasta do 2/3, jednak mała liczba badanych nie pozwala na wnioskowanie (4 z 6 osób).

Osoby prowadzące bloga w pytaniach dotyczących wagi prywatności w ich życiu oraz postrzeganej kontroli nad własnymi danymi, udzielały odpowiedzi świadczących o przywiązywaniu mniejszej wagi do prywatności (średnio 4,20, to o 0,27 mniej niż ogół) oraz mniejszej kontroli nad osobistymi informacjami w Internecie (3,20, o 0,54 mniej niż ogół). Co ciekawe, wśród osób prowadzących mikroblogi tendencje są przeciwne – prawie wszyscy stwierdzili, że prywatność jest bardzo ważna (średnia 4,86) oraz zadeklarowali wysoki stopień kontroli nad informacjami o nich w Internecie (średnio 4,29).

5.3. Etap II – pogłębione wywiady indywidualne

5.3.1. Metodologia

Zasadniczym etapem badania były wywiady z osobami wyselekcjonowanymi z grupy ankietowanych. Ze względu na eksploracyjny charakter badania wykorzystano metodę pogłębionego wywiadu swobodnego ze standaryzowaną listą poszukiwanych informacji. Celem było przede wszystkim obudzenie w respondentach chęci opowiedzenia o własnych doświadczeniach i przemyśleniach oraz uzyskanie odpowiedzi na określone wcześniej, ogólne pytania badawcze. Przygotowano listę poszukiwanych, która stanowiła pobieżny scenariusz wywiadu oraz miała ułatwić kategoryzację i porównanie otrzymanych odpowiedzi.

Uczestnicy badania zostali wybrani spośród ankietowanych, którzy pozostawili dane kontaktowe i zadeklarowali się jako osoby aktywnie korzystające z opisanych w kwestionariuszu usług internetowych. Przyjętym kryterium do oceny aktywności była średnia odpowiedzi dotyczących działalności w Internecie, które wymagają publikacji. Średnia wyliczana była przy założeniu, że odpowiedź *codziennie* ma wartość 5, a odpowiedź *wcale* ma wartość 1. Jako minimalną wartość przyjęto 2,0. Przy takim kryterium liczba osób, z którymi można było przeprowadzić wywiady, wyniosła 21. Wszystkie osoby otrzymały wiadomość e-mail o tej samej treści, z prośbą o propozycję terminu i miejsca wywiadu.

Ostatecznie autorowi udało się przeprowadzić wywiady z dwunastoma osobami. Jeden adres e-mail okazał się niepoprawny, a pozostałe osoby nie zdecydowały się odpowiedzieć na wiadomość z zaproszeniem do wywiadu.

Początkowym założeniem było przeprowadzenie wywiadów z taką samą liczbą osób na studiach niestacjonarnych i stacjonarnych, ale nie udało się go zrealizować. W pierwszym etapie badania wzięła udział znacznie mniejsza liczba studentów ze studiów niestacjonarnych (23 osoby) niż stacjonarnych (58 osób). Tylko cztery osoby ze studiów zaocznych zostawiły w ankiecie dane kontaktowe, a dodatkowo dwie z nich zadeklarowały bardzo niską częstotliwość korzystania z Internetu i mediów społecznych. Z dwóch osób, którym wysłano wiadomość e-mail z prośbą o spotkanie, odpowiedziała tylko jedna.

Jeden wywiad został przeprowadzony przez Internet, z użyciem aplikacji do rozmów wideo, pozostałe osobiście. Najkrótszy wywiad trwał około 25 minut, najdłuższy niemal półtorej godziny.

5.3.2. Etyka badania

Dane kontaktowe zawarte w kwestionariuszu zostały wykorzystane tylko do ustalenia terminu wywiadu, a po zakończeniu badania usunięte. Wywiady zostały nagrane na dyktafon cyfrowy, o czym badani zostali poinformowani przy umawianiu się na spotkanie oraz, ponownie, przed rozpoczęciem wywiadu. Nagrania posłużyły do opracowania wywiadów i nie zostaną opublikowane ze względu na prywatność badanych. Badani zostali zapewnieni o anonimowości ich wypowiedzi w opracowaniu badania – w pracy nie znajdują się żadne informacje, które mogłyby pozwolić na ich identyfikację. Badani poproszeni zostali również o zgodę na realizację kolejnego etapu badania, w którym przeprowadzona miała być analiza możliwości pozyskania informacji o badanych za pomocą ogólnodostępnych narzędzi internetowych i porównaniu ich z deklaracjami z wywiadu. Wszyscy uczestnicy badania zgodzili się na nagranie rozmowy oraz na przeprowadzenie trzeciego etapu badania.

5.3.3. Omówienie wyników

Przytoczone w niniejszym omówieniu fragmenty wywiadów wyróżnione są kursywą, a ewentualne dopiski autora są zamieszczone w nawiasach kwadratowych. W miejscach, w których przytoczono więcej niż jedną wypowiedź uczestników badania, każdy akapit jest fragmentem innego wywiadu.

5.3.3.1. Definiowanie i funkcje prywatności

Na początku wywiadu badani zostali zapytani o to, czym jest dla nich prywatność i czy wcześniej zastanawiali się nad tym zagadnieniem.

Wszyscy badani odpowiedzieli, że temat prywatności jest przez nich przemyślany. Dla wielu inspiracją były wydarzenia z ich życia:

> Miałem w liceum zajęcia dotyczące bezpieczeństwa i prawa w Internecie. Zajęcia zorganizowano po śmiesznej historii, ktoś założył mojej nauczycielce od języka polskiego profil na Facebooku. Na profilu nie było nic obraźliwego, ani żadnych epitetów (…). To było raczej zabawne niż obraźliwe, ale rozumiem, że [nauczycielka] mogła się [źle] poczuć.

Wśród uczestników badania znalazły się również osoby, dla których prywatność jest tematem poważnych przemyśleń od dłuższego czasu:

> Najbardziej interesuje mnie, jakie informacje udostępniam o sobie i ile z tego, co jest w Internecie zostanie na później. Gdy zdecyduję się usunąć jakieś informacje, to czy będę w stanie to zrobić.

> Od dawna interesowało mnie mocno to, jak dużo o nas wiedzą rodzice, jak dużo o nas wie państwo, jak dużo wiedzą o nas osoby, które pracują w różnych instytucjach i zbierają dane. W momencie, kiedy pojawia się Internet, te zagrożenia i myślenie stają się bardziej konkretne i namacalne – sami możemy wygooglać [przyp. autora – tzn. wyszukać w Google] różne dane.

Zgodnie z oczekiwaniami wszyscy respondenci odpowiedzieli na pytanie o to, czym jest prywatność, opisując swoje indywidualne, intuicyjne rozumienie prywatności, które zazwyczaj nie wyczerpywało wszystkich aspektów tego zjawiska, ale nie odbiegało również znacznie od przedstawionych w rozdziale 1.1. definicji.

Badani określali prywatność najczęściej jako **strefę**, do której dostęp dla innych osób mogą sami regulować.

> To strefa, o której nie chcemy, żeby inni wiedzieli, nie jest dostępna dla wszystkich.

> Prywatność to dla mnie taka sfera, w której ja decyduję, czy ktoś ma do niej wgląd czy nie.

Są takie sfery mojego życia, prywatnego, bardzo osobistego, czy też związanego z nie taką zupełnie osobistą sferą, ale z moją pracą, moją rodziną, o których nie chciałabym, żeby informacje wyciekały gdzieś szerzej.

Dla mnie to sfera, której nie chcę upubliczniać, chcę mieć pełną kontrolę nad tym, czy pewne informacje zdradzam jednej osobie, kilku lub pewnemu gronu, ale nie wyrażam zgody na to, aby była to informacja publiczna.

Chyba każdy człowiek ma swoją sferę prywatną, zupełnie osobistą, do której nie wpuszcza nikogo z zewnątrz. To jest przeznaczone tylko dla mnie i dla najbliższego grona znajomych, bliskich.

Niektórzy określali też prywatność poprzez metaforę **granicy**, której położenie regulują:

Myślę, że prywatność to taka granica, którą każdy sam ustala, a za nią jest właśnie prywatność. W zależności od różnych sytuacji, albo się pozwala przesuwać tę granicę albo nie.

Ograniczenia innych w stosunku do mnie. Granica, której inni nie mogą przekroczyć.

Inni – jako **kontrolę** nad własnymi informacjami osobistymi:

Nie ujawnianie zbyt wiele o sobie. To możliwość zachowania [się] w związkach [z innymi ludźmi] na dystans, zachowania dla siebie takich informacji, które uważa się za stosowne.

Jedna z odpowiedzi nawiązała do konceptu prywatności jako **autonomii osobistej** zaproponowanego przez Alana Westina (zob. sekcję *1.1.4. Wymiary prywatności*):

To, że ktoś nie wcina mi się w moje prywatne sprawy, nie ingeruje w to, co myślę, ani w to, co robię.

Wydaje się, że wszyscy badani uważali, że prywatność nie jest równoznaczna z trzymaniem informacji w tajemnicy. Jeden z badanych wprost zwrócił uwagę na rozgraniczenie pojęć prywatności i intymności:

To informacje dotyczące mnie, które odróżniają mnie od innych ludzi i mogę się nimi dzielić. Rozgraniczam prywatność i intymność. Nie traktuję prywatności jako czegoś, co jest moje, tylko moje, zamknięte dla innych.

Kolejna osoba zaproponowała szeroką definicję prywatności jako **życia osobistego**:

Ja traktuję prywatność jako swoje życie osobiste. To, co się dzieje poza pracą, poza szkołą, poza studiami, moje relacje z innymi ludźmi, to jest dla mnie prywatność.

Ta sama osoba, wypowiadając się o danych osobowych, informacjach gromadzonych i przetwarzanych przez rządy, firmy czy organizacje, w tym operatorów stron internetowych, powiedziała:

Na pewno niejedna firma ma teraz moje dane osobowe, a ja nie mam pewności, co ona z nimi teraz zrobi, jak je wykorzysta. W pewien sposób to jest jakaś prywatność, tylko że taka czysto formalna, podstawowa.

Rozdzielanie ochrony prywatności instytucjonalnej i społecznej jest zauważane przez nauki społeczne (boyd, 2008; Raynes-Goldie, 2010) i nazwane **społecznym kontekstem prywatności**. Zagadnienie zostało opisane w rozdziale *2.4. Media społeczne – problemy z prywatnością*.

Zupełnie przeciwne rozumienie prywatności zaprezentował kolejny badany. Jako jedyny traktował prywatność jako **mechanizm fizycznego bezpieczeństwa**, który pozwala zachować poufne informacje przed osobami niezaufanymi:

Tu jest ta granica, którą można przekroczyć, pomiędzy tym, co możesz udostępnić, a ile już nie powinieneś.(…) Rodzice uczulili mnie na tę kwestię. Tłumaczyli mi to na prostym przykładzie – wyobraź sobie, że siedzisz sobie na Gronie i piszesz o tym, że dostałeś od rodziców nowy rower. I teraz jak złodziej zobaczy na tym Gronie „o, temu kupili nowy rower" i ma Twój adres zamieszkania, imię nazwisko, kod pocztowy, wszystko. I w tym momencie przychodzisz, a roweru nie ma.

5.3.3.2. Pozbywanie się prywatności i całkowita z niej rezygnacja

Wyniki przeprowadzonej ankiety, po ograniczeniu ich do grupy osób, z którymi przeprowadzono wywiady, wskazały, że wszystkie te osoby uważają prywat-

ność za cenne dobro, z którego nie przychodzi im łatwo rezygnować (średnia 4,58 w pięciostopniowej skali Likerta). Podczas wywiadu w odpowiedzi na podobnie zadane pytanie jak w ankiecie, badani ponownie zadeklarowali wysoki stopień dbałości o własną prywatność.

Bardzo interesujące są przypadki dwóch badanych, którzy ze względu na swoją działalność hobbystyczną lub zawodową, zamieszczają dość dużo informacji o sobie na ogólnodostępnych stronach w Internecie:

> Mimo że interesuję się prywatnością, to wcale dużo jej nie mam i jest to moja decyzja. Większość czynności, które wykonuję aktualnie, jest skierowana do szerokiej grupy osób. To, co kiedyś było dla mnie prywatne, teraz jest bardzo publiczne – przestałem przejmować się ochroną pewnych informacji o mnie. (…) Ryzykuję oczywiście w ten sposób, że ktoś, poszukując informacji o mojej osobie, tych zawodowych, trafi na informacje, które są czysto prywatne. Nie jest tak łatwo rozdzielić komunikację prywatną i publiczną [w Internecie].

> Może to kwestia tego, co ja w życiu robię – jestem przewodnikiem turystycznym. Prowadzę zatem działalność częściowo publiczną, dane o mnie muszą być ogólnie dostępne. Część moich danych prywatnych jest dostępna w Internecie i nie mam problemu, aby dzielić się nimi z innymi ludźmi.

Publicznie dostępne informacje o tych osobach to imię i nazwisko, zdjęcie, adres e-mail oraz numer prywatnego telefonu komórkowego. W pierwszym wypadku dodatkowo dostępne są informacje na profesjonalnym blogu badanego (w tym miejsce zatrudnienia), w drugim – notatka o podróżniczych dokonaniach na stronie organizacji przewodników turystycznych.

Dla tych badanych prywatność jest ważna, ale badani potrafią z niej rezygnować w imię realizacji swoich ambicji, osiągnięcia korzyści, np. rozwoju zawodowego:

> Ja rezygnuję z prywatności po to, aby można mnie było łatwo odnaleźć i dzięki temu podnoszę swoją renomę i uzyskuję więcej zleceń.

Pozostali badani potrafili bez trudu podać sytuacje, w których utrata prywatności przynosi pożytek. Wymieniali odległe przykłady dotyczące życia gwiazd, programów typu reality show.

Ale także realne, codzienne przykłady jak np.: **kreowanie własnego wizerunku**:

Jeżeli ja odpowiednio przedstawię się na portalu społecznościowym, wyselekcjonuję dobre zdjęcia, podam podkoloryzowane, być może po części fałszywe informacje, to ktoś może mnie odebrać zupełnie inaczej i być może później, np. przy szukaniu pracy, będzie mi łatwiej.

Ułatwione **nawiązywanie i utrzymywanie kontaktu**:

Jeżeli zamykam się w sobie, jestem nieaktywna, to nie zyskuję interakcji z innymi.

I związane z nimi możliwość **rozwoju zainteresowań** i pomysłów:

Generalnie, aby dołączyć do grupy o konkretnych zainteresowaniach, trzeba najpierw ujawnić swoje zainteresowania, żeby znaleźć grono osób, które podobnymi rzeczami się interesują.

Jeżeli dzielę się swoimi ideami, to inne osoby mogą pomóc mi je rozwinąć o nową wizję czy pomysł.

Dzielenie się własną prywatnością opisywano jako **transakcję wymienną**, w dwóch wariantach.

1. Firma-klient:

Jeśli na Facebooku są różnego rodzaju konkursy z nagrodami, to często wymaga się podania jakichś danych prywatnych.

Jeżeli mam się zarejestrować [na stronie internetowej] i podać swoje dane osobowe, to zastanawiam się czy korzyści, które wyniosę z tego serwisu są wystarczające.

2. Człowiek-człowiek:

To transakcja wymienna, coś-za-coś. Jeżeli odsłaniam się całkowicie przed kimś, to mam nadzieję, że ta druga strona podobnie się zachowa, czyli czegoś od niej chcę. Taki handel wymienny.

Jeżeli ja staję się bardziej otwarta i więcej mówię o sobie, to to samo zyskuję z powrotem.

Jedna z badanych dodała kolejny argument, że **prywatność instytucjonalna** nie zawsze jest traktowana przez młodych ludzi jako istotny element ich prywatności:

> Podawanie danych osobowych to nie jest rezygnacja z prywatności. Tak samo programy lojalnościowe – to oczywiste, jak inaczej można [z nich] skorzystać. Zawsze jest wybór, co można podać. A jak się nie chce podawać to nie trzeba korzystać. (…) Gromadzenie danych [przez firmy] to bardzo użyteczna sprawa – dzięki temu marketingowcy mogą bardziej dostosować produkty do moich potrzeb.

Wszyscy badani zdecydowanie **nie zgodzili się ze stanowiskiem radykalnej transparencji** (zob. sekcję *1.2. Krytyka prawa do prywatności*), które zostało zaprezentowane stwierdzeniem: *Jeżeli ktoś jest człowiekiem bez żadnej skazy i nie ma nic do ukrycia, to prywatność nie jest mu potrzebna*. Większość uznała, że prywatność jest potrzebna każdemu człowiekowi:

> Każdy człowiek, bez względu na to, czy ma jakieś grzeszki, czy ich nie ma, czy jest osobą kryształowo czystą, czy coś ma na sumieniu, to potrzebuje takiej przestrzeni tylko i wyłącznie dla siebie.

Dwie osoby zwróciły uwagę na to, że **informacje, które są łatwo dostępne, tracą swoją wartość**:

> Nie chodzi o to, czy się wstydzisz swoich wad i zachowań, tylko są pewne rzeczy, nawet fajne o tobie, które chcesz zachować dla siebie. (…) Jak są super fajne rzeczy, które mi się przydarzają, to nie mam ochoty ich wszystkim opowiadać. Wydaje mi się wtedy, że sama je trochę tracę.

> Myślę, że to jest kwestia tego, że kiedy mamy dostęp do wszystkiego, to tego nie szanujemy. Jeżeli wszyscy mają dostęp do tego, co ty nazywasz swoją prywatnością, to te informacje strasznie się trywializują.

Jedna osoba zauważyła, że radykalna transparencja prowadzi do **bezpieczeństwa**, ale mimo to nie może być zastosowana do najbardziej osobistych informacji:

> Upubliczniając wszystko, też możemy czuć się bezpiecznie – jeżeli wszyscy wszystko o nas wiedzą, to nic się nie ukryje, a nasze życie jest bardziej transparentne

i mniej podatne na ataki z zewnątrz. Ale gdy mówimy z drugą osobą emocjach, to musi to być prywatne. To ważne, aby w takiej komunikacji obie strony czuły się bezpiecznie, wiedząc, że nikt nie będzie w to ingerował.

Jeden z badanych skojarzył pytanie z niskim stopniem prawnej ochrony prywatności w Stanach Zjednoczonych:

Kojarzy mi się system amerykański – jedyne, co się liczy, to numer ubezpieczenia. Oni są w stanie opisać całe Twoje życie, wszystko, co robiłeś, po tym twoim numerze. W Polsce jest ustawa o ochronie danych osobowych, a tam nie ma. Nie rozumiem, jak oni mogą tak żyć i funkcjonować.

Jedna badana zauważyła, że największy problem związany ze stanowiskiem radykalnej transparencji dotyczy **niejednorodnej publiczności** (zob. sekcję *2.4.1. Niejednorodna publiczność*):

Każdy ma jakieś wady, poza tym wszystkie cechy mogą być odbierane w różny sposób – np. bogate życie towarzyskie może być plusem dla znajomych, ale wadą dla szefa.

5.3.3.3. Funkcje prywatności

Badani zostali zapytani o funkcję, jaką pełni w ich życiu prywatność. Większość udzieliła podobnych odpowiedzi dotyczących poczucia bezpieczeństwa, komfortu i siły związanych z posiadaniem kontroli:

Czuję się lepiej, tj. bezpieczniej, zdrowiej, jeżeli czuję, że pewne informacje są całkowicie w mojej kontroli.

Dla dobrego samopoczucia, aby czuć się komfortowo.

Można się czuć bezpieczniej. Jak nie udostępniasz swoich danych, to trudniej Cię „wyhaczyć" [czyli znaleźć czuły punkt].

Myślę, że jeżeli człowiek ma prywatność, to jest silniejszy. Jeżeli opowiadamy wszystkie swoje prywatne rzeczy, to później ktoś może nas w bardzo łatwy sposób zaskoczyć, wyciągnąć [coś], czego byśmy nie chcieli. Myślę, że im więcej zachowujemy dla siebie, tym mamy większą kontrolę.

Następnie badani zostali poproszeni o uszeregowanie pięciu funkcji prywatności opracowanych przez Westina (1967) i Pedersena (1997) (zob. sekcję *1.1.2. Rozwój teorii Alana Westina i Irwina Altmana*). Użyte w badaniu funkcje prywatności to:

- **Autonomia osobista**: ułatwia uniknięcie zdominowania czy zmanipulowania.
- **Ulga emocjonalna**: odpoczynek od napięć życia społecznego, ról, wymagań.
- **Samoocena**: umożliwia eksperymentowanie i odkrywanie własnego Ja oraz ukrywanie przed innymi niepożądanych jego części.
- **Ograniczona i chroniona komunikacja**: ustala granice interpersonalne oraz pozwala zachować informacje osobiste wyłącznie dla osób zaufanych.
- **Kreatywność**: pozwala na popełnianie błędów, angażowanie się w kreatywne doświadczenia, rozwój idei oraz rozwiązywanie problemów.

Większość badanych bez problemu zrozumiała opis wszystkich funkcji i zgodziła się, że prywatność w ich życiu faktycznie wypełniają opisane role. Niektórzy badani mieli problem z określeniem ich dokładnej kolejności:

> To wszystko jest tak powiązane, że ciężko mi określić kolejność. Co pięć sekund mogłabym to zmieniać. Jakbyś spytał za godzinę, to byłoby odwrotnie. Jestem na takim etapie, że wszystko jest dla mnie na pierwszym miejscu.

> Wszystkie 5 wydaje mi się bardzo trafnych, tzn. trzy bardzo, dwie – odrobinę dla mnie mniej istotnych.

Większość badanych za dwie najważniejsze funkcje prywatności uznała **ograniczoną i chronioną komunikację** (średnia pozycja 1,91 – 6 razy wskazana jako najważniejsza) oraz **autonomię osobistą** (średnia pozycja również 1,91 – 4 wskazania jako najważniejsza). Ulga emocjonalna została wskazana jako trzecia (średnia 3,27), samoocena – czwarta (średnia 3,45). Najmniej ważną funkcją prywatności jest dla badanych kreatywność (średnia 4,45 – 7 wskazań jako najmniej ważna).

Jeden z badanych zaproponował **rozszerzenie katalogu funkcji prywatności**:

> Dodałbym kolejną funkcję – ochrona komunikacji działających za pomocą technologii. Np. tego, czy jesteśmy w miarę pewni, czy ktoś nie podsłuchuje naszego telefonu, albo nasze maile są odpowiednio chronione.

Jedna badana powiedziała, że funkcja *ulga emocjonalna* nie jest według niej związana z prywatnością.

5.3.3.4. Zarządzanie prywatnością w Internecie

Badani zostali zapytani, czy w ich odczuciu kontrola przepływu informacji prywatnych jest w Internecie łatwiejsza, czy trudniejsza niż w rzeczywistości. Większość uczestników badania uważa, że zarządzanie prywatnością w Internecie jest znacznie trudniejsze. Jedni zwracali uwagę na **możliwość utraty kontroli nad prywatnymi informacjami**, głównie ze względu na niemal nieograniczoną możliwość kopiowania i rozpowszechnienia informacji w Internecie:

> Gdy jedna osoba będzie miała dostęp do naszych danych, to może ją rozpowszechnić dalej w ciągu kilku sekund, kilku minut, w świecie rzeczywistym jest dużo trudniej.

> Dużo trudniejsza. Bo gdy ktoś wrzuci film na YT, gdzie leżysz zalany w trupa i nic nie zrobisz. Możesz poprosić osobę, która go zamieściła o usunięcie, ale czasem może to przynieść efekt odwrotny od zamierzeń. W rzeczywistości [offline] jest dużo węższy krąg odbiorców niż w Internecie.

> To jest haczyk Internetu – tobie się wydaje, że masz kontrolę nad tym przekazem, a tu raz coś poszło i już zupełnie tracisz kontrolę. To jest właśnie złudne, że coś wrzucasz i myślisz, że będziesz miał [nad tym] kontrolę (…) a może to być wykorzystane w różny sposób.

W drugim z powyższych cytatów badany wspomina o tzw. efekcie Streisand. W Internecie często okazuje się, że próby cenzurowania lub usuwania informacji nie tylko są nieskuteczne, ale wręcz przynoszą efekt przeciwny od zamierzonego. Rozgłos towarzyszący próbie zatuszowania niechcianych informacji powoduje, że internauci masowo starają się zapewnić, aby były one łatwo dostępne. Sprzyjają temu łatwość kopiowania i rozpowszechniania informacji w Internecie, możliwość tworzenia niezliczonej ilości *mirrorów*, czyli kopii przygotowywanych w celu zapewnienia alternatywnego dostępu do zasobów, czy udostępnianie plików w rozproszonych SieciachP2P (ang. *peer-to-peer*). Nazwa zjawiska pochodzi od nazwiska Barbary Streisand, która wytoczyła proces przeciwko ekologicznemu aktywiście, który w ramach środowiskowego projektu, opisującego erozję kalifornijskiego wybrzeża, zamieścił w Internecie fotografie przedstawiające rezydencję Streisand widzianą z lotu ptaka. Aktorka, chcąc chronić własną prywatność, nieumyślnie sprawiła, że fotografię zobaczyły miliony internautów (Greenberg, 2007).

Większość badanych zwracała uwagę na fakt, że nie możemy w pełni kontrolować **publikacji innych osób**, zwłaszcza w porównaniu do rzeczywistości fizycznej.

Generalnie [w Internecie] nie mamy kontroli – każdy może o nas coś napisać lub zamieścić. Nie da się go całego obejrzeć, aby zobaczyć, czy coś o nas zamieszczono czy nie, więc z definicji prywatność w Internecie jest niekontrolowana.

W Internecie nie ma za bardzo jak się bronić. Tak, myślę, że w życiu realnym jest łatwiej kontrolować swoje dane prywatne. W życiu realnym jesteś 100% w nim, natomiast w Internecie, jesteś tylko w kilku kilkunastu procentach – to może zostać zagarnięte przez pozostałe osoby.

W dobie Internetu potrzebujemy dużo więcej kompetencji i inwencji, aby zachować swoją prywatność […] Wiem, że inni mogą wpływać na nasz wizerunek w Internecie i to jest znacznie trudniejsze w kontrolowaniu. Wszystko, co robię w rzeczywistości, może być zdigitalizowane i wykorzystane przeciwko mnie. Możemy kontrolować siebie, ale nie możemy kontrolować pozostałych 7 miliardów osób na świecie.

Badani zwracali także uwagę na **trwałość danych zamieszczanych w Internecie**:

Internet robi publicznym dla każdego i na wieki to, co niekoniecznie chciałbym, aby było publiczne. Nawet jeżeli jest chronione technicznie, nawet, jeżeli w praktyce daną treść zobaczy niewiele osób, to potencjalnie może to zobaczyć każdy i teraz i w odległej przyszłości.

Najbardziej się boję tego jak będzie, gdy umrę, co wtedy zostanie. Czy będą wtedy jakieś wielkie repozytoria wiedzy, w których będzie można się dowiedzieć o mnie wszystkiego?

Tak. Obawiam się, że jak usunę konto w portalu społecznościowym, to te dane pozostaną na serwerach – mimo że mam święte prawo do usunięcia własnych danych, to nie jestem pewna czy tak się stanie.

Jedna z badanych życzyłaby sobie, aby w Internecie obowiązywało ***prawo do bycia zapomnianym*** (zob. sekcję *3.1.1. Polityki prywatności*):

Chciałabym, żeby informacje, które zamieszczam, po jakimś czasie traciły swoją ważność – i ja powinnam o tym decydować.

Dwójka badanych wskazała na brak skutecznych i łatwych narzędzi do rozwiązania **problemu niejednorodności audytorium**:

> Ja jestem taki heavy user i dużo informacji z mojego życia prywatnego jest zamieszczonych w Internecie. (…) Na Facebooku mam 500 kontaktów, z czego 30 jest z jednej pracy, 30 z drugiej, 15 z projektu, 50 z byłej szkoły, 100 znajomych z uczelni. Nad tym nie da się zapanować i te granice pomiędzy pracą, szkołą się zacierają. Co z tego, że podzielę ich sobie na grupy, jak nagle się okazuje, że stary znajomy z podstawówki nagle pracuje w tym samym zawodzie i spotkamy się na gruncie profesjonalnym.

> Coraz trudniej jest zachować swoją prywatność, korzystając z portali społecznościowych. (…) Chciałabym rozdzielić swoje profile prywatne i zawodowe, ale to nie jest takie łatwe. Bardzo mało młodych ludzi ma konta na portalach profesjonalnych, tylko na Facebooku.

Jedna z badanych uważała przeciwnie niż większość, że **zarządzanie prywatnością w Internecie jest łatwiejsze niż w rzeczywistości**. Ta osoba deklarowała bardzo intensywne korzystanie z sieci społecznościowych oraz bardzo wysoki stopień wykorzystania zaawansowanych funkcji prywatności:

> Łatwiej. Ja jestem bardziej świadoma. W Internecie można wszystko zdefiniować, są ustawienia prywatności. Twoja świadomość tego, co robisz – jak komentujemy to wiemy, że może dotrzeć to do wielu osób (…) Moje dane prywatne są widoczne tylko dla zdefiniowanych osób. (…) Pozostałe kwestie, te, nad którymi nie mogę zapanować, dla mnie się nie liczą.

5.3.3.5. Obawy – publikowanie przez osoby trzecie

Badanych zapytano, czy obawiają się, że inne osoby, mogą zamieścić w Internecie ich dane prywatne lub nieprawdziwe, krzywdzące informacje na ich temat oraz czy jedna z tych sytuacji już się im przydarzyła.

Zaobserwowano dwie główne postawy. Po pierwsze, **brak obaw**. Badani najczęściej opowiadali o zaufanym gronie znajomych, na których mogą liczyć:

> Nie obawiam się (…). Przynajmniej z tego względu, że ludzie, a przynajmniej najbliższy krąg moich znajomych, ludzi, z którymi łączą mnie bliskie powiązania towa-

rzyskie, koleżeńskie układy, to raczej nie są tacy ludzie, którzy by mogli jakieś niepochlebne opinie wrzucać na mój temat.

Nie… jeżeli ktoś publikuje o mnie informacje, to są to moi znajomi, ale mam nad tym kontrole – widzę, gdy jestem oznaczona na zdjęciach. Nigdy nie musiałam poprosić ich o usunięcie zdjęć, zwykle przed zamieszczeniem konsultują ze mną ten fakt.

Trochę te zagrożenia traktuję mniej poważnie. Gdyby ktoś oczerniał mnie w realu, twarzą w twarz, albo pisemnie… ciągle traktuję życie realne bardziej poważnie, jak prawdziwe życie, a Internet trochę tak jakby na niby życie. Więc nawet gdyby ktoś się pode mnie podszywał to uważałabym to za mniej ważne niż takie prawdziwe.

Po drugie, **pasywny fatalizm**, czyli postawa, którą można wyrazić zdaniem: nie mogę obawiać się czegoś, co jest poza moją kontrolą.

Nie przeszkadza mi to – oczywiście, że taka sytuacja może się zdarzyć, ale jako że jest to całkowicie poza moją kontrolą, to nic w związku z tym nie robię.

Nie mam takich obaw. Zawsze jest ryzyko, że moje dane zostaną ujawnione, na zasadzie np. sprzedaży danych osobowych, ja nad tym nie panuje. Nie martwię się też tym, że hackerzy włamią się do portalu społecznościowego i ukradną moje dane, bo to jest całkowicie poza moją kontrolą.

Może być tak, że jakaś zupełnie obca osoba może, widząc mnie na jakimś zdjęciu, napisać coś niemiłego czy niepochlebnego na mój temat. Ale to już jest w zasadzie niezależne ode mnie.

Kilkoro badanych próbowało **aktywnie wyszukiwać**, a czasem także **kontrolować** informacje pojawiające się w Internecie na ich temat, np. za pomocą wyszukiwarek internetowych:

Wiem o tym, obawiam się i staram się kontrolować czy ktoś nie napisał o mnie nic niepochlebnego (…). Czasami wyszukuję moje imię i nazwisko w wyszukiwarce.

Wpisuje w wyszukiwarkę na Facebooku swoje imię i nazwisko i po prostu przeglądam. Nie spotkałam się z fikcyjnymi kontami odnośnie mojej osoby. Robię to po prostu z ciekawości.

Próbowałam wyszukiwać informacje o sobie w Internecie i odnoszę wrażenie, że z jednej strony jest ich dosyć mało, ale z drugiej czuję, że nie mam pełnej kontroli np. nad tym, jakie moje zdjęcia się tam pojawiają.

W Internecie są moje błędne dane osobowe – do mojego imienia i nazwiska są przypisane błędne informacje. (…) [Od momentu, gdy się o tym dowiedziałam] zaczęłam skanować wyszukiwarki pod kątem możliwości odnalezienia mojego imienia i nazwiska. Przejrzałam, napisałam wiadomości do tych ludzi, którzy mogliby zmienić te informacje – w kilku miejscach sprostowali tę informacje, ale nie wszędzie.

Drugim sposobem na realizację kontroli jest korzystanie z wbudowanych w portale społecznościowe funkcji informowania o (oznaczeniu) publikowanym zdjęciu, aktualności itp. W przypadku oznaczenia przez innego użytkownika, ten otrzymuje powiadomienie o przypisaniu jego profilu do opublikowanego obiektu. Zależnie od ustawień prywatności, oznaczenie może również wymagać potwierdzenia przez oznaczonego użytkownika lub też nie.

Jeżeli ktoś publikuje o mnie informacje, to są to moi znajomi, ale mam nad tym kontrolę – widzę, gdy jestem oznaczona na zdjęciach.

Kontrola tagowania bywa jednak dla badanych **kłopotliwa towarzysko**:

Strasznie nie lubię, gdy ktoś mnie oznacza na Facebooku. Wiem, że można to „zdjąć", ale potem sobie myślę, że to można odebrać, jako coś niemiłego… i nie wiem, co można z tym zrobić.

Mniej więcej połowa badanych stwierdziła, że zdarzyły się w ich życiu sytuacje, w których ich **prywatność została naruszona z powodu Internetu**. Najczęściej były to drobne naruszenia związane z zamieszczaniem informacji o badanych przez inne osoby. Po ich reakcji były one kasowanie przez osoby, które je opublikowały, lub administrację portalu społecznościowego:

Zdarzyło mi się, że ktoś udostępnił moje prywatne informacje w portalu społecznościowym. Zgłosiłam ten fakt administracji portalu, zaznaczyłam, że to z powodu naruszenia prywatności i samo było to potem przez administratorów usunięte – to było zdjęcie. Ono mnie nie kompromitowało, ale po prostu nie chciałam. Oczywiście, chciałam się skontaktować z osobą, która zamieściła to zdjęcie, ale nie było reakcji.

Moja koleżanka napisała w komentarzu do jakiegoś zdjęcia informacje, które wysłałem jej wcześniej w SMS-ie i nie miała ich nikomu innemu przekazać. (…) Innym razem koleżanka wrzuciła zdjęcie, w którym nie wyglądałam zbyt korzystnie. Uważam, że powinnam mieć możliwość samodzielnego usunięcia takich treści.

Kilka razy poprosiłem [znajomych] o usunięcie mojego zdjęcia, ale to drobiazgi.

Z drugiej strony jedna z badanych opowiedziała, jak **informacje o jej dłuższej nieobecności, które zamieściła w Internecie, mogły doprowadzić do obrabowania jej domu**:

Jakiś czas temu okradziono mój dom, w czasie, gdy ja byłam na wakacjach. Zamieściłam taką informację jako status komunikatora internetowego i wydaje mi się, że jest to powiązane. Od tamtej pory staram się nie informować o miejscu swojego pobytu.

5.3.3.6. Obawy – techniczne bezpieczeństwo informacji

Wielu badanych, odpowiadając na pytania o obawy związane z zagrożeniami dla ich prywatności, odpowiadała, że najbardziej boi się o **bezpieczeństwo bankowości elektronicznej**.

Zdecydowana większość badanych korzysta z programu antywirusowego, (np. firewall, programy antyspamowe, programy szyfrujące) natomiast nie wszyscy badani wiedzieli, czym są inne programy zabezpieczające ich komputery i w związku z tym deklarowali, że z nich nie korzystają lub o tym przynajmniej nie wiedzą. Zwłaszcza programy typu firewall czy antyspamowe potrafią czasem pracować na tyle niezauważalnie, że użytkownik komputera może nie wiedzieć, czy ma taki program zainstalowany na komputerze, czy nie. Ponadto do oprogramowania antyspamowego należałoby też wliczyć filtry antyspamowe, z których korzystają usługi e-mailowe w chmurze, np. popularny Gmail.

Badani charakteryzowali się szerokim przekrojem zachowań dotyczących usuwania historii przeglądania – część nigdy tego nie robi, nawet korzystając z komputerów publicznych (w bibliotece czy na uczelni).

Badani korzystają z haseł o różnym stopniu skomplikowania. Większość stwierdziła, że ustanawia raczej trudne do rozszyfrowania kombinacje. Stopień skomplikowania haseł nie wydaje się zależny od kompetencji informatycznych i internetowych. Tylko jedna osoba, deklarująca bardzo wysokie umiejętności techniczne,

korzystała z programu do zarządzania hasłami z wbudowanym generatorem losowych haseł. Ta sama osoba stwierdziła również:

> Mnie się wydaje, że zabezpieczenia techniczne służą nie ochronie mojej prywatności, ale bezpieczeństwa i integralności moich danych. (…) Włamanie na moje konto bankowe czy wykradzenie danych z komputera to prawie, że fizyczna krzywda.

Wyjątkiem była jedna z badanych, która deklarowała się jako mało aktywny użytkownik Internetu i komputerów, stwierdzając, że zabezpieczanie się poprzez używanie trudnych haseł prowadzi do odwrotnego niż zamierzony skutku:

> Staram się używać jak najprostszych haseł. Jeżeli ktoś by się rzeczywiście zastanowił, to przypuszczam, że wpadłby na to, jakie jest hasło wprowadzone. Generalnie ludzie wychodzą z założenia, że kodując pewne rzeczy staramy się jak najbardziej zakryć zakamuflować, a te najprostsze rzeczy najbardziej się sprawdzają. Mam znajomego, który swoją pocztę opatrzył najróżniejszymi zabezpieczeniami, a już dwa razy się zdarzyło, że ktoś, mimo tych zabezpieczeń, włamał mu się na pocztę i ją wyczyścił.

5.3.3.7. Opinie – obowiązek korzystania z prawdziwej tożsamości

Podczas wywiadu zapytano, co badani sądzą o następującym pomyśle: do połączenia z Internetem wymagana jest autoryzacja prawdziwym imieniem i nazwiskiem. Pytanie było zainspirowane pomysłem walki z cyberterroryzmem, zaproponowanym podczas szczytu G8 w 2011 roku przez ówczesnego prezydenta Francji – Nicholasa Sarkozy (Mackenzie, 2011).

Większość respondentów **nie wierzyła w skuteczność** takiego systemu jako rozwiązania problemu cyfrowej przestępczości, a jedynie uciążliwe, technicznie i psychologicznie, dla zwykłych użytkowników:

> Byłoby to nadużyciem kontroli społeczeństwa. Z jednej strony to dobrze wiedzieć więcej o przestępcach, ale z drugiej strony czułabym się nieco ograniczona, osobiście bym się z tym czuła źle.

> Załóżmy, że mój tata poda swoje [prawdziwe imię i nazwisko], bo prowadzi firmę i to mu to będzie potrzebne, chociażby do logowania się na konto. Albo moja mama. Właśnie takie osoby. A inni będą potrafili to obejść, nawet nie przestępcy, ale na przykład młodzież.

Niektórzy badani nie zgodziliby się na takie rozwiązanie, uważając je za próbę wprowadzenia **cenzury**, a nawet za niebezpieczne zbliżenie się do korzystania z metod charakterystycznych dla **totalitaryzmu**:

> Taki pomysł wynika z bezradności władz w walce z przestępczością. A po drugie po to, żeby kontrolować zwartość zamieszczaną w Internecie. Uważam, że bardzo mocno ograniczyłoby to kreatywność internautów.

> Zawsze jest niebezpieczeństwo, że strona kontrolująca może pójść za daleko i stworzyć państwo totalitarne, w którym państwo kontroluje całe życie swoich obywateli.

Dwoje badanych uważało, że nawet **obecnie nie można korzystać z Internetu w anonimowy sposób**:

> Mnie osobiście nie przeszkadzałoby to, że każdy mój ruch w Internecie jest śledzony – już tak przecież jest! To nie jest spoko, w ogóle nie jest to spoko, ale jeżeli zgadzasz się korzystanie z Internetu to zgadzasz się i z kontrolą. Nie protestowałabym, ale robiąc różne rzeczy w Internecie pamiętałabym o tym, że ta kontrola istnieje.

> Przecież i teraz nie można. Jeżeli ktoś jest przestępcą i popełnia przestępstwo w Internecie to i tak go znajdą. Co do samego pomysłu – podoba mi się taki pomysł. Ja nie mam szacunku dla ludzi, którzy nie mają odwagi podpisać się swoim imieniem i nazwiskiem. Jak ktoś się anonimowo wypowiada, to albo się tego wstydzi albo jest tchórzem.

5.3.3.8. Opinie – wykorzystanie mediów społecznych przez pracodawców i rekruterów

Badani zostali poproszeni o wypowiedź na temat wykorzystania informacji zdobytych w mediach społecznych w procesach rekrutacyjnych. Zdecydowana większość osób uważa za całkowicie naturalne, że rekruterzy korzystają z portali społecznościowych, aby lepiej poznać kandydatów. Dla większości nie miał znaczenia fakt, że w procesach selekcji pracowników używane są także portale nieskoncentrowane na biznesie, ale ogólne (jak Facebook czy Nasza-Klasa). Głównym argumentem była **odpowiedzialność ludzi za zamieszczane przez nich informacje w Internecie**:

Moim zdaniem jest to etyczne zachowanie, ludzie głównie sami wrzucają informacje o sobie i powinni się liczyć z tym, że mogą zostać wykorzystane przez pracodawców.

Pracodawca musi wiedzieć, kogo zatrudnia, a przecież zawsze możemy kontrolować, przynajmniej w pewnym stopniu, informacje, które są o nas dostępne – wiemy, jakie zdjęcie wstawiliśmy, jakie zaznaczyliśmy poglądy polityczne. Jeżeli te informacje o nas są dostępne publicznie, nie widzę problemu.

Tak, jak najbardziej. To świadczy o człowieku, jeżeli ja umieszczam jakieś zdjęcia, które mogłyby mnie kompromitować, to świadczy tylko i wyłącznie o mnie. Później to może się jakoś przejawić w pracy. Ja jestem za, ja bym sprawdzała wszystkich.

Ma prawo – sami jesteśmy odpowiedzialni i to nasza sprawa, aby dbać o swój wizerunek w Internecie.

Trójka badanych uważała inaczej. Główny argument, który podawali przeciwko, to **brak możliwości przełożenia informacji zdobytych o kandydacie na portalu społecznościowym na jego przydatność w przyszłej pracy**.

Te informacje, które są w portalach społecznościowych o tobie, jakiekolwiek by one nie były (obraźliwe, ekshibicjonistyczne) – nie będą nigdy zrozumiałe dla ludzi z zewnątrz ze względu na swój lokalny charakter. Inne rzeczy z kolei po prostu nie powinny być brane pod uwagę na serio, w kontekście zawodowym.

Nie myślę, że nie. Chociaż ludzie często odkrywają się zupełnie i wtedy można wielu rzeczy dowiedzieć się o takim kandydacie. Czy to jest etyczne… no nie wiem… jeżeli człowiek gdzieś zaczyna pracę, to kim on naprawdę jest i co może zaoferować, zostaje szybko zweryfikowane. Chociaż niektórzy pracodawcy zabezpieczają się w ten sposób. Można też przecież pojawić się na zdjęciu zamieszczonym przez kogoś innego. Jeżeli pracodawca chce, to przecież może sprawdzać potencjalnego pracownika, ale czy to jest etyczne – myślę, że nie do końca.

To raczej śliska sprawa. Rozumiem pracodawcę, który chce sprawdzić przyszłego pracownika. Ale z drugiej strony pracodawca ma możliwości, aby sprawdzić pracownika – poprzez rozmowę, CV itd. Jeśli za pomocą tych narzędzi nie potrafi zweryfikować czy osoba się nadaje, czy nie… Nie, to jest faktycznie naganne.

5.3.3.9. Polityki prywatności i ustawienia prywatności

Mniej więcej dla połowy badanych termin polityki prywatności nie był całkowicie zrozumiały. Część z nich myliła go z ustawieniami prywatności profilu, a część po prostu nie zdawała sobie sprawy, że taka nazwa jest używana na zapisy regulaminu portalu społecznościowego dotyczące kwestii przetwarzania informacji prywatnych.

Jeden badany przyznał, że aktywnie **śledzi polityki prywatności** trzech portali społecznościowych, z których intensywnie korzysta (Facebook, YouTube i Google+), i jego zdaniem niepokojące fragmenty **polityki prywatności są napisane niejasno**:

> Myślę, że język używany w regulaminach jest niekonsekwentny. Z jednej strony pełny banałów, które nic nie mówią, ale są zrozumiałe przez laika, a z drugiej strony zawiły sposób opisania, co bardziej kontrowersyjnych przepisów. Poza tym brakuje części konkretnych wpisów – np. o rodzajach zabezpieczeń. Kolejną niepokojąca kwestią jest to, że warunki mogą być zmienione – wystarczy zmiana na minutę i wtedy skopiować nasze dane.

Druga osoba, która przegląda polityki prywatności w używanych serwisach społecznościowych, również zwróciła uwagę na **konieczność uproszczenia zapisów polityki prywatności**:

> Tak, szukam zwykle w tych umowach takich punktów, w których określa się czy moje dane będą przekazywane innym firmom. (…) [Ich] język jest średnio zrozumiały. Na przykład można się skupić na wyszukaniu jednej informacji, natomiast żeby przeczytać cały regulamin – to jest ciężko. Myślę, że fajnie by było gdyby zastosowano system podobny jak w licencjach Creative Commons, żeby było znaczki oznaczające poszczególne rozwiązania i opisane takim językiem potocznym, a jakiś taki tam drobny druczek prawniczy żeby był osobno.

Najczęstszą odpowiedzią było stwierdzenie, że **pomimo nieprzeczytania regulaminów badani prawdopodobnie wiedzą, co się w nich znajduje**:

> Mniej więcej wiem, na co się zgadzam. Czytałam informacje, gdy FB wprowadzał zmiany, także czuję się poinformowana.

Większość badanych zainteresowała się i przynajmniej w pewnym stopniu **dostosowała ustawienia prywatności profilu w portalach społecznościowych**.

> Dopasowałam je do swoich preferencji, nawet dostosowuję je do poszczególnych osób i grup znajomych. Mam różne grupy znajomych, między innymi instytucje i miejsca, jako dodane jako osoby, interesują mnie ich aktualności np. jaka jest impreza w klubie, ale nie chce żeby oni mogli oglądać moje zdjęcia.

Trójka badanych wykorzystuje **zaawansowane ustawienia prywatności**, tj. podział znajomych na grupy, dostosowanie widoczności różnego rodzaju treści dla różnych grup osób:

> Do publicznej wiadomości są moje imię i nazwisko i zdjęcie profilowe. Większość moich informacji na Facebooku jest widoczna dla moich znajomych lub tylko bliskich znajomych. Na portalu biznesowym widoczny jest cały profil.

> Na FB późno wprowadziłem podział na grupy i podzielenie kilkuset znajomych na grupy byłoby dość traumatyczne – mam grupę osób, które są zupełnie wykluczone z obserwowania tego co się u mnie dzieje – to kontakty zawodowe. Mam też grupę osób bardzo bliskich, których widzą znacznie więcej aktualizacji niż inni. Pozostałe grupy mają taki sam stopień dostępu, podzieliłem ich na różne konteksty, aby mieć łatwiejszy dostęp do takiej skategoryzowanej listy znajomych.

Jedna z tych trzech osób uważa, że **ustawienia prywatności nie zawsze działają zgodnie z intencją użytkownika**:

> Wydaje mi się, że ustawienia prywatności czasem „nawalają" – korzystam z list znajomych na czacie i nie powinnam widzieć statusów zablokowanych znajomych, a widzę. I zgaduję, że oni także mnie widzieli – choć nie powinni.

Badani nie byli zgodni, odpowiadając na pytania o widoczność możliwości zmiany ustawień prywatności oraz o łatwość zmiany tych ustawień. Nawet zaawansowani użytkownicy **narzekali na zbyt duży stopień skomplikowania ustawień prywatności** w portalu Facebook:

> To bardzo rozbudowany system, wielu osobom nie chce się „przeklinać" przez wszystkie ustawienia.

Zmiana i dostosowanie ustawień wydawały mi się zbyt skomplikowane żeby się w to angażować.

Jak ktoś nie jest zorientowany, to na pewno jest trudna. Czasem lepiej zorientowane osoby zamieszczają na Facebooku informacje jak lepiej chronić swój profil.

Łatwo trafić do ustawień prywatności, ale po przejściu do nich łatwo się zniechęcić i zgubić w gąszczu okienek.

Musiałam dłuższą chwilę poświęcić i nie jest to bardzo łatwe. Wolałabym, żeby przy dodawaniu nowej osoby do znajomych istniała możliwość ograniczenia widoczności moich rzeczy – wybrać, że widoczne jest dla niej lub niego to, to i to. Teraz samemu trzeba dochodzić do tego, że jest taka możliwość.

Pozostali badani uważali, że zmiana ustawień **jest łatwa, jednak wymaga od użytkownika nakładu pracy**:

Raczej łatwa, główny wymóg to wola, trzeba chcieć. Wystarczy chwilę pomyśleć i to zrobić.

5.3.3.10. Zachowania, publikowanie

Mimo poczucia kontroli, które dają ustawienia prywatności, żaden z badanych nie był w stanie odpowiedzieć precyzyjnie i pewnie na wszystkie pytania o dostępność informacji na swój temat w Internecie. Większość badanych potrafiła bez problemu odpowiedzieć negatywnie na pytania o tzw. dane sensytywne, np. poglądy polityczne, religijne, informacje o partnerze, a także dokładny adres zamieszkania. Jednak w przypadku mniej wrażliwych danych, np. ukończonych szkół, adresie e-mail, numerze telefonu, fotografiach, częściej badani bez wahania potrafili odpowiedzieć *tak, te informacje o mnie są dostępne w Internecie*, niż *nie*. Negatywna odpowiedź zawsze wiązała się z dłuższym zastanowieniem i często wyrażana była bez pewności.

Brak pełnej wiedzy o tym, co faktycznie dostępne jest o nas w Internecie, nie jest szczególnie zaskakujący: informacje prywatne były publikowane w różnym czasie, w różnych miejscach, dostępne zatem dla różnych grup ludzi. Ponadto jak pisałem wcześniej (np. sekcji *2.2. Strukturalne cechy Internetu*), informacje w wersji cyfrowej są długo przechowywane, mogą być łatwo skopiowane

i opublikowane na innej stronie internetowej – nawet bez wiedzy osoby, której dotyczą.

Wielu badanych korzystało w przeszłości z portali społecznościowych, na które już regularnie nie zagląda, ale niekoniecznie skasowało swój profil w tych portalach. W wielu przypadkach opuszczanym przez badanych był serwis Grono.net, a niektórzy mówili również o Naszej-Klasie. Większość użytkowników na początku swojej przygody z portalami społecznościowymi zamieszcza w nich bardzo dużo informacji prywatnych. To zjawisko zostało bardzo ciekawie opisane, zwłaszcza w kontekście starszych użytkowników mediów społecznych, przez jedną z badanych:

> Moja klasa z liceum spotkała się w zasadzie pierwszy raz po maturze, ponad 20 lat, w komplecie, tylko dzięki temu, że udało nam się odnaleźć przez Naszą-Klasę, potem nawiązać kontakty i rzeczywiście nastąpiło w realu spotkanie. I tak jak pamiętam, część osób bardzo mocno podchodziło do tego tak… nazwałabym to... bardzo dużo informacji na swój temat wrzucała. I to takich informacji o sytuacji finansowej, rodzinnej, czyli takie rzeczy, które wydaje mi się, nie powinny być dostępne dla wszystkich. Według moich standardów, ich prywatność została za bardzo wyeksponowana. Internet jest takim ciekawym narzędziem, że niektórym pewnie się wydaje, że można tam wrzucić wszystko i dostęp do tego będzie miała tylko wąska grupa ludzi. (…) To jest chyba taki generalny trend, że w pierwszym momencie, gdy zakładamy konto w portalu społecznościowym to wrzucamy wszystko, co się da, czyli i zdjęcie swoje, dzieci, męża, domek, samochód wakacje tu czy tam. Wszystko leci, w tym wszystkie dane personalne.

Nawet jeżeli po okresie bardzo dużego otwarcia na portale społecznościowe przychodzi refleksja nad zagadnieniem prywatności w Sieci, a wraz z nią wycofanie się, nie można mieć gwarancji, że dane zostały faktycznie skasowane lub dostęp do nich jest kontrolowany. Być może stąd bierze się trudność w udzieleniu odpowiedzi przez badanych.

Dwie osoby zwróciły w czasie wywiadu uwagę na **problem niechcianych znajomych** w portalach społecznościowych, czyli otrzymywania niepożądanych zaproszeń do sieci kontaktów lub też posiadanie w niej niechcianej osoby. Odrzucenie zaproszenia lub usunięcie osoby z sieci kontaktów może być odebrane negatywnie, analogicznie jak w rzeczywistości afrontem byłaby np. odmowa nawiązania konwersacji. Odrzucenie zaproszenia lub usunięcie osoby z sieci kontaktów zazwyczaj nie wiąże się w portalach społecznościowych z wysłaniem infor-

macji o tym fakcie, ale może zostać zauważone przez brak oznaczenia znajomości pomiędzy użytkownikami. Jedna osoba **korzysta z portali społecznościowych pod pseudonimem, aby uniknąć tego problemu**:

> Ukrywam się po to, żeby selekcjonować osoby, od których przyjmuję zaproszenia. Często głupio byłoby mi czasem odmówić, np. dlatego, że większość moich znajomych posiada tę osobę wśród swojego grona znajomych i wypadałoby, żebym ja też miała (np. chodziliśmy do podstawówki razem), ale nie chcę się dzielić z nimi tym, co tam umieszczam. Po prostu sama wolę wysyłać zaproszenia i w ten sposób regulować to, z kim jestem w relacji.

Inny badany mówił natomiast o **trudności z usunięciem niechcianych znajomych**:

> Mój znajomy narzekał na to, że dodał do znajomych takich ludzi, których teraz musi śledzić, nudzi go to, chciałbym odznaczyć, jako swoich znajomych, ale nie chce ich urazić. Jest różnica miedzy znajomym z życia codziennego, a takim znajomym z Sieci. Nie każdy znajomy prawdziwy musi być znajomym w Sieci.

Problem wynika często z różnych zachowań dotyczących rozszerzenia sieci kontaktów – niektórzy użytkownicy portali społecznościowych ostrożnie dobierają *znajomych*, podczas gdy inni wysyłają zaproszenia wszystkim, nawet pobieżnie znanym osobom. Użytkownicy **dostosowują zwykle własne zwyczaje publikowania do posiadanej grupy kontaktów**. Problem niechcianych znajomych utrudnia realizację obranej strategii rozszerzania sieci kontaktów (ang. *friending behaviour*, zob. sekcję *2.4.1. Niejednorodna publiczność*). Nasila się on, gdy użytkownik portalu społecznościowego stara się mieć niewielką liczbę zaufanych znajomych i chciałby utrzymywać z nimi bliskie relacje, używając portalu społecznościowego.

5.4. Etap III – weryfikacja

Podczas trzeciego etapu pracy autor postawił się w sytuacji osoby znającej jedynie podstawowe informacje o badanym – takie jak imię i nazwisko, wygląd oraz ogólną informację o miejscu zamieszkania lub aktywności. Następnie, za pomocą ogólnie dostępnych narzędzi i rozmaitych technik wyszukiwawczych, spróbował odnaleźć możliwie największą liczbę informacji o badanym w Internecie.

Celem badania była weryfikacja, czy istnieją rozbieżności pomiędzy deklaracjami badanych dotyczącymi stopnia zabezpieczenia informacji o nich, a faktycznym stanem ich dostępności. Ten etap badania odbywał się tuż po przeprowadzeniu wywiadu, najczęściej jeszcze tego samego, ale zawsze nie później niż następnego dnia. Ta metoda miała służyć ograniczeniu możliwego wpływu wywiadu na zachowanie badanych – wywiad mógł wpłynąć na postrzeganie ochrony informacji osobistych w Internecie i spowodować na przykład zmianę ustawień prywatności w portalach społecznościowych przez badanych.

W przypadku dwunastu badanych osób wszyscy, o których udało się odnaleźć informacje w Internecie, mieli pewne pojęcie o tym, jakie dane o nich dostępne są w Internecie i nie zdarzyło się, żeby to pojęcie było skrajnie niezgodne z prawdą. Tylko o jednej badanej osobie udało się w trakcie trzeciego etapu dowiedzieć więcej niż określiła w wywiadzie, ale nie były to informacje wrażliwe, czyli takie, które można by było wykorzystać przeciwko niej – były to wpisy na forum hobbistów grafiki.

Aż w czterech przypadkach nie udało się dotrzeć do żadnych danych dotyczących badanego. Wydaje się, że głównym powodem utrudniającym dotarcie do pożądanych informacji była popularna kombinacja imienia i nazwiska badanego. Znalezienie informacji na temat *Jana Kowalskiego* jest znacznie utrudnione z prozaicznego powodu – trudno odfiltrować wyniki i uzyskać oczekiwany rezultat wyszukiwania. Ten efekt potęguje jeszcze sytuacja, w której istnieją publicznie znane lub z innego powodu popularne w Internecie osoby o tym samym imieniu i nazwisku. Sytuacji nie poprawiały wyszukiwarki na portalach społecznościowych, które zwykle nie mają wbudowanych przydatnych funkcji wyszukiwawczych, np. nie pozwalają na zawężanie wyników według dynamicznych kryteriów, czy na użycie choćby prostych operatorów. Głównym i zwykle wystarczającym kryterium oceny relewantności wyników jest fakt posiadania *wspólnych znajomych* z wyszukiwaną osobą, a w następnej kolejności ich liczba. Wyszukiwarki ogólne oraz wyszukiwarki ludzi (np. 123People, Pipl) również nie ułatwiają odnalezienia konkretnych osób – trudno za ich pomocą wykorzystać dodatkowe informacje o badanym, np. miejsce zamieszkania, wiek czy wygląd, aby uzyskać rozsądne ilościowo i trafne wyniki wyszukiwania. Facebook umożliwia filtrowanie wyników według trzech kryteriów: miejsca zamieszkania, ukończonych szkół (wraz z możliwością podania roku jej ukończenia) oraz miejsca pracy. Filtrowanie wyników wyszukiwania według miejsca zamieszkania jest możliwe obecnie także w wyszukiwarce Pipl.

Prawdziwa jest również odwrotna zależność – bardzo szybko i skutecznie wyszukuje się informacje o osobach, które mają unikalną kombinację imienia

i nazwiska. To samo zjawisko wiąże się z wykorzystaniem oryginalnych pseudonimów. Dwukrotnie w trakcie badania autor odkrył wiele informacji o badanych przez następujący schemat: po odnalezieniu profilu w portalu społecznościowym, na którym podany był pseudonim badanego, to właśnie pseudonim, a nie imię, i nazwisko stało się kluczem do dalszych poszukiwań.

W pozostałych przypadkach zakres informacji dostępnych w Internecie o badanych był zbliżony do określonego podczas wywiadu. Stwierdzenie to jest istotne zwłaszcza dla osób, o których udało się znaleźć wiele informacji dostępnych publicznie w Internecie. Wszyscy w trakcie wywiadu stwierdzali, że wiele informacji o nich jest dostępnych w Internecie i mieli ku takiej otwartości własne powody, opisane bardziej szczegółowo w poprzedniej sekcji.

Przed przeprowadzeniem badania, autor uważał, że ten etap może wykazać tzw. *paradoks prywatności*, czyli różnicę pomiędzy deklarowanymi postawami, a zachowaniami (zob. sekcję *2.5. Paradoksy prywatności*). Okazuje się, że nawet jeżeli taki paradoks zaistniał wśród badanych osób, to jego odkrycie może być niemożliwe na poziomie porównania deklaracji o zachowaniach i faktycznych zachowań. Tak właśnie, bazując na błędnym założeniu, zaprojektowano trzeci etap badania. Deklaracje badanych dotyczące ich własnych zachowań związanych z publikowaniem informacji osobistych w Internecie były zbieżne z ich faktycznymi zachowaniami.

Z drugiej strony, być może ograniczenia ustanowione na początku badania okazały się zbyt restrykcyjne, aby symulować realne możliwości, jakimi dysponują osoby, które są zdeterminowane, aby zdobyć informacje prywatne zamieszczone w Internecie. Samo odnalezienie profilu poszukiwanej osoby na portalu społecznościowym jest znacznie łatwiejsze, jeżeli mamy z taką osobą pośrednie więzi społeczne, tj. wspólnych znajomych. Wśród technik *miękkich*, socjologicznych, które mogłyby zostać zastosowane w celu *wyłudzenia* informacji prywatnych, wymienić należy przede wszystkim prowokację polegającą na wysłaniu zaproszenia do kręgu znajomych, skierowanego do osoby-celu w portalu społecznościowym. W badaniu mogłyby zostać wykorzystane także *twarde* techniki, takie jak statystyczna analiza danych – Kosinski, Stillwell, Graepel (2013) wykazali, że tylko dzięki analizie *lajków* użytkowników Facebooka można uzyskać bardzo wysokie współczynniki pewności nawet dla takich przewidywanych czynników, jak orientacja seksualna (75% do 88% pewności), poglądy polityczne (85% pewności) czy wyznawana wiara (82% pewności). Kolejną furtką, która może być wykorzystana przez osoby pragnące zdobyć prywatne informacje, a która z oczywistych względów nie została wykorzystana w badaniu, to wszelkiego rodzaju próby włamań

do prywatnych kont użytkowników przez złamanie haseł, zainstalowanie oprogramowania szpiegowskiego itp.

5.5. Podsumowanie badania

Z badania wynika, że prywatność w mediach społecznych jest istotnym tematem dla użytkowników portali społecznościowych i innych stron umożliwiających dzielenie się treściami. Prywatność jest przez nich rozumiana na różne sposoby, ale zaproponowane przez badanych definicje zawierają się w zaproponowanych przez badaczy tej problematyki. Podczas wywiadów określali oni prywatność przez metafory strefy lub granicy, wewnątrz której znajdują się ich informacje prywatne, i o których dzieleniu się z innymi decydują samodzielnie. Inni definiowali prywatność jako kontrolę nad przepływem prywatnych informacji.

Badanie potwierdziło, że istnieją dwie istotne dychotomie umożliwiające zrozumienie zachowań użytkowników: podziały na społeczny i instytucjonalny kontekst prywatności oraz na prywatność psychologiczną i fizyczną. Kontekst prywatności różni się w zależności od tego, dla jakiej grupy odbiorców ograniczany jest dostęp do informacji prywatnych. Społeczny kontekst dotyczy ludzi, których znamy osobiście – rówieśników, współpracowników, nauczycieli czy rodziny. Kontekst instytucjonalny oznacza kontrolę nad informacjami osobistymi, które mogą być gromadzone i przetwarzane przez podmioty, takie jak: administratorzy stron internetowych, media społeczne, firmy zajmujące się reklamą w Internecie czy wreszcie instytucje państwowe. Społeczny kontekst wydaje się wielu osobom ważniejszy. Prawdopodobnie przyczynia się do tego większa postrzegana realność takich zagrożeń – łatwiej wyobrazić sobie presję społeczną będącą efektem udostępnienia prywatnych informacji nieodpowiednim osobom z bliskiego kręgu społecznego, niż enigmatyczne zagrożenie wynikające np. z niewłaściwego wykorzystania naszych danych przez administratora portalu społecznościowego. Zagrożenie prywatności w kontekście instytucjonalnym może mieć poważniejsze skutki, ale zazwyczaj nie jest uważane za realne.

Istnieje wiele motywacji, dla których ludzie zamieszczają własne informacje prywatne w internetowych mediach społecznych. Rezygnacja z części prywatności może być związana z potrzebami zawodowymi lub pomaga w realizacji hobby. Służy też kreowaniu własnego wizerunku wśród znajomych, ale także odpowiada na potrzeby rynku pracy. Udostępnianie własnych informacji osobistych bywa też częścią dwóch rodzajów transakcji: firma-klient oraz człowiek-człowiek. W pierwszym przypadku, dane osobowe mogą być niezbędne do realizacji celu

klienta (np. zakupu produktu przez Internet), ale również mogą być ceną, jaką płaci się za skorzystanie z usługi. Kosztem związanym z prywatnością jest w takim wypadku zgoda na przetwarzanie danych osobowych lub na otrzymywanie informacji reklamowych. Transakcja człowiek-człowiek to najbardziej zróżnicowana i najtrudniejsza do zdefiniowania motywacja. Udostępnianie własnych informacji jest warunkiem koniecznym do nawiązania i utrzymywania kontaktów w mediach społecznych. Umożliwia zacieśnienie więzi i budowanie wzajemnego zaufania (zob. sekcję *2.6. Kapitał społeczny a prywatność online*). Rezygnacja z prywatności w mediach społecznych może w końcu wynikać z powstałej tam normy zachowania – badani mówili, że oczekują od własnych *znajomych* w portalach społecznościowych dzielenia się prywatnymi informacjami, gdyż oni sami się tak zachowują.

Badani, pytani o obawę przed naruszeniem ich prywatności, mówili często o bezpieczeństwie ich danych – zwłaszcza danych finansowych. W kontekście społecznym – użytkownicy mediów społecznych wiedzą, że naruszenia prywatności się zdarzają, ale sami raczej się ich nie obawiają. Najczęściej wskazywali własne zachowanie jako czynnik zapewniający bezpieczeństwo ich informacji osobistych w Internecie – większość uważa, że najważniejsze jest odpowiedzialne zamieszczanie prywatnych informacji. Badani mówili często również o bezpieczeństwie wynikającym z uważnego powiększania kręgu *znajomych* w mediach społecznych, zapraszanie do niego wyłącznie zaufanych osób. Część badanych nie obawia się naruszeń prywatności, zwłaszcza związanych z możliwością zamieszczenia czy rozpowszechnienia prywatnych danych przez osobę trzecią, bo uważa, że takie sytuacje są całkowicie poza ich kontrolą i z tego powodu nie warto się nimi przejmować.

Portale społecznościowe oferują obecnie bardzo bogate możliwości dostosowania ustawień prywatności, od zmiany dostępu do całego profilu, po ograniczanie widoczności pojedynczych informacji dla wybranej grupy osób. Jednak nie wszyscy użytkownicy portali chcą lub potrafią zmienić te ustawienia. Ilość czasu, jaki trzeba poświęcić, aby określić własne wymagania, jest często nieproporcjonalna do spodziewanych przez użytkownika korzyści. Regularne zarządzanie *znajomymi* wymaga świadomego podjęcia działania, które w świecie rzeczywistym nie ma odzwierciedlenia. Dodatkowo żaden portal społecznościowy nie może zagwarantować poprawnego działania tych funkcji. Nie dziwi więc fakt, że większość badanych uznała, że zarządzanie dostępnością informacji osobistych w Internecie jest trudniejsze niż w rzeczywistości. Jako powody wskazywała głównie: możliwość łatwego powielenia danych, ich trwałość w czasie, brak możliwości kontroli nad informacjami zamieszczonymi przez inne osoby oraz problemy zwią-

zane z niejednorodnością i niewidocznością publiczności (opisane w sekcji *2.4. Media społeczne – problemy z prywatnością*). Tylko jedna osoba w badaniu uznała, że narzędzia do zarządzania prywatnością pozwalają skutecznie kontrolować przepływ informacji osobistych w mediach społecznych. W rzeczywistości zasady, które regulują sposób rozpowszechniania naszych informacji osobistych, rzadko są wyrażone explicite, tylko opierają się na normach i przypuszczeniach. Program jest zdyscyplinowany, udziela dostępu do informacji jedynie wybranym osobom. Precyzyjna, techniczna możliwość dostosowania ustawień prywatności może swoją dosłownością dawać użytkownikowi poczucie kontroli.

Jedna spośród dwunastu osób biorących udział w II etapie badania stwierdziła, że informacje zamieszczone przez nią w portalu społecznościowym były powodem bardzo poważnego naruszenia prywatności. W czasie wyjazdu na wakacje, o którym poinformowała znajomych przez portal Facebook, dokonano włamania do jej domu. Pozostałe osoby mówiły najczęściej o niezręcznych sytuacjach towarzyskich, np. o zamieszczeniu przez znajomego zdjęcia czy informacji, która miała pozostać w węższym gronie. Portale społecznościowe oferują często możliwość zgłoszenia zdjęcia czy postu jako nieodpowiedniego, ale w przypadku drobnych naruszeń, takich jak te, o których mówili badani, można samodzielnie usunąć powiązania z profilem albo poprosić osobę, która zamieściła treści, o ich usunięcie. Właśnie w ten drugi sposób badani najczęściej rozwiązywali takie problemy.

Niektórzy badani regularnie kontrolują dotyczące ich treści zamieszczane w Internecie. Większość twierdziła, że przynajmniej raz wyszukiwała własne imię i nazwisko poprzez wyszukiwarkę internetową lub przez portal społecznościowy. Niektórzy korzystają również z powiadomień o tagowaniu, ale czasem rezygnują z możliwości usunięcia znacznika w obawie, że zostanie to źle odebrane.

Badani zamieszczają w Internecie, najczęściej na swoich profilach w mediach społecznych, wiele informacji osobistych. Zwykle udostępniają publicznie podstawowe dane: imię, nazwisko, miejsce zamieszkania (miasto), jedno lub kilka zdjęć, na których można ich rozpoznać. Wiele osób zamieszcza dla swoich znajomych dodatkowe informacje, np. o ukończonych szkołach, wieku lub dacie urodzenia, swoich gustach, zainteresowaniach i opiniach (np. poprzez dostęp do *polubionych* stron), a także udostępnia swój adres e-mail. Zdecydowanie rzadziej badani przyznawali się do zamieszczenia numeru telefonu, a prawie nigdy nie udostępniali wprost informacji o swojej orientacji seksualnej, partnerze czy poglądach politycznych i religijnych.

Badani raczej wiedzą, co można o nich znaleźć w Internecie, choć nie pamiętają dokładnie, gdzie i w jakim zakresie udostępnili te informacje. Akt publikowania

w Internecie nie jest jednorazowy, a raz zamieszczone dane, nawet jeżeli zapominane, mogą być wciąż dostępne. Wydaje się, że badani czasem nie starali się przypomnieć, czy zdecydowali się zamieścić np. pełną datę urodzenia w portalu społecznościowym, ale raczej odpowiadali sobie na pytanie: czy (teraz) tak bym zrobił? Trzeci etap badania, którego celem była weryfikacja, czy zachowania badanych są zgodne z ich deklaracjami, nie pozwolił na udowodnienie ani obalenie tezy, że w Internecie można znaleźć o nas więcej niż nam się wydaje.

Autor uważa, że badani zdają sobie sprawę, jak bardzo nierozłączne i wzajemnie przenikające są światy *online* i rzeczywisty; a w związku z tym, jak duże szkody potrafi wyrządzić brak troski o ochronę własnych danych prywatnych oraz wizerunku w Internecie. Trudniej odpowiedzieć na pytanie, co z tą wiedzą robią. Z badania wynika, że większość nie czytała regulaminów portali społecznościowych, z których korzysta i nie do końca zdaje sobie sprawę, w jaki sposób ich dane są przez nie przetwarzane. Duża część nie korzysta także z oferowanych przez portale społecznościowe ustawień prywatności, a nawet jeśli tak – to zwykle w ograniczonym stopniu, nie wykorzystując ich pełnych możliwości. Głównym zabezpieczeniem prywatnych danych jest zatem zdrowy rozsądek, zamieszczanie w Internecie tylko takich informacji, które bez problemu można ujawnić dowolnej osobie. Tylko, czy korzystając z mediów społecznych w ten sposób, można wykorzystać w pełni ich potencjał i budować z ich pomocą społeczne relacje? Myślę, że nie – dzielenie się prywatnymi informacjami w mediach społecznych może być dobrą podstawą do budowania słabych więzi społecznych, a w rezultacie, do gromadzenia kapitału społecznego. Należy postawić także kolejne pytanie – jak wielu użytkowników mediów społecznych kieruje się, tak jak większość badanych, zdrowym rozsądkiem?

6. PODSUMOWANIE

Celem niniejszej pracy była próba znalezienia odpowiedzi na pytania dotyczące znaczenia i statusu prywatności w dynamicznym środowisku Internetu, ze szczególnym uwzględnieniem mediów społecznych.

Przyjmuje się, że koncept prywatności, w dzisiejszym ujęciu tego terminu, został określony pod koniec XIX wieku przez prawników amerykańskich: Samuela Warrena i Lousa Brandeisa, jako *prawo do bycia pozostawionym w spokoju*. Prywatność została wciągnięta w nurt dyskursu psychologicznego i socjologicznego w latach 60. XX wieku. Alan Westin zdefiniował ją jako prawo jednostki, grupy lub instytucji do podejmowania decyzji o czasie, zakresie i sposobie komunikacji ze światem zewnętrznym. Według Irwina Altmana prywatność to kontrola jednostki nad dostępem do niej samej. Ten sam psycholog, wspólnie z Dalmasem Taylorem, zaproponował termin *otwierania się*, czyli świadomego bądź nieświadomego procesu odkrywania informacji o sobie przed wybranymi osobami.

Najnowsze teorie prywatności – teoria integralności kontekstowej prywatności Helen Nissenbaum oraz teoria zarządzania prywatnością komunikacji Sandry Petronio – zwracają największą uwagę na kontekst, w jakim następuje odkrywanie się. Nissenbaum uważa, że informacje o jednostce w jednym kontekście mogą być prywatne (i jako takie chronione), natomiast w innym – wręcz przeciwnie. Naruszenie integralności kontekstowej informacji prywatnych, lub prościej ujmując – naruszenie prywatności – następuje, gdy informacje prywatne wydostają się poza odpowiedni kontekst. Petronio nie odwołuje się bezpośrednio do Nissenbaum, ale w pewnym sensie formalizuje jej teorię – opisuje proces ujawnia-

nia informacji prywatnych, określony indywidualnymi i dynamicznymi regułami ustalonych przez właściciela informacji prywatnych. W teorii Petronio nieustanie ścierają się dwie siły – potrzeba ujawniania informacji prywatnych oraz potrzeba zachowania prywatności. W związku z ich działaniem zasady przepływu informacji prywatnych są nieustannie zmieniane i negocjowane z innymi.

Nie ma wątpliwości, że naruszenia prywatności *online* mogą być równie dotkliwe jak sytuacje jej naruszenia w świecie fizycznym. Jednak na zagadnienia prywatności w Internecie trzeba spoglądać z innej perspektywy – właściwości świata fizycznego i *online* są różne. Strukturalne cechy Internetu, takie jak trwałość, łatwość kopiowania, przetwarzania oraz wyszukiwania oraz duży zasięg informacji, w znacznym stopniu utrudniają kontrolę przepływu własnych informacji prywatnych. Przestrzeń cyfrowa jest usieciowiona – normą, ustanowioną przez media społeczne, jest raczej dzielenie się informacjami, niż powstrzymywanie się od dzielenia. Kolejnym problemem związanym z prywatnością w Internecie jest niejednorodna i niewidzialna publiczność. W świecie fizycznym sytuacje społeczne są oddzielone naturalnymi granicami – przestrzennymi, czasowymi i społecznymi. Znając odbiorców, potrafimy dostosować treść i formę komunikatu, tak aby proces otwierania się nie przyniósł negatywnych skutków. Publiczność w Internecie nie jest tak rozdzielona – poza komunikacją prywatną, treści zamieszczane w Internecie trafiają do szerokiego grona odbiorców. Problem wynikający z połączenia odbiorców z różnych kontekstów społecznych w niejednorodną publiczność badacze tematu nazywają *zapaścią kontekstu*.

Portale społecznościowe umożliwiają regulację dostępu do publikowanych treści (przez tzw. ustawienia prywatności), ale wiele osób nie zdaje sobie sprawy z istnienia takich narzędzi, inne nie potrafią albo nie chcą z nich korzystać. Badacze prywatności w Internecie zauważyli, że wiele osób nie podejmuje działań mających na celu ochronę własnej prywatności w Internecie, mimo że deklaruje wysoki poziom troski o nią. Zjawisko to zostało nazwane *paradoksem prywatności*. Istnieje kilka hipotez próbujących je wyjaśnić. Często zwraca się uwagę na wysoki stopień skomplikowania ustawień prywatności – aby dokładnie je skonfigurować, trzeba poświęcić czas i wysiłek. Żaden portal społecznościowy nie gwarantuje niezawodności ustawień. Rozpatrując problem na gruncie teorii racjonalnego wyboru, zauważono, że jednostka, która podejmuje decyzję związaną z udostępnieniem w Sieci własnych danych, posiada niekompletne informacje. W takiej sytuacji podjęta decyzja nie ma w pełni racjonalnych przesłanek. Można skutecznie i łatwo ocenić koszty związane z ochroną prywatności w Internecie (np. czas spędzony na zapoznanie się z ustawieniami prywatności czy rezygnacja z podzielenia

się ze znajomymi jakąś informacją). Problem pojawia się natomiast przy ocenie korzyści – są one odsunięte w czasie i niepewne (brak naruszenia prywatności). Na podjęcie decyzji wpływa również, naturalny dla ludzi, nierealny optymizm – zdecydowana większość osób ocenia siebie powyżej mediany, np. większość kierowców uważa się za lepszych od przeciętnych. Podobnie, większość Internautów sądzi, że nie zdarzy im się utrata kontroli nad własnymi informacjami w Sieci.

Jedną z korzyści z zamieszczania informacji prywatnych w Internecie, na którą wskazują badacze Sieci, jest możliwość budowania w ten sposób kapitału społecznego. Kapitał społeczny to niematerialne zasoby powstałe ze związków międzyludzkich, których wartość opiera się na relacjach społecznych, współpracy i zaufaniu jednostek w społeczeństwie. Nie ma zgody, co do wpływu wykorzystania Internetu na głębokie relacje międzyludzkie, ale większość badaczy tematu uważa, że szybkość i łatwość wymiany informacji w Internecie sprzyja tworzeniu *pomostowego* kapitału społecznego. Ten rodzaj kapitału społecznego opiera się na słabych więziach i sprzyja m.in. rozprzestrzenianiu się unikalnej informacji. Większość relacji nawiązywanych i utrzymywanych w portalach społecznościowych to właśnie słabe więzi.

Rozróżnia się trzy główne sposoby ochrony prywatności w Internecie: regulacje prawne, rynkową samoregulację oraz samodzielną dbałość użytkowników o własne dane. W Stanach Zjednoczonych, ojczyźnie najbardziej popularnych portali społecznościowych, nie istnieje wiele praw chroniących prywatność użytkowników Internetu. Prawodawstwo Unii Europejskiej oraz krajów członkowskich dotyczące ochrony danych osobowych jest znacznie bardziej rozbudowane. W Polsce działa Generalny Inspektorat Ochrony Danych Osobowych, który nakłada na administratorów osobowych baz danych obowiązki dotyczące gromadzenia i przetwarzania danych. Żadna instytucja nie ma prawa przetwarzać danych osobowych bez wiedzy i zgody osoby, do której one należą. Każda osoba ma prawo zażądać możliwości wglądu do własnych danych oraz ich poprawienia. Unia Europejska przedstawiła w 2012 roku projekt reformy przypisów o ochronie danych, w którym zaproponowano między innymi: ujednolicenie przepisów w krajach członkowskich, łatwiejszy dostęp do własnych danych, a także tzw. *prawo do bycia zapomnianym*, czyli prawo usunięcia danych osobowych na wniosek osoby, której dotyczą.

Niektórzy badacze uważają, że stosowanie prawa, aby chronić prywatność użytkowników Internetu, jest mało skuteczne. Inni, że obowiązki nakładane na firmy internetowe podnoszą koszty ich działalności i tym samym ograniczają ich rozwój. Według nich te problemy zostaną uregulowane zasadami wolnego rynku.

Jeśli użytkownikom będzie zależało na tym, aby administratorzy mediów społecznych dbali o ich prywatne dane, to firmy takie jak Facebook same zadbają o odpowiednie narzędzia i edukację użytkowników. Zwolennicy takiego rozumowania twierdzą, że portale społecznościowe opierają swój model biznesowy na dzieleniu się treściami przez ich użytkowników. W związku z tym firmy internetowe mają swój wymierny interes w tym, aby użytkownicy nie doświadczali przykrych sytuacji, które mogą spowodować zmniejszenie częstotliwości lub rezygnację korzystania z portalu.

Najlepszym sposobem ochrony prywatności użytkowników jest stosowanie przez nich samych różnych strategii ochrony. Wyróżnia się pasywne i aktywne metody ochrony prywatności. Do najczęściej stosowanych pasywnych metod należy tzw. *strategia budowania płotów*, czyli ograniczenie publikowania informacji oraz selektywne rozszerzenie sieci kontaktów. Skrajną formą tej strategii jest całkowita rezygnacja z zamieszczania własnych treści w Internecie. Metoda budowania płotów może być rozszerzona o wykorzystanie ustawień prywatności. Niektórzy wskazują na minusy pasywnych strategii ochrony prywatności – stosując je, ograniczamy nasze kontakty z internetowym otoczeniem i w ten sposób rezygnujemy z korzyści, jakie dają media społeczne – np. osłabiamy rozwój słabych więzi społecznych niezbędnych do budowania kapitału społecznego. Poza tym, jak uważają niektórzy badacze, naruszenia prywatności związane z interakcjami ze społeczeństwem, to tylko wierzchołek góry lodowej – znacznie większe zagrożenie dla prywatności stanowi nieuprawnione gromadzenie i przetwarzanie danych przez dostawców Internetu, instytucje prywatne oraz publiczne (np. rządy czy służby mundurowe). Aktywne metody mają na celu zarządzanie informacjami prywatnymi, które już znalazły się w Sieci. Wiele osób korzysta z wyszukiwarek internetowych, szukając wpisów powiązanych z ich imieniem i nazwiskiem. Nieliczni zadają sobie trud związany z wystosowaniem próśb do administratorów strony internetowych o usunięcie lub poprawienie danych.

Podczas wywiadów przeprowadzonych przez autora, aktywni użytkownicy mediów społecznych wybrani spośród studentów IINiSB UW, zaprezentowali szereg interesujących postaw dotyczących prywatności w mediach społecznych. Na podstawie badania można wnioskować m.in., istnienie wyraźnego rozróżnienia pomiędzy społecznym, a instytucjonalnym kontekstem prywatności. Większość osób mniej obawia się przetwarzania ich prywatnych informacji przez różnego rodzaju instytucje, niż naruszenia prywatności polegającego na udostępnieniu tych samych informacji nieodpowiednim osobom z ich społecznego kręgu. Wśród wielu powodów zamieszczania w Sieci prywatnych danych respondenci

wskazywali najczęściej: nawiązywanie i podtrzymywanie kontaktów ze znajomymi (głównie ze świata *offline*), kreowanie własnego wizerunku (prywatnego i zawodowego), chęć realizacji zawodowej lub rozwoju zainteresowań. Niektórzy badani zauważyli, że społeczną normą zachowania w portalach społecznościowych jest dzielenie się informacjami, a powstrzymywanie się od dzielenia nie jest odbierane pozytywnie.

Uczestnicy badania w zdecydowanej większości deklarowali dbałość o swoje dane prywatne, ale nie było to powodem do rezygnacji z korzystania z mediów społecznych. Pytani o swoje obawy, mówili najczęściej o bezpieczeństwie w bankowości elektronicznej. Większość osób deklarowała, że nie musi obawiać się o swoją prywatność w mediach społecznościowych, gdyż *odpowiedzialnie* publikuje informacje o sobie oraz ma zaufane grono znajomych w portalach społecznościowych. Inne osoby reprezentowały przeciwne stanowisko – wiedząc, że media społeczne mogą być źródłem naruszenia prywatności, nie traktowały tych obaw poważnie. Uważały, że niezależnie od ich obecności w portalach społecznościowych, nigdy nie będą mieli pełnej kontroli nad informacjami prywatnymi w Internecie. Większość respondentów doświadczyła jedynie drobnych naruszeń prywatności w mediach społecznych – opisywali oni publikację niepożądanego zdjęcia czy informacji przez znajomego. Jedna osoba opisała przypadek kradzieży, prawdopodobnie umożliwionej przez zamieszczenie w Internecie informacji o wyjeździe na wakacje.

W większości badani publikowali w Internecie podobne rodzaje informacji o sobie – podstawowe dane, takie jak imię i nazwisko, miejsce zamieszkania (miasto) oraz zdjęcia, na których można ich rozpoznać. Nierzadko zamieszczali również informacje o zainteresowaniach, prawie nigdy zaś – wrażliwych informacji, np. o orientacji seksualnej, poglądach politycznych i religijnych.

Niniejsza praca nie wyczerpuje tematu prywatności w mediach społecznych. Wiele kwestii zostało omówionych pobieżnie – zwłaszcza działalność organizacji pozarządowych (takich jak EPIC czy Panoptykon), zagadnienia prawne i techniczne. Dodatkowo wybrany charakter badania nie pozwala na ekstrapolację wyników. W trakcie pisania tej pracy zmieniło się też samo środowisko mediów społecznych. Wśród rodzących się trendów szczególnie interesująca wydaje się możliwość definiowania terminu ważności informacji elektronicznych. Z technologicznego punktu widzenia realne jest zaimplementowanie funkcji automatycznie kasujących pliki komputerowe po określonym terminie. W 2012 roku dużą popularność zdobyło oprogramowanie mobilne, pozwalające na wysłanie multimediów innym użytkownikom programu, w którym wiadomość kasowana jest

automatycznie po maksymalnie 10 sekundach od wyświetlenia. Niektórzy analitycy Internetu widzą w *kasowalnych mediach społecznych* rozwiązanie problemów z prywatnością w Internecie (Gillette, 2013). Można się spodziewać, że takie i podobne innowacje zostaną wykorzystane przez inżynierów tworzących popularne portale społecznościowe. Analizując rozwój Internetu, można zauważyć, że firmy, które obecnie są najpopularniejszymi stronami w Internecie, powstały z pozornie absurdalnych pomysłów. Twórcy Google zdecydowali się niegdyś ściągnąć cały Internet na pamięć komputera, a następnie stworzyć wyszukiwarkę internetową na rynku przesyconym podobnymi usługami. Facebook powstał jako strona, na której można było oceniać atrakcyjność studentów i studentek. Najprawdopodobniej prędzej czy później do walki o uwagę i prywatne dane użytkowników włączy się kolejny gracz i ustali nowe reguły od nowa. Nie ma wątpliwości, że debata na temat prywatności w mediach społecznych będzie trwała przynajmniej przez kilka najbliższych lat, a coraz silniejszy głos będą mieli ich użytkownicy i obywateli, wspierani przez prawo oraz organizacje pozarządowe.

BIBLIOGRAFIA

Abram C. (2006), *Welcome to Facebook, everyone. The Facebook Blog*. Facebook [online], dostęp 10 maja 2012. Dostępny w Internecie: http://blog.facebook.com/blog.php?post=2210227130

Acquisti A. (2004), *Privacy in Electronic Commerce and the Economics of Immediate Gratification. Human Factors.*

Acquisti A., Gross R. (2006), *Imagined communities: Awareness, information sharing, and privacy on the Facebook* [w:] P. Golle & G. Danezis (Eds.), *Proceedings of 6th Workshop on Privacy Enhancing Technologies* (Vol. 4528(4), s. 36–58). Cambridge, U.K. Robinson College. doi:10.1007/11957454_3

Allen A. L. (2000), *Gender and Privacy in Cyberspace* [w:] *Stanford Law Review, 52*(5), s. 1175–1200. doi:10.2307/1229512

Altman I. (1975), *The Environment and Social Behavior* [w:] *Environment And Behavior* (Vol. 20, s. 34–61). Brooks/Cole. doi:10.1177/0013916506295569

Bader C. (2014), *The End of the Facebook Era* [w:] *Chris Bader's Svbtle* [online], dostęp 17 stycznia 2014. Dostępny w Internecie: http://takeaswig.com/the-end-of-the-facebook-era

Bargh J. A. & McKenna K. Y. A. (2004), *The internet and social life* [w:] *Annual review of psychology55*, s. 573-90. doi:10.1146/annurev.psych.55.090902.141922

Barnes S. B. (2006), *A privacy paradox: Social networking in the United States* [w:] *First Monday, 11*(9), s. 11–15. First Monday [online], dostęp 10 maja 2012. Dostęp w Internecie: http://firstmonday.org/issues/issue11_9/barnes/index.html

Barth A., Datta A., Mitchell J. C. & Nissenbaum H. (2006), *Privacy and Contextual Integrity: Framework and Applications* [w:] *2006 IEEE Symposium on Security and Privacy SP06, 79*(1), 184-198. Ieee. doi:10.1109/SP.2006.32

Belleghem V., Eenhuizen M. & Elias V. (2011), *Social Media Around The World 2011* [online], dostęp 10 maja 2012. Dostęp w Internecie: http://www.slideshare.net/stevenvanbelleghem/social-media-around-the-world-2011

boyd danah & Donath J. (2004), *Public displays of connection* [w:] *BT Technology Journal, 22*(4), 71–82 [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.danah.org/papers/PublicDisplays.pdf

boyd danah & Ellison N. B. (2007), *Social Network Sites: Definition, History, Scholarship.* [w:] *Journal of Computer-Mediated Communication, 13*(1), s. 1–19 [online], dostęp 10 maja 2012. Dostępny w Internecie: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

boyd danah & Hargittai E. (2010), *Facebook privacy setting: Who cares?* [w:] *First Monday, 15*(8) [online], dostęp 10 maja 2012. Dostępny w Internecie: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

boyd danah (2008), *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence* [w:] *Convergence: The International Journal of Research into New Media Technologies, 14*(1), s. 13–20, UNIVERSITY OF LUTON. doi:10.1177/1354856507084416

boyd danah (2009), *Taken Out of Context: American Teen Sociality in Networked Publics* [w:] *SSRN Electronic Journal, 359*(23), s. 2478–82. doi:10.2139/ssrn.1344756

boyd danah (2010a), *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications* [w:] Z. Papacharissi (Ed.), *Networked Self: Identity, Community, and Culture on Social Network Sites* (s. 39–58). Routledge [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.danah.org/papers/2010/SNSasNetworkedPublics.pdf

boyd danah (2010b), *Quitting Facebook is pointless; challenging them to do better is not.* [w:] *Apophenia* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.zephoria.org/thoughts/archives/2010/05/23/quitting-facebook-is-pointless-challenging-them-to-do-better-is-not.html

Brian M. (2012), *New Google account users are now forced to sign up to Gmail and Google+* [w:] *The Next Web* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://thenextweb.com/google/2012/01/20/new-google-account-users-are-now-forced-to-sign-up-to-gmail-and-google/

Burgoon J. K., Parrott R., Le Poire B. A., Kelley D. L., Walther J. B. & Perry D. (1989), *Maintaining and Restoring Privacy through Communication in Different Types of Relationships. Journal of Social and Personal Relationships, 6*(2), s. 131–158. Sage Publications. doi:10.1177/026540758900600201

Burke M., Marlow C. & Lento T. (2009), *Feed Me: Motivating Newcomer Contribution in Social Network Sites* [w:] *CHI '09 Proceedings of the 27th international conference on Human factors in computing systems* (Vol. 73, s. 945–954). ACM. doi:10.1145/1518701.1518847

Burke M., Marlow C. & Lento T. (2010a), *Social network activity and social well--being* [w:] *Proceedings of the 28th international conference on Human factors in computing systems – CHI '10* (s. 1909). New York, New York, USA: ACM Press. doi:10.1145/1753326.1753613

Child J.T. & Petronio S. (2011), *Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet* [w:] *Computer-mediated communication in personal relationships,* s. 21–40 [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.heinz.cmu.edu/~acquisti/shb/Petronio.pdf

Child Jeffrey T., Pearson J. C. & Petronio S. (2009), *Blogging, communication, and privacy management: Development of the Blogging Privacy Management Measure* [w:] *Journal of the American Society for Information Science and Technology, 60*(10), s. 2079–2094. Wiley Online Library. doi:10.1002/asi.21122

Ciocchetti C. A. (2007), *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors* [w:] *American Business Law Journal, 44*(1), s. 55–126 [online], dostęp10 maja 2012. Dostępny w Internecie: http://works.bepress.com/corey_ciocchetti/4

Citron D. (2010), *BRIGHT IDEAS: Helen Nissenbaum's Privacy in Context: Technology, Policy, and the Integrity of Social Life* [w:] *Concurring Opinion* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.concurringopinions.com/archives/2010/01/bright-ideas-helen-nissenbaums-privacy-in-context-technology-policy-and-the-integrity-of-social-life.html

CNBC (2009), *Google's Privacy* [w:] *Inside the Mind of Google. CNBC Video* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.cnbc.com/id/15840232/?video=1372176413

Debatin B. (2011), *Ethics, Privacy, and Self-Restraint in Social Networking* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (s. 47–60). Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6_5

Debatin B., Lovejoy J. P., Horn A.-K. & Hughes, B. N. (2009), *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences* [w:] *Journal of Computer-Mediated Communication, 15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

DeCew J. (1997), *Pursuit of Privacy: Law, Ethics, and the Rise of Technology* [w:] *Ethics* (Vol. 109), Cornell University Press.

DeCew J., & Zalta, E. N. (2008), *Privacy* [w:] *The Stanford Encyclopedia of Philosophy (Fall 2008 Edition)* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://plato.stanford.edu/archives/fall2008/entries/privacy/

Dimicco J. M., Geyer W., Millen D. R., Dugan C. & Brownholtz, B. (2009), *People Sensemaking and Relationship Building on an Enterprise Social Network Site* [w:] *2009 42nd Hawaii International Conference on System Sciences* (s. 1–10). IEEE. doi:10.1109/HICSS.2009.343

DiMicco J., Millen D. R., Geyer W., Dugan C., Brownholtz B. & Muller M. (2008), *Motivations for social networking at work* [w:] *Proceedings of the ACM 2008 conference on Computer supported cooperative work – CSCW '08* (s. 711). New York, New York, USA: ACM Press. doi:10.1145/1460563.1460674

Ducklin P. (2009), *Sophos Australia Facebook ID probe 2009* [w:] *Sophos Press Office online* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://nakedsecurity.sophos.com/2009/12/06/facebook-id-probe-2009/

Dwyer C. & Hiltz S. R. (2007), *Trust and Privacy Concern Within Social Networking Sites : A Comparison of Facebook and MySpace Trust and privacy concern within social networking sites : A comparison of Facebook and MySpace* [w:] *Formation Systems Journal, 28*(6), 13. doi:10.1.1.148.9388

Eckersley P. (2010), *How Unique Is Your Web Browser* [w:] M. J. Atallah & N. J. Hopper (Eds.), *Privacy Enhancing Technologies* (Vol. 6205, s. 1–18). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-14527-8

Efrati A. (2012), *The Mounting Minuses at Google+. The Wall Street Journal* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://online.wsj.com/article/SB10001424052970204653604577249341403742390.html?mod=e2tw

Electronic Privacy Information Center (2010), *Complaint, request for investigation, injunction, and other relief before the Federal Trade Commission* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

Ellison N. B., Steinfield C. & Lampe C. (2007), *The Benefits of Facebook "Friends": Social Capital and College Students' Use of Online Social Network Sites* [w:] *Journal of Computer-Mediated Communication, 12*(4), 1143–1168. doi:10.1111/j.1083--6101.2007.00367.x

Ellison N. B., Vitak J., Steinfield C. & Gray R. (2011), *Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Vol. 10, s. 19–32). Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Europa. Press releases RAPID (2010), *Komisja Europejska przedstawia strategię poprawy skuteczności unijnych przepisów dotyczących ochrony danych* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=1&language=PL&guiLanguage=fr

European Commission (2011), *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. Perception* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Facebook Newsroom (2011), *Platform* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://newsroom.fb.com/content/default.aspx?NewsAreaId=137

Facebook (2009), *Facebook's Privacy Policy – Full Version* [w:] *Facebook* [online], dostęp 10 maja 2012. Dostępny w Internecie: https://www.facebook.com/note.php?note_id=+322194465300

Facebook (2012), *Zasady wykorzystania danych* [w:] *Facebook* [online], dostęp 10 maja 2012. Dostępny w Internecie: https://www.facebook.com/about/privacy/

Federal Trade Commission (2007), *Fair Information Practices Principles* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Filiciak M., Danielewicz M., Halawa M., Nowotny A. & Mazurek P (2010), [w:] *Młodzi i media: nowe media a uczestnictwo w kulturze.* Centrum Badań nad Kulturą Popularną SWPS [online], dostęp 10 maja 2012. Dostępny w Internecie: http://bi.gazeta.pl/im/9/7651/m7651709.pdf

FindPeopleonPlus (2012), *Google+ Infographic v2* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://findpeopleonplus.com/statistics

Gillette F (2013), *Snapchat and the Erasable Future of Social Media* [w:] *Bloomberg BusinessWeek* [online], dostęp 5 czerwca 2013. Dostępny w Internecie: http://www.businessweek.com/articles/2013-02-07/snapchat-and-the-erasable-future-of-social-media

GlobalWebIndex (2013), *Infographic: Facebook Active Usage (Q3 2013)* [w:] GlobalWebIndex [online], dostęp 17 stycznia 2014. Dostępny w Internecie: https://www.globalwebindex.net/products/infographic/infographic-facebook-active-usage-q3-2013

Google: Investors Relation (2012), *Google Announces Fourth Quarter and Fiscal Year 2011 Results* [w:] *Google* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://investor.google.com/earnings/2011/Q4_google_earnings.html

Greenberg A. (2007), *The Streisand Effect*. Forbes.com [online], dostęp 13 stycznia 2013. Dostępny w Internecie: http://www.forbes.com/2007/05/10/streisand--digg-web-tech-cx_ag_0511streisand.html

Griffin E. (2011), *Communicion Privacy Management Theory of Sandra Petronio* [w:] *A First Look at Communication Theory* (8th ed., s. 168–180). McGraw-Hill Humanities/Social Sciences/Languages.

Grimmelmann J. (2009), *Saving Facebook* [w:] *Iowa Law Review*, (September 2008), s. 1137–1206 [online], dostęp 10 maja 2012. Dostępny w Internecie: http://ssrn.com/abstract=1262822

Gross R., & Acquisti A. (2005), [w:] *formation Revelation and Privacy in Online Social Networks (The Facebook case)* [w:] *Human Factors*, 71–80. ACM Press [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Hambridge S. (1995), *Netiquette Guidelines* [w:] *Network Working Group* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://tools.ietf.org/html/rfc1855

Harris Interactive (2001), *Privacy Notices Research Final Results* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.ftc.gov/bcp/workshops/glb/supporting/harris results.pdf

Hoadley C. M., Xu H., Lee J. J. & Rosson M. B. (2010), *Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry* [w:] *Electronic Commerce Research and Applications, 9*(1), s. 50–60. Elsevier B.V. doi:-10.1016/j.elerap.2009.05.001

IBOPE (2007), *Zogby Poll: Most Americans Worry About Identity Theft* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://www.ibopezogby.com/news/2007/04/03/zogby-poll-most-americans-worry-about-identity-theft/

iStratebyLabs (2014), *3 Million Teens Leave Facebook In 3 Years: The 2014 Facebook Demographic Report* [w:] *iStratebyLabs* [online], dostęp 17 stycznia 2014. Dostępny w Internecie: http://istrategylabs.com/2014/01/3-million-teens-leave-facebook-in-3-years-the-2014-facebook-demographic-report/

Jensen C., Potts C. & Jensen C. (2005), *Privacy practices of Internet users: Self-reports versus observed behavior* [w:] *International Journal of Human-Computer Studies, 63*(1–2), s. 203–227. doi:10.1016/j.ijhcs.2005.04.019

Joinson A. N. & Paine C. B. (2007), *Self-disclosure, privacy and the Internet* [w:] A. Joinson, K. McKenna, T. Postmes & U.-D. Reips (Eds.), *Oxford handbook of Internet Psychology* (2nd ed., s. 236–252). Oxford: Oxford University Press.

Joinson A. N., Houghton D. J., Vasalou A. & Marder B. L. (2011), *Digital Crowding: Privacy, Self-Disclosure, and Technology* [w:] S. Trepte & L. Reinecke (Eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, s. 33–45. Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Kaznowski D. (2010), *Media społeczne czy społecznościowe? That is the question* [w:] *Networked Digital Age* [online], dostęp 10 maja 2012. Dostępny w Internecie: http://networkeddigital.com/2010/12/09/media-spoleczne-czy-spolecznosciowe-that-is-the-question/

Kirkpatrick M. (2010), *Zuckerberg Says The Age of Privacy is Over* [w:] *ReadWriteWeb* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

Kirkpatrick M. (2011), *Google to Luanch Major New Social Network Called Circles, Possibly Today (Updated)* [w:] *ReadWriteWeb* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.readwriteweb.com/archives/google_to_launch_major_new_social_network_called_c.php

Kiss J. (2010), *Facebook: Did anyone really quit?* [w:] *The Guardian: The Digital Content Blog* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.guardian.co.uk/media/pda/2010/jun/01/digital-media-facebook

Kosinski M., Stillwell D. & Graepel T. (2013), *Private traits and attributes are predictable z: digital records of human behavior* [w:] *Proceedings of the National Academy of Sciences*, 2–5. doi:10.1073/pnas.1218772110

Krämer N. C. & Haferkamp N. (2011), *Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (s. 127–141). Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Lacy S. (2006), *Facebook: Opening the Doors Wider* [w:] *Bloomberg Businessweek* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.businessweek.com/technology/content/sep2006/tc20060912_682123.htm

Lessin S. W. (2011), *Tell Your Story with Timeline. Blog na Facebooku* [online], dostęp 10 maja 2013. Dostępny w Internecie: https://www.facebook.com/note.php?note_id=10150289612087131

Lewis K. (2011), *The Co-evolution of Social Network Ties and Online Privacy Behavior* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy*

and Self-Disclosure in the Social Web (s. 91–110). Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Lewis K., Kaufman J. & Christakis N. (2008), *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network* [w:] *Journal of Computer-Mediated Communication, 14*(1), 79–100. doi:10.1111/j.1083-6101.2008.01432.x

Mackenzie I. (2011), *Sarkozy questions "neutral" net at e-G8 forum* [w:] *BBC News* [online], dostęp 13 stycznia 2013. Dostępny w Internecie: http://www.bbc.co.uk/news/technology-13518871

MacKinnon C. A. (1989), *Toward a Feminist Theory of the State.* Cambridge: Harvard University Press. doi:10.1177/0090591796024001004

Mansour S. (2007), *2504 Steps to closing your Facebook account* [w:] *stevenmansour's blog* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.stevenmansour.com/en/writings/2007/july/23/2504_steps_closing_your_facebook_account.

Margulis S. T. (2003), *On the Status and Contribution of Westin's and Altman's Theories of Privacy* [w:] *Journal of Social Issues, 59*(2), s. 411–429. doi:10.1111/1540-4560.00071

Marwick A., Murgia-Diaz D. (2010), *Youth, privacy and reputation (literature review)* [w:] *Berkman Center Research*, (5) [online], dostęp 10 maja 2013. Dostępny w Internecie: http://ssrn.com/abstract=1588163

Mayer A., Puller S. L. (2008), *The old boy (and girl) network: Social network formation on university campuses* [w:] *Journal of Public Economics, 92*(1–2), s. 329–347. doi:10.1016/j.jpubeco.2007.09.001

Mazer J. P., Murphy R. E. & Simonds C. J. (2007), *I'll See You On "Facebook": The Effects of Computer-Mediated Teacher Self-Disclosure on Student Motivation, Affective Learning, and Classroom Climate* [w:] *Communication Education, 56*(1), s. 1–17. Communication Education. doi:10.1080/03634520601009710

Mazur A. (2004), *Projekt badań: O prywatności i jej granicach w badaniach socjologicznych. Wpływ budowy pytań dotyczących prywatności badanych na jakość danych* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.autopojetycznawiedza.republika.pl/materialy/polskie/projekt_badan.doc

McKeon M. (2010), *The Evolution of Privacy on Facebook* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://mattmckeon.com/facebook-privacy/

Moore A. D. (2008), *Defining Privacy* [w:] *Journal of Social Philosophy, 3*(9), s. 411-428. doi:doi:10.1111/j.1467-9833.2008.00433.x

Nie N. H. (2001), *Sociability, Interpersonal Relations, and the Internet: Reconciling Conflicting Findings* [w:] *American Behavioral Scientist, 45*(3), s. 420–435. doi:10.1177/00027640121957277

Nissenbaum H. (2004), *Privacy as Contextual Integrity* [w:] *Washington Law Review, 79*(1), s. 101–139. HeinOnline [online], dostęp 10 maja 2013. Dostępny w Internecie: http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/washlr79&section=16

Norbert P. A., Horne D. R., Horne D. A. (2007), *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors* [w:] *Journal of Consumer Affairs, 41*(1), s. 100–126. doi:10.1111/j.1745-6606.2006.00070.x

Pachal P. (2011), *Google Circles: The Dumbest Thing About Google+* [w:] *PCMAG.com* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.pcmag.com/article2/0,2817,2387808,00.asp

Papacharissi Z., Fernback J. (2005), *Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements* [w:] *Journal of Broadcasting Electronic Media, 49*(3), s. 259–281. Taylor & Francis Ltd. doi:10.1207/s15506878jobem4903_1

Papacharissi Z., & Gibson P. L. (2011), *Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (s. 75–89). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6_7

Parent W. A. (1983), *Privacy, Morality, and the Law* [w:] *Philosophy & Public Affairs, 12*(4), s. 269–288 [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.jstor.org/stable/2265374

Parlament Europejski (1995), *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* [w:] *Parlament Europejski, Rada* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pl:NOT

Pedersen D. (1997), *Psychological Functions of Privacy* [w:] *Journal of Environmental Psychology, 17*(2), s. 147–156. doi:10.1006/jevp.1997.0049

Pedersen D. (1999), *Model for types of privacy by privacy functions* [w:] *Journal of Environmental Psychology, 19*(4), s. 397–405. doi:10.1006/jevp.1999.0140

Peterson C. (2010), *Losing Face: An Environmental Analysis of Privacy on Facebook* [w:] *SSRN Electronic Journal*, (January), s. 1–38 [online], dostęp 10 maja 2013. Dostępny w Internecie: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1550211

Posner R. A. (1983), *The Economics of Justice*. Harvard University Press [online], dostęp 10 maja 2013. Dostępny w Internecie: http://books.google.com/books?id=CKEN0F07ChUC

Prensky M. (2001), *Digital Natives, Digital Immigrants* [w:] *On the Horizon, 9*(5), s. 1–6. MCB University Press [online], dostęp 10 maja 2013. Dostępny w Internecie: http://pre2005.flexiblelearning.net.au/projects/resources/Digital_Natives_Digital_Immigrants.pdf

Price B. A., Adam K. & Nuseibeh B. (2005), *Keeping ubiquitous computing to yourself: A practical model for user control of privacy* [w:] *International Journal of Human-Computer Studies, 63*(1–2), s. 228–253. doi:10.1016/j.ijhcs.2005.04.008

Prosser W. (1960), *Privacy* [w:] *California Law Review, 48*(3), s. 383–423 [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf

Putnam R. D. (2008), *Samotna gra w kręgle: upadek i odrodzenie wspólnot lokalnych w Stanach Zjednoczonych*. (P. Sadura, S. Szymański, & M. Ziółkowski, Eds.). Wydawnictwa Akademickie i Profesjonalne.

Raynes-Goldie K. (2010), *Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook* [w:] *First Monday, 15*(1–4) [online], dostęp 10 maja 2013. Dostępny w Internecie: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Ross B (2011), *Improved Friend Lists* [w:] *Blog na Facebooku* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://blog.facebook.com/blog.php?post=10150278932602131

Samuelson R. J. (2006), *A Web of Exhibitionists* [w:] *The Washington Post* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.washingtonpost.com/wp-dyn/content/article/2006/09/19/AR2006091901439.html

Sanghvi, R. (2006), *Facebook Gets a Facelift* [w:] *Blog na Facebooku* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://blog.facebook.com/blog.php?post=2207967130

Schmidt T. S. (2006), *Inside the Backlash Against Facebook* [w:] *Time U.S.* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.time.com/time/nation/article/0,8599,1532225,00.html

Schneider T. & Michael Z. (2006), *Identity and Identification in a Networked World* [w:] *First Monday, 11*(12) [online], dostęp 10 maja 2013. Dostępny w Internecie: http://firstmonday.org/issues/issue11_12/schneider/index.html

Sheehan K. B. (2002), *Toward a Typology of Internet Users and Online Privacy Concerns* [w:] *The Information Society, 18*(1), s. 21–32. doi:10.1080/01972240252818207

Shirky C. (2008), *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin Press.

Slee M. (2007), *Friends Lists* [w:] *Blog na Facebooku* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.facebook.com/blog/blog.php?post=7831767130

Social Statitics G. (2012), *Male/Female ratio* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://socialstatistics.com/

Steinfield C., DiMicco J. M., Ellison N. B. & Lampe C. (2009), *Bowling online* [w:] *Proceedings of the fourth international conference on Communities and technologies – C&T '09* (s. 245). New York, New York, USA: ACM Press. doi:10.1145/1556460.1556496

Steinfield C., Ellison N. B. & Lampe C. (2008), *Social capital, self-esteem, and use of online social network sites: A longitudinal analysis* [w:] *Journal of Applied Developmental Psychology, 29*(6), s. 434–445. Elsevier B.V. doi:10.1016/j.appdev.2008.07.002

Strahilevitz L. (2005), *A Social Networks Theory of Privacy* [w:] *The University of Chicago Law Review, 72*(3), s. 919–988. The University of Chicago Law Review. doi:10.2139/ssrn.629283

Stutzman Fred & Kramer-Duffield, J. (2010), *Friends only* [w:] *Proceedings of the 28th international conference on Human factors in computing systems – CHI '10* (s. 1553). New York, New York, USA: ACM Press. doi:10.1145/1753326.1753559

Stutzman F. (2006), *An Evaluation of Identity-Sharing Behavior in Social Network Communities* [w:] *Journal of the International Digital Media and Arts Association*, 1–7 [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.units.muohio.edu/codeconference/papers/papers/stutzman_track5.pdf

Sullivan B. B. (2005), *Kids, blogs and too much information* [w:] *MSNBC* [online], dostęp 10 maja 2010. Dostępny w Internecie: http://www.msnbc.msn.com/id/7668788/ns/technology_and_science-security/t/kids-blogs-too-much-information/

Thomson J. J. (1975), *The Right to Privacy* [w:] *Philosophy & Public Affairs, 4*(4), s. 295–314 [online], dostęp 10 maja 2013. Dostępny w Internecie: http://links.jstor.org/pss/2265075

Ugander J., Karrer B., Backstrom L. & Marlow C. (2011), *The Anatomy of the Facebook Social Graph* [w:] *Journal of Applied Physics*. arXiv: 0906.0934

Ulanoff, L. (2011), *Your Digital Debris Is Haunting You* [w:] *PCMAG.com* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.pcmag.com/article2/0,2817,2386635,00.asp

Utz S. & Krämer N. (2009), *The privacy paradox on social network sites revisited: The role of individual characteristics and group norms* [w:] *Cyberpsychology Journal of Psychosocial Research on Cyberspace, 3*(2), s. 1–11 [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1

Venice (2006), *Facebook Gets a Facelift* [w:] *Blog na Facebooku* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://blog.facebook.com/blog.php?post=2207967130&comment_id=18467300&offset=250&total_comments=729

Walther J. B. (2002), *Research ethics in Internet-enabled research: human subjects issues and methodological myopia* [w:] *Ethics and information technology, 4*(3), s. 205–16. Springer.

Walther J. B. (2011), *Introduction To Privacy Online* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (s. 3–8). Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Westin A. F. (2003), *Social and Political Dimensions of Privacy* [w:] *Journal of Social Issues, 59*(2), 431-453. doi:10.1111/1540-4560.00072

Yao M. Z. (2011), *Self-Protection of Online Privacy: A Behavioral Approach* [w:] S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (s. 111–125). Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6

Zespół Rzecznika Prasowego Biura GIODO (2012), *FACEBOOK POWINIEN UDOSTĘPNIĆ POLITYKĘ PRYWATNOŚCI PO POLSKU* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://www.giodo.gov.pl/1520001/id_art/4517/j/pl

Zuckerberg M. (2006), *An Open Letter z: Mark Zuckerbeg* [w:] *Blog na Facebooku* [online], dostęp 10 maja 2013. Dostępny w Internecie: http://blog.facebook.com/blog.php?post=2208562130

Zukowski T. & Brown, I. (2007), *Examining the influence of demographic factors on internet users' information privacy concerns+* [w:] *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries – SAICSIT '07* (s. 197–204). New York, New York, USA: ACM Press. doi:10.1145/1292491.1292514

W ostatnich kilku latach, zarówno w mediach, jak i w dyskursie naukowym, zagadnienie prywatności w Sieci pojawia ze wzrastającą częstotliwością. Wszystkie strony w dyskusji, niezależnie od zajmowanego stanowiska, zgadzają się, że zbieranie i przetwarzanie danych o użytkownikach Internetu jest coraz powszechniejsze, łatwiejsze, tańsze i stwarza coraz większe możliwości dla podmiotów zarządzających tymi danymi. Zjawisko to jest pogłębiane przez zachowanie użytkowników, którzy dobrowolnie zamieszczają prywatne informacje w Internecie, często nie zdając sobie sprawy z konsekwencji. W rezultacie za pomocą wyszukiwarki internetowej można odnaleźć takie informacje jak imię i nazwisko, fotografie, ukończone szkoły, adres zamieszkania czy numer telefonu komórkowego.

Osoby, które bardzo aktywnie korzystają z różnych narzędzi w Internecie, pozostawiają po sobie ślady, pozwalające wręcz na odtworzenie ich aktywności na przestrzeni wielu miesięcy, zainteresowań, poglądów – praktycznie kompletnego profilu psychologicznego.

(ze wstępu)

Cena 24,00 zł

9 788364 203206

ISBN 978-83-64203-20-6