HANNA GAWEŁ
Instytut Studiów Informacyjnych
Wydział Zarządzania i Komunikacji Społecznej, Uniwersytet Jagielloński

Analiza śladów cyfrowych z perspektywy informatologii i cyberbezpieczeństwa

Exploring Digital Shadows From an Information Science and Cybersecurity Perspective

SŁOWA KLUCZOWE: cyberbezpieczeństwo, informatologia, ślady cyfrowe, zarządzanie informacją
KEYWORDS: cybersecurity, digital footprints, information management, information science

Abstrakt

CEL/TEZA: Celem rozważań jest wypracowanie propozycji spojrzenia na potencjał prowadzenia badań w ramach nauk o komunikacji i mediach z wykorzystaniem śladów cyfrowych (ang. *digital footprints*, *digital shadows*, *digital traces*) z perspektywy informatologii oraz cyberbezpieczeństwa.
KONCEPCJA/METODYKA BADAŃ: W rozważaniach teoretycznych bazujących na przeglądzie literatury przedmiotu skupiono się na zdefiniowaniu pojęcia śladu cyfrowego i określeniu jego własności i znaczenia w kontekście nauk o informacji oraz pojęcia cyberbezpieczeństwa.
WYNIKI I WNIOSKI: Ślady cyfrowe dzięki swojej formie i zróżnicowanemu polu badawczemu pozwalają na prowadzenie wysoko jakościowych pod względem metodologicznym badań naukowych, w których mogą stanowić nie tylko źródło danych badawczych, ale również odzwierciedlenie zachowań informacyjnych użytkowników Internetu. W zależności od kontekstu dane te mogą być wykorzystywane na różne sposoby, np. jako niezbywalny element walki o władzę, prezentacja nastrojów społecznych czy też forma sztuki.
ORYGINALNOŚĆ/WARTOŚĆ POZNAWCZA: Ze względu na swoją unikatowość badania śladów cyfrowych mogą wspomóc rozwój różnego rodzaju narzędzi zabezpieczających aktywność cyfrową użytkowników sieci.

Wprowadzenie

Zarządzanie informacją jest jednym z elementów pozwalających użytkownikom cyfrowym funkcjonować w przestrzeni Internetu. Rozwijająca się infrastruktura sieciowa stanowi podwalinę środowisk wirtualnych, jak również różnego rodzaju platform społecznościowych. Oprócz klasycznych problemów związanych z zarządzaniem informacją, takich jak jej obieg, wykorzystanie czy archiwizacja, dochodzą również kolejne, związane bezpośrednio z działalnością użytkowników w sieci (Babik, 2019, 16). Obecnie informacja stała się nie tylko daną, ale nabrała też różnych własności. Raz rozpatrywana jest jako dobro, które posiada wartość, innym razem prezentuje się ją jako spoiwo łączące bądź też dzielące społeczności. Znaczenia tu nabierają ślady cyfrowe, będące jednym z rodzajów informacji, jakie można spotkać w przestrzeni cyfrowej. Ze względu na ich właściwości, takie jak seminiematerialny charakter, podatność na modyfikacje, niejednorodność oraz formę, stanowić mogą bogatą bazę badawczą. Unikatowość śladów cyfrowych sprawia, że mogą być one również elementem pozwalającym optymalizować procesy zarządzania informacją w ujęciu interdyscyplinarnym.

Ślady cyfrowe są ważne również ze względu na powszechnie panujące przekonanie, iż można być anonimowym w sieci. Jest to błędne przekonanie, ponieważ każde połączone siecią urządzenie posiada przypisany unikatowy adres internetowy, czyli IP. Każdorazowe korzystanie z sieci polega na wymianie informacji pomiędzy urządzeniami, które w swoich *log files* rejestrują wykonywane czynności oraz dane o przesyle informacji. To pokazuje, że każdorazowa działalność w sieci pozostawia po sobie ślady, które mogą zostać wykorzystane do różnych czynności (Brunton, Driscoll & Gillespie, 2014).

Ślady cyfrowe – próba zdefiniowania problemu

Kompleksowe ewidencjonowanie osobistych mediów i komunikacji było jednym z motorów rozwoju współczesnej cyfryzacji. Jeszcze w 1954 r. Vannevar Bush stworzył koncepcję mechanicznego urządzenia Memex, które przechowywałoby informacje o wszystkich przeczytanych książkach, nagraniach oraz komunikatach stworzonych przez użytkownika i dawałoby możliwość przeszukiwania zapisanego materiału (Bush, 1945). Kolejne etapy rozwoju cyfrowego pozwoliły na upowszechnienie różnego rodzaju udogodnień funkcjonowania w przestrzeni cyfrowej, ale doprowadziło to również do zwiększenia liczby generowanych codziennie śladów cyfrowych przez każdego użytkownika Internetu.

Termin „ślady cyfrowe" pojawił się w literaturze anglosaskiej na początku lat 2000–2010 (Anjewierden & Efimova, 2006; Girardin et al., 2008; Roberts, 2000; Weaver & Gahegan, 2007), gdzie występuje pod nazwami takimi jak *digital footprints*, *digital shadows* czy też *digital traces*. Pojawienie się w Polsce terminu „ślady cyfrowe" zbiegło się w czasie z zaistnieniem pojęcia „zarządzanie informacją". Informacja jest tu rozumiana jako dobro posiadające wartość, podobnie jak np. gotówka (Babik, 2019, 16), co przełożyło się również na sformalizowanie wartości informacji, m.in. poprzez utworzenie pierwszej

na świecie giełdy informacji (Yang, 2021). Choć różne określenia mogą wskazywać na odmienny przedmiot zainteresowania, opisują one mniej więcej to samo zagadnienie. Jednocześnie rodzi to potrzebę sformułowania propozycji bardziej jednoznacznego rozumienia pojęcia śladu cyfrowego, które wyznaczy przedmiot i zakres rozważań. Pojęcie to można opisać za pomocą dwóch następujących kryteriów:

- podmiotowego (kto tworzy?),
- przedmiotowego, odnoszącego się do zasobów (co jest?).

Zgodnie z kryterium podmiotowym przyjmuję, że ślad cyfrowy jest tworzony przez konkretną jednostkę, ale może też być generowany przez zbiorowość, z tym że metadane opisują wtedy działania pojedynczej osoby korzystającej z urządzenia pozwalającego na rejestrację śladu cyfrowego.

Ślady cyfrowe są definiowane jako dane wygenerowane przez indywidualną bądź zbiorową aktywność w sieci, co odnosi się do kryterium przedmiotowego pojęcia śladu cyfrowego. Informacje te są połączone z metadanymi w celu uzyskania całkowicie unikatowej mieszanki informacji, która jest w stanie udowodnić, że dany użytkownik posiada prawdziwą tożsamość. Jest to możliwe do osiągnięcia dzięki określonym wzorcom oraz powtarzalności – wskazują one, że istnieje tylko jeden użytkownik i wiele elementów, które reprezentują go cyfrowo. Co zatem składa się na ślady cyfrowe? Pierwszą kwestią jest ich lokalizacja, ponieważ część z nich znajduje się w *log files* urządzeń, z których korzystają użytkownicy, a część pozostaje w przestrzeni cyfrowej, rejestrowana przez przeglądarki, aplikacje, programy online oraz cyfrowe rzeczywistości. Powoduje to rozproszenie śladów cyfrowych nie tylko na różnych urządzeniach, ale także w świecie fizycznym oraz cyfrowym.

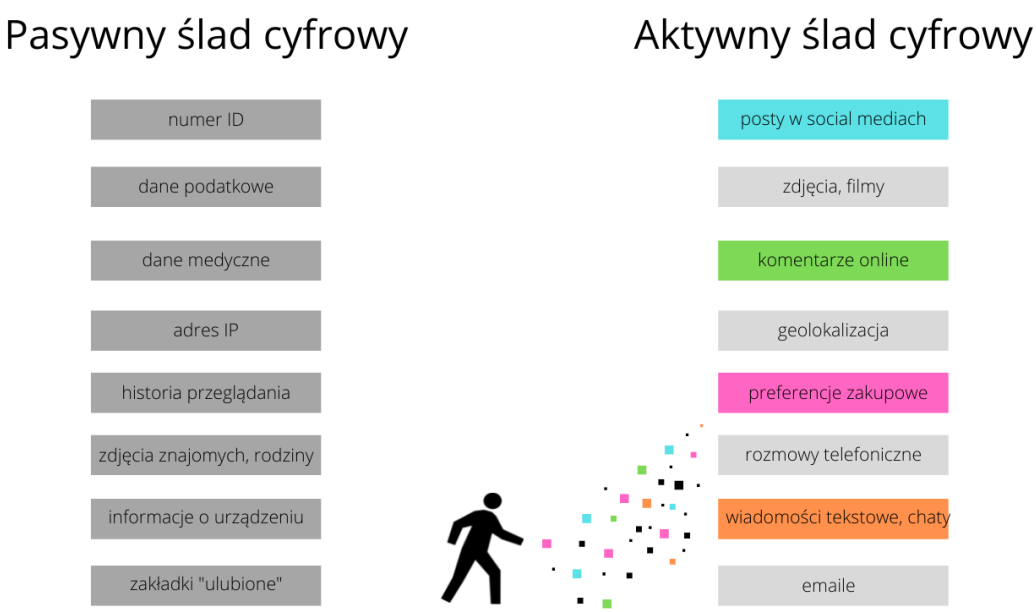
Zarządzanie śladami cyfrowymi, podobnie jak zarządzanie informacją, wiąże się z realizacją takich operacji, jak:

- generowanie śladów cyfrowych,
- pozyskiwanie śladów cyfrowych,
- gromadzenie śladów cyfrowych,
- przechowywanie śladów cyfrowych,
- udostępnianie śladów cyfrowych,
- dystrybucja śladów cyfrowych.

Praca ze śladami cyfrowymi ze względu na ich charakter oraz formę wymaga podobnego podejścia jak w przypadku zarządzania informacją. Ze względu na świadomość działania użytkownika ślady cyfrowe można podzielić na pasywne i aktywne.

Ślady cyfrowe pasywne są informacjami, które użytkownik w niezamierzony sposób pozostawia w trakcie swojej działalności w przestrzeni cyfrowej. Są to m.in. adres IP, lokalizacja bądź też historia przeglądania / historia aktywności.

Ślady cyfrowe aktywne to ślady utworzone przez świadomą działalność użytkownika. Przykładem takich śladów mogą być posty opublikowane w mediach społecznościowych, przesyłane zdjęcia, ale również korespondencja mailowa.



Rysunek 1. Przykłady pasywnych i aktywnych śladów cyfrowych. Źródło: opracowanie własne, 2022

Ze względu na stopień tajności ślady cyfrowe dzieli się na umożliwiające identyfikację osoby i anonimowe.

Ślady cyfrowe umożliwiające identyfikację osoby są danymi pozwalającymi na poznanie tożsamości cyfrowej, jak również fizycznej użytkownika, który w trakcie aktywności cyfrowej pozostawił po sobie ślady. Informacje te umożliwiają rozpoznanie użytkownika przy wykorzystaniu mniej lub bardziej zaawansowanego zestawu narzędzi rozpoznania z ogólnodostępnych źródeł (biały wywiad), jak również z wykorzystaniem elementów tzw. szarego i czarnego wywiadu.

Anonimowe ślady cyfrowe są danymi generowanymi anonimowo, przykładowo na forum internetowym przy użyciu pseudonimu. Obecnie na rynku istnieje wiele narzędzi, pozwalających na zapewnienie anonimowości w sieci. Są to:

- VPN (Virtual Private Network) – maskowanie adresu IP przez użytkowników. Jest to technologia polegająca na przekierowywaniu połączeń internetowych użytkowników w taki sposób, że urządzenia sieciowe są niemożliwe do wyśledzenia. VPN gwarantuje nie tylko anonimowość w Internecie, ale i bezpieczeństwo danych oraz ochronę przed atakami ze strony hakerów.
- Tor (The Onion Router) – bezpłatny serwis anonimizujący, pozwalający na zacieranie śladów cyfrowych w Internecie. Podczas surfowania za pomocą Tora ukrywa się adres IP komputera. Działa to na zasadzie trasowania cebulowego – przesyłane informacje są wielokrotnie szyfrowane w sposób warstwowy (Charzyński, 2021). Wiadomość jest opakowywana w kilka warstw szyfrowania, a następnie przechodzi

przez serie tzw. routerów cebulowych (serwerów). Routery te to specyficzne węzły sieciowe, z których każdy ma uprawnienia do odszyfrowania wyłącznie jednej warstwy, a następnie przekazania informacji do następnych serwerów. Po odszyfrowaniu ostatniej z nich wiadomość trafia do odbiorcy.

- Maszyny wirtualne – maszyna wirtualna (Virtual Machine, w skrócie VM), mówiąc najprościej, to komputer składający się jedynie z warstwy oprogramowania. Wirtualna stacja robocza jest zupełnie odizolowana od sieci, a jedyne dozwolone połączenia odbywają się za pomocą maszyny pośredniczącej, co pozwala na zachowanie anonimowości (Wen, Zhao & Wang, 2008).
- Freenet – to darmowe oprogramowanie, które umożliwia anonimowe udostępnianie plików, przeglądanie i publikowanie *freesites* (stron internetowych dostępnych tylko za pośrednictwem Freenetu) oraz czatowanie na forach bez obawy o cenzurę. Freenet jest zdecentralizowany, a dzięki temu mniej podatny na ataki. Jeśli jest używany w trybie darknet, w którym użytkownicy łączą się tylko ze swoimi znajomymi, bardzo trudno go wykryć (Clarke et al., 2001). Komunikacja między węzłami Freenetu jest szyfrowana i przekazywana przez inne węzły, dzięki czemu bardzo trudno ustalić, kto żąda informacji i jaka jest ich treść.
- Serwer proxy – to swego rodzaju pośrednik między komputerem, z którego operuje użytkownik, a serwerami hostingowymi z umieszczonymi na nich witrynami i serwisami, które chce on przeglądać (Weng & Lai, 2021). Ta swoista platforma działa na zasadzie pełnomocnictwa (działa w naszym imieniu) i podlega konfiguracji, dzięki której użytkownik otrzymuje dodatkowe opcje sieciowe, w tym anonimowość poprzez maskowanie IP (Lioudakis et al., 2007).
- System operacyjny Tails – (The Amnesic Incognito Live System, w przybliżonym tłumaczeniu Niezapamiętujący anonimowy system bieżący) może być używany na dowolnym komputerze, niezależnie od systemu operacyjnego zainstalowanego na tym komputerze (Dawson & Cárdenas-Haro, 2017). Oferuje swoim użytkownikom ochronę przed cenzurą, monitoringiem przez osoby trzecie i reklamą.
- Maile tymczasowe (ang. *burner emails*) – to maile aliasy, które można po zakończeniu korzystania zutylizować, nie niszcząc przy tym preferowanego konta mailowego.
- Alternatywne serwisy pocztowe – serwisy pocztowe typu Posteo.de, Tutanota, Mailbox.org czy też CTemplar, które oferują dodatkowe zabezpieczenia prywatności oraz ochronę korespondencji mailowej.
- Alternatywne wyszukiwarki internetowe – przeglądarki takie jak Brave, Ungoogled Chromium, Iridium oraz Epic. Nie buforują one danych przeglądania ani nie zapisują linków dla autosugestii podczas wpisywania adresu. Przeglądarki blokują również połączenia RTC, które mogą ujawnić adres IP użytkownika.
- Szyfrowane aplikacje komunikacyjne – aplikacje, które wykorzystują zabezpieczenia konwersacji, haseł oraz kontaktów. Do tej grupy zalicza się komunikatory takie jak: LINE, Dust, Silence, Threema.

Powyższa lista jest zaledwie zalążkiem rozwiązań dostępnych na rynku, dlatego nie należy traktować jej jako pełnej. Rozwój technologii cyfrowych umożliwia wykorzystanie różnego rodzaju rozwiązań, które mogą sprawić, że użytkownicy będą niewidoczni w sieci. Oprócz tego dobre praktyki zaobserwowane na podstawie działalności cyfrowej pokazują, że najlepsze rozwiązanie zapewniające anonimowość to wykorzystywanie kilku rozwiązań jednocześnie (Gouert & Tsoutsos, 2022; O'Brien et al., 2018; Walker & Hargittai, 2021).

Ze względu na działalność użytkowników w sieci ślady cyfrowe dzielą się na wprowadzane przez użytkownika i dane z czujników (sensorów).

Ślady cyfrowe wprowadzane przez użytkownika to informacje, których autorem jest dany użytkownik sieci. Dane te są wprowadzane poprzez wpisywanie, dyktowanie, wgrywanie do sieci. Te aktywne ślady danych z czasem się gromadzą i tworzą coraz dokładniejszy obraz tożsamości, rzeczy, preferencji, historii i stylu życia użytkownika, w tym jego/jej relacji.

Ślady cyfrowe pochodzące z czujników to informacje zbierane bezpośrednio przez urządzenia (np. czujniki ruchu, GPS, urządzenia z grupy IoT – Internet of Things), które gromadzą, przetwarzają oraz zapisują dane w czasie pracy. Urządzenia te mogą automatycznie komunikować się i wymieniać dane za pomocą sieci bez ingerencji człowieka. Co jest ważne i warte podkreślenia, po części użytkownik może mieć kontrolę nad śladami cyfrowymi. Można ją rozpatrywać jako element indywidualnego zarządzania informacją (Sapa, 2020) jedynie w przypadku, gdy użytkownik jest świadomym twórcą tych śladów, ale częściej nie ma on kontroli nad tym aspektem działalności sieciowej; często nie wie, jakiego rodzaju ani gdzie te ślady są pozostawiane w przestrzeni cyfrowej.

Ślady cyfrowe w kontekście zarządzania informacją

Współcześnie ludzie uzyskują dwie tożsamości, mianowicie „tożsamość rzeczywistą", która jest weryfikowana na podstawie oficjalnej dokumentacji papierowej, oraz „tożsamość cyfrową", określaną na podstawie korzystania przez daną osobę z Internetu, w tym historii wyszukiwania, usług online, forów, blogów oraz mediów społecznościowych (Pisano et al., 2017; Putikadyanto, Adriana & Efendi, 2021; Qin & Lowe, 2021). Dostęp do cyfrowej tożsamości jednostki często pozwala na tworzenie powiązań z rzeczywistą tożsamością danej osoby. Ślad cyfrowy reprezentuje obecność danej osoby w sieci i stanowi dowód jej tożsamości w świecie cyfrowym i rzeczywistym (Blinka & Smahel, 2009; Johns, 2018; Longo, 2018). Rejestruje on ślady i artefakty pozostawione przez osoby wchodzące w interakcje w środowisku cyfrowym (Sjöberg et al., 2016). Cyfrowe ślady w większości przypadków są trwałe i łączą przeszłość z teraźniejszością, niezależnie od przemian danej osoby i zmian w jej życiu (Щекотин, 2021). Wiesław Babik określa zarządzanie informacją jako „proces świadomego przepływu informacji" (Babik, 2019, 30). W kontekście zarządzania informacją ślady cyfrowe mogą być rozpatrywane jako źródło informacji, które uczestniczy w obiegu informacji, ale nie tylko. Ślady cyfrowe

są unikatowe dla każdego użytkownika, ponieważ wynikają z jego aktywności w sieci. Może się to wiązać z:

- prezentowaniem przez użytkownika prywatnych informacji (posty, tweety, zdjęcia);
- generowaniem śladów wiążących się z funkcjonowaniem w określonej bańce informacyjnej;
- budowaniem śladu cyfrowego na podstawie długości aktywności w sieci (im dłuższa, tym więcej śladów będzie generowanych);
- tworzeniem sztucznej tożsamości w sieci w zamierzonym celu (fikcyjne konta, trollowanie w sieci).

Jeśli przyjąć, że ślady cyfrowe składają się z informacji oraz przypisanego zestawu metadanych, można je badać pod kątem wartości danych, co da się wykorzystać w badaniach zachowań informacyjnych. Stwarza to bezprecedensowe możliwości gromadzenia danych zarówno eksperymentalnych, jak i obserwacyjnych w skali jednocześnie masowej i mikroskopowej; masowej w takim sensie, że badanych osób mogą być miliony, a dane rozrastać się do terabajtów; mikroskopowej zaś w takim sensie, że rejestrowane są indywidualne mikrointerakcje (Bujlow et al., 2015). Zamiast retrospektywnych raportów na temat zachowań i interakcji badanych ślady cyfrowe mogą dostarczyć szczegółowych zapisów codziennych czynności oraz częstotliwości i intensywności relacji społecznych. Podsumowując: ślady cyfrowe odzwierciedlają aktywność każdej osoby w sieci. Zautomatyzowany ślad cyfrowy stanowi rejestr zwyczajów, zainteresowań, wydarzeń, relacji i komunikacji, które są powiązane z fizycznym życiem danego użytkownika. Tak definiowane ślady cyfrowe w dużym stopniu wpisują się w informatologiczny obszar badań nad zachowaniami informacyjnymi ludzi (Sosińska-Kalata, 2013).

Ślady cyfrowe w kontekście cyberbezpieczeństwa

Ślady cyfrowe stanowią jeden z ważniejszych elementów badań w dziedzinie cyberbezpieczeństwa oraz informatyki śledczej. Na przykład osoby zajmujące się informatyką śledczą starają się określić legalność komunikacji i działań w sieci, aby zapobiegać przestępstwom takim jak nękanie, molestowanie czy nieuprawnione przekazywanie informacji. Jednym ze sposobów radzenia sobie z tym wyzwaniem jest analiza śladów cyfrowych, które „obiektywnie ujawniają" tożsamość danej osoby. Przykładowo: badacze osobowości sugerują, że osoby pozostawiają ślady behawioralne (nieświadome ślady działań, które mogą obiektywnie przedstawiać ich tożsamość, np. historie przeglądania stron internetowych), kiedy kontaktują się z innymi osobami (Dolin et al., 2018). W tym kontekście umiejętność właściwego zarządzania śladami cyfrowymi jest związana z prawidłowym i efektywnym korzystaniem z Internetu, co może wiązać się z rozwojem umiejętności cyfrowych, higieną cyfrową oraz ekologią informacji (Babik, 2014; Gaweł, 2021; Jachym, 2015). Jeśli chodzi o kwestię ograniczonej kontroli użytkowników nad przepływem informacji osobistych, można zauważyć, że ślady cyfrowe mogą stanowić wartościowy materiał cyfrowy, którego pozyskanie nie musi wiązać się z większymi trudnościami (Christl, 2017).

Część śladów pozostawianych nieświadomie jest agregowana poprzez pliki cookie, które rejestrują działalność użytkowników w sieci (Binns et al., 2018; Dudykevych & Nechypor, 2016; Wambach & Bräunlich, 2016). Pliki cookie to małe pliki tekstowe umieszczane na urządzeniu użytkownika podczas odwiedzania witryny internetowej. Można wyróżnić dwa ogólne rodzaje takich plików. Pliki cookie należące do tzw. pierwszej strony są używane głównie po to, aby przeglądanie stron było bardziej przyjazne dla użytkownika. Są one umieszczane przez odwiedzaną witrynę (pierwszą stronę). Często ich celem jest ułatwienie funkcjonowania strony internetowej, np. poprzez zapisywanie preferencji językowych. Plik cookie może gromadzić kompletne informacje o stronach odwiedzanych przez użytkownika tylko wtedy, gdy wszystkie te strony posiadają taki plik (Kumar & Shanker, 2019).

W ostatnich latach opracowano inne techniki, takie jak fingerprinting przeglądarki oraz kanwy, które uzupełniają i zastępują pliki cookie (Bezawada, Ray & Ray, 2021; Halstead et al., 2021; Nottingham, 2020). Techniki fingerprintingu pozwalają osobom trzecim na identyfikację użytkowników poprzez rozpoznawanie unikalnych kombinacji cech, takich jak własności urządzenia (laptop, smartfon, oprogramowanie bazowe), używana przeglądarka i zainstalowane czcionki. W przeciwieństwie do plików cookie, które użytkownicy mogą odrzucić lub usunąć (Chen et al., 2021; Englehardt et al., 2015), trudno jest ukryć odcisk palca przeglądarki, a zatem osoby przeglądające strony internetowe mogą być łatwo ponownie zidentyfikowane. W związku z tym fingerprinting to kolejna, jeszcze potężniejsza technika rejestrowania aktywności użytkowników w sieci. Cyberprzestępczość przekształciła się z nikczemnego hobby pojedynczych hakerów w wysoce zorganizowaną, międzynarodową sieć biznesową obejmującą każdy aspekt działań związanych z cyberatakami, w tym czarne rynki skradzionych danych, czego sporą część stanowią ślady cyfrowe użytkowników sieci.

W związku z szybką i masową zmianą w Internecie istnieją obawy, że użytkownicy nie są wystarczająco przeszkoleni, używają nieznanych narzędzi, nie mają doświadczenia w stosowaniu technologii, a w rezultacie stają się łatwym celem dla cyberprzestępców. W przypadku cyberprzestępczości osoby fizyczne często aktywnie uczestniczą w procesie oszustwa, którego stają się ofiarami, np. odpowiadając na wiadomość phishingową i podając prywatne informacje (Bajanthri & Sayeesh, 2022; Edwards, Peersman & Rashid, 2017; Maennel, Mäses & Maennel, 2018; Rege, 2009). Mogą one nie być wystarczająco podejrzliwe, mogą nie być w stanie wykryć oszukańczych wiadomości lub nie być wystarczająco uważne, aby zatrzymać oszukańczy proceder. Rutynowe manipulowanie czynnościami użytkowników w ramach ukierunkowanej reklamy internetowej może utrudnić dostrzeżenie oszukańczych manipulacji dokonywanych przez cyberprzestępców (Akdemir & Lawless, 2020; Boehmer et al., 2015; Borwell, Jansen & Stol, 2018; Hahm et al., 2009). W badaniach nad bezpieczeństwem cybernetycznym odchodzi się więc powoli od koncentrowania się na technologii na rzecz uznania kluczowego znaczenia ludzkiego postępowania, czynników społecznych i kulturowych. Prowadzi to do przesunięcia środka ciężkości badań w stronę zachowań informacyjnych

użytkowników, jak również treści przez nich generowanych, a stanowiących składową ich cyfrowej tożsamości.

Kluczowe problemy związane ze śladami cyfrowymi

Ślady cyfrowe stawiają przed badaczami szereg przeszkód, począwszy od wiarygodności danych i sposobu ich próbkowania, a skończywszy na kwestiach etycznych związanych z ich wykorzystaniem. Ślady cyfrowe jako dane stanowią paradoks w zakresie ochrony prywatności: informacje są jednocześnie zbyt odkrywcze, jeśli chodzi o ochronę prywatności, ale też niewystarczająco odkrywcze, jeśli chodzi o dostarczanie podstawowych informacji demograficznych potrzebnych badaczom społecznym. Często nie zawierają szczegółowych informacji o profilu demograficznym, które są standardem w badaniach ankietowych.

Drugą kwestią powiązaną z zarządzaniem informacją jest polityka informacyjna śladów cyfrowych. Ślady mogą być wytwarzane przez instytucje, społeczności i przede wszystkim przez indywidualnych użytkowników. Osoby prywatne, jak również zbiorowości czy instytucje gromadzą dane, aby zdobyć informacje niezbędne do realizacji określonego celu. Współczesna struktura sieci telekomunikacyjnej sprawia, że nie tylko instytucje, ale też jednostki stają się centrami informacyjnymi, a użytkownicy Internetu przyjmują zarówno rolę strażnika, jak i menadżera sieci informacyjnej. Część aspektów związanych z gromadzeniem, przetwarzaniem i archiwizacją śladów cyfrowych jest uregulowana prawnie oraz technologicznie, ale pozostaje nadal wiele białych pól dotyczących tego zagadnienia, wartych rozwinięcia w ramach rozwoju badań naukowych.

Kolejny problem to wykorzystywanie śladów cyfrowych wyszukanych za pomocą narzędzi przeznaczonych do procesu wyszukiwawczego. Choć z jednej strony celem specjalistów od informacji jest uzyskanie informacji, kwestię sporną stanowi wykorzystanie znalezionych śladów cyfrowych. Czy powinna istnieć możliwość wykorzystywania wszystkich śladów cyfrowych generowanych przez użytkowników, czy tylko niektórych? To pytanie dotyczy kwestii użycia, którą można rozpatrywać w kontekście etycznym, prawnym czy też komunikacyjnym.

Badacze stoją również przed wyzwaniem uogólniania zachowań w sieci na postępowanie poza nią. Interakcje online różnią się od tych offline w istotny sposób, m.in. ze względu na zniesienie ograniczeń geograficznych i czasowych związanych z komunikacją twarzą w twarz. Na przykład możliwość oczekiwania na odpowiedź na wiadomość e-mail lub SMS albo na aktualizację statusu daje szansę na introspekcję oraz bardziej przemyślaną i strategiczną autoprezentację (Ellison, Heino & Gibbs, 2006). Anonimowość, na którą pozwalają pewne platformy internetowe, daje użytkownikom możliwość wymyślenia zupełnie nowej postaci. Budzi to wątpliwości co do wiarygodności danych z profili demograficznych. Anonimowość może także umożliwiać wygłaszanie wulgarnych wypowiedzi, które przewijają się w wielu rozmowach w sieci, ale są nie do pomyślenia poza nią, lub do tego zachęcać (Crace, 2016; Woods & Ruscher, 2021). Różnice między

trybami komunikacji online i offline były przedmiotem wielu badań koncentrujących się na ich porównywalnym bogactwie, czyli szerokości pasma dostępnego dla przekazu wskazówek werbalnych i wizualnych.

Przepaść cyfrowa związana z mniej lub bardziej rozwiniętymi kompetencjami informacyjnymi rodzi dodatkowe obawy dotyczące uogólniania danych z populacji online na populacje offline. Ludzie korzystający z Internetu są zazwyczaj młodsi, lepiej wykształceni i zamożniejsi niż ogół społeczeństwa, co również rodzi istotne pytania o możliwość powielania, a nawet wzmacniania rozwarstwienia społecznego (Horvát & Hargittai, 2021; Lawless, Schrader & Mayall, 2007; Nguyen, Hunsaker & Hargittai, 2019). Nawet tam, gdzie dostęp do technologii jest możliwy, umiejętności korzystania z niego są nierównomiernie rozłożone, co może prowadzić do nierównego poziomu uczestnictwa w różnych przestrzeniach cyfrowych i przez co ślady cyfrowe w większości będą pochodziły od aktywnych członków społeczności sieciowej.

W kierunku badań z wykorzystaniem śladów cyfrowych

Ślady cyfrowe stanowią dzisiaj szerokie i zróżnicowane pole badawcze, na którym można wskazać kilka obszarów, takich jak prywatność, zastosowanie śladów cyfrowych oraz metodologia badań śladów cyfrowych.

Prywatność to wieloaspektowy konstrukt, który został zdefiniowany przez badaczy z różnych dziedzin nauki. Definicje obejmują „prawo do bycia pozostawionym w spokoju", „stan ograniczonego dostępu lub izolacji" oraz „kontrolę dostępu do siebie i ujawniania informacji" (Koops & Galič, 2021, 6). Rozwój cyfryzacji skierował uwagę na jeden z aspektów prywatności: pojęcie prywatności informacji, czyli „roszczenia jednostek, grup lub instytucji do decydowania o tym, kiedy, w jaki sposób i w jakim zakresie informacje o nich są przekazywane innym" (Koops & Galič, 2021, 29). Nie tylko pojęcie to i jego definicja są dość niejasne. Również jego pomiar okazuje się trudny.

Użytkownicy Internetu są dość zaniepokojeni swoją prywatnością i ryzykiem związanym z ujawnianiem informacji. Paradoksalnie zachowania użytkowników sieci niekoniecznie odzwierciedlają tę postawę, co jest zjawiskiem powszechnie nazywanym paradoksem prywatności (Chhabra, 2022; Davis, 2003; Øverby, 2021). Ludziom zależy na tym, aby mieć wiedzę (oraz kontrolę) nad informacją. Ważna jest dla nich wiedza o tym, kto zarządza informacją, do czego zostanie ona wykorzystana, wreszcie jakie dane są zbierane. Jednocześnie obserwuje się przypadki internetowego ekshibicjonizmu informacyjnego, który eksponuje informacje w sieci, w tym świadome ślady cyfrowe. Wiąże się to z ciekawym pojęciem rachunku prywatności (Alotaibi, 2017; Min & Kim, 2015), który można rozumieć jako ważenie zysków oraz strat związanych z udostępnianiem informacji. Jeśli postrzegane korzyści przeważają nad postrzeganym ryzykiem, istnieje większe prawdopodobieństwo ujawnienia informacji; natomiast jeśli postrzegane ryzyko przeważa nad ewentualnymi korzyściami, prawdopodobieństwo ujawnienia informacji jest mniejsze. Zagadnienie rachunku prywatności w kontekście badania śladów

cyfrowych może stanowić rozwojowy kierunek badań informatologicznych.

Ślady cyfrowe da się wykorzystać na dwa sposoby. Jeden z nich jest pozytywny: ślady cyfrowe pozostawione przez mieszkańców cyberprzestrzeni mogą pomóc zmienić cyberśrodowisko na lepsze, uczynić je piękniejszym i wygodniejszym. Druga opcja może budzić zdecydowany sprzeciw: jest to sposób na nadzorowanie i kontrolowanie użytkowników. Ludzie zaczynają zostawiać ślady cyfrowe dosłownie od kołyski, kiedy nie potrafią jeszcze mówić, a co dopiero mówić o korzystaniu z komputera. Istotną rolę odgrywają w tym rodzice, zamieszczający zdjęcia i historie swoich dzieci w mediach społecznościowych (Steinberg, 2016). Nastolatki aktywnie korzystają z Internetu, ale często nie wiedzą, jak robić to bezpiecznie (Walrave et al., 2016; Wójcik, 2021). Jednocześnie literatura naukowa nie prezentuje korzyści z posiadania śladów cyfrowych, nie jest to również powszechnie omawiany temat w edukacji cyfrowej. Otwiera się tu kolejna duża luka badawcza, ponieważ należy opracować interwencje edukacyjne, które wzmocnią pozycję użytkowników sieci i zapewnią im ochronę, a także uzupełnią ich dotychczasowe strategie zarządzania śladami cyfrowymi, co wiąże się z kuratorstwem danych cyfrowych.

Zakończenie

Badania śladów cyfrowych rozwijają się w różnych kierunkach, a ich właściwości budzą zainteresowanie reprezentantów wielu dyscyplin naukowych. Z jednej strony traktowanie śladów informacyjnych jako źródła danych sytuuje badania w nurtach badań o komunikacji i mediach. Z drugiej strony aspekty problematyki związanej z właściwościami śladów cyfrowych pozwalają dostrzec badania z ich wykorzystaniem w dziedzinie psychologii, cyberbezpieczeństwa czy też kognitywistyki.

Ślady cyfrowe są interdyscyplinarnym obszarem, związanym z działalnością człowieka w przestrzeni cyfrowej. Zasygnalizowane aspekty teoretyczne śladów informacyjnych otwierają nowe perspektywy badawcze i implikują szereg pytań, na które mogą odpowiedzieć m.in. badacze informacji. Tak jak prehistoryczne malowidła naskalne, ślady cyfrowe to jeden z dowodów rozwoju ludzkości, który w przyszłości będzie stanowić przegląd aktywności współczesnego człowieka w sferze cyfrowej.

Bibliografia

Akdemir, Naci; Lawless, Christopher J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet Research*, vol. 30, no. 6, pp. 1665–1687. doi:10.1108/intr-10-2019-0400

Alotaibi, Mutlaq B. (2017). Determinants of information disclosure intention in mobile commerce: an extended privacy calculus model. *International Journal of Computer Applications in Technology*, vol. 56, no. 4, pp. 319–329. doi:10.1504/ijcat.2017.10009944

Anjewierden, Anjo; Efimova, Lilia (2006). Understanding weblog communities through digital traces: a framework, a tool and an example. In: Robert Meersman, Zahir

Tari, Pilar Herrero eds. *Lecture notes in computer science. On the move to meaningful internet systems 2006: OTM 2006 Workshops*, vol. 4277. Berlin, Heidelberg: Springer, pp. 279–289. doi:10.1007/11915034_51

Babik, Wiesław (2014). O konsumpcji informacji w e-społeczeństwie z punktu widzenia ekologii informacji. W: Beata Taraszkiewicz, red. *Ekologia informacji w e-społeczeństwie*, s. 7–25. https://depot.ceon.pl/bitstream/handle/123456789/17699/Ekologia%20informacji%20-%20Taraszkiewicz.pdf?sequence=1#page=7 (odczyt: 12.04.2022).

Babik, Wiesław (2019). Zarządzanie informacją: ważne wyzwanie współczesności. W: Wiesław Babik red. *Zarządzanie informacją*. Warszawa: Wydaw. Stowarzyszenia Bibliotekarzy Polskich, s. 15–32.

Bajanthri, Bhagya; Sayeesh M. (2022). A study on various phishing techniques and recent phishing attacks. *International Journal of Advanced Research in Science, Communication and Technology*, vol. 2, issue 2, pp. 296–302. doi:10.48175/ijarsct-2870

Bezawada, Bruhadeshwar; Ray, Indrakshi; Ray, Indrajit (2021). Behavioral fingerprinting of Internet-of-Things devices. *WIREs Data Mining and Knowledge Discovery*, vol. 11, issue 1. doi:10.1002/widm.1337

Binns, Reuben et al. (2018). Third party tracking in the mobile ecosystem. In: *Proceedings of the 10th ACM Conference on Web Science: WebSci '18*, pp. 23–31. doi:10.1145/3201064.3201089

Blinka, Lukas; Smahel, David (2009). Fourteen is fourteen and a girl is a girl: validating the identity of adolescent bloggers. *CyberPsychology & Behavior*, vol. 12, no. 6, pp. 735–739. doi:10.1089/cpb.2009.0044

Boehmer, Jan; LaRose, Robert; Rifon, Nora J.; Alhabash, Saleem; Cotten, Shelia R. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology*, vol. 34, no. 10, pp. 1022–1035. doi:10.1080/0144929x.2015.1028448

Borwell, Jildau; Jansen, Jurjen; Stol, Wouter (2018). Human factors leading to online fraud victimisation: literature review and exploring the role of personality traits. In: John McAlaney, Lara A. Frumkin, Vladlena Benson eds. *Psychological and behavioral examinations in cyber security*. Hershey, PA: IGI Global, pp. 26–45. doi:10.4018/978-1-5225-4053-3.ch002

Brunton, Finn; Driscoll, Kevin; Gillespie, Tarleton (2014). Culture digitally: spam, and the challenge of chasing shadows. *Journal of Broadcasting & Electronic Media*, vol. 58, no. 4, pp. 687–697. doi:10.1080/08838151.2014.966366

Bujlow, Tomasz; Carela-Español, Valentin; Solé-Pareta, Josep; Barlet-Ros, Pere (2015). Web tracking: mechanisms, implications, and defenses. http://arxiv.org/abs/1507.07872 (odczyt: 22.03.2022).

Bush, Vannevar (1945). As we may think. *The Atlantic Monthly*, vol. 176, no. 1, pp. 101–108. https://www.ias.ac.in/article/fulltext/reso/005/11/0094-0103 (odczyt: 22.03.2022).

Charzyński, Błażej (2021). Sieć Tor, przeglądarka i trasowanie cebulowe: wszystko, co musisz wiedzieć. https://scroll.morele.net/poradniki/siec-tor-przegladarka-i-trasowanie-cebulowe-wszystko-co-musisz-wiedziec/ (odczyt: 23.03.2022).

Chen, Quan; Ilia, Panagiotis; Polychronakis, Michalis; Kapravelos, Alexandros (2021). Cookie swap party: abusing first-party cookies for web tracking. In: *Proceedings of the Web Conference 2021: WWW '21*, pp. 2117–2129. doi:10.1145/3442381.3449837

Chhabra, Sakhhi (2022). Why does privacy paradox exist? A qualitative inquiry to understand the reasons for privacy paradox among smartphone users. *Journal of Electronic Commerce in Organizations*, vol. 20, no. 1, pp. 1–20. doi:10.4018/jeco.292470

Christl, Wolfie (2017). *Corporate surveillance in everyday life: how companies collect, combine, analyze, trade, and use personal data on billions: a report by Cracked Labs, Vienna, June 2017*. Vienna: Cracked Lab: Institute for Critical Digital Culture. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf (odczyt: 23.03.2022).

Clarke, Ian; Sandberg, Oskar; Wiley, Brandon; Hong, Theodore W. (2001). Freenet: a distributed anonymous information storage and retrieval system. In: Hannes Federrath ed. *Designing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings*. Berlin, Heidelberg: Springer, pp. 46–66. doi:10.1007/3-540-44702-4_4

Crace, John (2016). A meeting at Trolls Anonymous: a humorous sketch imagining what would happen if vicious online commentators met face to face. *Index on Censorship*, vol. 45, no. 3, pp. 30–31. doi:10.1177/0306422016670334

Davis, Charles N. (2003). Electronic access to information and the privacy paradox: rethinking practical obscurity and its impact on electronic freedom of information. *Social Science Computer Review*, vol. 21, no. 1, pp. 15–25. doi:10.1177/0894439302238968

Dawson, Maurice; Cárdenas-Haro, Jose Antonio (2017). Tails Linux operating system: remaining anonymous with the assistance of an incognito system in times of high surveillance. *International Journal of Hyperconnectivity and the Internet of Things*, vol. 1, no. 1, pp. 47–55. doi:10.4018/IJH1oT.2017010104

Dolin, Claire; Weinshel, Ben; Shan, Shawn; Hahn, Chang Min; Choi, Euirim; Mazurek, Michelle L.; Ur, Blasé (2018). Unpacking perceptions of data-driven inferences underlying online targeting and personalization. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems: CHI '18*, paper 493, pp. 1–12. doi:10.1145/3173574.3174067

Dudykevych, Valery; Nechypor, Vitalii (2016). Detecting third-party user trackers with cookie files. In: *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, pp. 78–80. doi:10.1109/infocommst.2016.7905341

Edwards, Matthew; Peersman, Claudia; Rashid, Awais (2017). Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. In: *Proceedings of the 26th International Conference on World Wide Web Companion: WWW '17 Companion*, pp. 1291–1299. doi:10.1145/3041021.3053889

Ellison, Nicole; Heino, Rebecca; Gibbs, Jennifer (2006). Managing impressions online: self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication*, vol. 11, issue 2, pp. 415–441. doi:10.1111/j.1083-6101.2006.00020.x

Englehardt, Steven; Reisman, Dillon; Eubank, Christian; Zimmerman, Peter; Mayer, Jonathan; Narayanan, Arvind; Felten, Edward W. (2015). Cookies that give you away: the surveillance implications of web tracking. In: *Proceedings of the 24th International Conference on World Wide Web: WWW '15*, pp. 289–299. doi:10.1145/2736277.2741679

Gaweł, Hanna (2021). Ekologia informacji w świecie cyfrowym: jak użytkownicy mediów społecznościowych radzą sobie z przeładowaniem informacyjnym? W: Paloma Korycińska red. *Horyzonty informacji*, t. 2. Kraków: Uniwersytet Jagielloński: Biblioteka Jagiellońska, s. 47–65. https://ruj.uj.edu.pl/xmlui/handle/item/287477 (odczyt: 23.03.2022).

Girardin, Fabien; Calabrese, Francesco; Fiore Filippo Dal; Ratti, Carlo; Blat, Josep (2008). Digital footprinting: uncovering tourists with user-generated content. *IEEE Pervasive Computing*, vol. 7, issue 4, pp. 36–43. doi:10.1109/mprv.2008.71

Gouert, Charles; Tsoutsos, Nektarios Georgios (2022). Dirty metadata: understanding a threat to online privacy. *IEEE Security & Privacy*, pp. 2–9. doi:10.1109/msec.2022.3148091

Hahm, Jinsun; Ji, Hyung Ki; Jeong, Je Young; Oh, Dong Hoon; Kim, Seok Hyeon; Sim, Kwee-Bo; Lee, Jang-Han (2009). Detection of concealed information: combining a virtual mock crime with a P300-based Guilty Knowledge Test. *CyberPsychology & Behavior*, vol. 12, no. 3, pp. 269–275. doi:10.1089/cpb.2008.0309

Halstead, Ben; Koh, Yu Sing; Riddle, Patrizia; Pechenizkiy, Mykola; Bifet, Albert; Pears, Russel (2021). Fingerprinting concepts in data streams with supervised and unsupervised meta-information. In: *2021 IEEE 37th International Conference on Data Engineering (ICDE)*, pp. 1056–1067. doi:10.1109/icde51399.2021.00096

Horvát, Emőke-Ágnes; Hargittai, Eszter (2021). Birds of a feather flock together online: digital inequality in social media repertoires. *Social Media + Society*, vol. 7, issue 4. doi:10.1177/20563051211052897

Jachym, Wioletta (2015). Potrzeba kształcenia kompetencji informacyjnych w kontekście ekologii informacji. W: Wioletta Jachym, Jan Pojedyniec red. *Teraźniejszość i przyszłość informacji naukowej*. Tarnów: Wydaw. Państwowej Wyższej Szkoły Zawodowej w Tarnowie, s. 27–45.

Johns, Marcus (2018). "On my days off, I'm an elf": psychic pain and resolution in cyberspace. In: Andrea Marzi ed. *Psychoanalysis, identity, and the Internet: explorations into cyberspace*. New York, NY: Routledge, pp. 167–179. doi:10.4324/9780429478864-7

Koops, Bert Jaap; Galič, Maša (2021). Unity in privacy diversity: a kaleidoscopic view of privacy definitions. *South Carolina Law Review*, vol. 73, no. 2. doi:10.2139/ssrn.3864099

Kumar, Sumit; Shanker, Ravi (2019). Understanding the behaviour of privacy in mobile apps and detecting privacy leaks. In: *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, pp. 1253–1258. doi:10.1109/icicict46008.2019.8993361

Lawless, Kimberly A.; Schrader, P.G.; Mayall, Hayley J. (2007). Acquisition of information online: knowledge, navigation and learning outcomes. *Journal of Literacy Research*, vol. 39, no. 3, pp. 289–306. doi:10.1080/10862960701613086

Lioudakis, Georgios V. ; Koutsoloukas, Eleftherios A.; Dellas, Nikolaos; Kapellaki, Sofia; Prezerakos, George N.; Kaklamani, Dimitra I.; Venieris, Iakovos S. (2007). A proxy for privacy: the discreet box. In: *EUROCON 2007: The International Conference on "Computer as a Tool"*, pp. 966–973. doi:10.1109/EURCON.2007.4400521

Longo, Marco (2018). Exploring the subtle mental boundary between the real and the virtual. In: Andrea Marzi ed. *Psychoanalysis, identity, and the Internet: explorations into cyberspace*. New York: Routledge, pp. 51–74. doi:10.4324/9780429478864-3

Maennel, Kaie; Mäses, Sten; Maennel, Olaf (2018). Cyber hygiene: the big picture: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28–30, 2018, Proceedings. In: *Secure IT Systems*, pp. 291–305. doi:10.1007/978-3-030-03638-6_18

Min, Jinyoung; Kim, Byoungsoo (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, vol. 66, issue 4, pp. 839–857. doi:10.1002/asi.23206

Nguyen, Minh Hao; Hunsaker, Amanda E.; Hargittai, Eszter (2019). Digital inequality in older adults' online social engagement and social capital. *Innovation in Aging*, vol. 3, supplement 1, p. 920. doi:10.1093/geroni/igz038.3353

Nottingham, Mark (2020). Not similar to cookies: device and browser fingerprinting as sensitive personal data. *SSRN Electronic Journal*. doi:10.2139/ssrn.3890545

O'Brien, Patrick; Young, Scott W. H.; Arlitsch, Kenning; Benedict, Karl (2018). Protecting privacy on the web: a study of HTTPS and Google Analytics implementation in academic library websites. *Online Information Review*, vol. 42, issue 6, pp. 734–751. doi:10.1108/oir-02-2018-0056

Øverby, Harald (2021). The privacy paradox. In: Sushil Jajodia, Pierangela Samarati, Moti Yung eds. *Encyclopedia of cryptography, security and privacy*. Berlin–Heidelberg: Springer. doi:10.1007/978-3-642-27739-9_1619-1

Pisano, Luca; Mastropasqua, Isabella; Cerniglia, Luca; Erriu, Michela; Cimino, Silvia (2017). Adolescents' online and offline identity: a study on self-representation. In: *European Proceedings of Social & Behavioural Sciences*, pp. 15–25. doi:10.15405/epsbs.2017.05.3

Putikadyanto, Agus Purnomo Ahmad; Adriana, Iswah; Efendi, Agik Nur (2021). Presentation culture in the digital age: online identity representation on social media. In: *Proceedings of the International Congress of Indonesian Linguistics Society (KIMLI 2021)*. doi:10.2991/assehr.k.211226.011

Qin, Yue; Lowe, John (2021). Is your online identity different from your offline identity? A study on the college students' online identities in China. *Culture & Psychology*, vol. 27, no. 1, pp. 67–95. doi:10.1177/1354067x19851023

Rege, Aunshul (2009). What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, vol. 3, no. 2, pp. 494–512. https://www.researchgate.net/profile/Aunshul_Rege/publication/228373590_What's_Love_Got_to_Do_with_It_Exploring_Online_Dating_Scams_and_Identity_Fraud/links/556758a408aefcb861d387ba/Whats-Love-Got-to-Do-with-It-Exploring-Online-Dating-Scams-and-Identity-Fraud.pdf (odczyt: 12.04.2022).

Roberts, Graham (2000). Tangled web: tales of digital crime from the shadows of cyberspace: Richard Power Que Corporation, 2000. *Network Security*, vol. 2000, issue 11, p. 8. doi:10.1016/s1353-4858(00)85022-9

Sapa, Remigiusz (2020). Subject structure of the research area on collaborative information behaviour. *Aslib Journal of Information Management*, vol. 72, no. 5, pp. 813–835.

Sjöberg, Mats; Chen, Hung-Han; Floréen, Patrik; Koskela, Marcus (2016). Digital me: controlling and making sense of my digital footprint. *International Workshop on Symbiotic Interaction*. https://library.oapen.org/bitstream/handle/20.500.12657/27711/1002295.pdf#page=168 (odczyt: 23.03.2022).

Sosińska-Kalata, Barbara (2013). Obszary badań współczesnej informatologii (nauki o informacji). *ZIN: Zagadnienia Informacji Naukowej. Studia Informacyjne*, t. 51, nr 2, s. 9–41.

Steinberg, Stacey B. (2016). Sharenting: children's privacy in the age of social media. *Emory Law Journal*, vol. 66, issue 4, pp. 839–884. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/emlj66&section=27&casa_token=d4r4-uFeb8gAAAAA:mvIe4QcD35sAJjD4z-AvG7N_6Q30Ww8T6k-DylOInVmmUdB-12Zgm-AWrBjjPPfh92C4tTctOPg (odczyt: 22.03.2022).

Walker, Ashley Marie; Hargittai, Eszter (2021). Drills and spills: developing skills to protect ones privacy online. In: Eszter Hargittai ed. *Handbook of digital inequality*. Cheltenham: Edward Elgar Publishing, pp. 358–372. doi:10.4337/9781788116572.00033

Walrave, Michel; Ponnet, Koen; Vanderhoven, Ellen; Haers, Jacques; Segaert, Barbara eds. (2016). *Youth 2.0: social media and adolescence: connecting, sharing and empowering*. Cham: Springer. https://play.google.com/store/books/details?id=vUYWDAAAQBAJ (odczyt: 22.03.2022).

Wambach, Tim; Bräunlich, Katharina (2016). Retrospective study of third-party web tracking. In: *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, pp. 138–145. doi:10.5220/0005741301380145

Weaver, Stephen D.; Gahegan, Mark (2007). Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*, vol. 97, no. 3, pp. 324–350. doi:10.1111/j.1931-0846.2007.tb00509.x

Wen, Yan; Zhao, Jinjing; Wang, Huaimin (2008). Hiding "real" machine from attackers and malware with a minimal virtual machine monitor. In: *Proceedings of the 4th International Conference on Security and Privacy in Communication networks SecureComm '08*, pp. 1–10. doi:10.1145/1460877.1460904

Weng, Jian; Lai, Junzuo (2021). Proxy re-encryption. In: Sushil Jajodia, Pierangela Samarati, Moti Yung eds. *Encyclopedia of cryptography, security and privacy*, pp. 1–6. Berlin–Heidelberg: Springer. doi:10.1007/978-3-642-27739-9_1453-1

Woods, Freya A.; Ruscher, Janet B. (2021). Viral sticks, virtual stones: addressing anonymous hate speech online. *Patterns of Prejudice*, vol. 55, issue 3, pp. 265–289. doi:10.1080/0031322x.2021.1968586

Wójcik, Szymon (2021). Zagrożenia internetowe dla młodzieży: klasyfikacja, skala występowania w Polsce oraz profilaktyka. *Acta Universitatis Nicolai Copernici. Pedagogika*, t. 39, nr 1, s. 171–200. doi:10.12775/aunc_ped.2020.008

Yang, Zeyi (2021, November 30). Another big data exchange opens in Shanghai. https://www.protocol.com/bulletins/china-big-data-exchange (odczyt: 22.03.2022).

Щекотин, Евгений Викторович (2021). Цифровые следы как новый источник данных о качестве жизни и благополучии: обзор современных тенденций. *Вестник Томского государственного университета*, № 467, с. 170–181. doi:10.17223/15617793/467/21