DOI: https://doi.org/10.13166/zar/BHZT8300

ANNA SEMRAU
Akademia Ekonomiczno-Humanistyczna w Warszawie

MEDIA SPOŁECZNOŚCIOWE A ORGANY ŚCIGANIA

Streszczenie

Media społecznościowe wykorzystujemy na różne sposoby, głównie mają służyć nam do rozrywki, słuchania muzyki, oglądania filmów. Mamy komunikatory do rozmów i połączeń online. Chwalimy się zakupem nowego domu, wakacjami, dziećmi, psami, sukcesami w pracy, w szkole. Chcemy się pokazać znajomym jak dobrze nam się wiedzie. Niestety zapominamy o tym, że nie koniecznie tylko nasi znajomi przeglądają nasze wpisy. Również służby chętnie korzystają z mediów społecznościowych. Tysiące zapytań i wniosków płynie do portali społecznościowych z prośbą o udostępnienie danych. Jesteśmy inwigilowani pod każdym kątem jednak trzeba dodać, że to co zamieszczamy jest dobrowolne. Artykuł ma zobrazować jakie dane mogą uzyskać organy ścigania wnioskując o nie do media społecznościowych. Wskazać, że należy mądrze korzystać z tych mediów, gdyż na własne życzenie możemy przekazać dane o sobie tym co do których wolelibyśmy by nie wiedziały o nas za dużo. Media też są wykorzystywane przez organy, gdyż po pierwsze przenieśliśmy się w czasach covid do Internetu a ponadto w organach pracują również ludzie młodzi którzy doskonale wiedzą, że jest to cenne źródło informacji.

Abstract

The media that our clients have in different ways are movies, videos, movies. We have instant messaging to chat and connect online. We boast about buying a new home, holidays, children, dogs, successes at work and at school. Now we show ourselves how well we want each other. Unfortunately, we forget that our friends are not only browsing our entries. with support for social media. Thousands of laws and set up on social networks with data sharing. We are under surveillance from all angles changing the need to add that we publish publications about the site. They are being prosecuted in law enforcement or in an offense against social media. Everyone knows that you should use these media wisely, because we have the opportunity to provide data about ourselves to those about whom we would like to know about a lot of us. The media are also citizens by perfectly well, because first of all we moved to the Internet in the times of covid and, additionally, in the authorities, citizens know that it is a valuable source of information.

Słowa kluczowe: *media społeczne, analiza informacji, otwarte źródła informacji, służby śledcze, służby bezpieczeństwa.*

Keywords: *Social media, information analysis, open sources of information, investigative services, security services.*

Wprowadzenie

Pojawienie się Internetu miało dla przeciętnego obywatela taką samą wagę jak pojawienie się druku przed wiekami. Nagle Internet stał się narzędziem do szybkiej komunikacji z dowolnego miejsca na świecie[1]. Służby śledcze często korzystają z tego typu zasobów przed przystąpieniem do dalszych działań wywiadowczych. Facebook posiada dwa miliardy użytkowników a 14 milionów jest z Polski. Jak wskazują badania 79% użytkowników codziennie korzysta z różnych narzędzi Facebook. Statystycznie przeciętny użytkownik spędza dwie godziny dziennie korzystając z tego narzędzia. Nie zawsze korzysta z komunikatora czy do ściągnięcia filmów, muzyki, wielu użytkowników portali wykorzystuje do

[1] B. Woźniak, *Internetowy czat w świetle prawa karnego*, „Prokuratura i Prawo" 2011, nr 1, s. 86.

pozyskania danych o tym co dzieje się na świecie. Media społecznościowe w tym Facebook czy Twitter zastępują wręcz nam media tradycyjne. Również YouTube, Instagram i szereg innych aplikacji posiada wielu miłośników. Swój profil na Facebooku ma nawet najbardziej znany świadek koronny Sokołowski Jarosław jeden z członków zorganizowanej grupy przestępczej. Na początku roku 2020 dokonano aresztowania słynnego przestępcy Janusza M, człowiek był Europejskim Nakazem Aresztowania szukany i dokonano aresztu na terenie Włoch. Do tego aresztowania przyczyniła się partnerka tego poszukiwanego, gdyż udostępniła w mediach społecznościowych zdjęcie różnych miejsc w których się znajdowała. Po nitce do kłębka śledczy znaleźli ukochanego dziewczyny[2].

Są też pozytywne zatrzymania. W Olsztynie trwały poszukiwania zaginionego mężczyzny. Dzięki komunikatowi w mediach społecznościowych policjanci odnaleźli poszukiwanego zaginionego. Jest to dowód na to jak publikowanie wizerunków takich osób jest ważne, dociera do milionów odbiorców. Odbiorcy mogą też taką treść przekazywać dalej[3].

W latach 90-tych używanie Internetu było w zasadzie anonimowe, dekadę później, kiedy pojawiły się portale społecznościowe typu Twitter, Facebook, Nasza Klasa ludzie masowo zaczęli się dopisywać, zakładać konta podając swoje dane, wczytując swoje prawdziwe zdjęcia. Ludzie zaczęli wpisywać do internatu dosłownie wszystko. W 2011 roku z Internetu wyciągnięto więcej danych jednostkowych niż w całej historii ludzkości do 2010 roku.

Media społecznościowe wykorzystujemy na wszelaki sposób, do rozmów telefonicznych pozyskiwania danych o naszych znajomych, ściągania piosenek czy filmów. W mediach chętnie pokazujemy nasze domy, miejsca, które odwiedzamy, chwalimy się dziećmi, nową pracą

[2] Janusz M miał oszukać skarb państwa, https://wiadomosci.gazeta.pl/wiadomosci/7,114883,25560694,janusz-m-mial-oszukac-skarb-panstwa-na-50-mln-zl-wpadl-we.html, (odczyt 11.03.2022).

[3] Poszukiwany mężczyzna odnaleziony, https://olsztyn.policja.gov.pl/o02/aktualnosci/74077,Poszukiwany-mezczyzna-odnaleziony-dzieki-publikacji-wizerunku-w-mediach-spoleczn.html, (odczyt 11.03.2022).

i innymi sukcesami. Pokazujemy wszystko co dobre w naszym życiu, żeby zakomunikować znajomym jak nam się dobrze wiedzie[4].

Facebook jest kopalnią wiedzy, wiedzą o tym też organy ścigania. W 2009 roku w Bostonie została brutalnie zamordowana masażystka, prokuratura nie miała dowodów na winę podejrzanego, jednak poszła o krok do przodu. Prokuratura poprosiła Facebook o dane z profilu, otrzymała dostęp do kont podejrzanego, do poczty odbiorczej, do adresów IP z których się podejrzany łączył. Facebook udostępnił wpisy podejrzanego, zdjęcia jego i znajomych. To spowodowało, że zabójca został wyśledzony[5].

Polskie organy ścigania również proszą Facebook o dane, lecz sprawa przekazania danych jest utrudniona. Facebook w Polsce działa jako spółka prawa irlandzkiego i uważa, że polskie prawo ją nie obowiązuje w tym zakresie. Gdyby była spółką polską podlegałaby pod ustawę o świadczenie usług drogą elektroniczną. W myśl art. 18 tej ustawy można organom wydać przetwarzane dane na potrzebę prowadzonych postępowań.

W Polsce agencje śledcze typu policja, prokuratura, CBA, ABW i inne mogą swobodnie bez żadnej kontroli korzystać z danych jakie sami pozostawimy w sieci. Uprawnienie takie służby otrzymały w 2016 roku po wprowadzeniu ustawy o policji i ustaw dotyczących służb specjalnych. Jest tylko jeden problem, ustawa w żaden sposób nie przewiduje w jaki sposób kontrolować to co pobierają służby specjalnie na nasz temat. Dane z takich źródeł pozwalają stworzyć profil każdego człowieka, otrzymują dane poufne, nawet związane z naszymi poglądami politycznymi. Jest to pełna inwigilacja.

Sytuacja inaczej ma się w przypadku prób uzyskania danych z Facebook czy Google, tutaj każdy wniosek firmy rozpatrują indywidualnie i arbitralnie. Około połowy wniosków zostaje odrzuconych. Facebook podaje, że procedura rozpatrywania wniosków o przekazanie danych jest bardzo rygorystyczna. Każdy nakaz musi być szczegółowo uzasadniony, musi istnieć powód i podstawa prawna. Wnioski niejasne zbyt ogólne zostają

[4] Media społecznościowe, https://www.polskieradio.pl/10/5366/Artykul/2680730,Media-spolecznosciowe-w-walce-z-przestepcami, (odczyt 11.03.2022).

[5] Co Facebook przekazuje, https://zaufanatrzeciastrona.pl/post/c-facebook-przekazuje-organom-scigania/, (odczyt 11.03.2022)

odrzucone. Jeśli zaś organ prosi o udostępnienie np. zdjęcia czy jakiegoś filmu z osi Facebook wymagany jest nakaz rewizji wystawiony zgodnie z zasadami federalnymi w postępowaniu karnym[6].

Biały wywiad, OSINT, jednoźródłowe informacje

Zasadniczo w polskim prawie nie ma takich pojęć jak biały wywiad, OSINT (akronim Open Source Intelligence) czy też jednoźródłowe informacje. Doktryna posiada swoje dwoje propozycje K. Mroziewicz określa biały wywiad jako „analizę informacji z legalnych dostępnych źródeł"[7] Nieco inną propozycję na określenie definicji „OSINT, to wynik przeprowadzenia pewnych czynności w stosunku do informacji. Są one specjalnie poszukiwane, porównane z sobą co do treści, wybierane są te najważniejsze dla odbiorcy procesu"[8].

Ponadto istnieją inne terminy związane z czterema etapami analizowania pozyskanych źródeł.

- Open Source Data (OSD), dane w stanie surowym, pochodzące z pierwotnego źródła, w postaci drukowanej, z nośników telewizyjnych, radiowych, stron internetowych,
- Open Source Information (OSIF), dane zebrane w pierwszym etapie, przechodzą wstępną analizę, zgrupowane w jednym dokumencie, przekazuje się je osobie zarządzającej a następnie rozpowszechnione,
- Open Soirce Intelligence (OSINT), zaplanowane pozyskanie informacji, wybrane dane zostają przekazane do wyselekcjonowanej grupie odbiorców zgodnie z zapytaniem,

[6] Co Facebook przekazuje, https://zaufanatrzeciastrona.pl/post/c-facebook-przekazuje-organom-scigania/, (odczyt 11.03.2022)

[7] K. Mroziewicz, Czas pluskiew, Wydawnictwo „Sensacje XX wieku", Warszawa 2007. s.334

[8] G. Dobrowolsk, W. Filipkowski, M. Kisiel – Dorohnicki, W. Rakoczy, Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu (w:) L. K. Paprzycki Z. Rau (red.), Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu, Warszawa 2009, s. 279.

- Validated OSINT (OSINT-V), dane zweryfikowane, można tym danym przypisać wysoki poziom pewności, potwierdzone przez inne tajne źródła lub inne pewne otwarte źródła[9].

W literaturze spotyka się szereg klasyfikacji wskazując, że źródeł otwartych jest bardzo wiele. Wymieniono też te które mogą być przydatne w pracy organów ścigania.

1. Media tradycyjne, czyli prasa drukowana, telewizja informacyjna, radia, literatura szeroko pojmowana
2. Internet, czyli internetowe wydania gazet czy czasopism, blogi, mikro blogi, portale społecznościowe, wikis, serwisy wideo, serwisy fotograficzne, strony internetowe przedsiębiorców, rejestry domen WHOIS, mapy, zdjęcia satelitarne, zdjęcia lotnicze
3. Usługi komercyjne, czyli podmioty które specjalizują się przygotowaniem sprofilowanych raportów i analiz, wydawnictwa marketingowe,
4. Literatura niszowa, czyli analizy, informacje dostępne tylko przez wyspecjalizowane kanały, generowane przez środowiska akademickie, organizacje państwowe i pozarządowe. Mówi się czasami w tej sytuacji o szarym wywiadzie, który różni się tym od białego, że utrudniony jest dostęp do informacji.
5. Bazy danych i katalogi[10].

Wykorzystywanie przez służby śledcze danych pozyskanych przede wszystkim z Internetu są głównym elementem działań wykrywaczach. Niestety również grupy przestępcze czy terrorystyczne również korzystają z otwartych źródeł informacji[11].

[9] NATO Open Source Intelligence Handbook, listopad 2001 r., s. 3

[10] G. Dobrowolski,W. Filipkowski, M. Kisiel-Dorohnicki, W. Rakoczy, Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu (w:) L. K. Paprzyck i Z. Rau (red.) Praktyczne elementy…, *op. cit*., s. 281–282.

[11] E. Wójcik, Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej, http://m.wspia.eu/file/21440/44-wójcik.pdf (odczyt 11-03-2022).

Istotnym aspektem związanym z białym wywiadem są metadane. Metadane to to inaczej „dane o danych", lub też „informacja o informacji". Metadane mogą odegrać ważną rolę w pracach służb specjalnych. Każde zdjęcie zrobione aparatem cyfrowym jest opatrzone w metadane, czyli służby specjalne będą znać datę i czas wykonania, ustawienie kamery, lokalizacji. Służby mogą uzyskać nawet miniaturę oryginalnego kadru. Takie dane udostępniają np. Twitter i Instagram a to może ułatwić organom ścigania poszukiwanie osób zaginionych czy ściganych. To jak skutecznym może być wykorzystanie metadanych zdjęć jest widoczne na przykładzie El Chapo meksykańskiego przywódcy kartelu narkotykowego który został złapany właśnie na skutek pobranych metadanych. Kiedy jeden z żołnierzy wojsk rosyjskich udostępnił na Twitterze zdjęcia z wnętrza czołgu wyposażone w metadane geolokalizacyjne ujawniło to obecność wojsk rosyjskich na terenie Ukrainy[12].

Podobna sytuacja była, gdy amerykański żołnierz opublikował zdjęcie w Internecie czego skutkiem było atak pocisków moździerzowych na Irak. Kilka helikopterów zostało zniszczonych w wyniku tego nalotu[13].

Warto też dodać, że dużą ilość tego typu informacji dostarczają też blogi czy serwisy informacyjne. Czasami, żeby zakupić jakiś przedmiot trzeba podać swoje dane, zawsze dane te są podawane razem z adresem IP. Taki adres wskazuje z jakiego adresu było połączenie i zakup więc służby dokładnie wiedzą, gdzie szukać osoby. To pomocne dane dla procedury śledczej. Adam Savage prowadzący program Mythbusters zaprosił wręcz złodziei do swojego domu. Na twisterze zamieścił swoje zdjęcie z samochodu podpisując je, że właśnie jedzie do domu. Z pomocą wtyczki do przeglądarki Mozilla FireFox/Exif Viewer bez problemu można uzyskać takie dane jak

- Specyfikacja sprzętu
- czas zrobienia zdjęcie
- wielkość zdjęcia

[12] Zanim wgrasz wakacyjne zdjęcie do sieci, https://niebezpiecznik.pl/post/zanim-wgrasz-wakacyjne-zdjecia-do-sieci/, (odczyt 11.03.2022).

[13] Metadane, pokaż mi swoje zdjęcie, https://www.purepc.pl/metadane-pokaz-mi-swoje-zdjecie-a-powiem-ci-kim-jestes, (odczyt z dnia 11.03.2022).

- dokładne położenie urządzenia robiącego to zdjęcie wysłane przez GPS. Mało tego, EXIF Viewer proponuje nawet zdjęcie satelitarne tego miejsca. W ramach białego wywiadu służby specjalne mogą też obserwować serwisy aukcyjne, w celu wyszukiwania przedmiotów skradzionych wcześniej.

SOCMINT

Termin „SOCMINT" został po raz pierwszy użyty przez D. Omanda, J. Bartletta oraz C. Millera dla organizacji Demos[14]. Według ich definicji SOCMINT to dane pozyskane za pomocą mediów społecznościowych. Media społecznościowe odnoszą się zarówno do serwisów społecznościowych jak i serwisów informacyjnych czy też gry komputerowe. Media społecznościowe głównie Facebook czy Twitter są propozycjami zamiennymi dla radia czy telewizji. Stały się kanałami informacyjnymi. Serwis społecznościowy, czyli serwis internetowy istnieje przez zgromadzenie się w nim społeczności. Serwisy społecznościowe pozwalają ludziom łączyć się z sobą, wymieniać poglądy i informacje na tematy najróżniejsze. Każdy użytkownik serwisu może utworzyć swój własny profil i wykreować w sposób dowolny swój własny wizerunek[15].Social Media Intelligence (Socmint) to wykorzystanie technik w celu pozyskania cennych informacji o osobie, grupie osób, rodzinie, firmie, instytucji. Media społecznościowe są obecnie ważną częścią pracy wywiadowczej. Również detektywi korzystają w swojej pracy z portali społecznościowych. Pobieranie danych za pomocą SOCMINT-u opiera się na uzyskaniu danych oficjalnych, zawartych w Internecie dobrowolnie. Oczywiście są osoby, które ukrywają swoje dane profilowe i żeby mieć dostęp do tych danych należy zostać „znajomym", detektywi takie czynności zostanie znajomym dla własnych celów nazywają grą operacyjną[16]. Socjalmint

[14] Omand, J. Bartlett, C. Miller, #Intelligence, Demos, London 2012, s. 9.
[15] https://pl.wikipedia.org/wiki/Serwis_spo%C5%82eczno%C5%9Bciowy, odczyt 20.05.2022
[16] https://dkdetektyw.pl/socmint/, odczyt 20.05.2022

w swoim zakresie obejmuje działania zarówno białego wywiadu jak i czarnego. Czarny wywiad polega na zebraniu informacji od właścicieli danych serwisów społecznościowych. Istnieją przepisy uprawniające organy ścigania do dostępu do danych osób fizycznych na portalu społecznościowym[17]. Przykładem działania Socialmint spoza OSINT, czyli białego wywiadu jest Geofedia. Jest to amerykański program, który pozwala w czasie rzeczywistym analizę zdjęć, lokalizacji czy nagrań publikowanych na platformach dostępnych ogólnospołecznie m.in. Facebook, Twitter, Instagram czy YouTube[18]. Jednym z klientów Geofedia był FB. FB próbował ustalić osobę, która weszła bez zaproszenia do biura Marka Zuckerberga a potem chwaliła się danymi w mediach społecznościowych[19]. Geofedia była również wykorzystywana przez amerykańską policję w celu śledzenia osób biorących udział w protestach które wybuchły w 2014 roku[20]. Media społecznościowe są wykorzystywane przez organy ścigania co najmniej od dekady. Również w Polsce organy ścigania wykorzystuje media do śledzenia ruchów protestujących. Przykładem może być marsz Niepodległości jaki odbył się 11 listopada 2020 roku, w którym doszło do podpalenia mieszkania. Zdjęcia i nagrania z tego zdarzenia błyskawicznie znalazły się na Facebooku i innych portalach społecznościowych. Nawet policja publikowała informacje o tym zdarzeniu na swoich portalach społecznościowych. Policja warszawska pokazała najpierw na twisterze potem szerszy materiał na Facebooku

[17] Więcej na temat podziału na biały, czarny i ewentualnie szary wywiad zob. w niniejszej publikacji rozdział: K. Bayer-Ryśkiewicz, J. Bitner, P. Waszkiewicz, Szary wywiad. Krytyczna analiza definicji pojęcia w literaturze polskiej oraz anglojęzycznej., w: P. Waszkiewicz (red.), Media społecznościowe w pracy organów ścigania, Warszawa 2021, s. 151-169, https://doi.org/ 10.5281/zenodo.4625055.

[18] E. Oritz, Facebook, Twitter, Instagram block Geofeedia tool used for police surveillance, https://www.nbcnews. com/tech/internet/facebook-twitter-instagram-block-geofeedia-tool-used-police-surveillance-n664706, odczyt 20.05.2022

[19] C. Lecher, R. Brandom, Facebook caught an office intruder using the controversial surveillance tool it just blocked, https://www.theverge.com/2016/10/19/13317890/facebook-geofeedia-social-media-tracking-tool-mark-zuckerberg-office-intruder, odczyt 20.05.2022

[20] https://www.bbc.com/news/world-us-canada-37627086, odczyt 20.05.2022

co pozwoliło ustalić wiele interesujących szczegółów ze zdarzenia[21]. Policja wykorzystując media społecznościowe zbiera dane które mogą pełnić zarówno funkcję informacyjną, dowodową jak i poszlakową. W ramach działań policji była i nadal jest wykorzystywana metoda białego wywiadu. Niekiedy jest ona wręcz konieczna, już w ramach prowadzenia samego postępowania przygotowawczego policja ochoczo korzysta z tych źródeł informacji[22]. W zależności od rodzaju sprawy policja dostaje różne narzędzia białego wywiadu do swoich rąk, można sobie wyobrazić sprawę prowadzoną w postępowaniu przygotowawczym w zakresie spraw gospodarczych. Policja posiada dostęp do wywiadowni gospodarczych, różnego rodzaju rejestrów. Policja na tej podstawie może ustalić wiek podejrzanego, adres zamieszkania, znajomych, powiązania kapitałowe, zainteresowania. Stan majątków[23].Również służby specjalne korzystają ze wszystkich możliwych źródeł informacji. W polskim porządku prawnym uznaje się za służby specjalne takie instytucje jak Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne[24]. Metodyka pracy takich organów jak ABW czy CBA bardziej zbliżona jest do pracy policji. Służby te mają nie tylko na celu niejawne pozyskanie informacji za pomocą wywiadu czy kontrwywiadu. Znacząca część danych podlegających późniejszej analizie pochodzi właśnie z otwartych jej źródeł. Większość amerykańskich specjalistów d.s. wywiadu uważa, że około 80% pozyskanych informacji pochodzi z białych źródeł informacji. Agencje specjalne mają w swoich strukturach osoby specjalizujące się w analizie informacji, w ABW działa

[21] Fotoreporter ranny na Marszu Niepodległości: Nikt mnie nie przeprosił. Policja strzelała, gdzie popadnie, w: https://www.rp.pl/Spoleczenstwo/201119736-Fotoreporter-ranny-na-Marszu-Niepodleglosci-Nikt-mnie-nie – -przeprosil-Policja-strzelala-gdzie-popadnie.html, odczyt 20.05.2022

[22] K. Radwaniak Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2 (11), s. 88.

[23] K. Radwaniak, P.J. Wrzosek, Biały wywiad w Policji – pozyskiwanie i analiza infomacji ze źródeł otwartych [w:] J. Konieczny (red.), Analiza informacji w służbach policyjnych i specjalnych, Warszawa 2012, s. 138.

[24] 8 Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego orazAgencji Wywiadu (Dz. U. 2002 Nr 74 poz. 676) art. 11

specjalne Biuro Informacji i Analiz, również CBA taki dział wykorzystuje do analiz danych[25].

W niektórych państwach w służbach specjalnych istnieją wyspecjalizowane organy które zajmują się tylko pozyskiwaniem danych pochodzących ze źródeł otwartych. Przykładem może być Open Source Center (OSC) działające od 2005 roku w strukturach amerykańskiej CIA[26]. Pentagon w oficjalny już sposób śledzi konta użytkowników na portalach społecznościowych. W ten sposób Pentagon chciał między innymi stłumić protesty antyrządowe. Stany Zjednoczone dokonywały analiz z zakresu Big Data, badania miały ustalić w jaki sposób wpływ na media społecznościowe mogą się przyczynić na przewidywania zachowani ludzkich. Po konferencji w Kojowie w 2016 roku powstał artykuł, który wzbudził zainteresowanie wśród dziennikarzy. Badacze wskazywali jakie wpisy pojawiające się w mediach społecznościowych wpływały na zachowania społeczeństwa i jak wpływało to na protesty w Stanach jakie wybuchły po wygraniu przez prezydenta w 2016 roku wyborów. Badacze ustalili, że protesty te można było przewidzieć[27].

Badania pokazują, że korzystanie zbyt częste z mediów społecznościowych wpływa niekorzystnie na ludzką psychikę i postrzeganie świata. Nadużywanie portali wpływa na naszą kondycję również fizyczną, zaburzenia w odżywianiu, problemem ze snem, agresją. Coraz częściej jednak problemy te są poruszane przez różne środowiska, aby uświadomić korzystającym, że korzystanie z portali jest szkodliwe i prowadzi do uzależnienia. Nie sposób uznać, że portale społecznościowe mają swój walor społeczny, poznawczy. Wiele par połączyło się dzięki istnieniu portali, po latach znaleźć można przyjaciela z lat szkolnych. Serwisy dają możliwość zapisu do różnych grup społecznych i uczestniczenia w nich. Tym samym portale te są wykorzystywane do celów przekazywania

[25] Zarządzenie Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu (M.P. z 2010 r. Nr 76, poz. 953), § 3 ust. 1.

[26] Open Source Information System (OSIS) [w:] http://www.globalsecurity.org/intell/systems/osis.htm, odczyt 20.05.2022

[27] https://zaufanatrzeciastrona.pl/post/media-spolecznosciowe-jako-narzedzie-inwigilacji-dla-pentagonu/, odczyt 20.05.2022

nam informacji w taki sposób, aby na nas wpłynąć. Mowa tu o różnych kampaniach reklamowych, ale też o kampaniach wyborczych.

Według raportu Digital 2000 w Polsce było 30,63 mln ludzi korzystających z Internetu. Liczba ta wzrosła o 2,3 % w stosunku do rok, u poprzedniego i następnego. Pierwsze miejsce w Polsce zajmuje YouTube. Aż 92% internautów korzysta z platformy udostępniania plików wideo. Drugie miejsce objął Facebook i aż 86% internautów przyznaje się do jego korzystania. 55% wszystkich ludzi na świecie korzysta z Internetu. Nawet w środkowej Afryce 22% całej jej populacji korzysta z Internetu[28].

Z całą stanowczością media społecznościowe to główne źródło informacji i miejsce przetwarzania treści cyfrowych. W Facebook wystarczy rozmawiać czy wyrazić za pomocą smartfon jakieś zainteresowanie a urządzenia mobilne same odszyfrują i klasyfikują zainteresowania użytkownika. Urządzenia również dokonują analizy pod kątem geolokalizacji. Snapchat bardzo popularny zwłaszcza wśród młodzieży udostępnił tzw. snapy. Dwie osoby zliczają wspólnie dni wysyłając do siebie codziennie snapy, i nie muszą to być rozmowy, ale zdjęcia miejsc, zdjęcia ulicy, muru. Dane te są poddane analizie i służą pozyskaniu informacji o samym użytkowniku i jego otoczenia. Młode pokolenie, ale nie tylko bardzo lubi udostępniać wszystko co fajne i czym można się pochwalić. Mówi się też, że jeśli ktoś w stanach zjednoczonych ma otwartą aplikację Facebook to Facebook słucha i analizuje[29].

Podsumowanie

Zmiany w sieci internetowej zachodzą tak szybko jak zmiany technologiczne i społeczne. Również użytkownicy Internetu zmieniają swoje preferencje co do portali. Należy tu wspomnieć o portalu Myspace który w latach 2004-2008 miał więcej użytkowników niż Facebook. W Polsce większość użytkowników Naszej Klasy przeniosła się na Facebook. Jeden z pierwszych polskich portali społecznościowych grono.net zupełnie przestał istnieć. Facebook jest liderem

[28] https://datareportal.com/reports/digital-2020-poland, odczyt 20-05-2022
[29] G. Scott – Wielka Czwórka, *Ukryte Dna Amazon, Aplle, Facebook i Google*, s.131

w swojej branży i wygląda na to, że nic nie jest wstanie mu zagrozić. Dla osób urodzonych po 1986 roku sieci społecznościowe są czymś zupełnie naturalnym. Te osoby też zupełnie nie widzą problemu umieszczania w Internecie danych o sobie. Nie ma żadnej refleksji nad tym, że dane te są upowszechniane wszystkim, każdy użytkownik może uzyskać dane o osobie, którą przegląda. Warto pamiętać o symetrii w wykorzystaniu OSINT. Wszystkie metody zbierania informacji jawnych stoją otworem również przed voyerystą lub potencjalnym przestępcą, od stalkera do włamywacza czy osoby planującej zamach na zdrowie czy życie. Powstał serwis z aplikacją Foursquare za pomocą którego można zameldować się w aktualnym miejscu. Nie ma lepszych danych dla potencjalnych włamywaczy czy osób, które chcą coś nam zrobić[30].

Analizowani jesteśmy również przez organy ścigania, w myśl przepisów ustawy z dnia 6 kwietnia 1990 r. o Policji w art.14 można przeczytać, że Policja w celu rozpatrywania, zapobiegania i wykrywania przestępstw i wykroczeń obok czynności dochodzeniowo-śledczych i administracyjno-porządkowych ma prawo wykonywać czynności operacyjno-rozpoznawcze[31]. Co w przypadku policji sprowadzają się do czynności ustalenia sprawcy i wykrycia dowodów w sprawie.

Biały wywiad wydaje się być metodą uniwersalną, lecz istnieją obszary, gdzie nie jest on przydatny, problemem też może być bariera językowa. Brakuje specjalistów, którzy biegle władają takimi językami jak chiński, arabski, hindu, farsi czy pasztu.

Należy się zastanowić czy ludzie sami nie stwarzają dla siebie potencjalnego niebezpieczeństwa. Facebook i inne portale społecznościowe są bazą danych o nas na własne życzenie. Jesteśmy stale poddani inwigilacji jednak jest ona zaakceptowana przez użytkownika.

Media społecznościowe stały się globalnym narzędziem używanym w życiu codziennym oraz zawodowym. W związku ze wzrostem ich znaczenia w pracy organów ścigania, należy regularnie przeprowadzać badania weryfikujące sposób i częstotliwość wykorzystywania mediów społecznościowych w ich codziennej pracy.

[30] P. Konieczny, Proszę obrabuj mnie! http://niezbędnik.pl/post/prosz-obrabuj-mnie/, dostęp 20-05-2022

[31] Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz.U.2011, nr 7, poz.58

References

Akty prawne

Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz.U.2011, nr 7, poz.58

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2002 Nr 74 poz. 676).

Zarządzenie Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu (M.P. z 2010 r. Nr 76, poz. 953).

Literatura

Dobrowolski G, Filipkowski W, Kisiel-Dorohnicki M, Rakoczy W., Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu (w:) L. K. Paprzycki Z. Rau (red.), Praktyczne zagadnienia przestępczości zorganizowanej i terroryzmu, Warszawa 2009, s. 279.

Woźniak B., Internetowy czat w świetle prawa karnego, „Prokuratura i Prawo" 2011, nr 1.

Mroziewicz K., Czas pluskiew, Wydawnictwo „Sensacje XX wieku", Warszawa 2007.

NATO Open Source Intelligence Handbook, listopad 2001 r.

Omand D, Bartlett J, Miller C., #Intelligence, Demos, London 2012, s. 9.

Radwaniak K, Wrzosek P.J., Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych [w:] J. Konieczny (red.), Analiza informacji w służbach policyjnych i specjalnych, Warszawa 2012.

Radwaniak K., Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2 (11).

Scott G. - Wielka Czwórka, Ukryte Dna Amazon, Aplle, Facebook i Google.