VOL. 54 STUDIA POLITOLOGICZNE
DOI: 10.33896/SPolit.2019.54.5

Magdalena Tomaszewska-Michalak
ORCID: 0000-0001-5441-0396

Prawne aspekty pozyskiwania informacji w Internecie

Słowa kluczowe:
prawne aspekty infobrokeringu, pozyskiwanie informacji w Internecie, phishing, sock puppetry

Wprowadzenie

Nie jest tajemnicą, że pozyskiwanie informacji z różnych źródeł zawsze leżało w zakresie zainteresowania takich instytucji, jak służby chroniące porządek publiczny czy agencje wywiadowcze. Wejście w posiadanie odpowiednich informacji było i jest również istotne z punktu widzenia podmiotów prywatnych. Firmy sprawdzające swoich kontrahentów czy pracodawcy usiłujący pozyskać dodatkową wiedzę o kandydatach do pracy nie stanowią obecnie przypadków odosobnionych. Pozyskiwanie informacji nie występuje jednakże jedynie na poziomie instytucjonalnym czy pracowniczym. Szybki postęp technologiczny bowiem sprawił, że nierzadko każdy z nas ma możliwość znalezienia w Internecie informacji dotyczących konkretnego zagadnienia czy interesującej go osoby. Obecne czasy każą zatem spojrzeć na informację jako dobro, które w niepowołanych rękach może stanowić zagrożenie lub działać na niekorzyść jednostki. Dlatego też na zagadnienie pozyskiwania informacji powinno spojrzeć się szerzej – nie tylko z perspektywy technicznych możliwości, jakie istnieją w tym zakresie, ale również jak na zjawisko społeczne mające określone konsekwencje oraz na działanie podlegające odpowiednim ograniczeniom prawnym. Celem niniejszego artykułu jest zatem wskazanie społeczno-prawnych problemów związa-

nych z pozyskiwaniem oraz wykorzystywaniem informacji zamieszczonych w Internecie.

Analizując zagadnienie pozyskiwania informacji w Internecie, należy zwrócić uwagę na pojęcia takie jak tzw. biały wywiad / wywiad jawnoźródłowy (ang. OSINT – *open source intelligence*) oraz przeciwstawiany mu tzw. czarny wywiad. Nie istnieje jedna oficjalna definicja białego wywiadu[1], jednakże pojęcie to w literaturze tłumaczone jest jako pozyskiwanie informacji z jawnych oraz ogólnodostępnych źródeł. Zgodnie z definicją przyjętą przez NATO w 2002 roku biały wywiad polega na poszukiwaniu informacji pochodzących z jawnych źródeł za pomocą legalnych metod i środków[2]. Przywołana publikacja odwołuje się co prawda do pozyskiwania informacji w celu usprawnienia pracy wywiadu, jednakże zawarte w niej zostało również twierdzenie świadczące o tym, że jej autorzy dostrzegli możliwość korzystania z OSTINT nie tylko przez osoby pracujące w wywiadzie[3].

Przeciwieństwem białego wywiadu jest tzw. czarny wywiad, który polega na pozyskiwaniu informacji przy wykorzystaniu metod prawnie zakazanych użytkownikowi Internetu[4]. Poza białym i czarnym wywiadem istnieje pojęcie pośrednie – tzw. szary wywiad, który różni się od wcześniej wymienionych tym, że z jednej strony pozyskanie informacji w jego ramach jest nadal legalne, jednakże dostęp do szukanych danych może być trudniejszy niż w przypadku białego wywiadu (na przykład do materiałów konferencyjnych, archiwalnych informacji zamieszczonych na stronie internetowej)[5]. Ponadto niektóre działania podejmowane w ramach szarego wywiadu mogą zostać uznane za nieetyczne (na przykład wykorzystanie socjotechnik do pozyskania danych)[6]. Analizując możliwości pozyskania danych w Internecie, należy pamiętać, że niektóre metody szukania informacji pod względem legalności klasyfikowane są z uwzględnieniem kategorii podmiotu podejmującego wskazane działania.

---

1 B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 148–150.

2 *NATO Open Source Intelligence Handbook*, 2002, s. 5, http://www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf (dostęp: 21.01.2019).

3 Tamże.

4 Mogą to być jednakże metody, które są dopuszczalne podczas prowadzenia czynności wywiadowczych, takie jak podsłuchy czy kontrola korespondencji.

5 B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce…*, s. 150.

6 D. Mider, J. Garlicki, W. Mincewicz, *Pozyskiwanie informacji w Internecie metodą Google Hacking – biały, szary czy czarny wywiad?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20, s. 68–91.

Artykuł niniejszy skupiać będzie się na osobach fizycznych niebędących pracownikami służb czy wywiadów.

Prawne granice pozyskiwania informacji

Jednym z problemów, jaki pojawia się w omawianym zakresie, są prawne granice pozyskiwania informacji. Analizując polski kodeks karny[7] (dalej jako kk) zauważyć można, że przestępstwa z wykorzystaniem komputera do pozyskiwania danych opisane zostały w większości w rozdziale dotyczącym przestępstw przeciwko ochronie informacji. I tak artykuł 267 kk stanowi: „§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem".

Cytowany przepis jasno wskazuje, że próba uzyskania informacji poprzez łamanie czy też omijanie zabezpieczeń podlega karze. Obok tradycyjnych form nielegalnego uzyskiwania informacji (takich jak na przykład nieuprawnione otwieranie cudzej korespondencji) ustawodawca zauważył potrzebę włączenia do katalogu również nielegalnego uzyskania informacji poprzez przełamanie systemu informatycznego. Ponadto w polskim prawie karalne jest także wykorzystywanie podsłuchów lub oprogramowania pozwalającego na obserwowanie innej osoby. Ustawodawca polski penalizuje też samą ingerencję w zamieszczone dane. Stanowią o tym kolejne artykuły kk: „Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. […] Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub

[7] Ustawa z 6 czerwca 1997 roku – Kodeks karny t.j. Dz.U. z 2018 r., poz. 1600, ze zm.

utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3. […]".

Warto zwrócić uwagę na fakt, że krajowy prawodawca przewiduje surowszą odpowiedzialność w przypadku ingerencji w informatyczny nośnik danych, co podkreśla, jak istotne znaczenie ma tego rodzaju przestępstwo dla prawidłowej ochrony informacji.

Zgodnie z art. 269a kk również czynności prowadzące do zakłócania działania systemu informatycznego uznane zostały za nielegalne i mogą podlegać karze. Warto wspomnieć, że wprowadzeniu wskazanych wyżej przepisów nie towarzyszyło wyłączenie odpowiedzialności w wyjątkowych przypadkach, takich jak na przykład nieuprawniony dostęp do systemu informatycznego w celu testowania efektywności wprowadzonych zabezpieczeń. Błąd ten jednak naprawiony został w art. 269b § 1a kk („Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia), a także w art. 269c kk („Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody"). Wprowadzenie obu przepisów było konieczne dla skutecznego działania osób zajmujących się „legalnym hackingiem", a więc działaniem zmierzającym do poprawy bezpieczeństwa informatycznego podmiotów publicznych oraz firm prywatnych.

Warto podkreślić, że wszystkie omówione przepisy stanowią przestępstwa powszechne, a więc takie, które popełnione mogą być przez każdego człowieka. Oznacza to, że ustawodawca wskazał prawną granicę dopuszczalności pozyskiwania informacji w sposób legalny. Powyższe przepisy nie dają jednakże odpowiedzi na wszystkie sytuacje związane z możliwością pozyskiwania danych. Działania takie jak włamania do systemu informatycznego czy przełamywanie zabezpieczeń kryptograficznych nie budzą wątpliwości co do ich nielegalności. Wydaje się, że ustawodawca ustosunkował się również negatywnie do sytuacji pozyskiwania informacji na przykład w drodze uzyskania dostępu do systemu informatycznego w wyniku wejścia w posiadanie hasła zdobytego na skutek zastosowania

socjotechnik (art. 267 § 2 kk). Wskazuje on bowiem, że uzyskanie dostępu do systemu informatycznego przez osobę nieuprawnioną jest czynnością podlegającą odpowiedzialności karnej. W przeciwieństwie do § 1, kolejny § 2 art. 267 kk nie wymienia jednak konkretnych działań, które muszą zostać podjęte, aby nieuprawniony dostęp stał się karalny. Oznacza to penalizowanie samej sytuacji uzyskania nieuprawionego dostępu do danych bez względu na metody wykorzystane do osiągnięcia celu. W tym kontekście warto zwrócić dodatkowo uwagę na art. 287 § 1 kk stanowiący, że: „Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

Przepis ten penalizuje między innymi przestępstwo phishingu, a więc działania polegającego na skopiowaniu strony internetowej określonej instytucji (na przykład banku) w celu przekonania podmiotu korzystającego z witryny o jej prawdziwości i uzyskaniu w ten sposób pożądanych informacji. Formą phishingu może być również przesłanie wiadomości e-mailem z podaniem fałszywego nadawcy – podszywanie się pod podmiot, do którego odbiorca ma zaufanie (na przykład administrator poczty, instytucja państwowa)[8]. Współczesną odmianą phishingu jest tzw. *spear phishing* polegający na celowym doborze osób, które mają zostać ofiarami oszustwa[9]. Typowanie potencjalnych ofiar odbywa się na podstawie przeprowadzonego przez oszusta wywiadu środowiskowego (nierzadko opartego na białym wywiadzie).

Zgodnie ze statystykami umieszczonymi na stronie policji, w Polsce liczba przestępstw zawierających znamiona tzw. oszustwa komputerowego z roku na rok rośnie.

Warto zwrócić uwagę, że statystyka dotyczy jedynie postępowań wszczętych, a więc odnosi się tylko do tych przypadków, w których użytkownik zgłosił próbę oszustwa organom ścigania. Pogląd na to, jak dużą skalę mogą osiągnąć ataki phishingowe, może dać materiał przygotowany przez firmę Kaspersky Lab. W raporcie dotyczącym pierwszego kwartału 2018 roku podkreślone zostało, że tylko we wskazanym czasie program antyphishingowy Kaspersky Lab zapobiegł 90 245 060 próbom

8 Hasło: *Phishing*, „Słownik Języka Polskiego", https://sjp.pl/phishing (dostęp: 12.11.2018).

9 K. Jasiołek, *Spear phishing, czyli ataki spersonalizowane*, Komputer Świat, 13.08.2013, https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/spear-phishing-czyli-ataki-spersonalizowane/m5th9v9 (dostęp: 12.11.2018).

przekierowania użytkownika do witryn osób przeprowadzających atak[10]. Oczywiście pamiętać należy, że jest to jedno z wielu oprogramowań komercyjnych służących do zabezpieczania komputera użytkownika, nie jest to więc pełen obraz problemu.

Tabela 1. Statystyki przestępstwa w postaci oszustwa komputerowego (art. 287 kk)

Rok	Liczba wszczętych postępowań	Liczba stwierdzonych przestępstw
2016	4103	4207
2015	4105	3282
2014	2567	2154
2013	1768	1573
2012	1285	1351
2011	1012	1364
2010	838	623
2009	673	978
2008	472	404
2007	322	492
2006	285	444
2005	326	568
2004	229	390
2003	219	168
2002	114	368
2001	59	171

Źródło: http://statystyka.policja.pl (dostęp: 12.02.2019)

Kolejną istotną kwestią związaną z korzystaniem z pozyskiwanych informacji jest możliwość wykorzystania ich w charakterze dowodu w postępowaniu karnym. Artykuł 168a kpk, wprowadzony do kodeksu postępowania karnego nowelą z 11 marca 2016 roku[11], stanowi, że „Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub

[10] N. Demidova, T. Shcherbakova, M. Vergelis, *Spam and Phishing in Q1 2018*, Kaspersky.com, 23.05.2018, https://securelist.com/spam-and-phishing-in-q1-2018/85650/ (dostęp: 12.11.2018).

[11] Ustawa z 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw, Dz.U. z 2016 r., poz. 437.

za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego, chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności". Przepis ten oznacza, że nawet dowody pozyskane w drodze przestępstwa (na przykład włamania się do systemu informatycznego) mogą zostać legalnie wykorzystane w procesie karnym. Pamiętać jednak należy, że doktryna dopuszczenia tzw. owocu zatrutego drzewa nie wyklucza postawienia osobie zarzutów w związku ze sposobem zdobycia określonego dowodu.

Bardziej skomplikowana sytuacja w tym względzie rysuje się na gruncie postępowania cywilnego. Procedura ta warta jest w tym miejscu wspomnienia, gdyż nierzadko w toczących się przed sądem sprawach strony wykorzystują dowody zdobyte w sposób naruszający prawo (na przykład nagranie osoby bez jej zgody, wykorzystanie prywatnych e-maili czy informacji z prywatnej rozmowy toczącej się na portalu społecznościowym). W ramach procesu cywilnego nie ma zasady mówiącej o dopuszczalności lub niedopuszczalności dowodów zdobytych w sposób sprzeczny z obowiązującymi normami prawnymi. Dopuszczenie dowodu zależy zatem od rozważenia przez sąd określonych dóbr, a więc z jednej strony ustalenia prawdy materialnej pomocnej w rozstrzygnięciu sporu, a z drugiej naruszenia określonych praw jednostki (na przykład prawa do prywatności, prawa do tajemnicy korespondencji). O tym, że nie wyklucza się przez sąd wykorzystania „owocu zatrutego drzewa" świadczy chociażby wyrok Sądu Najwyższego z 23 kwietnia 2003 roku, w którym sędziowie uznali, że „nie ma zasadniczych powodów do całkowitej dyskwalifikacji kwestionowanego przez pozwaną dowodu z nagrań rozmów telefonicznych, nawet jeżeli nagrań tych dokonywano bez wiedzy jednego z rozmówców. Skoro strona pozwana nie zakwestionowała skutecznie w toku postępowania autentyczności omawianego materiału, to mógł on służyć za podstawę oceny zachowania się pozwanej w stosunku do pozwanego i możliwości sformułowania wniosku o nadużywaniu alkoholu przez pozwaną"[12]. Wskazany wyrok, dotyczący nagrań telefonicznych utrwalonych bez zgody jednej ze stron, przenieść można również na inne sytuacje, w których dowody zostały zdobyte z naruszeniem praw osób trzecich. Pamiętać jednakże należy, że niezależnie od przepisów prawnych wykorzystanie informacji pozyskanych w sposób niezgodny z prawem może zostać uznane za sprzeczne z zasadami etycznymi.

[12] Wyrok Sądu Najwyższego IV CKN 94/01.

Internetowe manipulacje – ochrona praw jednostki

Ze względu na postęp technologiczny i nowe sposoby wykorzystywania potencjału Internetu polski ustawodawca nie jest w stanie wprowadzić przepisów będących odpowiedzią na każdą sytuację rodzącą prawne wątpliwości w zakresie pozyskiwania informacji. Problem pojawia się na przykład podczas podszywania się pod inną osobę lub zakładania fałszywych kont w Internecie w celu bądź pozyskania określonych informacji, bądź ingerencji w nie. Ciekawym przykładem na polskim gruncie jest orzeczenie Sądu Rejonowego w Olsztynie z 21 lipca 2015 roku[13]. Oskarżoną w sprawie była kobieta, która chciała potwierdzić podejrzenia co do homoseksualnych skłonności swojego partnera. W tym celu wykorzystała znalezione wcześniej w Internecie zdjęcie przypadkowego mężczyzny. Wizerunek posłużył kobiecie do utworzenia fikcyjnego konta na portalu przeznaczonym do nawiązywania homoseksualnych kontaktów. Pod koniec 2014 roku mężczyzna, którego zdjęcie zostało wykorzystanie do założenia profilu, dowiedział się o tym fakcie i złożył zawiadomienie o popełnieniu przestępstwa. Kobiecie postawiono zarzut z art. 190a kk (tzw. stalking)[14], wskazując, że podszywanie się pod pokrzywdzonego i wykorzystanie jego wizerunku spowodowało wyrządzenie pokrzywdzonemu „[…] szkody osobistej poprzez przedstawienie go jako osoby o skłonnościach homoseksualnych poszukującej partnera seksualnego […]"[15]. We wskazanym przypadku sąd uniewinnił oskarżoną, uznając, że popełniony przez nią czyn nie wykazuje znamion przestępstwa z art. 190a, gdyż nie znała ona pokrzywdzonego i jej celem nie było wyrządzenie mu krzywdy. Sąd zatem nie uznał samego faktu wykorzystania czyjegoś wizerunku w celu założenia fikcyjnego konta za przestępstwo, które powinno być ścigane na podstawie przepisów prawa karnego, mimo iż mogła zostać naruszona reputacja pokrzywdzonego. Wskazany wyrok nie wyklucza jednak wystą-

[13] Wyrok Sądu Rejonowego w Olsztynie II K 497/15.

[14] Art. 190a kk: „§ 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3. § 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. § 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego".

[15] Wyrok Sądu Rejonowego w Olsztynie II K 497/15.

pienia z powództwem o naruszenie dóbr osobistych na gruncie prawa cywilnego[16].

Kwestia wyrządzania drugiej osobie szkody jest istotnym elementem przestępstwa podszywania się, który musiał wziąć pod uwagę sąd amerykański. Sprawa People v. Golb[17] dotyczyła nowojorskiego prawnika Ralpha Golba, który chcąc pomóc swojemu ojcu próbującemu rozpowszechnić jedną z głoszonych, a niedocenianych przez środowisko teorii naukowych, podszył się pod prof. Lawrence'a Schiffmana. Celem takiego postępowania było rozesłanie e-maili do pracowników naukowych, w których rzekomy prof. Schiffman przyznawał się do popełnienia plagiatu w stosunku do prac ojca R. Golba. Ponadto R. Golb stworzył kilka fikcyjnych tożsamości i na licznych blogach oskarżał prof. Schiffmana o kradzież pomysłów swojego ojca. Proces R. Golba toczył się kilka lat i ostatecznie zakończył skazaniem na karę dwóch miesięcy więzienia za przestępstwo podszywania się. Czyn, którego dopuścił się R. Golb, jest jedną z form tzw. *sock puppetry*, a więc działania polegającego na wykorzystywaniu fikcyjnej tożsamości w Internecie. Zasadniczo *sock puppet* ma znaczenie pejoratywne, gdyż wiąże się z tworzeniem alternatywnych kont (lub nadawaniem sobie pseudonimów) w celu oszukania osób korzystających z danego portalu (strony dyskusyjnej czy bloga)[18].

Obecnie definicja *sock puppet* rozszerzyła się, gdyż celem działania może być również manipulowanie opinią publiczną czy ominięcie zakazu administratora co do wypowiadania się na określonej stronie internetowej. Dla porządku warto wskazać, że pacynki, jak czasem nazywane jest opisywane to działanie w języku polskim, nie zawsze powinny być traktowane jako zjawisko negatywne. Na stronie regulującej zasady Wikipedii możemy przeczytać, że na przykład „Posiadanie wielu kont pozwala też na ochronę prywatności. Ktoś, kto jest znany publicznie lub w pewnym kręgu osób, może zostać rozpoznany z np. jego zainteresowań i dokonywanych edycji. Rozdział tych edycji między różne konta może pozwo-

[16] W tym celu można by powołać się na art. 23 kodeksu cywilnego w brzmieniu: „Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach". Ustawa z 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2019 r. poz. 1145).

[17] People v. Golb 23 N.Y.3d 455 (2014).

[18] „Sock puppet is a fake persona used to discuss or comment on oneself or one's work, particularly in an online discussion group or the comments section of a blog", WordSpy.com, https://wordspy.com (dostęp: 6.08.2018).

lić zachować anonimowość. Niektórzy użytkownicy, szczególnie administratorzy i biurokraci, używają pacynek, kiedy pracują na nie swoim komputerze, w celu uniknięcia przejęcia swojego głównego konta (często dysponującego narzędziami administracyjnymi) przez kradzież hasła"[19]. W większości przypadków alternatywne konta uważane są jednak za niezgodne z polityką działania portali internetowych czy stron dopuszczających do dyskusji pomiędzy użytkownikami platformy. Jednakże także w Wikipedii, mimo dostrzeżenia pewnych korzyści z wykorzystywania pacynek, dotyczące tegoż zasady zaczynają się od stwierdzenia: „Odradza się używania pacynek, gdyż może to doprowadzić do naruszania zasad ustalonych w Wikipedii, takich jak jedna osoba–jeden głos"[20]. Popularny w Polsce portal społecznościowy Facebook również wskazuje, że „Podstawą naszej społeczności jest autentyczność. Uważamy, że ludzie czują się bardziej odpowiedzialni za swoje wypowiedzi i działania, gdy znana jest ich prawdziwa tożsamość. Dlatego wymagamy od użytkowników Facebooka używania imion i nazwisk, którymi posługują się na co dzień"[21]. W innym miejscu tego samego dokumentu możemy przeczytać, że jedną z czynności niedozwolonych jest zakładanie fałszywych kont oraz podszywanie się pod inne osoby[22].

Przytoczone polityki idą zatem dalej niż uczynił to polski ustawodawca, zakazując lub znacznie ograniczając wykorzystywanie *sock puppets* bez względu na zamiary, w jakich tworzy się alternatywne konta. Rozwiązanie takie wydaje się słuszne, gdy bierzemy pod uwagę cel, jakim jest tworzenie zaufania pomiędzy użytkownikami portali społecznościach czy projektów takich jak Wikipedia. W tym kontekście ciekawie przedstawia się amerykańska sprawa United States v. Drew[23], w której jednym z zarzutów postawionych oskarżonej było właśnie złamanie zasad statutu serwisu społecznościowego MySpace poprzez założenie fikcyjnego konta na portalu. Lori Drew pragnęła w ten sposób zawrzeć znajomość internetową z koleżanką swojej nastoletniej córki – Megan Meier. Dowiedziała się bowiem, że M. Meier niepochlebnie wypowiada się na temat jej dziecka. Oskarżona założyła więc fikcyjne konto, podając się

---

19 Hasło: *Pacynka*, Wikipedia Wolna Encyklopedia, https://pl.wikipedia.org/wiki/Wikipedia:Pacynka (dostęp: 6.08.2018).

20 Tamże.

21 Facebook, Standardy Społeczności, *Integralność i autentyczność*, https://pl-pl.facebook.com/communitystandards/integrity_authenticity (dostęp: 6.08.2018).

22 Facebook, Centrum Pomocy, *Podszywanie*, https://pl-pl.facebook.com/help/212826392083694?helpref=search&sr=1&query=podszywanie (dostęp: 6.08.2018).

23 U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

za 16-letniego Josha Evansa i zaczęła korespondować z M. Meier. Po pewnym czasie rzekomy Josh zerwał znajomość, stwierdzając, że „[…] świat byłby lepszy bez Megan”[24]. Tego samego dnia M. Meier popełniła samobójstwo. Ważnym elementem procesu było rozstrzygnięcie kwestii, czy zachowanie L. Drew w postaci złamania zasad serwisu MySpace było przestępstwem federalnym w rozumieniu Computer Fraud and Abuse Act (CFAA)[25]. Ostatecznie sąd uznał, że w tym przypadku wyrok niekorzystny dla oskarżonej oznaczałby danie możliwości serwisom internetowym zakwalifikowania określonych zachowań do kategorii przestępstw. Byłoby to *de facto* przyznanie uprawnień ustawodawczych twórcom portali, co nie jest zgodne z postanowieniami amerykańskiej konstytucji.

Wszystkie opisane sprawy pokazują wyraźnie, że samo wykorzystanie *sock puppets* nie jest karane na podstawie prawa karnego powszechnie obowiązującego. Znaczenie ma w tym przypadku jednakże zamiar, w jakim ktoś używa pacynki, pozyskując lub manipulując informacją. Tylko bowiem w takim przypadku można zidentyfikować znamiona określonych przestępstw (na przykład oszustwa czy stalkingu). Brak regulacji prawnej w tym zakresie nie wyklucza jednakże wprowadzania zakazów stosowania *sock puppets* przez serwisy czy portale internetowe, które uważają takie zachowania za nieetyczne. Konsekwencją łamania zasad może być jednakże jedynie zablokowanie dostępu do określonych treści.

Dopuszczalność pozyskiwania i przetwarzania prywatnych danych

Kwestią wartą rozważenia w kontekście pozyskiwania danych w Internecie jest możliwość uzyskania informacji o pracowniku (lub kandydacie na pracownika) przez pracodawcę (lub potencjalnego pracodawcę). Nie jest bowiem tajemnicą, że firmy już podczas procesu rekrutacji coraz częściej poszukują dodatkowych informacji o osobie ubiegającej się o określone stanowisko zawodowe. Na pytanie o dopuszczalność sięgania po prywatne informacje o pracowniku (na przykład informacje dostępne na portalu społecznościowym) w dużej mierze odpowiada opinia tzw. Grupy

[24] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009), tłumaczenie własne.
[25] 18 U.S. Code § 1030.

Roboczej art. 29[26] na temat przetwarzania danych w miejscu pracy[27]. Poruszono w niej szereg kwestii związanych z przetwarzaniem danych osobowych pracownika oraz kandydata na pracownika (na przykład monitoring w miejscu pracy, monitorowanie aktywności pracownika w sieci itp.).

Z perspektywy niniejszego artykułu ciekawy wydaje się zwłaszcza problem możliwości wykorzystania informacji „białowywiadowczych" o kandydacie na pracownika (na przykład w sytuacji, gdy pracownik ma publiczny profil na portalu społecznościowym). Twórcy opinii wskazują, że sięganie w procesie rekrutacji po dodatkowe informacje, które nie zostały udzielone przez samego kandydata, jest dopuszczalne, ale jedynie wtedy, gdy spełnione zostaną określone przesłanki. Pierwszą jest poinformowanie kandydata w ogłoszeniu o pracę o podejmowaniu przez rekrutującego wskazanych działań – nie mogą one mieć zatem charakteru niejawnego. Po drugie, sięganie po omawiany rodzaj danych musi mieć podstawę prawną, a więc pracodawca wykazać powinien, że ma uzasadniony interes w tym, żeby pozyskiwać dodatkowe informacje o kandydacie. Przykładem takiego prawnie uzasadnionego interesu jest sprawdzenie przez pracodawcę, czy osoby nie obowiązuje zakaz konkurencji ze względu na to, że wcześniej zatrudniona była w określonej firmie (informacje o poprzednim zatrudnieniu mogą być zamieszczane na różnego rodzaju portalach zawodowo-biznesowych, jak na przykład LinkedIn czy Goldenline). Po trzecie, aby dopuszczalne było pozyskanie informacji z portali społecznościowych o kandydacie, konieczne jest ustalenie, w jakim zakresie profil danej osoby powiązany jest z celami biznesowymi. Po wypełnieniu powyższych wymagań i przeprowadzeniu odpowiednich kontroli możliwości pozyskania danych pracodawca może zbierać określone informacje znajdujące się na profilach publicznych kandydata, nie jest jednakże uprawniony do domagania się udostępnienia mu profilu rekrutowanej osoby, na przykład poprzez zaakceptowanie

[26] Grupa robocza do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych – tzw. Grupa Robocza art. 29, była niezależnym europejskim organem doradczym opiniującym zagadnienia związane z ochroną prywatności i danych osobowych. Została powołana na mocy art. 29 dyrektywy nr 95/46 Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Grupa ta została rozwiązana 25 maja 2018 r., a w jej miejsce została powołana Europejska Rada Ochrony Danych.

[27] Opinia Grupy Roboczej art. 29 nr 2/2017 z 8 czerwca 2017 r. na temat przetwarzania danych w miejscu pracy; opinia dostępna na stronie: https://uodo.gov.pl/data/filemanager_pl/18.pdf (dostęp: 15.11.2018).

zaproszenia do grona znajomych. Wskazane zalecenia pokazują zatem wyraźnie, że Grupa Robocza art. 29 zdawała sobie sprawę z faktycznego korzystania przez pracodawców z możliwości pozyskiwania informacji w Internecie i starała się wprowadzić obostrzenia w tym zakresie prowadzące do ochrony prywatności pracownika lub osoby kandydującej na określone stanowisko w firmie[28].

Metadane

Innym problemem związanym z pozyskiwaniem informacji w Internecie jest zagadnienie metadanych. Metadane to dane o danych, a więc szczegółowe informacje opisujące zasoby informacji[29]. Dla przeciętnego obywatela metadane wydają się abstrakcyjnym pojęciem i zdają się nie mieć wpływu na jego codzienne życie. Okazuje się jednak, że pozyskanie metadanych może dać wiele informacji na temat miejsca przebywania osoby, jej zainteresowań czy nawyków. Najprostszym przykładem są dane, jakie wyczytać można ze zdjęcia niewyczyszczonego z metadanych. Poza takimi wskazówkami, jak sposób wykonania zdjęcia (na przykład przysłona czy czas naświetlania), które mogą być przydatne dla osób zainteresowanych fotografią, z obrazu pozyskać można również informacje dotyczące daty i miejsca wykonania zdjęcia. Wykorzystanie wskazanych metadanych może mieć zarówno pozytywne, jak i negatywne skutki. Pozytywne dotyczą między innymi posłużenia się informacjami ze zdjęcia w celu ujęcia osoby podejrzanej o popełnienie przestępstwa. Przykładem takiej sprawy jest ujęcie Johna McAfee'ego poszukiwanego przez policję w związku z zabójstwem sąsiada. Jego miejsce przebywania zostało ujawnione dzięki zdjęciu, którym jedna z gazet zilustrowała wywiad ze zbiegiem. Dziennikarz wykonujący fotografię smartfonem nie wyłączył danych geolokalizacyjnych, co pozwoliło na ujęcie J. McAfee'ego i postawienie go przed sądem[30]. Pozyskiwanie metadanych może mieć jednak również i negatywne skutki. W 2007 roku doszło do zniszczenia helikopterów klasy Apache stacjonujących w amerykańskiej bazie w Iraku. Zlokalizowanie bazy stało się możliwe dzięki metadanym znajdującym

[28] Tamże.

[29] Hasło: *Metadane*, Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Metadane (dostęp: 15.11.2018).

[30] B. Weitzenkorn, *McAfee's Rookie Mistake Gives Away His location*, Scientific American, 4.12.2012, https://www.scientificamerican.com/article/mcafees-rookie-mistake/ (dostęp: 9.08.2018).

się w zdjęciach helikopterów zamieszczonych przez żołnierzy w Internecie[31]. Obecnie na stronie internetowej amerykańskiej armii można przeczytać, w jaki sposób unikać między innymi ujawniania informacji geolokalizacyjnych znajdujących się w fotografii[32].

Metadane oczywiście nie dotyczą jedynie zdjęć. Sama informacja o kilkukrotnym kontaktowaniu się z lekarzem określonej specjalności może – nawet bez wiedzy o treści rozmowy – być cenną wskazówką dotyczącą stanu zdrowia osoby. Podobne znaczenie będzie miała na przykład informacja o dzwonieniu na linię zaufania dla ofiar przemocy rodzinnej czy dla samobójców. Oczywiście uzyskanie akurat takich informacji wymaga dostępu do danych telekomunikacyjnych, które ujawniane są przez operatorów jedynie określonym podmiotom (art. 180d prawa telekomunikacyjnego[33]). Pozyskanie powyższych danych przez przeciętnego obywatela nie jest natomiast zgodne z prawem.

Część ujawnianych metadanych może mieć znaczenie nie tylko dla prawa jednostki do prywatności, ale również dla bezpieczeństwa publicznego. Przykładem takiego działania jest wykorzystywanie aplikacji rejestrujących aktywność sportową swoich użytkowników. Dobrą ilustracją opisanej sytuacji jest ujawnienie przez aplikację Strava mapy wskazującej trasy biegowe osób z niej korzystających. Analiza map pozwoliła na zlokalizowanie potencjalnych tajnych baz wojskowych[34]. Jak zatem widać z powyższych przykładów, metadane pozyskane w drodze legalnego, białego wywiadu mogą dostarczyć wielu informacji na temat miejsca przebywania osoby, jej nawyków czy sposobu spędzania wolnego czasu.

Internetowy biały wywiad a RODO

Pozyskiwanie podstawowych informacji w Internecie w ramach białego wywiadu nie stanowi obecnie większego problemu. Każda bowiem

---

[31] *Insurgents Destroyed US Helicopters Found in Online Photos*, „Live Science", 16.03.2012, https://www.livescience.com/19114-military-social-media-geotags.html (dostęp: 9.08.2018).

[32] Ch. Rodewig, *Geotagging Poses Security Risks*, 7.03.2012, https://www.army.mil/article/75165/geotagging_poses_security_risks (dostęp: 9.08.2018).

[33] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2018 r. poz. 1954 ze zm.

[34] A. Hern, *Fitness Tracking App Strave Gives Away Location of Secret US Army Bases*, „The Guardian", 28.01.2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (dostęp: 9.08.2018).

aktywność podjęta w sieci pozostawia po sobie ślad, który może być przydatny do stworzenia profilu zawodowego lub prywatnego określonej osoby. Przetwarzanie danych osobowych od dawna znajduje się w kręgu zainteresowania unijnych instytucji[35]. Szybki rozwój Internetu sprawił, że nie tylko stare problemy w tym zakresie stały się bardziej widoczne, ale pojawiły się nowe, związane z gromadzeniem danych osobowych. Dlatego też prawodawca unijny wprowadził mechanizm broniący przed nadmiernym przetwarzaniem danych. Tym mechanizmem jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[36] (dalej jako: RODO). Artykuł 17 RODO wprowadził tzw. prawo do bycia zapomnianym, które polega na możliwości zwrócenia się przez określoną osobę do administratora danych z żądaniem usunięcia przetwarzanych informacji dotyczących jednostki. W RODO wymienione zostały przesłanki, które powodują, że administrator musi dostosować się do prośby wnoszącego wniosek o usunięcie danych. Są to między innymi:

- zasada celowości – oznaczająca, że dane mogą być przetwarzane tylko do momentu, do którego jest to niezbędne ze względu na istotę gromadzenia danych; w sytuacji gdy zbieranie określonych informacji przestaje mieć pierwotny cel, administrator zobowiązany jest usunąć takie dane;
- cofnięcie zgody na przetwarzanie danych – dotyczy na przykład sytuacji, w której osoba najpierw wyraziła zgodę na przesyłanie jej informacji marketingowych, a po jakimś czasie takich informacji otrzymywać już nie chce;
- przetwarzanie danych od początku było niezgodne z prawem.

Prawodawca unijny pomyślał również o sytuacji, w której administrator danych dokonał upublicznienia zbieranych informacji (art. 17 ust. 2 RODO). W takim przypadku, w sytuacji skorzystania przez jednostkę z prawa do żądania usunięcia danych, administrator musi postarać się

[35] Patrz np. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. z 1995 r., L 281.

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. z 2016 r., L119.

również o usunięcie danych przez podmioty trzecie. W art. 17 została w tym zakresie zastosowana klauzula „podejmowania rozsądnych działań, w tym środków technicznych". Wydaje się, że dopiero konkretne sprawy toczące się w przyszłości pozwolą doprecyzować znaczenie powyższej klauzuli. Prawo do bycia zapominanym nie jest jednakże prawem absolutnym. Istnieją bowiem sytuacje, wobec których prawodawca uznał, że żądanie usunięcia danych nie będzie musiało zostać uwzględnione przez administratora danych (art. 17 ust. 3 RODO). Są to między innymi przypadki, gdy:

- upublicznienie informacji jest konieczne do wywiązania się z prawnego obowiązku ciążącego na administratorze,
- informacje przechowywane są do celów statystycznych, badań naukowych lub historycznych,
- przetwarzanie informacji wiąże się z korzystaniem z prawa do wolności wypowiedzi i informacji.

Warto zauważyć, że szczególnie w przypadku ostatniej przesłanki realizacja prawa do bycia zapomnianym może stanowić bardzo trudne zadanie. Rozważenie bowiem, czy w danym przypadku ważniejszy jest interes konkretnej osoby, czy też interes publiczny polegający na uzyskaniu określonej informacji, nie jest w praktyce łatwe.

Pierwsza istotna sprawa, która rozpatrywana była przed Trybunałem Sprawiedliwości UE w 2014 roku (a więc jeszcze przed wprowadzeniem przepisów RODO) w zakresie prawa do zapomnienia dotyczyła obywatela Hiszpanii Mario Gonzaleza (Sprawa Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González[37]). Żądał on usunięcia nieaktualnych już danych na jego temat, czego przedsiębiorstwo Google nie chciało uczynić, gdyż nie czuło się odpowiedzialne za treści zamieszczane w wyszukiwarce przez osoby trzecie. Sprawa dotyczyła zatem dwóch ważnych aspektów prawa do bycia zapomnianym. Pierwszy wiązał się z samą możliwością złożenia wniosku o usunięcie danych, która w czasie rozpatrywania sprawy nie była jeszcze uregulowana prawnie. W tym zakresie Trybunał Sprawiedliwości stwierdził, że: „[…] należy w szczególności przeanalizować kwestię, czy osoba, której dotyczą dane, ma prawo do tego, aby dana dotycząca jej informacja nie była już, w aktualnym stanie rzeczy, powiązana z jej imieniem i nazwiskiem poprzez listę wyświetlającą wyniki wyszukiwania mającego za punkt wyjścia to imię i nazwisko, przy czym stwierdzenie, iż takie prawo przysługuje, pozostaje bez związku z tym, czy zawarcie

[37] Wyrok Trybunału Sprawiedliwości UE C131/12.

na tej liście wyników wyszukiwania danej informacji wyrządza szkodę tej osobie. Ponieważ osoba ta może, ze względu na przysługujące jej i przewidziane w art. 7 i 8 karty prawa podstawowe, zażądać, aby dana informacja nie była już podawana do wiadomości szerokiego kręgu odbiorców poprzez zawarcie jej na takiej liście wyników wyszukiwania, prawa te są co do zasady nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki ten krąg odbiorców może mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby. Taka sytuacja nie ma jednak miejsca, jeśli ze szczególnych powodów, takich jak rola odgrywana przez tę osobę w życiu publicznym, należałoby uznać, że ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem tego kręgu odbiorców polegającym na posiadaniu, dzięki temu zawarciu na liście, dostępu do danej informacji"[38]. Takie postawienie sprawy dało początek dyskusjom na temat prawa do bycia zapomnianym, a w konsekwencji doprowadziło do wprowadzenia do RODO omawianego wcześniej art. 17. Niestety zarówno wyrok, jak i przepisy RODO dały jedynie pobieżne odpowiedzi co do kryteriów odmówienia osobie usunięcia informacji w ramach realizacji prawa do zapomnienia. Jest to zatem nadal sytuacja, którą powinno rozważać się w odniesieniu do konkretnego przypadku.

Drugi istotny aspekt poruszony w przytaczanym wyroku dotyczył odpowiedzialności ponoszonej przez przedsiębiorstwo Google za treści zamieszczane w wyszukiwarce przez osoby trzecie. W swoim orzeczeniu Trybunał Sprawiedliwości uznał, że właściciel wyszukiwarki jest odpowiedzialny za przetwarzane informacje, a tym samym, że jednostka ma prawo żądać usunięcia danych bezpośrednio od operatora wyszukiwarki.

* * *

Internet jest obecnie kopalnią informacji, które odpowiednio zinterpretowane mogą dostarczyć wiedzy na każdy interesujący poszukującego temat. Ze źródła tego korzystają zarówno podmioty publiczne, jak i pracodawcy czy osoby prywatne. Granice legalnego pozyskiwania danych reguluje prawo krajowe. Ze względu na szybki postęp technologiczny na rynku pojawia się jednakże coraz więcej narzędzi pozwalających na pozyskiwanie w sieci bardziej lub mniej „ukrytych" informacji. Rodzi to kolejne problemy natury nie tylko prawnej, ale również etycznej odnoszące się do kwestii pozyskiwania danych w Internecie. Wydaje się jed-

[38] Tamże.

nak, że jest to materia, której na chwilę obecną nie da się uregulować całościowo.

Streszczenie

Artykuł dotyczy możliwości pozyskiwania informacji w Internecie z perspektywy przepisów prawnych obowiązujących na terenie Polski. Poza niewątpliwymi korzyściami, jakie daje wykorzystanie komputera w życiu codziennym, rozwój technologiczny rodzi określone zagrożenia. Jednym z nich jest możliwość zdobywania informacji o jednostce za pomocą legalnych oraz nielegalnych metod działania. Celem artykułu jest próba analizy regulacji prawnych związanych z możliwością zbierania danych w Internecie.

Magda Tomaszewska

Legal Aspects of Obtaining Information on the Internet

Article deals with legal possibilities of obtaining information on the Internet. It indicates methods of obtaining information legally (such as open source intelligence) and methods recognized in Polish law as unlawful (such as activities aimed at disrupting the operation of an IT system). The article also discusses the issues of phishing, the use of false identity in the Internet (so-called sock puppetry), as well as the information potential of metadata analysis.

Key words: *infobrokering legal aspects, internet information retrieval, phishing, sock puppetry*

Bibliografia

Demidova N., Shcherbakova T., Vergelis M., *Spam and Phishing in Q1 2018*, Kaspersky.com, 23.05.2018, https://securelist.com/spam-and-phishing-in-q1-2018/85650/ (dostęp: 12.11.2018).

Hern A., *Fitness Tracking App Strave Gives Away Location of Secret US Army Bases*, „The Guardian", 28.01.2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (dostęp: 9.08.2018).

Jasiołek K., *Spear phishing, czyli ataki spersonalizowane*, Komputer Świat, 13.08.2013, https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/spear-phishing-czyli-ataki-spersonalizowane/m5th9v9 (dostęp: 12.11.2018).

Mider D., Garlicki J., Mincewicz W., *Pozyskiwanie informacji w Internecie metodą Google Hacking – biały, szary czy czarny wywiad?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20.

Rodewig Ch., *Geotagging Poses Security Risks*, 7.03.2012, https://www.army.mil/article/75165/geotagging_poses_security_risks (dostęp: 9.08.2018).

Stromczyński B., Waszkiewicz P., *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5.

Weitzenkorn B., *McAfee's Rookie Mistake Gives Away His location*, Scientific American, 4.12.2012, https://www.scientificamerican.com/article/mcafees-rookie-mistake/ (dostęp: 9.08.2018).