Paragraf 2 / 2023
https://doi.org/10.18778/2956-3747.2.01

Patryk Łuczyński*

Open Source Intelligence w kontekście wybranych czynów zabronionych

Streszczenie

Artykuł omawia kwestie związane z Open Source Intelligence. Opisane zostały w nim ogólne zagadnienia związane z metodami OSINT, a także ich ocena w kontekście art. 190a § 2 oraz art. 267 § 1 Kodeksu karnego, a także art. 107 ustawy o ochronie danych osobowych. Praca ma zachęcić do dyskusji nad prawnokarnymi zagadnieniami OSINT-u.

Słowa kluczowe: biały wywiad, OSINT, prawo karne, prawo do prywatności, kradzież tożsamości

Open Source Intelligence in the context of selected criminal offences

Abstract

This article discusses issues related to Open Source Intelligence. It describes general issues related to OSINT methods, as well as their assessment in the context of Articles 190a § 2 and 267 § 1 of the Penal Code, as well as Article 107 of the Personal Data Protection Act. The work is intended to encourage discussion of the criminal law issues of OSINT.

Keywords: white intelligence, OSINT, criminal law, right to privacy, identity theft

1. *Open Source Intelligence* (OSINT) – wprowadzenie

OSINT to w najprostszym ujęciu pozyskiwanie i analizowanie rozmaitych informacji z legalnych źródeł otwartych lub półotwartych. Pojęcie to utożsamia się z białym wywiadem, który z kolei przeciwstawia się tzw. czarnemu, polegającemu na zdobywaniu informacji ze źródeł zamkniętych, z wykorzystaniem środków i metod nielegalnych lub noszących znamiona przestępstwa[1]. Akceptując ww. utożsamienie, w dalszej części publikacji zamiennie będę posługiwał się terminem OSINT i biały wywiad, dla określenia metod, co do zasady, legalnego pozyskiwania danych z jawnych źródeł.

* Autor jest studentem IV roku prawa na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, e-mail: patryk.luczynski@edu.uni.lodz.pl.

1 Por. T. Pączkowski, *Biały wywiad. Materiały dydaktyczne Policji*, Katowice 2020, s. 5; B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 15–16.

W literaturze przedmiotu biały wywiad określa się zwykle jako jedną z metod wykorzystywanych w pracy operacyjno-rozpoznawczej służb[2]. Stwierdzenie jednak, że pozostaje on wyłącznie domeną organów ścigania, stanowiłoby daleko idące niedopowiedzenie, bowiem równie często wykorzystują go podmioty prywatne. Przejawem tego są działania tzw. headhunterów, czy po prostu osób zajmujących się rekrutacją pracowników, którzy w celu weryfikacji potencjalnego kandydata do pracy dokonują oceny jego sylwetki oraz danych wskazanych w dokumentach aplikacyjnych. Innym przykładem wykorzystania OSINT-u jest działalność zespołów bezpieczeństwa, które przy użyciu tego typu metod chronią przedsiębiorców, wykrywają wycieki danych lub nielojalnych współpracowników. Nie można tracić z pola widzenia, że omawiane metody wykorzystywane są też przez prawników m.in. przy weryfikacji potencjalnych partnerów biznesowych swoich klientów, okoliczności wskazywanych w aktach oskarżenia, czy przy przygotowaniu linii obrony. W końcu trzeba też wskazać, że OSINT pozostaje w zainteresowaniu przestępców, którzy dane zdobyte takimi technikami wykorzystują do celów przestępczych, np. uzyskując informację o miejscu pracy ofiary, jej statusie majątkowym, przyzwyczajeniach, słabych punktach.

Biały wywiad zakłada co do zasady uzyskiwanie danych jawnych, z wykorzystaniem legalnych metod. Wśród nich pierwszoplanowe znaczenie ma analiza informacji ogólnodostępnych, w szczególności tych dostępnych w sieci. W tym celu analitycy dogłębnie penetrują zasoby internetowe z wykorzystaniem odpowiednich parametrów[3] i oprogramowania[4], aby w ten sposób uzyskać dostęp również do takich treści, które są ukryte w sieci i niedostępne dla jej przeciętnego użytkownika. Nie bez znaczenia jest także analiza prasy tradycyjnej i elektronicznej, analiza zdjęć, nagrań audio i wideo, map, materiałów archiwalnych, wpisów w mediach społecznościowych, danych z ogólnodostępnych baz i rejestrów (np. Centralnej Ewidencji i Informacji o Działalności Gospodarczej, Krajowego Rejestru Sądowego, Portalu Rejestrów Sądowych). Nie można również zapominać o osobowych źródłach informacji (OZI), które mogą w wielu przypadkach dostarczyć najistotniejszych wiadomości potrzebnych do właściwego OSINT-u. W ramach prowadzenia białego wywiadu specjaliści wielokrotnie korzystają też z zasobów Darknetu[5] za pośrednictwem narzędzia TOR, czyli przeglądarki umożliwiającej dostęp do takich zasobów niedostępnych z poziomu standardowych przeglądarek[6], z zachowaniem znacznie wyższych standardów anonimowości niż przy normalnym korzystaniu z Internetu. Ponadto jedną z praktyk wykorzystywanych przez takie osoby jest praca wcieleniowa, polegająca na przenikaniu do zamkniętych grup dyskusyjnych, aby w ten sposób uzyskiwać informacje niezbędne dla swojej pracy. W praktyce zakres białego wywiadu i dobieranych metod jest uzależniony od szczegółowego celu, do którego zmierza podmiot analizujący.

OSINT jest zasadniczo powszechnie dostępną metodą zdobywania szerokiego zakresu informacji, które mogą być przydatne nie tylko do zaspokojenia ciekawości, ale przede wszystkim do podejmowania istotnych analiz i decyzji względem podmiotu, którego owe informacje dotyczą, np. decyzji o podjęciu lub zakończeniu zatrudnienia, podjęciu działań prawnych. Z drugiej strony takie działania stanowią istotną i bliżej niekontrolowaną ingerencję w prawo do prywatności. Zasadna jest więc analiza norm

2 Zob. K. Tylutki, *Informacja masowego rażenia – OSINT w działalności wywiadowczej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19, s. 166.

3 Np. operatorów wyszukiwania zaawansowanego, https://www.google.pl/intl/pl/help/operators.html (dostęp: 20.11.2022).

4 Przykładowo – oprogramowania umożliwiającego automatyczne pozyskiwanie informacji i ich przedstawianie w sposób graficzny (np. Maltego).

5 W ślad za D. Miderem wskazać należy, że Darknet to: „sieci, które intencjonalnie mają charakter ukryty, są bowiem tak zaprojektowane, aby maksymalizować anonimowość ich użytkowników, przez co są dostępne przy użyciu odpowiednich przeglądarek lub specjalistycznego oprogramowania" (D. Mider, *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 154).

6 Szerzej o sieci TOR i jej alternatywach w: M. Majorek, *Darknet. Ostatni bastion wolności w internecie?*, „Bezpieczeństwo. Teoria i praktyka" 2017, nr 4.

prawa karnego w stosunku do tego typu metod. O ile bowiem w założeniu biały wywiad ma opierać się na legalnych działaniach, o tyle nietrudno dostrzec, że przekroczenie granic prawa nie jest szczególnie trudne, a prostota uzyskiwania danych z wykorzystaniem tych metod sprzyja ich nadużywaniu i przekraczaniu zasad etycznych, a niejednokrotnie również norm prawnych. Z tego powodu w niniejszym opracowaniu omówione zostaną wybrane przepisy dotyczące białego wywiadu, przede wszystkim w kontekście stosowania go przez sektor prywatny.

2. Kradzież tożsamości a OSINT

Jak wcześniej wskazano, wśród metod OSINT-u znajduje się przenikanie w środowiska, głównie wirtualne, w celu bieżącego uzyskiwania informacji o danej społeczności lub jednostce – zarówno przez bierne obserwowanie działań członków takich grup, jak i przez czynne wchodzenie w interakcje z takimi osobami. W tym celu specjaliści posługują się zwykle tzw. profilami legendami. Są to konta w mediach społecznościowych oparte na fałszywej tożsamości. Ich celem jest umożliwienie zdobywania informacji przez OSINT-owca bez ujawniania własnych danych. Tworzenie takiego profilu jest czasochłonne i zakłada nie tylko utworzenie sylwetki „legendy" przez nadanie jej imienia, nazwiska, wieku, płci, określenie jej hobby, przebiegu edukacji lub kariery zawodowej, ale też opracowanie jej wizerunku – między innymi w tym celu powstały generatory sztucznych wizerunków twarzy[7].

Ponadto, aby legenda była wiarygodna, musi być na bieżąco aktualizowana[8]. Specjalista powinien zadbać m.in. o to, aby jego wykreowana postać poszerzała sieć wirtualnych znajomych, publikowała wpisy lub udostępniała zdjęcia. Użytkownicy wyczuleni są bowiem na osoby, które próbują dostać się do zamkniętych grup za pomocą profilów, które powstały chwile wcześniej, nie publikowały dotychczas żadnych treści, nie mają zbudowanego grona znajomych, czy wypełnionych podstawowych danych. Stworzenie takiej legendy trwa więc zwykle co najmniej kilka tygodni, zaś zapewnienie jej skuteczności i wiarygodności może wymagać nawet kilku lat sukcesywnej pracy. Warto też podkreślić, że profesjonalny OSINT wymaga zwykle stworzenia co najmniej kilku legend o różnych parametrach, np. płci, wieku, zawodzie. Dzięki temu specjalista ma możliwość przenikania do różnych grup, które często selekcjonują swoich członków według określonych kryteriów.

Posługiwanie się ww. metodami niesie za sobą ryzyko kradzieży cudzej tożsamości. Kodeks karny kryminalizuje taki czyn w art. 190a § 2, który w brzmieniu obowiązującym do 13.03.2023 r. zakładał, że kto podszywając się pod inną osobę, wykorzystuje jej wizerunek, dane osobowe lub inne dane, za pomocą których jest ona publiczne identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej, podlega odpowiedzialności karnej jak za przestępstwo stalkingu. Przepis ten został zmieniony na skutek nowelizacji k.k. z 7.07.2022 r.[9], w wyniku której w zakres znamion wchodzi już nie działanie sprawcy „w celu wyrządzenia szkody", lecz wystąpienie skutku w postaci „szkody majątkowej lub osobistej". W kontekście tego przepisu wskazać można pewne konkretne zagrożenia posługiwania się przez OSINT-owców fałszywą tożsamością. Pierwszym z nich jest stworzenie profilu legendy, który nieumyślnie oparty zostanie na danych istniejącej osoby. Drugim, stworzenie konta celowo opartego na takich danych, co służyć może np. szybszemu wzbudzeniu zaufania odbiorców. Na uwagę zasługuje też sama czynność pozyskiwania danych rzeczywistej osoby, które mają służyć opracowaniu profilu legendy.

7 Np. https://thispersondoesnotexist.com/ (dostęp: 16.11.2022).

8 Zob. A. Ziółkowska, *Biały wywiad jako ogólnodostępna forma cyberinwigilacji a bezpieczeństwo danych użytkowników urządzeń mobilnych*, „Wiedza Obronna" 2017, nr 3–4, s. 148 i n.

9 Ustawa z dnia 7 lipca 2022 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2022 r. poz. 2600).

Umiejscowienie art. 190a § 2 k.k. w rozdziale XXIII, wskazuje, że dobrem chronionym tym przepisem jest wolność człowieka w zakresie dysponowania własnymi danymi osobowymi[10], ale też od zagrożeń wynikających z posługiwania się przez inną osobę danymi pokrzywdzonego[11]. Czynnością wykonawczą jest podszycie się pod inną osobę, co oznacza podawanie się fałszywie za kogoś innego[12], przez wykorzystanie danych osobowych takiej osoby lub jej wizerunku[13]. Wystarczające jest przy tym jednorazowe wykorzystanie danych lub wizerunku innej osoby[14].

Dane osobowe nie mają swojej definicji na gruncie k.k. Należy zatem sięgnąć do znaczenia przyjętego na gruncie RODO[15], które w art. 4 pkt 1 definiuje je jako wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Takimi danymi mogą być: imię i nazwisko, adres, PESEL, numer dowodu osobistego. W skład danych osobowych wchodzi też wizerunek, rozumiany jest jako „podobizna, wyobrażenie, portret, obraz umożliwia identifikację danej osoby"[16].

Do 13.03.2023 r. omawiany występek miał charakter formalny. Dla jego bytu nie miało znaczenia, czy podszycie się pod inną osobę wprowadziło kogoś w błąd i czy doprowadziło do powstania szkody majątkowej lub osobistej. Istotne było samo podjęcie czynności podszycia się, a strona podmiotowa tego występku wymagała istnienia po stronie sprawcy zamiaru bezpośredniego i to w formie *dolus directus coloratus*. Sprawca miał działać w celu wyrządzenia szkody majątkowej lub osobistej, pokrzywdzonemu, pod którego się podszywał[17]. Wskazana nowelizacja k.k. doprowadziła do istotnej zmiany tych znamion. Aktualnie sprawca czynu nie musi już działać „w celu" wyrządzenia szkody pokrzywdzonemu, natomiast warunkiem wypełnienia znamion jest skutek jego działania (podszycia się), w postaci wyrządzenia szkody osobistej lub majątkowej takiej osobie. Przestępstwo zmienione zostało zatem z formalnego na materialne – znamienne skutkiem, które może być popełnione umyślnie, ale zarówno w zamiarze bezpośrednim, jak i ewentualnym. Zmiana ta może mieć istotne znaczenie praktyczne. Dotychczas trudno było udowodnić, że sprawca kradzieży tożsamości działał w zamiarze kierunkowym. Słusznie też w doktrynie poddawano w wątpliwość zasadność zawężenia sfery kryminalizacji tylko do zachowań z zamiarem kierunkowym i wyłączenia z niej działań sprawcy, który jedynie godził się, że jego działanie (podszywanie się) może wyrządzić szkodę pokrzywdzonemu[18].

Ustawodawca nie przybliżył, co rozumie przez szkodę majątkową lub osobistą. Pierwszą z nich będą wszelkie ujemne konsekwencje majątkowe dla pokrzywdzonego związane z działaniem sprawcy, które przejawiać się mogą w zmniejszeniu aktywów, spodziewanych korzyści lub w zwiększeniu się pasywów. Szkodą osobistą będzie natomiast taka, która ingeruje w szeroko rozumiane dobra osobiste pokrzywdzonego, która ma obniżyć jego reputację, ośmieszyć go, naruszyć jego godność. W doktrynie jako przykład tej szkody wskazuje się rozgłaszanie w imieniu ofiary informacji dotyczących wstydliwych dla niej szczegółów życia prywatnego czy umieszczanie anonsów erotycznych z telefonem ofiary w Internecie

10 K. Sowirka, *Przestępstwo „Kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, nr 1, s. 65.

11 Por. A. Zoll, [w:] *Kodeks karny. Część szczególna, t. II, Komentarz do art. 117–211a*, red. W. Wróbel, Warszawa 2017, s. 589.

12 https://sjp.pwn.pl/sjp/podszyc-sie;2502866.html (dostęp: 18.11.2022).

13 Por. A. Zoll, [w:] *Kodeks karny…*, s. 593.

14 Por. M. Mozgawa, [w:] *System Prawa Karnego, t. 10, Przestępstwa przeciwko dobrom indywidualnym*, red. J. Warylewski, Warszawa 2016, s. 469.

15 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (Dz.U.UE.L.2016.119.1).

16 https://sjp.pwn.pl/sjp/;2579940 (dostęp: 18.11.2022).

17 M. Mozgawa, [w:] *Kodeks karny. Komentarz, wyd. VII*, red. M. Mozgawa, Warszawa 2015, s. 509.

18 M. Mozgawa, [w:] *Kodeks…*, s. 510.

lub w innym mediach[19]. Może to być również np. podszywanie się pod lekarza i popieranie antynaukowych tez, które mogą naruszyć dobrą reputację takiej osoby.

W kontekście działalności osób trudniących się białym wywiadem konieczne jest wskazanie, że znamion omawianego przestępstwa nie wyczerpuje samo gromadzenie danych osobowych, nawet jeżeli zmierza ono do posłużenia się tożsamością istniejącej osoby. Działanie takie stanowiłoby jedynie przygotowanie do przestępstwa, które na mocy art. 16 § 2 k.k. karalne jest tylko wówczas, gdy ustawa tak stanowi, zaś art. 190a § 2 k.k., karalność takiego przygotowania nie przewiduje[20]. Znamion tego czynu przestępstwa nie będzie też wypełniało podszycie się pod osobę, która nie istnieje. W takim przypadku nie dochodzi bowiem do naruszenia dobra chronionego przedmiotowym przepisem. Kradzieżą tożsamości nie będzie również posługiwanie się danymi lub wizerunkiem osoby zmarłej, co związane jest z tym, że z ochrony omawianego przepisu korzystają osoby fizyczne, z którymi zgodnie z art. 8 k.c. mamy do czynienia od chwili narodzin do śmierci[21].

Warto też zwrócić uwagę, że omawiany występek nie został ujęty w katalogu czynów zabronionych stanowiących podstawę odpowiedzialności podmiotu zbiorowego wyrażonym w art. 16 u.o.p.z.[22] Ma to istotne znaczenie, biorąc pod uwagę, że OSINT-owcy często działają w imieniu lub w interesie takich podmiotów zbiorowych, np. biur wywiadu gospodarczego. Powyższe powoduje, że podmioty zbiorowe nie będą ponosiły odpowiedzialności nawet w razie przekroczenia granic legalności OSINT-u przez ich specjalistów.

Powyższa analiza prowadzi do wniosku, że co do zasady biały wywiad nie wyczerpuje znamion kradzieży tożsamości. W przypadku profilu legendy nieumyślnie opartego na danych istniejącej osoby, po stronie sprawcy nie zostaną wypełnione znamiona strony podmiotowej. Ocena działania sprawcy może być jednak odmienna, jeżeli celowo posługuje się on danymi innej osoby fizycznej (podszywa się pod nią). Dotychczas bowiem takie działanie mogło być uznane za wypełniające znamiona kradzieży tożsamości tylko wówczas, gdy sprawca działał „w celu" wyrządzenia takiej osobie szkody – w przypadku etycznego białego wywiadu taka sytuacja nigdy nie powinna mieć miejsca. Obecnie zaś cel działania sprawcy nie ma znaczenia. Jeżeli na skutek podszycia się pod inną osobę dojdzie do wyrządzenia jej szkody, odpowiedzialność poniesienie teraz sprawca, który chciał jej wyrządzenia, albo który przewidywał, że jego działanie (podszycie się pod daną osobę) może skutkować powstaniem takiej szkody, i godził się na to.

3. Bezprawne uzyskanie informacji a OSINT

Pozyskanie informacji przez osoby odpowiedzialne za OSINT odbywa się zwykle za pośrednictwem Internetu i związane jest z eksploatacją jego głębokich warstw, w tym z docieraniem do miejsc celowo ukrytych przed zwykłymi użytkownikami. Nie może budzić wątpliwości, że używanie w ramach białego wywiadu technik hackerskich, np. przełamywanie haseł lub wyłudzanie danych przez podszywanie się pod inne strony internetowe, wypełnia znamiona przestępstwa i nie może być uznane za legalne. Problem pojawia się przy wykorzystaniu metod, które zakładają np. uzyskanie dostępu do treści ukrytych w Internecie, ale niezabezpieczonych przed dostępem osób trzecich w żaden inny sposób bądź uzyskanie dostępu do treści ukrytych pod hasłem wykradzionym i upublicznionym w sieci przez inne osoby, a następnie wykorzystanym na potrzeby OSINT-u.

19 A. Michalska-Warias, [w:] *Kodeks karny. Komentarz*, red. T. Bojarski, Warszawa 2016, s. 532.

20 A. Lach, [w:] *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015, s. 99.

21 M. Siwicki, *Kradzież tożsamości – pojęcie i charakterystyka zjawiska*, „Edukacja Prawnicza" 2009, nr 11, s. 34.

22 Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz.U. z 2022 r. poz. 2600).

Opisane działania wymagają oceny w kontekście *hackingu*, który najogólniej oznacza sposób uzyskania dostępu do prywatnych danych za pośrednictwem sieci[23] lub uzyskanie nieuprawnionego dostępu do systemu komputerowego za pomocą specjalnych urządzeń[24]. Na gruncie k.k. *hacking* został uregulowany w art. 267 § 1 i 2. Pierwszy z tych przepisów przewiduje karalność uzyskiwania przez sprawcę dostępu do informacji dla niego nieprzeznaczonej, przez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej (teleinformatycznej) lub przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia. Drugi kryminalizuje uzyskiwanie bez uprawnienia dostępu do całości lub części systemu informatycznego. Przedmiotem ochrony ww. przepisów jest poufność informacji[25], tajemnica komunikowania się i dysponowania informacją[26]. Oba te występki popełnione mogą być jedynie umyślnie, w zamiarze bezpośrednim, a ich ściganie następuje na wniosek pokrzywdzonego.

Realizacja znamion występku określonego w art. 267 § 1 k.k. wymaga uzyskania przez sprawcę dostępu do nieprzeznaczonej dla niego informacji. Tą jest wiadomość lub suma wiadomości o osobie albo stanie rzeczy, dotycząca faktów, stanowiąca logiczną całość[27], do uzyskania której nie ma on upoważnienia wynikającego z ustawy, umowy lub woli nadawcy.

Uzyskanie przez sprawcę dostępu do informacji ma nastąpić w jeden ze sposobów określonych przez ustawodawcę. Z perspektywy OSINT-u najmniejsze znaczenie ma nieuprawnione otwarcie zamkniętego pisma. Takie działania niewątpliwie jest niezgodne z prawem i etyką, przez co wykracza poza granice białego wywiadu. Wśród sposobów bezprawnego uzyskania informacji, które wymagają szerszego omówienia, pozostaje podłączenie się do sieci telekomunikacyjnej oraz przełamanie albo ominięcie jej zabezpieczeń. Inne sposoby uzyskania przez sprawcę nieprzeznaczonej dla niego informacji, np. przez jej dobrowolne przekazanie przez osobę trzecią, pozostają poza regulacją ww. normy prawnej.

Sieć telekomunikacyjna zdefiniowana jest w art. 2 pkt 35 p.t.[28] jako systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną. Chodzi więc m.in. o sieci telefoniczne, komputerowe, w tym internetowe[29] rozumiane jako WI-FI lub sieć przewodowa. Podłączenie się do sieci telekomunikacyjnej polega na przyłączeniu do niej urządzenia odbiorczego, pozwalającego na pozyskiwanie przekazywanych za jej pośrednictwem informacji[30].

Przełamanie lub ominięcie zabezpieczeń nie zostało zdefiniowane w ustawie. Za P. Kardasem można przyjąć, że przełamanie zabezpieczenia to każda czynność, która ma umożliwić sprawcy dostęp do informacji, która może polegać na usunięciu zabezpieczenia przez jego zniszczenie w celu zniesienia jego funkcji ochronnej, jednakże bez zupełnego zniszczenia go[31].

---

23 M. Karpiuk, [w:] *Prawo nowych technologii. Wybrane zagadnienia*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, Warszawa 2015, s. 385.

24 Por. A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, s. 19.

25 F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 286.

26 W. Wróbel, D. Zając, [w:] *Kodeks karny. Część szczególna, t. II, Komentarz do art. 212-277d*, red. A. Zoll, Warszawa 2017, s. 643.

27 B. Kunicka-Michalska, *System Prawa Karnego, t. 8, Przestępstwa przeciwko państwu i dobrom zbiorowym*, red. L. Gardocki, Warszawa 2018, s. 940.

28 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 2581).

29 S. Hoc, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Legalis/el. 2020, art. 267.

30 A. Sakowicz, [w:] *Kodeks karny. Część szczególna, t. I, Komentarz*, red. M. Królikowski, R. Zawłocki, Warszawa 2017, s. 495.

31 P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, s. 71.

Znamię ominięcia zabezpieczeń nastręcza większych trudności. Ustawodawca wprowadził je do tekstu k.k. w 2008 r., uzasadniając to stanowiskiem specjalistów zajmujących się prawem informatycznym, że jest możliwe uzyskanie dostępu do zabezpieczonej informacji bez przełamywania, lecz z ominięciem jej zabezpieczeń[32]. Ominięciem zabezpieczeń będzie oddziaływanie na zabezpieczenia, które nie będzie skutkowało jego zniszczeniem lub naruszeniem[33]. Może ono polegać np. na wykorzystaniu socjotechnik, które pozwolą na nieuprawnione uzyskanie cudzego hasła dostępu bezpośrednio od jego dysponenta, fałszowaniu adresów stron internetowych i podszywaniu się pod inne strony, wprowadzaniu w błąd systemu poprzez zafałszowanie lokalizacji użytkownika lub adresu IP, wykorzystaniu luk w systemach operacyjnych za pośrednictwem odpowiedniego oprogramowania[34]. Według judykatury z przełamaniem lub ominięciem zabezpieczeń sieci telekomunikacyjnej będziemy mieli do czynienia m.in. w sytuacji przełamania hasła do konta użytkownika portalu społecznościowego[35] lub konta e-mail[36].

Niezależnie od tego, czy mówimy o przełamaniu, czy ominięciu zabezpieczenia sieci telekomunikacyjnej, warunkiem *sine qua non* jest istnienie zabezpieczenia. Rozumiane jest ono jako wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalnej lub specjalnego urządzenia bądź kodu[37]. Nie może budzić wątpliwości, że wejście w posiadanie informacji, która co prawda nie jest przeznaczona dla konkretnej osoby, ale która nie była zabezpieczona przed takim dostępem, nie wyczerpuje znamion opisanego występku. Ponadto przełamanie lub ominięcie zabezpieczeń powinno mieścić się w zamiarze sprawcy i musi wymagać jego aktywności. Z tego powodu, nie można uznać za przełamanie lub ominięcie zabezpieczenia uzyskanie informacji za pomocą rozszerzonych technik wyszukiwania informacji, w tym przeszukiwania treści nieindeksowanych przez przeglądarki internetowe, które umieszczone zostały na serwerach niezabezpieczonych co najmniej hasłem dostępu. O ile intencją osoby, która umieszcza informacje na stronie, podejmując następnie operacje mające na celu jej nieindeksowanie przez przeglądarki, a tym samym utrudnienie dostępu do niej przeciętnemu użytkownikowi Internetu, może być ukrycie tej informacji, o tyle nie można uznać tego za zabezpieczenie. Słusznie podnosi się w doktrynie, że ominięciem zabezpieczenia nie będzie dostanie się do informacji inną, niezabezpieczoną drogą[38] – a taką niewątpliwie jest umieszczenie informacji na serwerze niezabezpieczonym hasłem dostępu.

Podobnie należy oceniać podłączenie się do sieci telekomunikacyjnej za pośrednictwem loginu lub hasła udostępnionego bezpośrednio, lub pośrednio przez jej użytkownika, np. przez przekazanie ich albo pozostawienie niezabezpieczonych na widoku[39]. Działanie takie nie stanowi bowiem zabezpieczenia sieci telekomunikacyjnej i przez to nie można mówić o jego przełamaniu lub ominięciu.

Odmiennej oceny wymaga kwestia wykorzystania danych logowania do takiej sieci, które opublikowane zostały np. w darknecie, w wyniku ich wykradzenia lub zdobycia w inny nielegalny sposób. Co prawda w takiej sytuacji osoba, która prowadzi biały wywiad i wykorzystuje takie hasła, nie jest zwykle sprawcą ich kradzieży, to jednak wykorzystanie takiego hasła i uzyskanie informacji jest nieetyczne i przekracza granice dopuszczalnego prawem OSINT-u. Wskazać należy, że co do zasady przeciętny

32 Uzasadnienie do projektu ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2008 r. nr 214 poz. 1344).

33 Por. P. Kardas, *Prawnokarna*..., s. 71–73.

34 Por. F. Radoniewicz, *Odpowiedzialność karna*..., s. 293.

35 Wyrok SR w Wałbrzychu z dnia 11.10.2017 r. sygn. akt: II K 1036/16, LEX nr 2421166.

36 Wyrok SO w Częstochowie z dnia 29.05.2018 r. sygn. akt: VII Ka 312/18, LEX nr 2504770.

37 W. Wróbel, D. Zając, [w:] *Kodeks*..., s. 649.

38 A. Adamski, *Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r.*, „Przegląd Sądowy" 1998, nr 11–12, s. 150; K. Lipiński, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, s. 1152.

39 K. Lipiński, [w:] *Kodeks karny*..., s. 1152; Wyrok SA w Szczecinie z dnia 14.10.2008 r., sygn. akt: II AKa 120/08, LEX nr 508308.

użytkownik sieci chroni swoje dane za pomocą loginu i hasła. Wykradnięcie tych danych i opublikowanie ich w jasnej lub ciemnej stronie Internetu nie może być postrzegane jako niezabezpieczenie informacji przez ich właściciela – tak jak należy oceniać np. podanie komuś hasła dostępu lub umieszczenie go na obudowie monitora. Unicestwienie limitowanego dostępu do konta przez wykorzystanie nielegalnie zdobytego hasła należy więc według mnie oceniać w kategorii przełamania zabezpieczenia. Słusznie zwracają uwagę W. Wróbel i D. Zając, że: „każde uzyskanie dostępu do informacji z wykorzystaniem bezprawnie uzyskanego »klucza« dostępu do informacji (hasła, klucza szyfru, klucza do sejfu, w którym złożono dokumenty) będzie stanowić realizację znamion art. 267 § 1. Za przyjęciem powyższej interpretacji przemawiają te same względy, które nakazują traktować posłużenie się kradzionym kluczem jako włamanie”[40]. Odmienne zaopatrywanie na tę kwestię wyraził Sąd Apelacyjny w Szczecinie w wyroku z dnia 14.10.2008 r. w sprawie o sygn. akt: II AKa 120/08.

Drugą formą *hackingu* jest kryminalizowane w art. 267 § 2 k.k. uzyskanie bez uprawnienia dostępu do całości lub części systemu informatycznego. System taki nie został zdefiniowany w k.k. W art. 1 lit. a Konwencji o cyberprzestępczości[41] przyjęto, że jest to każde urządzenie lub grupa wzajemnie połączonych, lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych. W praktyce będzie to np. komputer, smartfon, ale też pralka lub lodówka wyposażona w mikroprocesor i Internet[42], portal internetowy, aplikacja mobilna.

Uzyskaniem dostępu jest powzięcie możliwości korzystania z zasobów danego systemu, czyli przetwarzanych w nim danych[43]. Czynność ta może nastąpić np. przez wykorzystanie podejrzanego hasła wprowadzanego przez inną osobę[44], użycie własnych danych logowania jednak z przekroczeniem posiadanych uprawnień (np. logowanie się do systemu informatycznego pracodawcy przez pracownika, któremu pracodawca wypowiedział stosunek pracy). Uprawnienie dostępu do systemu może wynikać z ustawy, umowy, ale też z wewnętrznych aktów obowiązujących w danej organizacji zarządzającej systemem. Warto podkreślić, że sprawca nie musi działać w celu uzyskania dostępu do danych znajdujących się w systemie. Celem sprawcy może być np. przejęcie zdalnej kontroli nad komputerem, w celu wykonania zmasowanych ataków na określone strony internetowe[45]. Istotne jest jedynie uzyskanie dostępu do systemu informatycznego bez uprawnienia.

Na marginesie wskazać należy na różnice pomiędzy występkiem z art. 267 § 1 k.k. a kryminalizowanym w art. 267 § 3 k.k. zakładaniem lub posługiwaniem się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem, w celu uzyskania informacji. Podstawową różnicą jest charakter tych czynów – pierwszy z nich ma bowiem charakter skutkowy w tym znaczeniu, że do wypełnienia jego znamion konieczne jest uzyskanie przez sprawcę dostępu do nieprzeznaczonej dla niego informacji. Drugi z tych występków nie wymaga osiągnięcia takiego skutku, bowiem dla jego bytu istotne jest jedynie działanie sprawcy „w celu uzyskania informacji” – nie ma więc znaczenia, czy faktycznie sprawca taką informację uzyska. Ponadto realizacja znamion czynu zabronionego z art. 267 § 3 k.k. nie wymaga ominięcia ani przełamania zabezpieczeń, przez co nie ma znaczenia, czy informacja, do której sprawca za pomocą urządzenia podsłuchowego, wizualnego, innego urządzenia lub oprogramowania uzyskał dostęp, była zabezpieczona. W doktrynie wskazuje się też, że art. 267 § 3 k.k. kryminalizuje przechwytywanie

40 W. Wróbel, D. Zając, [w:] *Kodeks*..., s. 643.

41 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).

42 A. Behan, *Współczesne systemy informatyczne a typy przestępstw z art. 267 Kodeksu karnego*, „Palestra” 2020, nr 2, s. 31–32.

43 Por. F. Radoniewicz, *Odpowiedzialność karna*..., s. 296.

44 A. Lach, [w:] *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Warszawa 2020, s. 1242.

45 P. Bogacki, *„Hacking” w ujęciu art. 267*, „Monitor Prawniczy” 2020, nr 17, s. 925.

danych podczas ich przesyłania, zaś art. 267 § 1 k.k. skupia się na uzyskaniu nieuprawnionego dostępu do danych przechowywanych w urządzeniu (serwerze, prywatnym laptopie itd.)[46].

Prowadzenie białego wywiadu co do zasady nie powinno prowadzić do naruszenia ww. norm prawnych. Czynności takiego wywiadu nie zakładają podłączania się do sieci telekomunikacyjnej (teleinformatycznej) ani omijania lub przełamywania zabezpieczeń, w celu uzyskania dostępu do informacji. Specjalista ma korzystać ze źródeł otwartych, a zatem nie powinien sięgać do systemów informatycznych, do których nie ma uprawnienia, jak też nie powinien stosować urządzeń podsłuchowych lub oprogramowania pozwalającego na bezprawne przechwytywanie informacji.

4. Nielegalne przetwarzanie danych a OSINT

OSINT zakłada gromadzenie i analizowanie różnorakich danych, w tym o podmiotach gospodarczych, ale też o osobach fizycznych. Najlepszą ilustracją gromadzenia i analizowania danych osób fizycznych jest biały wywiad stosowany przez specjalistów ds. rekrutacji, czy też przez prawników.

Pozyskiwanie, analizowanie, przechowywanie i wykorzystywanie danych osobowych rodzi ryzyko naruszenia normy sankcjonowanej wyrażonej w art. 107 u.o.d.o.[47] w typie podstawowym (ust. 1) lub kwalifikowanym (ust. 2). Kryminalizują one przetwarzanie danych osobowych, w sytuacji, gdy jest ono niedopuszczalne prawnie albo gdy osoba przetwarzająca nie jest do tego uprawniona. Typ kwalifikowany wejdzie w grę, gdy przedmiotem czynności wykonawczej będą dane szczególnych kategorii[48].

Pojęcie danych osobowych zostało już omówione. Na tym etapie warto wskazać, że danymi osobowymi nie będą informacje o osobie zmarłej[49]. Szczególne kategorie danych, zwane też danymi wrażliwymi, zostały wskazane w art. 9 ust. 1 RODO. W ich skład wchodzą dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej.

Przedmiotem ochrony wskazanych przepisów jest ochrona danych osobowych przed nieuprawnionym przetwarzaniem i związana z tym ochrona prywatności. Czynność sprawcza omawianego występku polega na niedopuszczalnym przetwarzaniu danych osobowych albo ich przetwarzaniu przez osobę nieuprawnioną. Blankietowy charakter omawianych przepisów powoduje, że odkodowanie zakresu kryminalizacji wymaga odwołania się do przepisów RODO, które regulują zasady ochrony danych osobowych[50].

Przetwarzanie zdefiniowane jest w art. 4 pkt 2 RODO, jako operacja lub zestaw operacji wykonywanych na danych osobowych, lub zestawach danych osobowych w sposób zautomatyzowany, lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie, lub łączenie, ograniczanie, usuwanie, lub niszczenie. Katalog operacji przetwarzania danych ma charakter otwarty. Realizacja chociażby jednej z takich czynności, przy uwzględnieniu, że będzie ona miała miejsce w sposób

46 F. Radoniewicz, *Odpowiedzialność karna*..., s. 305.

47 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781).

48 Por. J. Łuczak-Tarka, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, s. 532.

49 P. Fajgielski, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, red. P. Fajgielski, Warszawa 2022, s. 105.

50 M. Nawacki, *Kryminalizacja naruszenia ochrony danych osobowych*, „Studia Prawnoustrojowe UWM" 2021, nr 52, s. 312.

zautomatyzowany albo niezautomatyzowany i odbywać będzie się na danych osobowych bądź ich zestawach, przesądza o tym, że mamy do czynienia z ich przetwarzaniem[51].

Pierwszym z czynów penalizowanych przez omawiany przepis jest nielegalne przetwarzanie danych. Większość przedstawicieli doktryny za nielegalne uznaje przetwarzanie danych przez sprawcę w sytuacji, gdy nie może on skutecznie powołać się na żadną z przesłanek legalizujących wynikających z art. 6 ust. 1 lub art. 9 ust. 2 RODO[52]. Spotkać można jednak szersze poglądy, które za nielegalne uważają też przetwarzanie dokonane z naruszeniem zasad wynikających z art. 5 RODO, np. zasady ograniczenia celu, rzetelności i przejrzystości[53]. Drugie z tych stanowisk nie jest jednak przekonujące i nadmiernie rozszerzałoby zakres kryminalizacji omawianego przepisu.

Przesłanki legalizujące wskazane są w art. 6 ust. 1 i art. 9 ust. 2 RODO. Określają one sytuacje, w których przetwarzanie danych jest dozwolone. Pierwszy z tych przepisów odnosi się do danych osobowych zwykłych, wskazując, że przetwarzanie jest zgodne z prawem, m.in. gdy osoba, której dane dotyczą, wyrazi na nie zgodę (lit. a), przetwarzanie jest konieczne dla wykonania umowy, której podmiot danych jest stroną (lit. b) bądź ma na celu wypełnienie obowiązku prawnego przez administratora (lit. c). Drugi przepis odnosi się do danych wrażliwych. Uchyla on zakaz przetwarzania takich danych m.in. gdy osoba, której dane dotyczą, wyrazi na nie wyraźną zgodę (lit. a), przetwarzanie dotyczy danych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (lit. e) lub gdy jest ono niezbędne do ustalenia, dochodzenia, lub obrony roszczeń, lub w ramach sprawowania wymiaru sprawiedliwości przez sądy (lit. f).

Drugim z penalizowanych czynów jest nieuprawnione przetwarzanie danych. Wśród podmiotów uprawnionych do przetwarzania pierwszoplanowe znaczenie ma administrator danych zdefiniowany w art. 4 pkt 7 RODO. Jest nim osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który ustala cele i sposoby przetwarzania danych. Może on przetwarzać dane, gdy występuje po jego stronie choćby jedna z przesłanek legalizujących. Uprawnionym jest też podmiot przetwarzający, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). Dane mogą być też przetwarzane przez inne osoby, jeżeli zostaną one upoważnionego do tego przez administratora lub podmiot przetwarzający – i tylko w granicach takiego upoważnienia.

Z uwagi na bezpośrednie sprzężenie omawianych norm karnych z przepisami RODO, należy zwrócić uwagę na zakres zastosowania tego aktu. W kontekście OSINT-u najważniejsze wydaje się wyłączenie uregulowane w art. 2 ust. 1 lit. c RODO, który przewiduje, że akt ten nie ma zastosowania w razie przetwarzania danych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. W motywie 18 RODO wyjaśniono, że chodzi o przypadki przetwarzania, które odbywa się bez związku z działalnością zawodową lub handlową. Z perspektywy podmiotów, których specjaliści prowadzą biały wywiad, istotne wydaje się niewłączenie art. 107 u.o.d.o. do katalogu czynów zabronionych będących podstawą odpowiedzialności podmiotów zbiorowych na podstawie u.o.p.z.

Podsumowując, omówiony przepis ogranicza pole legalnego białego wywiadu. Przetwarzanie danych osób fizycznych dokonywane może być jedynie przez osobę uprawnioną i tylko w razie istnienia podstawy legalizującej taką czynność. W praktyce OSINT-owcy ani ich ewentualni zleceniodawcy nie identyfikują się jako administratorzy danych. Trudno też uznać, aby ich działania mogły być oparte na którejś z przesłanek legalizujących wskazanych w art. 6 lub art. 9 RODO. W przypadku profesjonalnego białego wywiadu wykluczone jest też powołanie się na działanie w czysto osobistym lub domowym charakterze.

51 W. Chomiczewski, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, s. 156.

52 J. Łuczak-Tarka, [w:] *Ustawa…*; P. Barta, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Legalis/el. 2021, art. 107.

53 P. Poniatowski, *Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne*, „Prokuratura i Prawo" 2021, nr 10, s. 73–77.

5. Podsumowanie

OSINT jest obecnie jedną z popularniejszych metod pozyskiwania i analizowania danych w sektorze prywatnym. W świecie, w którym jednostki niejednokrotnie dzielą się każdym elementem swojego życia w sieci, pozyskanie informacji staje się coraz łatwiejsze. Biały wywiad może być oceniany w różnoraki sposób. Niewątpliwie ma on wiele plusów, np. pozwala na wykrycie nieprawidłowości i to zarówno w ramach czynności prowadzonych przez organy ścigania, jak i w branży prywatnej, chociażby poprzez ujawnianie nielojalnych współpracowników, wycieków danych albo rzetelności kontrahentów. Z drugiej strony niesie on za sobą szereg zagrożeń. Brak regulacji prawnych, które określałyby jego ramy, powoduje, że wykorzystywany jest on nie tylko przez osoby kierujące się dobrymi intencjami, ale również przez przestępców, którzy w oparciu o uzyskane z otwartych źródeł dane zbierają cały komplet informacji o swojej przyszłej ofierze, tworzą i posługują się fałszywymi tożsamościami.

Z przeprowadzonej analizy płynie wniosek, że biały wywiad prowadzony zgodnie z założeniami – etycznie i z wykorzystaniem jawnych źródeł, nie wypełnia znamion występku kradzieży tożsamości ani *hackingu*. Według mnie jednak działania takie będą zwykle wypełniały znamiona występku nieuprawnionego przetwarzania danych osobowych, na co powinni zwrócić uwagę specjaliści trudzący się tymi metodami.

Niezależnie od tego trzeba zwrócić uwagę, że biały wywiad zakłada nieujawnianie faktu prowadzenia takich działań osobie, o której gromadzone są informacje, i przeprowadzanie ich z wykorzystaniem metod i narzędzi zapewniających anonimowość, np. VPN-ów, maszyn wirtualnych, sieci TOR. Sprawia to, że uzyskanie przez pokrzywdzonego informacji, iż stał się „ofiarą" OSINT-u, staje się niezwykle utrudnione, a jeszcze trudniejsze staje się zidentyfikowanie sprawcy takiego działania.

Konieczne jest też podkreślenie, że niniejsze omówienie ma charakter przyczynkowy i nie obejmuje omówienia wszystkich możliwych typów przestępstw, których znamiona mogą wypełniać działania osoby prowadzącej biały wywiad.

Bibliografia

Adamski A., *Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r.*, „Przegląd Sądowy" 1998, nr 11–12.

Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001.

Barta P., [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Legalis/el. 2021, art. 107.

Behan A., *Współczesne systemy informatyczne a typy przestępstw z art. 267 Kodeksu karnego*, „Palestra" 2020, nr 2.

Bogacki P., *„Hacking" w ujęciu art. 267*, „Monitor Prawniczy" 2020, nr 17.

Chomiczewski W., [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018.

Fajgielski P., [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, red. P. Fajgielski, Warszawa 2022.

Hoc S., [w:] *Kodeks karny. Komentarz*, red. R. Stefański, Legalis/el. 2020, art. 267.

Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.

Karpiuk M., [w:] *Prawo nowych technologii. Wybrane zagadnienia*, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, Warszawa 2015.

Kunicka-Michalska B., [w:] *System Prawa Karnego, t. 8, Przestępstwa przeciwko państwu i dobrom zbiorowym*, red. L. Gardocki, Warszawa 2018.
Lach A., [w:] *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015.
Lach A., [w:] *Kodeks karny. Komentarz*, wyd. III, red. V. Konarska-Wrzosek, Warszawa 2020.
Lipiński K., [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021.
Łuczak-Tarka J., [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019.
Majorek M., *Darknet. Ostatni bastion wolności w internecie?*, „Bezpieczeństwo. Teoria i praktyka" 2017, nr 4.
Michalska-Warias A., [w:] *Kodeks karny. Komentarz,* red. T. Bojarski, Warszawa 2016.
Mider D., *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21.
Mozgawa M., [w:] *Kodeks karny. Komentarz, wyd. VII*, red. M. Mozgawa, Warszawa 2015.
Mozgawa M., [w:] *System Prawa Karnego*, t. 10, *Przestępstwa przeciwko dobrom indywidualnym,* red. J. Warylewski, Warszawa 2016.
Nawacki M., Kryminalizacja naruszenia ochrony danych osobowych, „Studia Prawnoustrojowe UWM" 2021, nr 52, https://doi.org/10.31648/sp.6615
Pączkowski T., *Biały wywiad. Materiały dydaktyczne Policji*, Katowice 2020.
Poniatowski P., *Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne*, „Prokuratura i Prawo" 2021, nr 10.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Sakowicz A., [w:] *Kodeks karny. Część szczególna, t. I, Komentarz*, red. M. Królikowski, R. Zawłocki, Warszawa 2017.
Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015.
Siwicki M., *Kradzież tożsamości – pojęcie i charakterystyka zjawiska*, „Edukacja Prawnicza" 2009, nr 11.
Sowirka K., *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, nr 1.
Tylutki K., *Informacja masowego rażenia – OSINT w działalności wywiadowczej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19.
Wróbel W., Zając D., [w:] *Kodeks karny. Część szczególna, t. II, Komentarz do art. 212–277d*, red. A. Zoll, Warszawa 2017.
Ziółkowska A., *Biały wywiad jako ogólnodostępna forma cyberinwigilacji a bezpieczeństwo danych użytkowników urządzeń mobilnych*, „Wiedza Obronna" 2017, nr 3–4.
Zoll A., [w:] *Kodeks karny. Część szczególna, t. II, Komentarz do art. 117–211a*, red. W. Wróbel, Warszawa 2017.

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (Dz.U.UE.L.2016.119.1).
Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz.U. z 2022 r. poz. 2600).
Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 2581).
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781).
Uzasadnienie do projektu ustawy z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2008 r. nr 214 poz. 1344).

Orzecznictwo

Wyrok SA w Szczecinie z dnia 14.10.2008 r., II AKa 120/08, LEX nr 508308.
Wyrok SO w Częstochowie z dnia 29.05.2018 r., VII Ka 312/18, LEX nr 2504770.
Wyrok SR w Wałbrzychu z dnia 11.10.2017 r., II K 1036/16, LEX nr 2421166.

Źródła internetowe

https://sjp.pwn.pl/sjp/;2579940 (dostęp: 18.11.2022)
https://sjp.pwn.pl/sjp/podszyc-sie;2502866.html (dostęp: 18.11.2022)
https://thispersondoesnotexist.com/ (dostęp: 16.11.2022)