Erwin Ryter[1]

KRADZIEŻ TOŻSAMOŚCI JAKO EFEKT NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ŚWIETLE RODO, USTAW KARNYCH ORAZ INNYCH REGULACJI PRAWNYCH W DOBIE ROSNĄCEJ CYBERPRZESTĘPCZOŚCI

IDENTITY THEFT AS A RESULT OF BREACH OF PERSONAL DATA PROTECTION IN THE CONTEXT OF GDPR, PENAL LAWS AND OTHER LEGAL REGULATIONS IN THE ERA OF INCREASING CYBERCRIME

Otrzymano: 26.10.2019 Zaakceptowano: 14.04.2020 Opublikowano: 26.06.2020
DOI: 10.5604/01.3001.0014.1391
Artykuł Oryginalny
Źródło finansowania – badania własne

Streszczenie

Przedmiotowa publikacja ma na celu zwrócenie uwagi na powszechnie występujący problem kradzieży tożsamości zarówno w przestrzeni wirtualnej w związku z rosnącym postępem technologicznym oraz coraz bardziej znaczącym zaangażowaniem społeczeństwa w cyberprzestrzeń, która stała się obszarem nie tylko kultury i rozrywki, ale także przestrzenią do wykonywania pracy, jak również realizacji zwykłych codziennych czynności, w toku których dochodzi do przepływu, ujawnienia oraz za-

[1] Mgr Erwin Ryter, Katedra Prawa karnego Wykonawczego, Uniwersytet Łódzki, autor do korespondencji: Erwin Ryter, e-mail: doradztwoprawne.ryter@op.pl, ORCID: 0000-0002-6024-9997.

DOI: 10.5604/01.3001.0014.1391

mierzonego bądź niezamierzonego przekazywania swoich danych osobowych, niestety często jeszcze bez zachowania jakichkolwiek środków ostrożności. Wielość oraz różnorodność zarówno wytycznych, jak i innych regulacji prawnych, pozwala przypuszczać, że dziedzina związana ze sferą ochrony danych osobowych oraz bezpieczeństwa w cyberprzestrzeni jest bardzo rozwojowa i należy się jej szczególna uwaga w dobie mocno postępującej informatyzacji, do której należy się przystosować w jak najwyższym stopniu. Co istotne, zwrócenie uwagi na ścieżkę, po której dochodzi do kradzieży tożsamości, a zapoczątkowaną najczęściej zwykłym ludzkim błędem lub zaniedbaniem, prowadzi do wniosku, iż podnoszenie świadomości w tej materii ma kluczowe znaczenie i należy temu poświęcić jak najwięcej zainteresowania.

Słowa kluczowe: kradzież tożsamości, cyberprzestępczość, wyciek danych, naruszenie ochrony danych, RODO, naruszenie dóbr osobistych

Abstract

The objective of this paper is to draw attention to the widespread problem of identity theft in virtual space as a result of increasing technological progress and increasing involvement of the society in cyberspace, which has become an area not only of culture and entertainment, but also work, as well as ordinary daily activities where flow, disclosure and deliberate or unintentional transfer of personal data take place – unfortunately, often without any precautions. The multitude and diversity of both guidelines and other legal regulations suggest that the field of personal data protection and cyberspace security is evolving significantly and deserves special attention in the times of intensive implementation of IT solutions; this field requires the highest possible degree of adaptation. Importantly, drawing attention to the path of identity theft, most often initiated by a simple human error or negligence, leads to the conclusion that raising awareness in this area is crucial and that as much attention as possible should be devoted to this issue.

Key words: identity theft, cybercrime, data leak, data protection breach, GDPR, violation of personal rights

1. Cel artykułu, jego uzasadnienie oraz zastosowana metoda badawcza

Przed poddaniem w analizę kwestii odnoszących się *stricte* do istoty kradzieży tożsamości, będącej *meritum* niniejszego opracowania, autor pragnie w pierwszej kolejności zwrócić uwagę na znaczenie i wyjaśnienie pojęcia „tożsamość", które – jak wyraźnie daje się zauważyć – zasadniczo zyskało na znaczeniu, zwłaszcza w dobie zarówno aktualnych transformacji prawnych, dynamicznych przemian społeczno-gospodarczych, jak również postępującej informatyzacji. Prezentowane zagadnienie, tj. traktujące bezpośrednio na temat kradzieży tożsamości, już jakiś czas temu stało się przedmiotem zwiększonego zainteresowania nie tylko na gruncie dziedziny prawa ochrony danych osobowych, lecz także innych nauk, takich jak m.in. psychologia, antropologia, nauki społeczne, socjologiczne czy filozoficzne. Każda z tych specjalności odmiennie akcentuje i postrzega problem tożsamości, jak również powiązanych z nią zagadnień oraz dylematów. Niemniej autor pragnie skupić się wyłącznie na prawnym ujęciu tematyki tożsamości, w tym jej kradzieży, która coraz częściej staje się przedmiotem przestępczych działań w przestrzeni, jaką jest środowisko techniki i technologii informatycznej podlegające z jednej strony – intensywnemu rozwojowi, zaś z drugiej – narażeniu na działalność przestępczą jawiącą się najczęściej w postaci ataków hakerskich.

W nawiązaniu do powyższego, zasadniczym celem niniejszego opracowania jest przede wszystkim zwrócenie uwagi na istotę kradzieży tożsamości poprzez pryzmat pojęcia „tożsamość", zwłaszcza w jego prawnym znaczeniu, zaś w dalszej perspektywie, przejście na grunt praktycznych rozważań odnoszących się do aktualnych problemów związanych z kradzieżą tożsamości, będących następstwem dynamicznie rozwijających się mechanizmów oraz metod jakimi posługują się sprawcy tego czynu.

Kluczowe – w ocenie autora – jest również zwrócenie uwagi na istotność wybranych zagadnień poruszonych w artykule oraz różnorodnych mechanizmów wykorzystywania czyjejś tożsamości w powiązaniu ze współczesnym rozumieniem jej sensu oraz znaczenia jako wartości identyfikującej każdego człowieka.

Trudno także nie zauważyć, że tożsamość jako dobro narażone przede wszystkim na cyberataki, ale również na inne sieciowe zagrożenia, zasługuje na szczególne zainteresowanie potencjalnego czytelnika, poprzez

DOI: 10.5604/01.3001.0014.1391

wzniecenie w nim zwiększonej świadomości na temat istotnych zagrożeń znajdujących się w jego otoczeniu, często nieuświadomionych i przez to niestety bagatelizowanych. Pochylenie się nad zagadnieniem nabierającym coraz bardziej doniosłego znaczenia w dobie dynamicznie rozwijającej się informatyzacji jest – zdaniem autora – sprawą znacznej wagi, nie pozwalającą na bezrefleksyjne przejście obok wyeksponowanego tematu.

Prezentując oraz badając wybrane zagadnienia, autor wykorzystał metodę dogmatyczno-prawną, dzięki której dokonał analizy istniejących regulacji prawnych w kontekście omawianej materii. W szczególności zostały podjęte rozważania w kwestiach odnoszących się zarówno do zagrożeń jakie niesie ze sobą kradzież tożsamości, jak również te związane z przeglądem wybranego materiału normatywnego traktującego na temat uwydatnionych dylematów i rozważań.

2. Rozważania wstępne

Termin *identity* tłumaczony jako tożsamość, wprowadził do nauk społecznych w latach 50. XX wieku Erik Erikson – psycholog, odwołujący się do tradycji postfreudowskiej[2].

Tożsamość osobistą można uznać za unikatowy, specyficzny dla jednostki i względnie stabilny sposób określania, rozumienia i doświadczania siebie, będący wyrazem dążenia do osiągnięcia osobistej autonomii i wewnętrznej integracji. Tożsamość jako taka stanowi o indywidualności i niepowtarzalności każdego człowieka[3].

Katarzyna Waszczyńska ujmuje w swojej pracy tożsamość jako pojęcie złożone i wieloaspektowe, odnoszące się do jej odmiennych znaczeń, takich jak np.: tożsamość jednostki oznaczająca zdolność człowieka do określenia tego kim jest; tożsamość grupy jako zdolność jej członków do postrzegania siebie w związku z wzajemnym oddziaływaniem; tożsamość społeczna odwołująca się do określenia przynależności do jakiejś grupy społecznej; tożsamość kulturowa mogąca stanowić wyraz postawy jednostki względem dziedzictwa przeszłości czy tożsamość etniczna, zwana także narodową, dla której jedną z charakterystycznych cech jest określenie roli tego rodzaju toż-

[2] K. Waszczyńska, *Wokół problematyki tożsamości*, „Rocznik Towarzystwa Naukowego Płockiego" 2014, nr 6, s. 50.

[3] K. Kwapis, E. Brygoła, *Tożsamość osobista w ujęciu emotywno-refleksyjnym: zawartość, funkcje i procesy kształtowania tożsamości*, „Opuscula Sociologica" 2014, nr 4, s. 34.

samości jako zaspokajanie psychologicznej potrzeby osobistego bezpieczeństwa, przynależności, pamięci o własnych korzeniach i związanymi z nią wspólnotowością, językiem, zwyczajami, rytuałami, religią, symbolami itd.[4]

Najbardziej interesujące – z punktu widzenia niniejszego artykułu – jest poczucie tożsamości jednostki, które opiera się na subiektywnym sposobie postrzegania siebie przez jednostkę, poszukującą odpowiedzi na pytanie, kim jest[5].

Nie tylko w powszechnym rozumieniu, lecz przede wszystkim na podstawie własnych spostrzeżeń autora, w tym biorąc pod uwagę cel niniejszego opracowania, pojęcie tożsamości osoby fizycznej może – w określonej sytuacji – odpowiadać pojmowaniu tego terminu także jako danych osobowych, które w charakterystycznym ujęciu identyfikują osobę fizyczną, tj. w sposób nieskomplikowany i zarazem jednoznaczny, a zatem najczęściej za pomocą imienia i nazwiska, numeru PESEL, a także dodatkowo jeszcze miejsca zamieszkania. Oczywiście wskazane powyżej dane, nie są informacjami, które każdorazowo pozwolą w sposób wyczerpujący na identyfikację każdego człowieka. Bowiem uwierzytelnianie osoby fizycznej[6] dokonywane jest zazwyczaj za pomocą szerszego katalogu informacji, w zależności od danej sytuacji, często także – jeśli dochodzi do niego w systemach informatycznych – za pomocą indywidualnie przypisanych loginów, PIN-ów, identyfikatorów bądź haseł dostępu. Zgodnie z powyższym, dane osobowe osoby fizycznej mogą kreować jej tożsamość rozumianą jako postrzeganie własnej osoby w ujęciu zmierzającym do wyraźnego odróżnienia jej od innych ludzi. A zatem informacje, które pozwalają na identyfikację osoby, mogą składać się na jej tożsamość ze względu na cechy wyróżniające tę osobę spośród innych osób, tj. określające to, kim ta osoba jest, jaką posiada osobowość, charakter bądź upodobania, dzięki czemu osobę tę można „odnaleźć w tłumie", czyli zidentyfikować.

Ponadto odwołując się do znaczenia pojęcia „tożsamość"[7] zdefiniowanego w Słowniku Języka Polskiego PWN, spotkać się można z ujęciem go jako „identyczność", „świadomość siebie", gdy dotyczy to jednego

[4] K. Waszczyńska, *Wokół problematyki tożsamości*, „Rocznik Towarzystwa Naukowego Płockiego" 2014, nr 6, s. 53–58.

[5] M. Wójcicka, *Tożsamość w procesie komunikacji*, „Artes Humane" 2016, nr 1, s. 56.

[6] Uwierzytelnienie oznacza udowodnienie, że dana osoba posiada pewną tożsamość i/ lub jest uprawniona do wykonania pewnych czynności. Zob. *Podręcznik europejskiego prawa o ochronie danych osobowych*, pobrany z https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pl.pdf, dostęp: 22.10.2019.

[7] Zob. *Słownik Języka Polskiego PWN*.

DOI: 10.5604/01.3001.0014.1391

człowieka bądź też pojęcie to można określić jako „fakty, cechy, dane personalne pozwalające zidentyfikować jakąś osobę".

Z rozporządzenia 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 (ogólne rozporządzenie o ochronie danych)[8] można wywieść pojęcie tożsamości, szczególnie w związku z wykładnią art. 4 ust. 1, zgodnie z którym przez tożsamość osoby fizycznej można rozumieć jeden z elementów pojęcia „danych osobowych", na który składają się cechy określające indywidualne właściwości każdej osoby fizycznej, a zatem jej imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dzięki tym cechom staje się możliwa identyfikacja konkretnej osoby fizycznej.

Rozpatrując aktualne problemy wiążące się z zagadnieniem tożsamości, na gruncie analizowanej materii, warto wskazać na możliwość jej bezprawnego wykorzystania poprzez dokonanie kradzieży bądź jej przywłaszczenia. W praktyce oznacza to, w szczególności, podszywanie się pod dane innej osoby bądź pod jej wizerunek, celem popełnienia czynu zabronionego, najczęściej w postaci wyrządzenia określonej szkody bądź krzywdy tej osobie, której ukradzione lub przywłaszczone dane dotyczą.

W dobie aktualnych uwarunkowań technicznych i szybkiego rozwoju informatyzacji[9] powstanie na tym tle społeczeństwa informacyjnego[10] przyczyniło się do rozwoju takich form przestępczości, jak np. kradzież tożsamości[11]. Zjawisko społeczeństwa informacyjnego, które zostało zde-

[8] 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016).

[9] Jest to proces, który wciąż postępuje i polega na racjonalnym wykorzystaniu uprzednio wprowadzonych już danych do systemów informatycznych w możliwie największym dopuszczalnym zakresie przez inne systemy informatyczne. Informacja została zaczerpnięta ze strony https://pl.wikipedia.org/wiki/Informatyzacja, dostęp: 22.10.2019.

[10] Jest to społeczeństwo, w którym towarem staje się informacja traktowana jako szczególne dobro niematerialne, równoważne lub cenniejsze nawet od dóbr materialnych. Informacja została zaczerpnięta ze strony https://pl.wikipedia.org/wiki/Spo%C5%82ecze%C5%84stwo_informacyjne, dostęp: 22.10.2019.

[11] K. Sowirka, *Przestępstwo kradzieży tożsamości w polskim prawie karnym*, „Ius Novum" 2013, nr 1, s. 64.

finiowane w 1963 r. przez japońskiego naukowca Tadao Umesao, stworzyło podwaliny do powstania form przestępczości, do których zaliczyć można kradzież tożsamości[12]. Do Europy pojęcie to dotarło w 1978 roku za pośrednictwem pary socjologów, Simona Nory i Alaina Minca, w sprawozdaniu przedłożonym prezydentowi Francji[13].

Nie należy zapominać, iż aktualnie najczęściej spotykane sytuacje, w których może dochodzić do kradzieży tożsamości, nieuchronnie wiążą się z szeroko ujmowaną przestępczością komputerową[14], a zatem różnorakimi formami działań ukierunkowanych na zachwianie bezpieczeństwem w sieci czy w systemach informatycznych, jak również dążeniem do udostępniania czy rozpowszechniania informacji na temat osób fizycznych w sieci Internet. Przestępczość komputerową postrzega się także jako działania dążące do uskutecznienia różnego rodzaju oszustw komputerowych, zorganizowania sabotażu, piractwa komputerowego bądź też niszczenia lub zaboru danych z systemów informatycznych.

Warto wskazać, że aktualnie obowiązujący kodeks karny[15] nie operuje *stricte* pojęciem przestępstwa komputerowego, mimo iż w doktrynie prawniczej, jak również w orzecznictwie, termin ten pojawia się dość regularnie w kontekście rozpatrywania czynów zabronionych z art. 287 § 1 k.k., znajdujących powiązanie z nielegalną działalnością w cyberprzestrzeni bądź takim postępowaniem sprawcy, które zawiera się w manipulowaniu informacjami w systemach informatycznych bez żadnego upoważnienia.

Przestępstwo oszustwa komputerowego stało się między innymi przedmiotem rozważań Sądu Okręgowego Warszawa–Praga w Warszawie w V Wydziale Karnym w sprawie V K 217/15, który podał, że do istoty oszustwa komputerowego należy to, że sprawca, działając bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji albo zmienia, usuwa lub wprowadza nowy zapis na danych informatycznych[16].

Na przykład Renata Jedlińska definiuje przestępczość komputerową jako nową i jedną z najszybciej rozwijających się form przestępczości trans-

[12] J. Grabowska, A. Kaczmarczyk, *Kradzież tożsamości z art. 190a § 2 k.k. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016, nr 4, s. 86.

[13] I.A. Jaroszewska, *KPP Monografie. Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 3.

[14] Zob. K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2/24, s. 39–43.

[15] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2019, poz. 1950 t.j.) – zwana dalej k.k.

[16] Wyrok Sądu Okręgowego Warszawa–Praga w Warszawie, V Wydział Karny z dnia 21.07.2017 r., sygn. akt V K 217/15, LEX nr 2675229.

DOI: 10.5604/01.3001.0014.1391

granicznych, będącą następstwem aktualnego trybu życia i nieustannego korzystania z Internetu[17].

Ten rodzaj przestępczości można zatem zakwalifikować do czynów ujętych przede wszystkim jako kategoria przestępstw przeciwko ochronie informacji, zwłaszcza na gruncie występków wymienionych od art. 267 do art. 269b k.k.

Z kolei, jak wskazuje Agnieszka Kania, do kategorii przestępstw komputerowych można ponadto zakwalifikować takie typy czynów zabronionych, których sposób popełnienia będzie decydował o ich „komputerowym charakterze". Mowa tu o czynach ujętych w: art. 278 § 2 k.k. – uzyskanie cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej; art. 293 § 1 k.k. – paserstwo programu komputerowego; art. 285 k.k. – oszustwo telekomunikacyjne czy art. 287 k.k. – oszustwo komputerowe[18].

A zatem szeroko rozumiane pojęcie kradzieży tożsamości w dzisiejszych czasach stanie się najprawdopodobniej problemem narastającym ze względu na coraz bardziej wyrafinowane i doskonałe techniki jej zaboru przez wyspecjalizowanych oszustów, w celach związanych z działalnością naruszającą obowiązujący porządek prawny.

3. Zagadnienia prawnokarne kradzieży tożsamości

Zagadnienie tzw. kradzieży tożsamości zostało spenalizowane w art. 190a § 2 k.k. Zgodnie z brzemieniem tego artykułu, kto podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe[19] w celu

[17] K. Jedlińska, *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1 (126), t. 2, s. 185.

[18] Zob. A. Kania, *Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni*, „CBKE e-Biuletyn" 2009, nr 1, s. 6.

[19] Definicja danych osobowych została zawarta w art. 4 ust. 1 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L Nr 119, s. 1) – zwane dalej RODO, zgodnie z którym są to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Z kolei możliwa do zidentyfikowania osoba fizyczna to osoba, którą można pośrednio lub bezpośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

wyrządzenia jej szkody majątkowej lub osobistej, podlega karze pozbawienia wolności do lat 3. Należy jednak zauważyć, że pojęcie „podszywania się pod inną osobę", ujmowane w powszechnym tego słowa znaczeniu jako kradzież tożsamości, stanowi jedno w kilku czynów zabronionych ujętych w grupie przestępstw spenalizowanych w art. 190a k.k., obejmujących podejmowanie przeciwko innej osobie działań, takich jak uporczywe nękanie poprzez istotne naruszanie jej prywatności czy kradzież tożsamości w związku z podszywaniem się pod inną osobę bądź wykorzystaniem jej wizerunku.

Głównym przedmiotem ochrony jest tu szeroko rozumiana wolność, w aspekcie zarówno wolności „od czegoś" (od strachu, od nagabywania, od niechcianego towarzystwa innej osoby), jak i wolności „do czegoś" (przede wszystkim do zachowania swojej prywatności). Ubocznym przedmiotem ochrony zdają się tu być zdrowie człowieka (psychiczne, fizyczne), jego nietykalność cielesna, nienaruszalność korespondencji itp.[20]

Będące przedmiotem zainteresowania niniejszego artykułu przestępstwo kradzieży tożsamości zostało wprowadzone ustawą z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny[21] jako nowy typ przestępstwa, polegający na podszywaniu się pod inną osobę i wykorzystaniu jej wizerunku bądź innych danych ją identyfikujących, w celu wyrządzenia jej określonej szkody majątkowej lub osobistej.

Przestępstwo z art. 190a § 2 k.k. określa czyn zabroniony naruszający nie tylko wolności, ale również dobra osobiste[22], wśród których wymienić można ochronę danych osobowych oraz prawo do prywatności[23].

---

[20] M. Mozgawa, *Komentarz do art. 190a k.k.*, w: *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el 2019.

[21] Ustawa z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny (Dz.U. 2016, poz. 1137).

[22] W kwestii pojęcia i ochrony dóbr osobistych, o których mowa w art. 23 ustawy z dnia 24 kwietnia 1964 r. Kodeks Cywilny (Dz.U. 2019, poz. 1145 t.j.). – zwanej dalej k.c., jakimi są m.in. nazwisko lub pseudonim bądź wizerunek osoby, które mogą składać się na tożsamość osoby fizycznej, a także okoliczności jej kradzieży, wiele razy wypowiadały się sądy powszechne. M.in. Sąd Rejonowy w Piotrkowie Trybunalskim w wyroku z dnia 20 czerwca 2017 r., VII K 770/16, wskazał na podanie danych osobowych innej osoby podczas kontroli biletów w autobusie (LEX nr 2342713). Z kolei jako ewidentną sytuację kradzieży tożsamości wskazał Sąd Rejonowy w Nidzicy w wyroku z dnia 14 marca 2017 r., II K 315/16, utworzenie z wykorzystaniem wizerunku pokrzywdzonego oraz jego danych osobowych (w postaci imienia i nazwiska, adresu zamieszkania i nazwy szkoły, do której uczęszcza) dwóch profili na portalu społecznościowym, profilu na komunikatorze internetowym i czacie, na których sprawca korespondował z innymi osobami jako pokrzywdzony (LEX nr 2322333).

[23] J. Grabowska, A. Kaczmarczyk, *Kradzież tożsamości z art. 190a § 2 k.k. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016, nr 4, s. 86.

DOI: 10.5604/01.3001.0014.1391

Omawiane przestępstwo, a zatem kradzież tożsamości, jest przede wszystkim, popełniane w celach przestępczych, co może przybrać postać podszywania się pod dane osobowe innej osoby np. po to, aby założyć fałszywe konto w banku i zaciągnąć kredyt, pożyczkę lub inne zobowiązanie, założyć fałszywą działalność gospodarczą w celu wyłudzenia podatku VAT, przywłaszczyć wynajętą rzecz, dokonać zakupów online, utworzyć fałszywy profil w sieci czy wejść w proces „prania brudnych pieniędzy". Jako przykład bezprawnego zastosowania ukradzionej tożsamości podaje się także dokonanie oszustwa w handlu online, jak również rozpowszechnianie pornografii, a nawet ułatwianie kontaktów pedofilskich.

Przed nierozważnym zamieszczaniem zdjęć dzieci w Internecie – w związku z niebezpieczeństwem kradzieży tożsamości – przestrzegał wielokrotnie Urząd Ochrony Danych Osobowych, wskazując na powszechnie występujące wśród użytkowników sieci sytuacje, takie jak zamieszczanie fotografii czy publikowanie informacji o innych osobach. W skrajnych przypadkach nierozważne dysponowanie danymi w sieci, a zwłaszcza tymi, które dotyczą dzieci, może stać się nawet źródłem pożywki dla osób o skłonnościach pedofilskich[24].

W orzecznictwie sądowym bardzo często spotyka się rozstrzygnięcia ustalające, iż charakter popełnionego czynu zabronionego – w przypadku postępowania karnego w sprawie o kradzież tożsamości – wyczerpuje nie tylko dyspozycję art. 190a § 2 k.k., ale także art. 286 § 1 k.k., albowiem sprawca oprócz posłużenia się danymi innej osoby i podszycia się pod nią, przykładowo zaciągając zobowiązanie, z góry zakłada, iż nie będzie go spłacał, a zatem wprowadza pożyczkodawcę w błąd nie tylko co do tożsamości pożyczkobiorcy, ale także i samego zamiaru spłaty, a konkretnie jego braku.

Przestępstwo kradzieży tożsamości związane jest coraz częściej z wciąż rosnącym postępem technologicznym, zwłaszcza w systemach informatycznych, w których brak jest możliwości bezpośredniej identyfikacji osoby fizycznej przez inną osobę. Identyfikacja ta następuje bowiem na zasadzie użycia określonych danych przypisanych konkretnej osobie, np. loginu i hasła do internetowego konta bankowego, do którego za pomocą tych danych może się dostać osoba inna niż faktycznie uprawniona do

[24] Zob. informacje zamieszczone przez Generalnego Inspektora Ochrony Danych Osobowych w poradniku „Ochrona danych osobowych w czasie wakacji", pobrane z: https://uodo.gov.pl/pl/71/119, dostęp: 06.03.2020 r.

dysponowania nimi. Nowoczesny i intensywny styl życia prowadzi ponadto coraz częściej do dokonywania różnego rodzaju transakcji handlowych w sieci, a przez to i konieczności wirtualnego posługiwania się danymi, które wskutek nieodpowiedniego zabezpieczenia bądź zawodnego działania systemów informatycznych mogą zostać przechwycone przez przestępców trudniących się pozyskiwaniem i bezprawnym wykorzystywaniem tych danych, zwłaszcza na etapie uwierzytelniania, za pomocą różnego rodzaju danych, które powinny być znane wyłącznie osobie, której te dane dotyczą. W niektórych sytuacjach szczególnie przydatny przy tym procesie może się okazać podpis elektroniczny.

Analiza spraw oraz rozstrzygnięć sądowych dotyczących losów osób pokrzywdzonych przestępstwem z art. 190a § 2 k.k. prowadzi do wniosku, iż narastającym obecnie problemem w przestrzeni IT, narażonej w sposób znaczny na cyberataki, jest brak bezpiecznych procedur uwierzytelniania danych, tj. w taki sposób, aby ograniczyć ryzyko kradzieży tożsamości do poziomu możliwego do zaakceptowania. Na problem ten zwrócił w szczególności uwagę Urząd Ochrony Danych Osobowych, który regularnie mierzy się ze skargami ze strony osób fizycznych, stanowiącymi o tym, że nawet posługiwanie się kwalifikowanym podpisem elektronicznym przedstawia zagrożenie dla ich prywatności, a pośrednio także może narażać na kradzież tożsamości, co może mieć związek z ujawnianiem w tym podpisie numeru PESEL osoby, która się tym podpisem posługuje.

W swoim wystąpieniu z dnia 14.06.2019 r. Prezes UODO zwrócił się do Ministra Cyfryzacji o rozważenie wprowadzenia stosownych zmian ustawowych celem dostosowania aktualnych regulacji prawnych dotyczących kwalifikowanego podpisu elektronicznego do zasad wyrażonych w RODO[25]. W szczególności Prezes UODO zwrócił uwagę na to, że o ile pobieranie od osoby fizycznej numeru PESEL – w celu zweryfikowania jej tożsamości – w związku ze składaniem wniosku o wydanie certyfikatu kwalifikowanego podpisu elektronicznego, jest uzasadnione i adekwatne do tego procesu, o tyle wątpliwe, z uwagi na zagrożenie bezpieczeństwa danych, wydaje się już być ujawnianie tego numeru podczas posługiwania się tym podpisem. Może to mieć znaczenie szczególnie dla ułatwienia

[25] Zob. wystąpienie Prezesa Urzędu Ochrony Danych Osobowych do Ministra Cyfryzacji z dnia 14.06.2019 r., ZSPU.023.97.2019.PM, pobrane z: https://uodo.gov.pl/pl/search?s=wyst%C4%85pienie%20Prezesa%20Urz%C4%99du%20Ochrony%20Danych%20Osobowych%20do%20Ministra%20Cyfryzacji%20z%20dnia%2014.06.2019%20r.%2C%20ZSPU.023.97.2019.PM&page=2, dostęp: 25.10.2019.

DOI: 10.5604/01.3001.0014.1391

kradzieży tożsamości przez ujawnienie numeru PESEL w wielu miejscach, co może odbywać się poza zupełną kontrolą osoby, której ta dana dotyczy i narażać ją może na przykre konsekwencje. Co istotne, jakkolwiek numer PESEL wciąż jeszcze powszechnie jest stosowany w wielu sytuacjach uwierzytelniania tożsamości osoby fizycznej, to jednak zauważyć należy, że jako dana unikalna i tym samym niepowtarzalna, w świetle m.in. ustawy z dnia 24 września 2010 r. o ewidencji ludności[26], czy ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych[27], nie jest daną, w stosunku do której przyjęto zasadę bezwzględnej jawności i dostępności, co jednak w sferze świadomości społeczeństwa nie wydaje się być tak oczywiste. Pozwala to zatem na uznanie, iż posługiwanie się numerem PESEL odbywać się powinno z dużą dozą rozwagi oraz ostrożności w określonych stosunkach bądź okolicznościach, w celu zapobiegnięcia kradzieży tożsamości, której w wielu przypadkach, dzięki prostym zasadom postępowania można byłoby uniknąć.

Kradzież danych może mieć miejsce także w związku z powiększającymi się bazami szerokich danych osobowych, do których hakerzy dostają się za pomocą coraz nowszych technik włamywania i wykradania ich w związku ze specjalnie opracowanymi metodami. Co istotne, dane osobowe mają swoją określoną wartość rynkową[28] i zarazem stanowią bardzo atrakcyjną zdobycz dla przestępców.

Kradzież tożsamości niesie za sobą także poważne szkody dla obrotu gospodarczego. Wykorzystanie przez środowiska przestępcze baz danych powoduje osłabienie zaufania do handlu elektronicznego, elektronicznych instrumentów płatniczych i innych usług[29].

Na niebezpieczeństwo kradzieży tożsamości narażona jest praktycznie każda osoba, w stosunku do której doszło do zaboru jej danych w postaci imienia, nazwiska oraz numeru PESEL, ze względu na to, że w powszechnym obrocie pożyczkowym, szczególnie w instytucjach pozabankowych,

[26] Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz.U. 2019, poz. 1397 t.j.).

[27] Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. 2020, poz. 332 t.j.).

[28] Wartość pojedynczej danej osobowej, w zależności od stopnia jej szczegółowości, jak również przydatności dla określonych celów, może się wahać pomiędzy kilkoma, a kilkudziesięcioma groszami za rekord (np. w przypadku adresu e-mail, numeru telefonu), poprzez kilka złotych w przypadku danych kontaktowych do osoby zainteresowanej konkretną ofertą, a skończywszy nawet na cenie 100 zł i więcej za jeden rekord, gdy są to dane osoby zainteresowanej uzyskaniem kredytu. Informacje pobrane z https://www.forbes.pl/finanse/ile-sa-warte-nasze-dane-osobowe-handel-i-wycieki/mztm8kx, dostęp: 25.10.2019.

[29] A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3, s. 30.

do zaciągnięcia zobowiązania wystarczy podanie zaledwie kilku danych, zwłaszcza przy zawieraniu transakcji o charakterze online. Zarówno numer dowodu osobistego, jak i adres zamieszkania, przestępca może wskazać jako dane fikcyjne, które nie będą podlegały szczególnej weryfikacji przez instytucje nie będące bankami. Proceder ten jest tym bardziej trudny do szybkiego wykrycia ze względu na to, że osoba, której dane ukradziono i następnie użyto do zaciągnięcia zobowiązania finansowego, najczęściej dowiaduje się o jego istnieniu dopiero na etapie wszczętej przeciwko niej egzekucji, co zazwyczaj następuje w kilka miesięcy po tym, jak jej dane zostały wykorzystane w tym właśnie niecnym celu.

Choć przybieranie cudzej tożsamości nie jest niczym nowym i jest opisywane w literaturze już od starożytności, to jednak obecny rozwój społeczeństwa informacyjnego nadał temu zachowaniu nowy wymiar. Jest to zachowanie niewątpliwie groźne nie tylko dla pokrzywdzonych, ale również dla gospodarki, gdyż oprócz wyrządzenia bezpośrednich szkód majątkowych, osłabia zaufanie do handlu elektronicznego, elektronicznych instrumentów płatniczych i innych usług[30].

Wskutek wejścia w życie RODO, z jeszcze większym rozmachem, nagłaśniane są przez media sprawy wycieków danych, które mogą mieć miejsce zarówno wśród znanych i liczących się na rynku potentatów, jak i urzędów bądź innych instytucji publicznych. Sytuacje te w sposób znaczący wpływają na osłabienie ich wizerunku i podkopują zaufanie do nich, jak również wzmagają roszczeniowe postawy coraz bardziej świadomego swoich praw społeczeństwa[31], które ma obecnie możliwość korzystania z ogólnodostępnej wiedzy w tym zakresie.

Kradzież tożsamości może być także następstwem codziennego nieostrożnego dysponowania swoimi danymi, powierzania ich przypadkowym osobom bądź też może nastąpić wskutek nieprzemyślanego operowania nimi przez osoby uprawnione do dostępu do tych danych, które swoją pracę wykonują na niezabezpieczonych lub prywatnych komputerach. Z kradzieżą tożsamości nieuchronnie może się także wiązać problem

[30] *Ibidem*.

[31] Od momentu wejścia w życie RODO Prezes Urzędu Ochrony Danych Osobowych organizuje liczne spotkania oraz konferencje, mające na celu propagowanie wiedzy w zakresie ochrony danych osobowych pod hasłami takimi jak: „Twoje dane, twoja sprawa", „Ochrona danych osobowych w szkołach i placówkach oświaty", „Dzień ochrony danych osobowych". Zob. „Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2018".

DOI: 10.5604/01.3001.0014.1391

naruszenia dóbr osobistych. A zatem odpowiedzialność sprawcy tego przestępstwa może się sprowadzać zarówno do poniesienia stosowanej kary na gruncie odpowiedzialności wynikającej z kodeksu karnego, jak i odpowiedzialności odszkodowawczej wynikającej z regulacji zawartych w kodeksie cywilnym.

Kwestią naruszenia dóbr osobistych w wyniku kradzieży tożsamości zajął się Sąd Okręgowy we Wrocławiu w orzeczeniu z dnia 30.01.2014 r., w którym stwierdził, że w przypadku pokrzywdzonego powoda „na skutek wydania na jego nazwisko dowodu osobistego i prawa jazdy osobie nieuprawnionej, doszło do naruszenia dóbr osobistych powoda, którego zakres i charakter można określić mianem «kradzieży tożsamości»"[32]. Stan faktyczny niniejszej sprawy sprowadzał się do tego, że przestępca, po podstępnym uzyskaniu od pokrzywdzonego jego danych, w tym kopii dowodu osobistego oraz kopii prawa jazdy, złożył następnie stosowny wniosek do jednego z urzędów o wydanie nowego dowodu osobistego, wskutek rzekomego zagubienia poprzedniego, zaś urzędnik przyjmujący wniosek – mimo oczywistych różnic – nie zwrócił uwagi na to, że zarówno przedstawione przez oszusta zdjęcie, jak i złożony przez niego podpis, zasadniczo różnią się od poprzednio dostarczonych przez prawdziwego właściciela ukradzionych danych. Dalej Sąd ten stwierdził, że „zgodnie z wyraźnym brzmieniem art. 23 k.c., nazwisko człowieka stanowi jego dobro osobiste. Podobnie należy traktować imię, które łącznie z nazwiskiem, określa tożsamość osoby fizycznej. Nazwisko, ujmowane jako potwierdzenie przynależności danej osoby do rodziny, z której się wywodzi dany człowiek, stanowi jednocześnie podstawę identyfikacji danej osoby w społeczeństwie". W sprawie tej, wskutek kradzieży tożsamości, osoba pokrzywdzona – mimo swej oczywistej niewinności – była później postrzegana przez pryzmat osoby nierzetelnej, z uwagi na niekorzystną historię kredytową oraz wszczęte przeciwko niej liczne postępowania egzekucyjne na kwoty rzędu kilkudziesięciu tysięcy złotych. W ten sposób doszło nie tylko do popełnienia na szkodę tej osoby przestępstwa z art. 190a § 2 k.k. oraz 286 § 1 k.k., ale także wyrządzenia jej krzywdy w znaczeniu cywilnoprawnym, rodzącym możliwość żądania zapłaty zadośćuczynienia ze strony nieostrożnego urzędu, co też na gruncie tegoż procesu Sąd uznał za zasadne, zasądzając w ten sposób odpowiednią sumę.

[32] Wyrok Sądu Okręgowego we Wrocławiu Wydział I Cywilny z dnia 30.01.2014 r., I C 411/13, LEX nr 1848555.

W art. 190a § 2 k.k. chroniona jest tożsamość danej osoby i wolność od zagrożeń wynikających szczególnie z dzisiejszych sposobów komunikacji, w których inna osoba może działać na „rachunek" pokrzywdzonego[33].

To działanie na czyiś rachunek może w szczególności polegać na posługiwaniu się danymi identyfikującymi inną osobę bez jej wiedzy oraz zgody. Może także mieć miejsce sytuacja, w której sprawca przestępstwa posłuży się częściowo danymi jednej, a częściowo danymi innej osoby, np. wykorzysta imię i nazwisko jednej osoby, zaś adres zamieszkania drugiej. Generalnie intencją sprawcy przy tego rodzaju działaniu jest co do zasady wprowadzenie w błąd odbiorcy tych informacji celem bezprawnego ich wykorzystania przez sprawcę.

Tytułem przykładu, działaniem mogącym wyrządzić szkodę majątkową, będzie próba polecenia bankowi, z podszyciem się pod posiadacza rachunku i wykorzystaniem danych z jego dowodu osobistego, przekazania określonej kwoty z rachunku na cel charytatywny. Działaniem mającym wyrządzić szkodę osobistą będzie natomiast złożenie w gazecie ogłoszenia o świadczeniu przez daną osobę usług seksualnych[34]. Istotnym jest, że dla zaistnienia bytu przestępstwa z art. 190a § 2 k.k. nie jest konieczna jego powtarzalność czy też uporczywość, jak to może mieć miejsce przy innego rodzaju czynach zabronionych, np. przy nękaniu[35], albowiem wystarczy jednokrotne wypełnienie znamion tego występku, aby podlegać odpowiedzialności karnej, co jest jak najbardziej uzasadnione i pożądane z uwagi na to, że już jednorazowe wykorzystanie cudzych danych w celach przestępczych, może mieć dla ofiary wręcz dramatyczne konsekwencje. Znane są bowiem przypadki zaciągnięcia zobowiązań na jedną osobę – wskutek kradzieży tożsamości – nawet o wartości kilkuset tysięcy złotych[36].

Oprócz ujęcia kradzieży tożsamości w art. 190a § 2 k.k., Kodeks karny przewiduje także inne regulacje, dzięki którym możliwe jest postawienie zarzutów sprawcom tego przestępstwa, mianowicie: art. 267 k.k., na podstawie którego odpowiedzialności karnej podlegają osoby, które bez

[33] A. Zoll, *Art. 190 (a)*, w: *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, Wolters Kluwer Polska, [online] https://sip.lex.pl/#/commentary/587374872/543452, dostęp: 12.01.2020.

[34] *Ibidem*.

[35] Zob. art. 190a § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny.

[36] W stanie faktycznym zawartym w wyroku Sądu Okręgowego we Wrocławiu Wydział I Cywilny z dnia 30.01.2014 r. w sprawie I C 411/13, na szkodę pokrzywdzonego sprawca zaciągnął kilka pożyczek i kredytów, w tym jeden kredyt hipoteczny opiewający na kwotę 499 000 zł.

DOI: 10.5604/01.3001.0014.1391

uprawnienia uzyskały dostęp do informacji dla nich nieprzeznaczonych lub uzyskały dostęp do całości lub części systemu informatycznego; art. 268 k.k., zgodnie z którym odpowiedzialności karnej podlegają osoby, które nie będąc do tego uprawnione, niszczą, uszkadzają, usuwają lub zmieniają zapis informatyczny istotnej informacji albo w istotny sposób udaremniają lub znacznie utrudniają osobie uprawnionej zapoznanie się z nią; art. 269a k.k., w świetle którego odpowiedzialności karnej podlegają osoby, które nie będąc do tego uprawnionymi, poprzez transmisję, zniszczenie, usunięcie, uszkodzenie utrudniają dostęp lub zmianę danych informatycznych, w istotnym stopniu zakłócają pracę systemu komputerowego lub sieci teleinformatycznej; art. 269b k.k., na podstawie którego karze pozbawienia wolności podlega również osoba, która wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełniania innych przestępstw, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, jak również art. 270 k.k. stanowiący o tym, że każdy, kto w celu użycia za autentyczny podrabia, przerabia lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności od trzech miesięcy do lat pięciu.

Jak słusznie zauważył Marek Mozgawa, przestępstwo podszywania się pod inną osobę ma charakter formalny, a zatem bezskutkowy, co oznacza, że zostaje ono dokonane już z chwilą podszycia się, czyli fałszywego podania się za pokrzywdzonego, przy wykorzystaniu jego wizerunku lub danych osobowych. Dla bytu tego przestępstwa nie ma zatem znaczenia, czy szkoda, do wyrządzenia której zmierza sprawca w rzeczywistości, wystąpiła czy też nie[37]. Dzięki takiej interpretacji możliwe jest zatem pociągnięcie do odpowiedzialności karnej sprawcy, który wszedł w nielegalne posiadanie danych, a następnie je wykorzystał, choć mógł nie zaznać z tego tytułu żadnych realnych korzyści dla siebie.

[37] M. Mozgawa, *Komentarz do art. 190a § 2 k.k.*, w: *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el 2019.

4. Ogólne rozporządzenie o ochronie danych osobowych, a przestępstwo kradzieży tożsamości

Niezwykle istotne – z perspektywy autora – są sytuacje jednoznacznie sprzyjające kradzieży tożsamości. Jako jedną z najczęściej występujących i stwarzających sposobność na bezprawne wykorzystanie czyiś danych jest niekontrolowany wyciek danych osobowych, zwany także utratą danych.

Pojęciem tym określa się sytuację, w której dane mogą wprawdzie dalej istnieć, ale administrator utracił nad nimi kontrolę lub do nich dostęp bądź nie jest już w ich posiadaniu[38].

W odniesieniu do ogólnego rozporządzenia o ochronie danych osobowych, do kradzieży tożsamości może najczęściej dojść wskutek utraty kontroli nad danymi, a zatem najczęściej w wyniku zaburzonej ochrony technologii informatycznych wspomagających ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkową utratą[39]. W praktyce oznaczać to może poważne skutki naruszenia danych osobowych, o czym mowa w art. 33 ust. 1 RODO.

W powyższym przepisie został wyrażony cel w postaci ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych[40]. Kradzież tożsamości będzie w tym wypadku jednym w wielu skutków, jaki może wystąpić w wyniku naruszenia ochrony i bezpieczeństwa danych.

Naruszenie danych osobowych zostało zdefiniowane w art. 4 pkt 12 RODO i jest to „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

Do naruszenia bezpieczeństwa danych może dojść najczęściej w sytuacji świadomego, a zatem zawinionego działania osoby przetwarzającej

---

[38] M. Gawroński, Z. Piotrowska, *Zarządzenie incydentami*, w: *Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami*, red. M. Gawroński, Warszawa 2018, s. 396.

[39] Ochrona przed wyciekami danych poprzez zastosowanie odpowiednich technologii informatycznych ma na celu ochronę informacji stanowiących tajemnicę przedsiębiorstwa, jak również ochronę danych osobowych, danych prawnych oraz danych finansowych. Informacja została zaczerpnięta ze strony https://pl.wikipedia.org/wiki/Ochrona_przed_wyciekami_informacji, dostęp 23.10.2019.

[40] W. Chomiczewski, *Administrator i podmiot przetwarzający*, w: E. Bielak-Jomaa, D. Lubasz, *RODO Ogólne Rozporządzenie o Ochronie Danych. Komentarz*, Warszawa 2018, s. 710.

DOI: 10.5604/01.3001.0014.1391

dane, będącej na przykład pracownikiem danej instytucji, jak również wskutek niezamierzonego postępowania bądź też zaniedbania, które finalnie doprowadziło do wycieku danych, którego skutki mogą się ujawnić dopiero w przyszłości. Problemem praktycznym w tego typu sytuacjach jest nie tylko sam fakt zaistnienia naruszenia, ale przede wszystkim możliwe długofalowe skutki dla osób fizycznych, które stały się ofiarami naruszenia ich danych, co często ma miejsce także w sytuacjach całkowicie od nich niezależnych. Dlatego wartym zauważenia i podkreślenia efektem obowiązków, jakie RODO nakłada na podmioty, wskutek działań których doszło do naruszenia bezpieczeństwa danych, jest obligatoryjność zgłoszenia naruszenia nie tylko organowi nadzorczemu, ale i także każdej osobie fizycznej, której dane zostały naruszone, w sytuacji stwierdzenia przez administratora wysokiego ryzyka naruszenia praw i wolności tych osób. Dzięki temu osoba fizyczna ma możliwość podjęcia – także we własnym zakresie – określonych czynności i środków zaradczych, mogących ją uchronić przed bezprawnym wykorzystaniem jej danych, nad którymi administrator utracił kontrolę wskutek zaistniałego wycieku. W przypadku braku powiadomienia osoby fizycznej o fakcie naruszenia bezpieczeństwa jej danych, osoba ta nie ma praktycznej możliwości zareagowania na tego typu sytuację i podjęcia jakichkolwiek działań prewencyjnych, które przynajmniej w częściowym stopniu mogą pomóc jej uchronić się przed zjawiskiem bezprawnego wykorzystania jej danych lub też odpowiednio wczesnego zareagowania, gdy już do takiego wykorzystania jej danych dojdzie. Istotnym bowiem jest, że każda osoba fizyczna, której dane naruszono i która została jednocześnie o tym fakcie poinformowana, będzie szczególnie zainteresowana podjęciem stosownych czynności zapobiegawczych poprzez samodzielne działania, w przeciwieństwie do administratora danych, u którego, mimo iż doszło do wycieku, nie zawsze będzie możliwość sprostania rozmiarowi incydentu, a tym samym zapewnienia skutecznej ochrony przed naruszeniem interesów danych osób, których wyciek danych dotyczy, zwłaszcza w sytuacjach, gdy ma to miejsce na dużą skalę.

A zatem zgodnie zatem z art. 34 ust. 1 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Następnie w art. 34 ust. 3 RODO wskazano sytuacje, w których nie ma potrzeby zgłaszania naruszenia osobie, której dane dotyczą i zostały naruszone. Mianowicie chodzi

o przypadki, w których administrator wdrożył odpowiednie środki techniczne i organizacyjne, w szczególności takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym oraz dostęp do tych danych lub zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą bądź też zawiadomienie osoby fizycznej o naruszeniu jej danych wymagałoby podjęcia przez administratora danych niewspółmiernie dużego wysiłku.

Z utratą danych może się ponadto wiązać problem ich dalszego istnienia, ale już poza kontrolą administratora danych, który nie ma już do nich żadnego dostępu i nie sprawuje nad nimi żadnej pieczy. Stwarza to potencjalnie duże ryzyko trafienia tych danych w niepowołane ręce i następnie wykorzystania ich w bezprawnych celach.

Wraz z naruszeniem bezpieczeństwa danych może dojść jednocześnie do naruszenia ich poufności[41], integralności[42] oraz dostępności[43]. Niebezpieczeństwo wycieku danych prowadzić zatem może do niekontrolowanego wykorzystania informacji o osobie fizycznej przez przestępców w celach związanych najczęściej w wyrządzeniem właścicielowi danych konkretnej szkody majątkowej. Ewidentnym przykładem wycieku danych na masową skalę, była sprawa badana przez Urząd Ochrony Danych Osobowych w związku z serwisem Morele.net Sp. z o.o., który z powodu niewdrożenia wystarczających środków technicznych i organizacyjnych, doprowadził do wycieku danych klientów sklepów internetowych.

W związku ze stwierdzonym naruszeniem, Urząd Ochrony Danych Osobowych wydaną przez siebie decyzją z dnia 10.09.2019 r.[44] nałożył na Morele.net Sp. z o.o. karę pieniężną w wysokości 2 830 410 zł, odpowia-

---

[41] Naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Zob. art. 5 ust. 1 lit. f RODO oraz Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 Grupy Roboczej art. 29 przyjęte w dniu 03.10.2017 r., ostatnio zmienione i przyjęte w dniu 06.02.2018 r.

[42] Naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych. Zob. art. 5 ust. 1 lit. f RODO oraz Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 Grupy Roboczej art. 29 przyjęte w dniu 03.10.2017 r., ostatnio zmienione i przyjęte w dniu 06.02.2018 r.

[43] Naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych.

[44] Zob. decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 10.09.2019 r. w sprawie ZSPR.421.2.2019.

DOI: 10.5604/01.3001.0014.1391

dającą kwocie 660 000 euro. Naruszenie danych osobowych dotyczyło około 2 200 000 klientów i polegało na nieuprawnionym dostępie do bazy danych klientów spółki. Zakres danych, których naruszenie dotyczyło był bardzo szeroki, albowiem w przypadku 35 000 osób, które składały wnioski kredytowe, odnosił się do następujących informacji: imię i nazwisko, adres poczty elektronicznej, numer telefonu, numer PESEL, seria i numer dokumentu tożsamości, data wydania dokumentu tożsamości, data ważności dokumentu tożsamości, wykształcenie, adres zameldowania, adres do korespondencji, źródło dochodu, miesięczny dochód netto, koszty utrzymania gospodarstwa domowego, liczba osób na utrzymaniu, stan cywilny, wysokość miesięcznych innych zobowiązań w instytucjach finansowych, informacja o wysokości zobowiązań alimentacyjnych i innych wynikających z wyroków sądowych. Interesującym jest, że pomimo stwierdzenia masowego naruszenia danych osobowych – na dzień wydania decyzji – nie stwierdzono istnienia dowodów na doznanie przez osoby, których wyciek dotyczył, szkód majątkowych. Jednak Urząd Ochrony Danych Osobowych stwierdził, że skoro doszło do naruszenia zasady poufności, to stanowi to szkodę niemajątkową, a zatem krzywdę, zaś dotknięte nią osoby fizyczne mogą odczuwać strach przez utratą kontroli nad swoimi danymi, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości czy także w ich efekcie – stratą finansową.

Powyższy przypadek obrazuje, jak łatwo w obecnych uwarunkowaniach o naruszenie bezpieczeństwa danych jak również, wskutek tego, zaimplementowanie doskonałego podłoża dla rozwoju działalności przestępczej. Sytuacja ta pokazuje również, że utrata kontroli nad danymi osobowymi może przebiegać całkowicie w oderwaniu od woli, jak i samego postępowania osoby fizycznej, która w celu realizacji niezbędnych dla niej czynności dokonała przekazania swoich danych osobowych, w tym takiego rodzaju informacji, które z łatwością mogą stać się atrakcyjnym łupem dla potencjalnych oszustów.

Z założenia ogólne rozporządzenie o ochronie danych osobowych miało nie tylko uregulować procesy przetwarzania danych osobowych poprzez ich ujednolicenie na obszarze obowiązywania RODO, lecz także miało za zadanie wspomóc administratorów danych we wdrażaniu właściwych środków organizacyjnych i technicznych, aby za ich pomocą, w sposób jak najdalej idący, wyeliminować czynniki oraz błędy narażające tych administratorów na różnego rodzaju wycieki danych skutkujące nie tylko utratą panowania nad nimi, ale także wykorzystania ich w celach dalece

odmiennych od tych, do których pierwotnie zostały zebrane. W ten sposób RODO, gdy jest właściwie wdrożone oraz w powiązaniu z innymi regulacjami odnoszącymi się do bezpieczeństwa danych, przyczynia się do ograniczenia coraz powszechniej dziś występującego zjawiska kradzieży tożsamości.

5. Kradzież tożsamości jako konsekwencja naruszenia ochrony danych osobowych w świetle wybranych regulacji prawnych

Najbardziej odczuwalnym skutkiem naruszenia bezpieczeństwa danych osobowych może być zagrożenie dla konkretnych osób fizycznych w postaci bezprawnego wykorzystania ich danych, a zatem najczęściej w celach przestępczych. Może to spowodować określony uszczerbek majątkowy bądź niemajątkowy, którego konsekwencje mogą się przekładać na utratę kontroli nad zarządzaniem własnymi danymi, ograniczenie praw i wolności, dyskryminację, naruszenie dóbr osobistych, w tym dobrego imienia, naruszenie poufnych informacji na temat osoby fizycznej czy wreszcie kradzież tożsamości, będącą tematem przewodnim niniejszego artykułu.

Kradzież tożsamości, jak sama nazwa wskazuje, występuje w związku z przestępczą działalnością danej jednostki lub nawet zorganizowanej grupy przestępczej trudniącej się tego typu procederem.

Naruszenie ochrony danych osobowych, zgodnie z art. 4 ust. 12 RODO, to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Do kwestii naruszenia ochrony danych osobowych odnoszą się także motywy RODO[45], w tym motyw 85 traktujący o powadze naruszenia i istocie jak najszybszego zawiadomienia o nim organu nadzorczego[46], celem zminimalizowania możliwych do wystąpienia negatywnych skutków tego zdarzenia. Natomiast motyw 87 zwraca szczególną uwagę na to, czy w danej

[45] RODO zawiera 173 motywy.

[46] W Polsce organem nadzorczym jest Urząd Ochrony Danych Osobowych, którego działalnością kieruje Prezes Urzędu Ochrony Danych Osobowych. W okresie wejścia w życie RODO, tj. od 25.05.2018 r., funkcję tę pełniła Edyta Bielak-Jooma, zaś od 16.05.2019 r., nowym Prezesem został Jan Nowak.

DOI: 10.5604/01.3001.0014.1391

organizacji wdrożono wszelkie odpowiednie środki techniczne oraz organizacyjne, aby było możliwe niezwłoczne wykrycie i stwierdzenie naruszenia ochrony danych osobowych, co także ma pomóc ograniczyć negatywne następstwa zaistniałego naruszenia.

Na gruncie prawa ochrony danych osobowych można twierdzić o kilku rodzajach naruszenia bezpieczeństwa danych, które skutkować mogą kradzieżą tożsamości. Biorąc pod uwagę opinię 03/2014 Grupy Roboczej Art. 29[47], rozróżnia się trzy typy naruszenia ochrony danych osobowych, mianowicie: naruszenie poufności, dostępności oraz integralności. Analogiczne rodzaje naruszeń danych osobowych zostały zawarte w wytycznych Grupy Roboczej Art. 29, dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679[48]. W wytycznych tych odniesiono się także do sytuacji naruszenia o charakterze transgranicznym[49] oraz naruszenia w jednostkach organizacyjnych spoza obszaru Unii Europejskiej.

W przypadku, w którym dochodzi do transgranicznego przetwarzania danych osobowych, naruszenie może wywierać wpływ na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim[50].

Wartym zauważenia jest także fakt, iż nie tylko RODO wprowadziło zasady nawiązujące do trybu postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych. Już bowiem na gruncie wcześniej obowiązujących regulacji prawnych, a zatem jeszcze przed wejściem w życie ogólnego rozporządzenia, zawracano w niektórych sytuacjach uwagę na konsekwencje związane z naruszeniem ochrony danych osobowych i to nie tylko w ujęciu tego zjawiska jako wyłącznego problemu osoby fizycznej, lecz także z punktu widzenia podmiotu, od którego dane naruszenie się rozpoczęło. I tak, np. na operatorów usług telekomunikacyjnych[51] na-

[47] Zob. Opinia 03/2014 Grupy Roboczej Art. 29 na temat powiadamiania o przypadkach naruszenia danych osobowych przyjęta w dniu 25.03.2014 r.

[48] Zob. Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 Grupy Roboczej art. 29 przyjęte w dniu 03.10.2017 r., ostatnio zmienione i przyjęte w dniu 06.02.2018 r.

[49] Naruszenie związane ze świadczeniem usług do innego państwa lub z innego państwa.

[50] Zob. Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 Grupy Roboczej art. 29, przyjęte w dniu 03.10.2017 r., ostatnio zmienione i przyjęte w dniu 06.02.2018 r.

[51] Zob. dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywę o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, art. 4

łożono obowiązek zawiadamiania poszkodowanych naruszeniem ochrony danych o jego wystąpieniu, w celu umożliwienia tym osobom podjęcia właściwej reakcji, w tym sprowadzającej się do zapobiegnięcia możliwym do wystąpienia szkodom, w tym także polegającym na bezprawnym wykorzystaniu tożsamości.

W aktualnym stanie prawnym firmy telekomunikacyjne stanowią tę kategorię podmiotów, które – w razie wystąpienia naruszenia ochrony danych osobowych – mają obowiązek zgłosić ten fakt Prezesowi UODO, a w niektórych sytuacjach także i osobie fizycznej, której naruszenie dotyczy. Takie obwarowania wynikają nie tylko z regulacji zawartych w ogólnym rozporządzeniu o ochronie danych osobowych, ale także wywodzą się z Rozporządzenia Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej, zwanego dalej też „rozporządzeniem Komisji (UE) Nr 611/2013", czy też ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[52]. Co interesujące, w przypadku tej kategorii przedsiębiorców, w przeciwieństwie do regulacji zawartej w art. 33 ust. 1 RODO, mają oni obowiązek zgłoszenia do organu nadzorczego naruszenia w terminie do 24, a nie – jak wynika z RODO – do 72 godzin od wykrycia incydentu. Podstawą prawną takiego wymogu jest art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013. Dodatkowo firma telekomunikacyjna, w razie wykrycia naruszenia ochrony danych, jak również w sytuacji ziszczenia się określonych przesłanek, ma ponadto obowiązek zawiadomić osobę, której dane dotyczą o zidentyfikowanym naruszeniu. Wynika to z art. 174a ust. 3 ustawy prawo telekomunikacyjne, zgodnie z którym, w przypadku gdy naruszenie danych osobowych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, dostawca publicznie dostępnych usług telekomunikacyjnych, oprócz powiado-

ust. 3 w brzmieniu zmienionym dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., zmieniającą dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337 z 18.12.2009.

[52] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2019, poz. 2460 t.j.).

DOI: 10.5604/01.3001.0014.1391

mienia Prezesa UODO, niezwłocznie zawiadamia o takim naruszeniu również abonenta lub użytkownika końcowego na zasadach określonych w art. 3 rozporządzenia Komisji (UE) nr 611/2013. Z kolei na podstawie art. 174a ust. 5 ustawy z dnia 16 lipca 2004 r. (Dz.U. 2019, poz. 2460 t.j.), zawiadomienie abonenta lub użytkownika końcowego będącego osobą fizyczną o naruszeniu nie jest wymagane, jeżeli dostawca publicznie dostępnych usług telekomunikacyjnych wdrożył odpowiednie techniczne i organizacyjne środki ochrony, które uniemożliwiają odczytanie danych przez osoby nieuprawnione oraz zastosował je do danych, których ochrona została naruszona. W tym wypadku ryzyko kradzieży tożsamości – mimo zaistniałego naruszenia – ograniczone jest do minimum i nie wymaga podejmowania specjalnych działań oraz środków zaradczych.

Do kwestii naruszenia ochrony danych osobowych warto się także odnieść w kontekście ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[53]. Z art. 44 tej ustawy wynika analogiczne zobowiązanie, jakie zostało nałożone przez art. 33 ust. 1 RODO na administratorów danych. Termin na zawiadomienie organu nadzorczego jest taki sam w przypadku obu regulacji i wynosi do 72 godzin od wykrycia naruszenia. Jednakże nieznaczna różnica występuje w związku z przekazywaniem administratorowi informacji na temat wykrytego naruszenia przez podmioty przetwarzające i odnosi się ona do tego, że w świetle powyższej ustawy pomioty te są zobligowane do zachowania 48-godzinnego terminu, zaś RODO kwestii tej nie reguluje. Jeśli zaś chodzi o zawiadamianie osób, których naruszenie dotyczy, to zarówno w przypadku RODO, jak i ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przesłanki jego wypełnienia pozostają analogiczne. Warto jednak wspomnieć o jednym wyjątku zawartym w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, mianowicie sprowadzającym się do tego, że opóźnienie, bądź nawet odstąpienie od powiadomienia osoby, której naruszenie dotyczy, może zostać zastosowane w sytuacjach, które mogłyby: wywołać ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych; utrudnić lub nawet uniemożliwić rozpoznawanie, zapobieganie, wykrywanie lub zwalczanie czynów zabronionych; utrudnić prowadzenie postępowa-

[53] Ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019, poz. 125).

nia karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia bądź wykroczenia skarbowe, a ponadto mogłyby spowodować zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego, jak również zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa, a także mogłoby istotnie naruszyć dobra osobiste innych osób.

Termin na maksymalnie 24-godzinne zawiadomienie organu nadzorczego o wykrytym naruszeniu wynika, podobnie jak w przypadku podmiotów telekomunikacyjnych, z Rozporządzenia eIDAS, czyli Rozporządzenia (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym i dotyczy dostawców usług zarejestrowanych – w przypadku kwalifikowanych usług zaufania – na stronie https://www.nccert.pl/uslugi.htm, zaś w przypadku niekwalifikowanych usług zaufania – na stronie https://www.nccert.pl/uslugiNK.htm.

Na koniec warto jeszcze odnieść się do regulacji zawartych w ustawie z dnia 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[54]. Zgodnie z nią, wszelkie incydenty danych są weryfikowane przez tzw. Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego, zwane także jako CSIRT-y, co jednak nie zwalnia administratorów danych z zawiadomienia organu nadzorczego o stwierdzonym naruszeniu ochrony danych osobowych na podstawie art. 33 ust. 1 RODO.

Wszystkie wskazane przykłady regulacji prawnych w zakresie sposobu oraz trybu zgłaszania naruszenia ochrony danych osobowych mają w możliwie jak najwyższym stopniu zapobiec narażeniu na niekontrolowaną utratę danych, której jednym ze skutków może być kradzież tożsamości konkretnej osoby lub grupy osób fizycznych.

W sytuacji, gdy naruszenie ochrony danych osobowych przybierze formę phishingu bądź działania złośliwego oprogramowania, można się spodziewać, że ten rodzaj naruszenia został ukierunkowany na cele związane z nielegalnym pozyskaniem określonych informacji oraz danych, co z łatwością może doprowadzić do kradzieży tożsamości. Atak phishingowy bardzo często stanowi następstwo nieuprawnionego ujawnienia danych osób, w efekcie czego bezprawne wykorzystanie tożsamości może być jedynie kwestią czasu.

---

[54] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezieczeństwa (Dz.U. 2018, poz. 1560, Dz.U. 2019, poz. 2020, 2248).

DOI: 10.5604/01.3001.0014.1391

W jednym z komunikatów, Prezes UODO ostrzegał przed możliwym atakiem phishingowym[55], wskutek przesyłania do osób maili z informacją o nieuprawnionym ujawnieniu danych osobowych z adresów tych osób. Następnie kliknięcie w odpowiedni link dzieliło już tylko właściciela e-mail o krok od ataku hackerskiego. Informacja była przesyłana do potencjalnych odbiorów z adresu łudząco przypominającego adres nieistniejącego już Biura Generalnego Inspektora Ochrony Danych Osobowych[56].

Jak zatem wynika z zaprezentowanych przykładów, sposobów naruszenia ochrony danych osobowych może być wiele, zaś zawsze ich najważniejszym celem będzie dążenie przez sprawców umyślnych naruszeń do pozyskania interesujących ich danych, co służyć ma zamiarom niezgodnym z obowiązującym porządkiem prawnym.

6. Cyberprzestępczość jako zjawisko poprzedzające kradzież tożsamości

Cyberprzestępczość może mieć miejsce w cyberprzestrzeni i jest logicznym następstwem intensywnego rozwoju tego obszaru, jak również może mieć bezpośredni związek z wykradaniem tożsamości w bezprawnych celach.

Pojęcie „cyberprzestrzeń" pojawiło się po raz pierwszy już w połowie lat 80. w opowiadaniu *Burning Chrome* Williama Gibsona, a następnie zostało spopularyzowane przez jego debiutancką powieść *Neuromancer*. Amerykański pisarz, uważany za prekursora cyberpunku, użył tego pojęcia do scharakteryzowania wirtualnej rzeczywistości, w której toczyły się losy jego bohaterów[57].

Aktualnie zarówno Internet, jak i związana z nim cyberprzestrzeń stanowią doskonałą bazę do anonimowego podejmowania przez użytkow-

[55] Phishing jest metodą oszustwa internetowego, które polega na wyłudzeniu od użytkownika jego poufnych danych. W wyniku takiego działania oszuści internetowi uzyskują numery kart debetowych i kredytowych, dostępy do elektronicznego konta bankowego czy też inne informacje, które pozwalają na kradzież ich pieniędzy. Obecnie proceder phishingu w bankowości występuje najczęściej pod postacią spamu rozsyłanego na adresy e-mail. Informacja pobrana ze strony https://serwisy.gazetaprawna.pl/finanse-osobiste/artykuly/1404462,co-to-jest-phishing.html, dostęp: 21.01.2019.

[56] Informacja zaczerpnięta ze strony https://www.uodo.gov.pl/pl/138/1218, dostęp 21.10.2019 r.

[57] M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4, [online] http://www.ebib.pl/2010/113/a.php?nowak, dostęp: 25.10.2019.

ników sieci określonych, nie zawsze stojących w zgodności z prawem, działań. Część z nich może zmierzać do nawiązywania kontaktów i prób uzyskania cennych – ze swojego punktu widzenia – informacji od innych użytkowników. Ponadto, z uwagi na intensywny rozwój generacji młodych eksploatatorów Internetu, można zaobserwować zjawisko wykształcenia się określonych podkultur, a zatem takich jak: gracze komputerowi, machinimiści, scenowcy i fanfikowcy, cyberpunki i cybergoci, hejterzy i wreszcie grupa będąca zainteresowaniem niniejszego artykułu, mianowicie hakerzy i piraci. Hakerzy, jak powszechnie wiadomo, stanowią groźną grupę użytkowników sieci, nastawioną na działalność niezgodną z prawem, co przejawia się w czynnościach związanych z wykradaniem haseł, atakowaniem kont innych użytkowników, łamaniem zabezpieczeń oprogramowań i wykradaniem bardzo cennych danych i informacji, a następnie szantażowaniem ich administratorów żądaniem zapłaty określonych kwot najczęściej pod rygorem ujawnienia wycieku danych. Ponadto hakerzy poprzez wprowadzenie określonego typu wirusa mogą dostać się do komputera i zainstalować w nim takie rejestratory, które przechwytują dane, nazwy kont dostępowych jak również cenne hasła. Dzięki temu z łatwością mają możliwość dostania się do kont internetowych swoich ofiar, w tym do ich rachunków bankowych.

Z kolei członkowie subkultury piratów naruszają prawa autorskie twórców gier komputerowych, filmów, muzyki lub oprogramowania, korzystając z ich kopii lub reprodukcji na komputerze osobistym bądź rozpowszechniając je wśród innych użytkowników[58].

Narastająca przestępczość w sieci stała się podłożem do wprowadzenia wielu regulacji prawnych odnoszących się do walki z tym procederem. I tak 23 listopada 2001 r. w Budapeszcie została sporządzona Konwencja Rady Europy o cyberprzestępczości[59], która zdefiniowała różne rodzaje bezprawności w sieci, a zatem: nielegalny dostęp (art. 2) związany głównie z zamiarem pozyskania danych informatycznych w wyniku naruszenia zabezpieczeń; nielegalne przechwytywanie danych (art. 3), które polega na bezprawnym uzyskiwaniu danych za pomocą określonych urządzeń technicznych; naruszenie integralności danych (art. 4), w związku z umyślnym niszczeniem, kasowaniem, uszkadzaniem, dokonywaniem zmian lub

[58] B. Kałdon, *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku*, „Seminare" 2016, tom 37, nr 2, s. 94.

[59] Zob. Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001, art. 2–6.

DOI: 10.5604/01.3001.0014.1391

usuwaniem danych informatycznych; naruszenie integralności systemu (art. 5), polegające na umyślnym bezprawnym i poważnym zakłócaniu funkcjonowania systemu informatycznego; niewłaściwe użycie urządzeń (art. 6), skutkujące popełnieniem przestępstwa; fałszerstwo komputerowe (art. 7), polegające na umyślnym, bezprawnym wprowadzeniu zmian, kasowaniu lub ukrywaniu danych informatycznych, w następstwie czego powstają dane nieautentyczne, które mogą być następnie wykorzystane przez sprawę jako dane autentyczne do różnych celów; oszustwo komputerowe (art. 8), którego najważniejszą istotą jest ingerencja w funkcjonowanie systemu informatycznego z zamiarem oszustwa lub uzyskania korzyści ekonomicznych dla siebie lub dla innej osoby. We wspomnianej Konwencji wyróżnia się także przestępstwa internetowe związane z pornografią dziecięcą jak również naruszające prawa autorskie i prawa pokrewne.

W Polsce obowiązująca ustawa z dnia 05.07.2018 r. o cyberbezpieczeństwie, która weszła w życie w dniu 28.08.2018 r., określa zadania takie jak: organizacja krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Ustawa ta jest efektem wdrożeniem do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (tzw. Dyrektywa NIS). Zobowiązuje ona państwa członkowskie do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa poprzez ustanowienie organów właściwych oraz pojedynczych punktów kontaktowych do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie krajowych strategii w zakresie cyberbezpieczeństwa[60].

Trzeba pamiętać, że jakkolwiek cyberprzestępczość wywodzi się z niezwykle ważnej dziedziny, jaką jest znaczny rozwój technologii informatycznej w cyberprzestrzeni, to jednak mimo tych istniejących zagrożeń, współczesny człowiek nie powinien zamykać się na te rozwiązania wyłącznie z obawy o swoje dane bądź też informacje, które do tej przestrzeni

[60] Informacja pobrana ze strony https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/, dostęp: 25.10.2019.

trafiają lub trafiły i mogą zostać wykorzystane w niewłaściwych celach. Osiągnięcia związane z postępującym rozwojem mają bowiem służyć człowiekowi, a stają się problemem jedynie wówczas, gdy są nadużywane, nieodpowiednio wykorzystywane oraz w sytuacji braku dostatecznej wiedzy na temat ochrony własnej przed bezprawną działalnością wykorzystujących brak wiedzy hackerów.

Podsumowanie

Przestępstwo kradzieży tożsamości, stało się obecnie ogólnoświatowym źródłem zagrożenia dla danych osobowych, mogących stanowić atrakcyjną formę wykorzystania zdobytych w nielegalny sposób informacji, w celu podjęcia przez sprawcę pozaprawnych działań. Przestępstwo to jest ponadto negatywną konsekwencją wzrostu znaczenia nowoczesnych technologii. Posłużenie się cudzą tożsamością daje w zasadzie nieograniczone możliwości jej wykorzystania w niecnych celach. Dane pozyskane nieuczciwie przez przestępców pochodzić mogą zarówno ze skradzionych dokumentów tożsamości, jak również mogą być nabywane w wyniku włamania do komputera bądź wyłudzenia danych i informacji na temat osoby fizycznej w inny sposób, często uniemożliwiający podjęcie w porę skutecznej reakcji obronnej przez ofiarę takiego czynu. Jednakże dzięki zarówno krajowym, jak i europejskim regulacjom prawnym, system stworzony do walki z cyberprzestępczością działa coraz lepiej i skuteczniej, wskutek zwłaszcza wciąż doskonalonych i modernizowanych metod przeciwdziałania i ochrony przeciwko tym nadużyciom. Jest to niezwykle pożądana dziedzina ukierunkowana na zwalczanie tych bezprawnych praktyk, biorąc pod uwagę fakt, iż skala kradzieży tożsamości niepokojąco wzrosła przy jednoczesnym dynamicznym rozwoju coraz bardziej wyrafinowanych metod jej dokonywania. W Polsce walkę z cyberprzestępczością realizuje Biuro do Walki z Cyberprzestępczością, które zostało utworzone w ramach struktury Komendy Głównej Policji w dniu 01.12.2016 r. Rola tej jednostki jest nieoceniona i zasługuje na szczególną aprobatę w dobie rosnącej cyberprzestępczości.

Statystyki odnoszące się do skali kradzieży tożsamości oraz wynikające z tego faktu poważne konsekwencje dla ofiar tego czynu są coraz bardziej alarmujące. Na przykład zgodnie ze informacjami udostępnionymi przez Biuro Informacji Kredytowej zjawisko kradzieży tożsamości w celu

DOI: 10.5604/01.3001.0014.1391

zaciągnięcia zobowiązania odznacza się niestety tendencją stale rosnącą. I tak w 2011 r. doszło do 7 185 prób wyłudzeń, a w 2014 r. już do 8 814[61].

Z perspektywy każdej pojedynczej osoby fizycznej można przyjąć, że najbardziej właściwą metodą, w celu zminimalizowania ryzyka związanego z kradzieżą tożsamości jest ochrona swoich danych we własnym zakresie, co jednak musi zostać poprzedzone odpowiednią formą edukacji i podniesieniem w tym zakresie świadomości społeczeństwa. Niestety, pomimo znaczącego przełomu w zakresie ochrony danych osobowych, do którego doszło wskutek implementowania RODO, społeczeństwo polskie wciąż jeszcze dysponuje zbyt niską świadomością znaczenia i rangi własnych danych osobowych. Pomimo tych przeszkód, obserwuje się w coraz większym stopniu sukcesywne przywiązywanie wzmożonej uwagi do dbałości o własne dane i ochronę swojej prywatności. Z drugiej strony, różnego rodzaju nadmierna bądź zwłaszcza nieprzemyślana aktywność w serwisach społecznościowych, dodatkowo wzmagają narażenie na atak ze strony cyberprzestępców, jak również ułatwia im to pozyskanie interesujących dla nich danych osób fizycznych.

Jedną z bardziej oczekiwanych regulacji prawnych, w celu zwiększonej eliminacji kradzieży danych, było ponadto wejście w życie w dniu 12.07.2019 r. ustawy z dnia 22.11.2018 r. o dokumentach publicznych (Dz.U. 2019, poz. 53), dzięki której zwrócono szczególną uwagę na problem związany z niekontrolowanym kopiowaniem dowodów osobistych, w których znajduje się szereg informacji uwierzytelniających tożsamość osoby fizycznej. Niepokojącym bowiem jest, iż mimo wzrostu świadomości społeczeństwa odnośnie potrzeby chronienia swoich danych, wciąż jeszcze obserwuje się dość powszechną praktykę polegającą na tzw. zastawianiu dokumentów tożsamości w zamian za wypożyczony sprzęt sportowy, jako zabezpieczenie ewentualnych roszczeń wynajmującego, jak również w związku z zatrudnieniem dochodzi do rutynowego kopiowania dowodów osobistych przez pracodawców bez wskazania pracownikom konkretnego celu i podstawy prawnej takiego utartego powszechnie zwyczaju. Sytuacje te mogą niestety rodzić pokusę do bezprawnego wejścia w posiadanie i następnie wykorzystania tych danych w przestępczych celach. Stąd też brak świadomości społeczeństwa stanowi najprawdopodobniej jeden z najpoważniejszych problemów związanych z poruszaną niniejszym artykułem tematyką, odnoszącą się do kradzieży tożsamości i jej negatywnych następstw, czemu w wielu

[61] Informacja pobrana ze strony https://www.bik.pl/poradnik-bik/jakie-moga-byc-konsekwencje-kradziezy-tozsamosci, dostęp: 25.10.2019.

przypadkach można było zapobiec. Warto zatem postulować zarówno cele, jak i efekty prowadzonych kampanii edukacyjnych, tak aby każda osoba fizyczna dysponowała choćby minimalną wiedzą odnoszącą się do codziennych zasad chroniących przed utratą swojej tożsamości bądź narażeniem jej na atak zarówno w cyberprzestrzeni, jak i w toku zwykłych codziennych procesów przetwarzania danych osobowych, których w dobie aktualnych czasów nie da się uniknąć.

Bibliografia

Literatura

Chomiczewski W., *Administrator i podmiot przetwarzający*, w: E. Bielak-Jomaa, D. Lubasz, *RODO Ogólne Rozporządzenie o Ochronie Danych. Komentarz*, Warszawa 2018.

Gawroński M., Piotrowska Z., *Zarządzenie incydentami*, w: *Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami*, red. M. Gawroński, Warszawa 2018.

Grabowska J., Kaczmarczyk A., *Kradzież tożsamości z art. 190a § 2 k.k. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016, nr 4.

Jaroszewska I.A., *KPP Monografie. Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.

Jedlińska K., *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1 (126), t. 2.

Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3.

Kałdon B., *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku*, „Seminare" 2016, tom 37, nr 2.

Kania A., *Oszustwo komputerowe na tle przestępczości w cyberprzestrzeni*, „CBKE e-Biuletyn" 2009, nr 1.

Kwapis K., Brygoła E., *Tożsamość osobista w ujęciu emotywno-refleksyjnym: zawartość, funkcje i procesy kształtowania tożsamości*, „Opuscula Sociologica" 2013, nr 4.

Mozgawa M., *Komentarz do art. 190a § 2 k.k.*, w: *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el 2019.

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4, [online] http://www.ebib.pl/2010/113/a.php?nowak, dostęp: 25.10.2019.

DOI: 10.5604/01.3001.0014.1391

Sowirka K., *Przestępstwo kradzieży tożsamości w polskim prawie karnym*, „Ius Novum" 2013, nr 1.

Waszczyńska K., *Wokół problematyki tożsamości*, „Rocznik Towarzystwa Naukowego Płockiego" 2014, nr 6.

Witek K., *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2/24.

Wójcicka M., *Tożsamość w procesie komunikacji*, „Artes Humane" 2016, nr 1.

Zoll A., *Art. 190 (a)*, w: *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, Wolters Kluwer Polska, [online] https://sip.lex.pl/#/commentary/587374872/543452, dostęp: 12.01.2020.

Akty prawne

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002.

Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337 z 18.12.2009.

Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001.

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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016).

Ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019, poz. 125).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2019, poz. 2460 t.j.).

Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz.U. 2019, poz. 1397 t.j.).

Ustawa z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny (Dz.U. 2016, poz. 1137).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560, Dz.U. 2019, poz. 2020, 2248).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2019, poz. 1950 t.j.).

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. 2020, poz. 332 t.j.).

Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 Grupy Roboczej art. 29 przyjęte w dniu 03.10.2017 r., ostatnio zmienione i przyjęte w dniu 06.02.2018 r.

Orzecznictwo

„Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2018".

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 10.09.2019 r. w sprawie ZSPR.421.2.2019.

Opinia 03/2014 Grupy Roboczej Art. 29 na temat powiadamiania o przypadkach naruszenia danych osobowych przyjęta w dniu 25.03.2014 r.

Wyrok Sądu Okręgowego Warszawa–Praga w Warszawie, V Wydział Karny z dnia 21.07.2017 r., sygn. akt V K 217/15, LEX nr 2675229.

Wyrok Sądu Okręgowego we Wrocławiu Wydział I Cywilny z dnia 30.01.2014 r., I C 411/13, LEX nr 1848555.

Wyrok Sądu Rejonowego w Nidzicy z dnia 14 marca 2017 r., II K 315/16, LEX nr 2322333.

Wyrok Sądu Rejonowego w Piotrkowie Trybunalskim z dnia 20 czerwca 2017 r., VII K 770/16, LEX nr 2342713.

Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 Grupy Roboczej art. 29 przyjęte w dniu 03.10.2017 r., ostatnio zmienione i przyjęte w dniu 06.02.2018 r.

Źródła internetowe

https://www.bik.pl/poradnik-bik/jakie-moga-byc-konsekwencje-kradziezy-tozsamosci, dostęp: 25.10.2019.

DOI: 10.5604/01.3001.0014.1391

https://www.forbes.pl/finanse/ile-sa-warte-nasze-dane-osobowe-handel-i-wycieki/mztm8kx, dostęp: 25.10.2019.

https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pl.pdf, dostęp: 22.10.2019.

https://pl.wikipedia.org/wiki/Informatyzacja, dostęp: 22.10.2019.

https://pl.wikipedia.org/wiki/Ochrona_przed_wyciekami_informacji, dostęp: 23.10.2019.

https://pl.wikipedia.org/wiki/Spo%C5%82ecze%C5%84stwo_informacyjne, dostęp: 22.10.2019.

https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/, dostęp: 25.10.2019.

https://serwisy.gazetaprawna.pl/finanse-osobiste/artykuly/1404462,co-to-jest-phishing.html, dostęp: 21.01.2019.

https://www.uodo.gov.pl/pl/138/1218, dostęp: 21.10.2019.

Informacje zamieszczone przez Generalnego Inspektora Ochrony Danych Osobowych w poradniku „Ochrona danych osobowych w czasie wakacji", pobrane z: https://uodo.gov.pl/pl/71/119, dostęp: 06.03.2020.

Wystąpienie Prezesa Urzędu Ochrony Danych Osobowych do Ministra Cyfryzacji z dnia 14.06.2019 r., ZSPU.023.97.2019.PM, pobrane z: https://uodo.gov.pl/pl/search?s=wyst%C4%85pienie%20Prezesa%20Urz%C4%99du%20Ochrony%20Danych%20Osobowych%20do%20Ministra%20Cyfryzacji%20z%20dnia%2014.06.2019%20r.%2C%20ZSPU.023.97.2019.PM&page=2, dostęp: 25.10.2019.