dr Jacek Copik
adiunkt, Wydział Nauk Ścisłych, Przyrodniczych i Technicznych
Uniwersytet Jana Długosza w Częstochowie
ORCID: 0000-0002-2490-048X
mgr inż. Martyna Drab
absolwentka, Wydział Nauk Ścisłych Przyrodniczych i Technicznych
Uniwersytet Jana Długosza w Częstochowie
ORCID: 0000-0003-0323-1456

BEZPRAWNE UZYSKANIE INFORMACJI JAKO REALNE ZAGROŻENIE DLA SPOŁECZEŃSTWA

Streszczenie
Informacja jest niezwykle istotnym i nieodłącznym elementem życia człowieka. Fakt ten najlepiej odzwierciedlają dane osobowe, stanowiące pewnego rodzaju identyfikator, bez którego trudno byłoby funkcjonować w społeczeństwie. Informacja to cenne dobro, jednak nie zawsze wykorzystuje się je we właściwy sposób. Bardzo często zdarzają się sytuacje, w których informacje pozyskiwane są niezgodnie z prawem, przez niepowołane osoby. W artykule zostały omówione cztery główne sposoby bezprawnego uzyskania informacji, do których należą: naruszenie tajemnicy korespondencji, podsłuchy, dostęp przez sieć bezprzewodową oraz hacking. Wspomniano także o równie istotnym zagrożeniu, jakim jest phishing. Ze względu na to, że każdy człowiek narażony jest na bezprawne uzyskanie informacji, bardzo ważne jest, aby wiedzieć, jak się przed nim chronić. Odpowiednia profilaktyka to podstawa bezpieczeństwa.

Słowa kluczowe: informacja, dane osobowe, podsłuch, *hacking*, *phishing*, bezpieczeństwo informacji

Wstęp

Trudno wyobrazić sobie świat bez tak istotnego komponentu, jakim jest informacja. Każdego dnia do człowieka dociera niezliczona ilość wiadomości. Szczególnie znaczącym rodzajem informacji są dane osobowe. Po wejściu w życie przepisów RODO[1], czyli unijnego rozporządzenia

[1] RODO – rozporządzenie ogólne o ochronie danych osobowych – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób

o ochronie danych, ochrona prawna naszych danych osobowych znacznie się poszerzyła. To wyjątkowo ważne, przede wszystkim ze względu na nieustanny postęp technologiczny. Prawie na każdym kroku można spotkać się z elektroniczną postacią danych i informacji. Wszelkie instytucje i podmioty przechowują je w różnego rodzaju systemach informatycznych. Niestety, wraz z pozytywną stroną cyfryzacji pojawia się także ta negatywna. Z uwagi na to, że informacje są bardzo cenne, dość często słyszy się o incydentach związanych z naruszeniem ich bezpieczeństwa, polegającym m.in. na bezprawnym pozyskaniu, zniszczeniu czy sfałszowaniu. Naruszenie tajemnicy korespondencji, podsłuchy, hacking – określany często jako nieuprawniona ingerencja w systemy i sieci komputerowe – to typowe przestępstwa przeciwko ochronie informacji. Nie można także zapomnieć o phishingu – tego rodzaju oszustwa uznawane są obecnie za prawdziwą plagę. Wynika to głównie ze specyfiki tej metody, czyli pozyskiwania informacji przez podszywanie się pod zaufane osoby czy instytucje.

Bezprawne uzyskanie informacji stanowi poważny problem, którego nie można całkowicie wyeliminować. Wobec tego w celu zminimalizowania ryzyka naruszenia ich bezpieczeństwa należy podejmować odpowiednie działania profilaktyczne i monitorujące. Słynne powiedzenie Hipokratesa „Lepiej zapobiegać, niż leczyć" odnosi się już nie tylko do zdrowia, lecz także można je wpisać w dziedzinę informacji. Uświadamia to, że profilaktyka odgrywa znaczącą rolę w ochronie tego, co ważne. Przede wszystkim bezpieczeństwo powinno być rozpatrywane wielopłaszczyznowo, gdyż na jego stan ma wpływ wiele składowych. Ponadto trzeba o nie zabiegać regularnie, a nie tylko wtedy, gdy sytuacja stanie się poważna. Dla przeciwdziałania zjawisku bezprawnego uzyskania informacji szczególnie istotna jest świadomość ludzi, że takie zagrożenie istnieje. Należy więc nieustannie rozpowszechniać i pogłębiać wiedzę na ten temat. Trzeba jednocześnie pamiętać, że to człowiek stanowi najsłabsze ogniwo procesu, na który składają się wszelkie działania wpływające na zachowanie bezpieczeństwa informacji.

Istota informacji

Właściwe przedstawienie problemu, jakim jest bezprawne uzyskanie informacji, wymaga wyjaśnienia pewnych podstawowych pojęć. Jednym z nich jest właśnie *informacja*, a termin ten doczekał się wielu różnych definicji. Informacja to przede wszystkim dane odpowiednio ukształtowane

fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119, ze zm.).

w istotną, użyteczną postać[2]. Na dane składają się różne elementy – znaki, liczby czy słowa. Jednak nie wszystkie dane będą stanowiły informacje; aby tak było, muszą one nieść pewną treść[3]. Już blisko 20 lat temu uznawano, że informacja stanowi jeden z istotnych składników rzeczywistości, na który pojawia się coraz większe zapotrzebowanie[4]. Jest to także czynnik mający wpływ na podejmowanie decyzji w każdej dziedzinie życia, zwiększający wiedzę lub zmniejszający niewiedzę decydenta oraz wnoszący pewną cząstkę nowości[5]. Czasem bardzo łatwo o przenikanie informacji przez różne bariery, w wyniku czego trafia ona do niepowołanych osób. Nie da się zaprzeczyć, że informacja odgrywa ogromną rolę w życiu człowieka. Potwierdza to fakt, że jedną ze swobód zapewnianych każdemu przez Konstytucję RP jest właśnie pozyskiwanie i rozpowszechnianie informacji[6]. Potrzeby informacyjne wynikają z różnych powodów. Zaliczyć można do nich m.in.: potrzeby bytowe, samorozwój, ciekawość, wrodzoną potrzebę budowania wiedzy o świecie, dorównanie innym, chęć dominacji czy związek z działalnością zawodową[7]. Coraz większe zapotrzebowanie na informację powoduje także zwiększanie liczby źródeł, z których ona pochodzi. Niestety, natłok informacji powoduje trudności w dokonywaniu prawidłowej selekcji, dotyczącej przede wszystkim ich wiarygodności i użyteczności dla danego odbiorcy. Informacja, która nie jest zgodna z rzeczywistością, a zawiera prawdziwe elementy i w sposób świadomy wprowadza odbiorcę w błąd, nazywana jest *fake newsem*[8].

Kwestię informacji dotyczących danych osobowych reguluje obecnie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., czyli w skrócie RODO, ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[9] oraz ustawa z dnia 14 grudnia 2018 r.

---

2 M. Grabowski, A. Zając, *Dane, informacja, wiedza*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 798, s. 8.

3 B. Stefanowicz, *Koncepcja pojęcia informacji*, „Wiadomości Statystyczne" 2010, t. 55, nr 7, s. 21.

4 Idem, *Informacja*, Szkoła Główna Handlowa w Warszawie, Warszawa 2004, s. 11.

5 M. Grabowski, A. Zając, op. cit., s. 7–16.

6 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483, z 2001 r. Nr 28, poz. 319, z 2006 r. Nr 200, poz. 1471, z 2009 r., Nr 114, poz. 946), art. 54 ust. 1.

7 B. Stefanowicz, *Informacyjne systemy zarządzania. Przewodnik*, Szkoła Główna Handlowa w Warszawie, Warszawa 2007.

8 K. Bąkowicz, *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, „Studia Medioznawcze" 2019, t. 20, nr 3(78), s. 281–282.

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

o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[10].

Według wymienionego wyżej rozporządzenia, dane osobowe stanowią informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli takiej, którą można bezpośrednio lub pośrednio zidentyfikować, np. na podstawie identyfikatora takiego jak imię, nazwisko, numer identyfikacyjny, identyfikator internetowy, dane o lokalizacji lub jeden bądź kilka szczególnych czynników określających tożsamość tej osoby[11]. Zatem do danych osobowych można zaliczyć m.in.: imię, nazwisko, datę urodzenia, PESEL, adres zamieszkania, numer telefonu czy wizerunek[12]. RODO wytypowało także dane osobowe szczególnej kategorii, m.in. ujawniające pochodzenie rasowe lub etniczne, poglądy, przekonania czy dane genetyczne[13]. Przetwarzanie tego typu danych podlega zasadom ściśle określonym w niniejszym rozporządzeniu.

Warto dodać, że RODO obejmuje również cyfrowe dane osobowe, które powstały w wyniku dynamicznie rozwijającej się technologii. Zalicza się do nich te, które funkcjonują w formie tradycyjnej, np. imię i nazwisko, dane kontaktowe oraz takie, które istnieją tylko w cyberprzestrzeni, np. adres e-mail, adres IP (ang. *Internet Protocol*, indywidualny numer urządzenia łączącego się z siecią)[14]. Należy przypomnieć, że będą one uznawane za dane osobowe tylko wtedy, gdy pozwolą na identyfikację konkretnej osoby.

Bezprawne uzyskanie informacji w świetle prawa

Powody pozyskiwania informacji są złożone. Informacje umożliwiają m.in. dostęp do pewnych obszarów, zapewniają różnego rodzaju korzyści, w tym majątkowe, a także mogą posłużyć do popełnienia kolejnych przestępstw[15]. Z tego względu są częstym obiektem zainteresowania przestępców. W dodatku postęp technologiczny pociąga za sobą pojawianie się coraz to nowszych technik nielegalnego zdobywania informacji. Wśród głównych metod takiego działania wyróżnia się naruszenie tajemnicy korespondencji, podsłuchy, wykorzystanie sieci bezprzewodowych oraz hacking.

---

10 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2019 r., poz. 125, z 2022 r., poz. 1700).

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., op. cit.

12 M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Wolters Kluwer, Warszawa 2018, s. 68.

13 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., op. cit.

14 E. Kuczma, *Cyber-dane osobowe jako dane osobowe nowej generacji*, „Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z nauk społecznych" 2017, nr 10, s. 64–65.

15 J. Kwaśnik, *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, „Annales Canonici" 2020, nr 16, [cz.] 1, s. 31–33.

Informacje, bez względu na rodzaj, chronione są na mocy prawa przez wiele aktów prawnych. W części szczególnej ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[16], zwanej dalej k.k., znajduje się rozdział poświęcony przestępstwom przeciwko ochronie informacji. Istotną rolę odgrywa w nim art. 267. Warto jednak zaznaczyć, że przestępstwo bezprawnego uzyskania dostępu do informacji godzi w konstytucyjne prawo do ochrony tajemnicy komunikowania się (art. 49) czy prawo do prywatności (art. 47)[17].

Próbując uszczegółowić powyższe informacje, należy bliżej przyjrzeć się wyżej cytowanemu art. 267 k.k. Paragraf 1 tego przepisu penalizuje uzyskanie dostępu do informacji przez osobę, dla której nie jest przeznaczona. Obejmuje on otwarcie zamkniętego pisma, czyli złamanie tzw. tajemnicy korespondencji, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie zabezpieczeń elektronicznych, magnetycznych czy informatycznych, tzw. hacking, lub innego szczególnego jej zabezpieczenia. Nieuprawnione zyskanie dostępu do systemu informatycznego karalne jest tak samo – bez względu na to, czy odnosi się do całości, czy tylko do jego części (art. 267 § 2 k.k.). Ten sam wymiar kary przewidziany jest także w przypadku założenia urządzenia podsłuchowego, wizualnego albo innego urządzenia czy oprogramowania lub posłużenia się nim przez osobę chcącą uzyskać informacje, do których nie jest uprawniona (art. 267 § 3 k.k.)[18]. Jak można zauważyć, karze podlega już samo uzyskanie dostępu do informacji lub systemu. Bez znaczenia jest więc to, czy sprawca czynu zapoznał się z daną informacją, czy nie. Taki zabieg ma na celu poszerzenie ochrony prawnokarnej, gdyż jak się okazuje, działania hackerów (czyli osób dokonujących hackingu) nie zawsze są ukierunkowane na pozyskanie informacji. Może także wystąpić taka sytuacja, w której sprawca nie ma umiejętności pozwalających mu na ich odczytanie. W dodatku udowodnienie, że sprawca zdobył informacje, mogłoby w niektórych przypadkach sprawić wiele trudności[19]. Wobec tego tak ważna jest forma i precyzja konstruowania przepisów prawnych.

Obecne brzmienie § 1 i § 2 art. 267 k.k. sprawia, że bezprawne uzyskanie dostępu do informacji czy systemu informatycznego jest karalne nawet wtedy, gdy nie doszło do złamania jakiegokolwiek zabezpieczenia. Może to być przykładowo zainstalowanie specjalnego oprogramowania umożliwiającego zdalną kontrolę nad komputerem. Ponadto, w wyniku no-

---

16 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (tj. Dz. U. z 2022 r., poz. 1138).

17 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., op. cit.

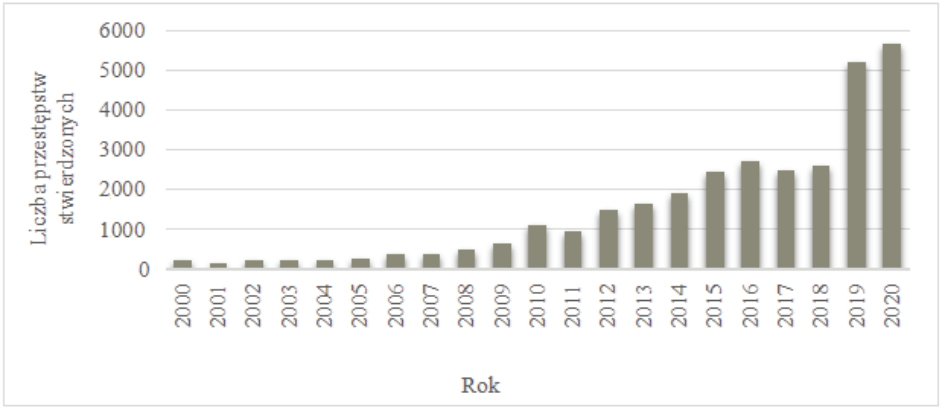
18 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

19 F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warszawa 2016, s. 287–289.

welizacji § 3 niniejszego artykułu, przewidziano karę za tzw. *sniffing*, czyli podsłuchiwanie za pomocą odpowiedniego programu wiadomości w sieci[20]. Powyższe zmiany jeszcze bardziej zwiększają pole ochrony prawnej, biorąc pod uwagę ciągle rozwijającą się technologię i kreatywność sprawców.

Zgodnie z § 4 art. 267 k.k. takiemu samemu wymiarowi kary jak w przypadku czynów z § 1–3 podlega osoba, która informację uzyskaną wymienionymi wcześniej sposobami ujawniła innej osobie lub grupie osób w dowolny sposób[21]. Należy zaznaczyć, że ściganie przestępstwa z § 1–4 art. 267 k.k. możliwe jest wyłącznie w wyniku złożenia wniosku przez pokrzywdzonego[22]. Z jednej strony może się to przyczyniać do pozornego zmniejszania skali zjawiska, gdyż w wielu przypadkach organy nie uzyskują wniosku o ściganie. Z drugiej jednak strony człowiek nie zawsze jest świadomy tego, że padł ofiarą przestępstwa, w szczególności cyberprzestępstwa. Na poniższym wykresie został przedstawiony rozkład przestępstw stwierdzonych z art. 267 k.k. w poszczególnych latach na podstawie statystyk policyjnych (ryc. 1).

Ryc. 1. Wykres przedstawiający liczbę przestępstw stwierdzonych z art. 267 k.k. na przestrzeni lat



Źródło: opracowanie własne na podstawie https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63625,Naruszenie-tajemnicy-korespondencji-art-267.html (dostęp: 03.02.2022).

[20] T. Pączkowski, *Słownik cyberbezpieczeństwa*, wyd. Szkoła Policji w Katowicach, Katowice, 2017, s. 52; M. Królikowski, R. Zawłocki (red.), *Kodeks karny – część szczególna. Tom II. Komentarz, art. 222–316,* 4. wydanie, Wydawnictwo C.H. Beck, Warszawa 2017, s. 490–491.

[21] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

[22] Ibidem.

Jak obrazuje powyższy wykres, w latach 2019–2020 nastąpił gwałtowny wzrost przestępstw penalizowanych z art. 267 k.k. Przyczynę można upatrywać m.in. w rozwoju wielu nowoczesnych metod nielegalnego zdobywania informacji w cyberprzestrzeni, a także zwiększeniu świadomości społecznej w zakresie omawianego zagadnienia.

Charakterystyka wybranych sposobów bezprawnego uzyskania informacji

Jak już wspomniano wcześniej, jednym ze sposobów pozyskania informacji niezgodnie z prawem jest naruszenie tajemnicy korespondencji. Przekazywane treści, bez względu na ich rodzaj, objęte są ochroną[23]. Przyjmuje się, że korespondencja to różne sposoby porozumiewania, z tym że proces ten odbywa się tylko na odległość. Nie ma jednak skonkretyzowanej prawnej definicji pojęcia tajemnicy korespondencji czy samej korespondencji. Mimo to uznaje się ją za jedną z wolności człowieka i obywatela, a zgodnie z kodeksem cywilnym za jedno z dóbr osobistych[24].

Warto nadmienić, że tajemnica korespondencji obejmuje różnorakie sposoby komunikowania, m.in. e-mail, komunikację telefoniczną, radiową czy nawet znaki świetlne. Istotne jest, że ochrona zawartych w korespondencji informacji przysługuje bez względu na to, kto jest ich odbiorcą i czego dotyczy treść[25]. Według kodeksu karnego naruszenie tajemnicy korespondencji związane jest z otwarciem zamkniętego pisma. Przez zamknięte pismo należy rozumieć wszelkie zabezpieczenia chroniące przed nieuprawnionym dostępem osób postronnych. Przykładowo więc będzie to zaklejona koperta, która może być rozerwana czy rozklejona[26].

Szczególną uwagę należy zwrócić na komunikację odbywającą się w formie elektronicznej, za pośrednictwem Internetu. Niestety, w takich przypadkach łatwiej o wszelkie naruszenia tajemnicy korespondencji. Przechwytywanie wiadomości, zmienianie ich treści, anulowanie przekazywania do grup czy hacking (zostanie omówiony w dalszej części) to tylko kilka zagrożeń,

---

[23] Prawo do tajemnicy korespondencji reguluje m.in. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2022 r., poz. 1138), ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2022 r., poz. 1360), ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2021 r., poz. 1062, z 2022 r. poz. 655), ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2021 r., poz. 576, z 2022 r. poz. 501) – w odniesieniu do tajemnicy telekomunikacyjnej, a także akty międzynarodowe.

[24] A. Gryszczyńska, *Tajemnica korespondencji*, „Monitor Prawniczy" 2015, R. 23, nr 24, s. 1336.

[25] Wyrok SA we Wrocławiu z 26 czerwca 2012 r., IACa 521/12, LEX nr 1238502; Wyrok SA w Krakowie z 23 listopada 2018 r., I ACa 169/18, LEX nr 2699135.

[26] M. Królikowski, R. Zawłocki (red.), op. cit., s. 495.

na które narażona jest poczta elektroniczna[27]. Warto pamiętać, że naruszenie tajemnicy korespondencji często idzie w parze z naruszeniem innych dóbr, wolności czy ochrony danych osobowych, również chronionych prawnie.

Nawiązując do kolejnego sposobu bezprawnego pozyskiwania informacji, przewidzianego w art. 267 § 3 k.k., należy podkreślić, że odpowiedzialności podlega osoba, która przede wszystkim nie jest uprawniona do uzyskania danej informacji[28], a ją pozyskuje. Decyduje o tym poufność wypowiedzi. Wypełnienie jednego ze znamion podsłuchu z powyższego paragrafu następuje wtedy, gdy rozmowie nadano poufny charakter zgodnie z wolą osób w niej uczestniczących, bez względu na przyczynę czy treść tej rozmowy, a nieuprawniona do zawartych w niej informacji osoba się z nią zapoznaje[29]. Zatem jeżeli dana osoba bierze udział w rozmowie lub jako osoba trzecia dostanie dorozumianą zgodę od rozmówców (np. w przypadku rozmowy telefonicznej z włączonym trybem głośnomówiącym), to zakłada się, że treści te są dla niej przeznaczone i może je utrwalać[30]. W takim przypadku nie można mówić o bezprawności działania.

Drugą przesłanką bezprawności czynu z art. 267 § 3 k.k. jest założenie urządzenia podsłuchowego, wizualnego, oprogramowania albo innego urządzenia lub posłużenie się nim. Przez określenie *urządzenie* rozumie się każdy przedmiot, który umożliwi zdobycie informacji – bez względu na to, czy jest on przeznaczony konkretnie do celów podsłuchowych, czy stosuje się go w życiu codziennym[31]. Sprawca finalnie nie musi jednak uzyskać dostępu do informacji, wystarczy, że podejmie działania w tym kierunku[32]. Nie ma także znaczenia to, czy zostaną one w jakiś sposób utrwalone[33]. Wobec powyższego urządzeniem, o którym mowa w art. 267 § 3 k.k., jest zarówno dyktafon, magnetofon, mikrofon kierunkowy, urządzenie podsłuchu elektromagnetycznego[34], jak i kamera, aparat fotograficzny czy telefon[35].

---

27 S. Jarosz-Żukowska, *Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w Internecie*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2008, t. 78, s. 28.

28 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

29 A. Lach, *Karne prawo – poufność jako kryterium bezprawnego uzyskania informacji – posłużenie się urządzeniami utrwalającymi obraz lub dźwięk: Postanowienie SN – Izba Karna z dnia 27 kwietnia 2016 r., III KK 265/15. Glosa*, OSP 2017, nr 11, s. 110.

30 Ibidem, s. 111.

31 J. Giezek (red.), *Kodeks karny: część szczególna. Komentarz*, Wolters Kluwer, Warszawa 2014, s. 989–990; A. Lach, op. cit., s. 111.

32 J. Giezek (red.), op. cit., s. 990.

33 A. Lach, op. cit., s. 111.

34 A. Góralski, *Techniczne środki inwigilacji oraz metody przeciwdziałania im*, „Wiedza Obronna" 2008, R. 35, nr 2, s. 117–119.

35 J. Giezek (red.), op. cit. s. 989–990.

W niniejszy zapis prawny wpisują się również urządzenia GPS, które instalowane w cudzym pojeździe umożliwiają uzyskanie takich informacji jak trasa jazdy i miejsce przebywania osoby podróżującej tym pojazdem[36]. Z kolei przedmioty prostej budowy, przykładowo lusterko lub aparat słuchowy, nie będą traktowane jako urządzenia podsłuchowe. Znamion § 3 nie wyczerpuje także zachowanie polegające na podsłuchiwaniu pod drzwiami bądź przez ścianę[37]. W odniesieniu do wykorzystywania oprogramowań w celach podsłuchowych wiąże się to z prowadzoną na szeroką skalę inwigilacją w obrębie cyberprzestrzeni. Jest to tzw. podsłuch komputerowy, który polega na instalowaniu programów inwigilujących na komputerze ofiary w celu przekazywania sprawcy dowolnych informacji. Należą do nich m.in. konie trojańskie, programy *spyware*, keyloggery oraz inne specjalne programy[38].

Jak wspomniano wyżej, jeżeli osoba utrwalająca rozmowę bierze w niej udział, to z punktu widzenia prawa karnego może ją utrwalać. Problem może się jednak pojawić na innych płaszczyznach. Otóż zarówno nagrywanie swojego rozmówcy, jak i podsłuch rozmowy, w której nagrywający nie bierze udziału, wiąże się z naruszeniem prawa do prywatności[39]. Bardzo często nagrania wykorzystywane są na potrzeby procesowe, jako dowód w sprawie. Decyzją Sądu Najwyższego dopuszczalne jest utrwalanie rozmów osób trzecich przez osoby prywatne dla celów dowodowych postępowania sądowego. Nie jest to jednak jednoznaczne z nadaniem uprawnienia do podsłuchu i wyłączenia odpowiedzialności karnej sprawcy[40]. Podczas rozstrzygania organy wymiaru sprawiedliwości biorą pod uwagę stopień społecznej szkodliwości. Zgodnie z art. 1 § 2 k.k., jeżeli czyn odznacza się znikomą społeczną szkodliwością, to nie uznaje się go za przestępstwo[41].

Kolejnym sposobem na pozyskiwanie informacji wbrew prawu jest wykorzystanie lokalnych sieci bezprzewodowych WLAN (ang. *Wireless Local Area Network*). Obecnie większość urządzeń wyposażona jest w interfejs wi-fi (ang. *Wireless Fidelity*), co jest dużym ułatwieniem, niestety nie tylko dla użytkownika, lecz także dla przestępcy, w szczególności wtedy, kiedy sieć nie jest chroniona. Wobec tego powinno się wystrzegać korzystania z sieci otwartych, głównie z uwagi na to, że przesyłane za ich pomocą

36 Postanowienie SN z 27 listopada 2019 r., V KK 505/18, LEX nr 2966120.
37 A. Lach, op. cit., s. 111–112.
38 F. Radoniewicz, op. cit., s. 304–305.
39 Wyrok SA w Gdańsku z 04 marca 2020 r., I ACa 363/19, LEX nr 3036500.
40 Postanowienie SN z 27 kwietnia 2016 r., III KK 265/15, OSNKW 2016/8/54.
41 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

dane mogą być widoczne dla wszystkich użytkowników znajdujących się w ich zasięgu[42]. Zgodnie z art. 267 § 1 k.k. osoba, która podłącza się do sieci telekomunikacyjnej, uzyskując w ten sposób dostęp do informacji nieprzeznaczonej dla niej, popełnia przestępstwo[43]. Uznaje się, że określenie to obejmuje zarówno sieci przewodowe, jak i bezprzewodowe[44]. Przez sieć telekomunikacyjną rozumie się określone systemy i urządzenia, dzięki którym za pośrednictwem przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną można nadawać, odbierać lub transmitować sygnały (art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne)[45]. Wobec tego, że sieć wi-fi stanowi jedno z mediów umożliwiających transmisję sygnałów, znajduje się w zakresie regulacji art. 267 § 1 k.k.

Niestety, w judykaturze występuje kwestia sporna dotycząca tego, jak rozpatrywać problem odpowiedzialności karnej zależnie od okoliczności. W szczególności chodzi o podłączanie się do otwartych sieci wi-fi, czyli takich, które nie są zabezpieczone hasłem. W przypadku podłączenia się do zabezpieczonej sieci bezprzewodowej, co wiąże się z przełamaniem jej zabezpieczeń, sprawca bezsprzecznie podlega karze. Mimo że otwarty charakter sieci WLAN jest wyrazem woli udostępniającego sygnał i nie powinno być w tej sytuacji zastosowania bezprawności, sprawa okazuje się bardziej złożona[46]. Wskutek tego w przedmiotowych sprawach organy wymiaru sprawiedliwości, dokonując oceny czynu, analizują okoliczności i określają stopień jego społecznej szkodliwości[47].

W przekazach medialnych, ale i w literaturze przedmiotowej często spotyka się określenie *hacking* (z ang. *hack* – włamywanie się). Definiuje się go jako uzyskiwanie nielegalnego dostępu do systemu komputerowego i odczytywanie informacji w nim zawartych[48], wywoływanie zakłóceń w funkcjonowaniu sieci i systemów lub potocznie jako łamanie haseł i zabezpieczeń czy wprowadzanie zamieszania w obrębie Internetu[49].

---

42 A. Behan, *Współczesne systemy informatyczne a typy przestępstw z art. 267 Kodeksu Karnego*, „Palestra" 2020, nr 2, s. 25.

43 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

44 Sejm Rzeczypospolitej Polskiej, VI kadencja, Prezes Rady Ministrów RM 10-51-08, druk nr 458, Warszawa, 18 kwietnia 2008 r.

45 Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2022 r., poz. 1648).

46 Szerzej na ten temat zob. A. Behan, op. cit.

47 Ibidem, s. 27.

48 https://dictionary.cambridge.org/pl/dictionary/english-polish/hack (dostęp: 25.01.2022).

49 F. Radoniewicz, op. cit., s. 22–32.

Przestępstwo hackingu w kodeksie karnym nie jest penalizowane przez jeden konkretny przepis prawny. Biorąc pod uwagę omawiany art. 267 k.k., sprawca może zostać ukarany zarówno z § 1, § 2, jak i § 3 tego przepisu. Za jedną z przesłanek hackingu uznaje się sformułowanie użyte w art. 267 § 1 k.k., które mówi o nieuprawnionym uzyskaniu dostępu do informacji poprzez przełamanie albo ominięcie zabezpieczeń[50]. Przez zabezpieczenia rozumie się wszelkie sposoby, które uniemożliwiają lub utrudniają sprawcy dostanie się do informacji, a do ich usunięcia potrzebna jest specjalistyczna wiedza, urządzenie czy kod, np. stosowanie haseł. Przełamanie zabezpieczeń polega więc na ich usunięciu albo ograniczeniu ich funkcji zabezpieczających na określony czas. Z kolei ominięcie odnosi się do takiego pokonania zabezpieczeń, które nie wywołuje ingerencji, np. wykorzystania luk systemów operacyjnych czy protokołów sieciowych[51]. Oba działania podlegają takiemu samemu wymiarowi kary. Kryminalizacja hackingu z § 2 art. 267 k.k. następuje w przypadku uzyskania bez uprawnienia dostępu do części lub całości systemu informatycznego przetwarzającego dane komputerowe[52]. Należy jednak zaznaczyć, że dane te są tylko nośnikiem informacji, a zatem posiadanie ich wcale nie oznacza, iż można odczytać ich znaczenie.

Hacking jest złożonym, dynamicznie rozwijającym się zjawiskiem. Wśród powszechnie znanych metod ukierunkowanych na bezprawne uzyskanie informacji znajdują się m.in. złośliwe oprogramowania, *sniffing* czy łamanie haseł. Złośliwe oprogramowania, tzw. *malware* (ang. *malicious software*), są bardzo często wykorzystywane przez hackerów. W zależności od tego, co przestępca chce uzyskać, dobiera odpowiednie narzędzia hackerskie. Z atakami, których celem jest przede wszystkim zdobycie danych czy informacji lub umożliwienie ich zdobycia, najczęściej związane są konie trojańskie, oprogramowania szpiegujące *spyware*, keyloggery, programy typu *backdoor*, *rootkit* czy *exploity*[53]. W przypadku sniffingu, przez który rozumie się przechwytywanie danych podzielonych na pakiety w trakcie transmisji, karalność z art. 267 § 3 k.k. zachodzi tylko wtedy, gdy dane przechwytywane są w czasie trwania ich przesyłania. W innych przypadkach czyn może zostać zakwalifikowany jako przestępstwo na podstawie § 1 lub 2 niniejszego artykułu[54].

---

50 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

51 J. Giezek (red.), op. cit., s. 988–989; M. Królikowski, R. Zawłocki (red.), op. cit., s. 496.

52 Wyjaśnienie terminów – szerzej zob. dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218/8).

53 F. Radoniewicz, op. cit., s. 79–82, 86–87.

54 Ibidem, s. 89–91, 304–305.

Omawiając problem bezprawnego uzyskiwania informacji, należy także wspomnieć o phishingu (ang. *password harvesting fishing* – łowienie haseł). Oszustwa phishingowe polegają na uzyskaniu ważnych danych i informacji poprzez wysyłanie nieprawdziwych komunikatów, powiadomień, z urzędów, banków, sklepów czy innych podmiotów i instytucji, a także systemów e-płatności. Najczęściej rozsyłane są w postaci e-maili oraz SMS-ów (SMiShing), skłaniając odbiorcę – poprzez podanie wiarygodnego powodu – do zaktualizowania danych lub dopłaty niewielkiej kwoty do rachunku lub przesyłki[55]. Otworzenie otrzymanego linku lub załącznika przekierowuje na fałszywą stronę przypominającą tę prawdziwą, w efekcie czego wszelkie wpisane dane przekazywane są przestępcom. Karalność phishingu regulowana jest w szczególności przez art. 287 k.k. mówiący o oszustwie komputerowym, jednak gdy podczas popełniania czynu dojdzie do przełamania lub ominięcia jakichś zabezpieczeń, może również wypełnić znamiona z art. 267 k.k.[56]

Profilaktyka bezpieczeństwa informacji

Profilaktyka odgrywa ważną rolę w budowaniu bezpieczeństwa, jednak aby była skuteczna, musi łączyć w sobie wiele różnych metod, zadań i środków ochrony. Stosowanie sprawnych systemów teleinformatycznych jest istotnym elementem ochrony informacji elektronicznej. Wśród powszechnie stosowanych rozwiązań znajdują się biometryczne mechanizmy kontroli dostępu i szyfrowanie[57]. Ponadto należy zadbać o zapewnienie trzech podstawowych założeń bezpieczeństwa informacji, wchodzących w skład tzw. triady CIA. Nazwa ta pochodzi od pierwszych liter angielskich odpowiedników poufności (*confidentiality*), integralności (*integrity*) oraz dostępności (*accessibility*)[58]. W celu pełniejszej ochrony systemów należy także zabezpieczać sieć lokalną zapewniającą połączenie z Internetem. Służą do tego tzw. zapory sieciowe (ang. *firewall* – ściana ogniowa), przez które

---

55 https://cik.uke.gov.pl/gfx/cik/userfiles/j-dubel/olsztyn/oeiizk/kodowanie_listopad/phishing.pdf (dostęp: 03.02.2022).

56 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, op. cit.

57 W. Drogoń, D. Mąka, M. Skawina, *Jak chronić tajemnice?*, Dom Wydawniczy Bellona, Warszawa 2004, s. 136–137, 143–144.

58 D. Popescul, *The confidentiality – integrity – accessibility triad into the knowledge security. A reassessment from the point of view of the knowledge contribution to innovation*, w: *Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage)*, Kuala Lumpur 2011, s. 1339.

przepływa cały ruch między sieciami[59]. Niestety, w praktyce okazuje się, że czasem nawet sprawne systemy zawodzą. Cyberprzestępcy w pierwszej kolejności szukają luk systemowych, a do niszczenia zabezpieczeń dochodzi tylko wtedy, gdy jest to konieczne.

Człowiek uważany jest za najsłabsze ogniwo bezpieczeństwa informacji. Nieuwaga, niewiedza, łatwowierność czy chęć ułatwienia sobie pracy bez myślenia o konsekwencjach to tylko kilka powodów, których skutkiem może być nieuprawniony dostęp do informacji. Bardzo pomocne w tej kwestii są adresowane do pracowników regularne szkolenia akcentujące możliwe nieprawidłowości. Niezwykle ważne jest podejmowanie działań profilaktycznych nie tylko wobec zespołów ludzkich, lecz także pojedynczych jednostek, w szczególności w odniesieniu do poruszania się po Internecie. Podstawowym mechanizmem obronnym jest silnie zbudowane hasło. Powinno ono zawierać około 12 znaków mieszanych, tj. litery małe, duże, cyfry i znaki specjalne[60]. Niestety, z analizy haseł pochodzących z tzw. wycieków wynika, że wielu użytkowników bagatelizuje te zalecenia[61]. Wobec tego coraz więcej serwisów internetowych podczas rejestracji stawia określone wymagania co do konstrukcji hasła. Jest to pewnego rodzaju rozwiązanie, które pozwala na jego wzmocnienie, jednak nadal nie daje gwarancji, że będzie ono skomplikowane i trudne do złamania. Hasła powinny być też regularnie zmieniane. Powszechną praktyką, która nie należy do bezpiecznych rozwiązań, jest stosowanie tego samego hasła do różnych kont[62] lub logowanie się do jednego konta za pomocą innego. Wielu użytkowników zapisuje także swoje hasła w ustawieniach przeglądarki. Wszystkie te działania są ułatwieniem tylko na pozór, gdyż znacznie zwiększają podatność na utratę chronionych informacji i danych. Dobrym pomysłem jest korzystanie z dwuetapowej weryfikacji, wykorzystującej dodatkowo potwierdzenie logowania kodem otrzymanym za pomocą SMS-a, połączenia głosowego lub aplikacji mobilnej[63], gdyż stanowi to pewnego rodzaju dodatkową tarczę ochronną.

Lista czynności pozwalająca na zwiększenie poziomu bezpieczeństwa jest długa. W celu ochrony m.in. przed phishingiem nie należy korzystać z linków i innych odnośników do stron logowania, formularzy kontaktowych, stron

---

59 J. Zych, *Teleinformatyka dla bezpieczeństwa*, Wydawnictwo Naukowe FNCE, Poznań 2018, s. 61–62.

60 K. Zawierucha, *Personal data in the aspect of IT usage – the end of anonymity*, „Scientific Journal of the Military University of Land Forces" 2021, t. 53, nr 1, s. 173.

61 https://cert.pl/posts/2022/01/co-wycieki-danych-mowia-o-haslach/ (dostęp: 13.02.2022).

62 K. Zawierucha, op. cit., s. 173.

63 https://www.google.com/landing/2step/?hl=pl#tab=how-it-works (dostęp: 13.02.2022).

dotyczących płatności wysyłanych w wiadomościach oraz upewniać się, czy wszelkie komunikaty otrzymane rzekomo od podmiotów publicznych lub instytucji są prawdziwe. Jak się okazuje, dokonanie większości przestępstw polegających na rozpowszechnieniu złośliwego oprogramowania poprzez wiadomość e-mail możliwe było w wyniku podjęcia określonego działania przez samą ofiarę, np. użycia przesłanego linku czy zaakceptowania fałszywego ostrzeżenia o bezpieczeństwie[64]. Dzieje się tak, ponieważ komunikaty oraz strony z umieszczonych w nich linków są bardzo wiarygodne, przez co wiele osób (także przez nieuwagę i pośpiech) ulega oszustwom.

Nie należy zapominać także o profilaktyce w obrębie pozostałych przestępstw przeciwko ochronie informacji, a zatem o zagrożeniu tajemnicy korespondencji i podsłuchach. Przede wszystkim należy się za każdym razem upewniać, czy adres, na który zostanie wysłana wiadomość, jest prawidłowy. Natomiast podsłuchy ze względu na dynamiczny postęp technologiczny coraz trudniej wykryć. Z pomocą jednak mogą przyjść kontrole dostępu do pomieszczeń lub monitoring weryfikujący, czy ktoś niepowołany znalazł się w danym miejscu, w którym taki podsłuch mógłby być zainstalowany.

Analiza badania własnego

Mając na uwadze prowadzone wyżej rozważania, w lutym 2022 r. przeprowadzono badanie z wykorzystaniem metody badawczej, jaką jest sondaż diagnostyczny. Jako technikę badawczą wybrano anonimową ankietę, a narzędzie badawcze – interaktywny kwestionariusz. Celem badania było sprawdzenie wiedzy respondentów na temat bezprawnego pozyskiwania informacji, charakteru podejmowanych przez nich zachowań w Internecie, a także sposobów ochrony informacji, w tym danych osobowych. W ramach badania założono problemy badawcze i hipotezy, które szerzej zostaną omówione w dalszej części artykułu. Ankieta została rozpowszechniona za pomocą Internetu na różnego rodzaju grupach i forach. W badaniu udział wzięły 154 osoby, zarówno kobiety (58,4%), jak i mężczyźni (41,6%). Ankietowani należeli do różnych grup pod względem wieku (16–25 lat – 53,3%, 26–39 lat – 21,4%, 40–59 lat – 20,8% oraz osoby powyżej 60 lat – 4,5%) i wykształcenia (podstawowe – 8,4%, zawodowe – 18,2%, średnie – 44,8% i wyższe – 28,6%).

Pierwsze dwa pytania odnosiły się bezpośrednio do doświadczeń badanych związanych z dwoma podstawowymi metodami bezprawnego

[64] https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf (dostęp: 13.02.2022).

uzyskania informacji – naruszeniem tajemnicy korespondencji oraz nagrywaniem rozmowy, a właściwie podsłuchem. Według 42,2% respondentów korespondencja, która była do nich zaadresowana, została przynajmniej raz otworzona lub przeczytana przez osobę niemającą na to zezwolenia, natomiast 24,7% nie wiedziało, czy taka sytuacja miała miejsce. Tylko 33,1% nigdy tego nie doświadczyło. Jeżeli chodzi o nagrywanie rozmów, w której uczestniczył respondent, to 46,1% przyznało, że co najmniej raz było nagrywanych, 26,6% nie było nagrywanych, a 27,3% nie miało na ten temat wiedzy. Badani zostali zapytani także, czy kiedykolwiek ich dane lub inne informacje zostały bezprawnie pozyskane przez inną osobę. Bez znaczenia jednak była tutaj okoliczność czy metoda, za pomocą której się to wydarzyło. Z analizy wynika, iż 27,2% badanych padło ofiarą zjawiska bezprawnego uzyskania informacji, z czego 59,6% przydarzyło się to kilkakrotnie. Niepokojącym sygnałem może być to, że aż 48,1% badanych przyznało, że nie są pewni, czy ich dane i informacje zostały nielegalnie pozyskane przez inne osoby.

W celu sprawdzenia wiedzy merytorycznej osób biorących udział w badaniu zadano im trzy pytania, które wraz z odpowiedziami zostały przedstawione poniżej (dla ułatwienia prezentacji wyników przy dwóch pytaniach przyjęto następującą skalę: 5 – zdecydowanie tak, 4 – raczej tak, 3 – raczej nie, 2 – zdecydowanie nie, 1 – nie wiem).

Pytanie nr 1. *Czy Pana/Pani zdaniem dozwolone jest nagrywanie rozmowy, w której się uczestniczy?* (tab. 1)

Tab. 1. Rozkład procentowy odpowiedzi respondentów na pytanie nr 1

5	4	3	2	1
12,3	23,4	26,6	27,3	10,4

Źródło: opracowanie własne na podstawie przeprowadzonego badania.

Pytanie nr 2. *Czym według Pana/Pani jest „hacking”?*

Najwięcej odpowiedzi (75,3% badanych) określiło ten termin jako włamywanie się do systemów i sieci. Z kolei 11,7% badanych uznało, że nie wie, czym jest hacking, a 11% – że jest to zdobywanie materiałów dowodowych przez podkładanie podsłuchów.

Pytanie nr 3. *Czy uważa Pan/Pani, że można bezprawnie uzyskać dostęp do jakichkolwiek informacji przez sieć bezprzewodową wi-fi?* (tab. 2)

Tab. 2. Rozkład procentowy odpowiedzi respondentów na pytanie nr 3

5	4	3	2	1
31,8	37	9,1	10,4	11,7

Źródło: opracowanie własne na podstawie przeprowadzonego badania.

Problem z pytaniami związanymi z cyberzagrożeniami w dużej mierze miały osoby w wieku od 40 lat wzwyż. Na pytanie dotyczące znajomości terminu hackingu 57,1% wszystkich badanych w wieku więcej niż 60 lat oraz 40,6% z przedziału wiekowego 40–59 lat udzieliło odpowiedzi: „nie wiem" lub ich odpowiedź była błędna. Osoby, które nie wiedziały, czym jest hacking, lub udzieliły błędnej odpowiedzi, w większości miały wykształcenie podstawowe (46,1% wszystkich badanych z tym wykształceniem), a następnie zawodowe (28,6%) i średnie (27,5%). W przypadku pytania o nagrywanie rozmów wiek i wykształcenie nie miały znaczenia.

Kolejne pytanie odnosiło się do zjawiska phishingu. Aż 82,5% badanych zadeklarowało, że otrzymywało „podejrzane" wiadomości e-mail lub SMS z linkiem, przy czym 29,9% otrzymywało je wielokrotnie. Tylko 17,5% nie było adresatem tego typu wiadomości. Jeżeli chodzi o ogólne zagrożenia w cyberprzestrzeni, 59,1% respondentów jest świadomych ich istnienia, a 33,8% uważa, że raczej są świadomi. Przyczyn niepewności można szukać w ciągle rozwijającej się przestępczości cybernetycznej. Osoba, która nie ma bieżącej wiedzy na ten temat, nie jest w pełni świadoma niebezpieczeństwa, przez co staje się bardziej podatna na zagrożenie. Niepokojącą postawą wydaje się sytuacja, w której osoby nieznające definicji najpowszechniejszego cyberzagrożenia, jakim jest hacking, twierdzą, że są (lub raczej są) świadome niebezpieczeństw czyhających w cyberprzestrzeni. Uznało tak 85% respondentów, którzy udzielili błędnej odpowiedzi na pytanie o hacking.

Ankietowani zapytani wcześniej, czy można w sposób bezprawny uzyskać dostęp do informacji poprzez bezprzewodową sieć wi-fi, zostali poproszeni o udzielenie odpowiedzi odnośnie do zabezpieczeń ich routerów lub innych urządzeń umożliwiającym im połączenie z Internetem. Okazało się, że zdecydowana większość chroni swoją sieć – 92,2% badanych, z czego 23,2% osób wykorzystuje do tego hasło domyślne – krótkie i bardzo

proste, zapisane zazwyczaj na obudowie urządzenia. Nieliczny odsetek respondentów nie posiada hasła w ogóle – 2,6% lub nie ma wiedzy na ten temat – 5,2%. Co ciekawe, z analizy wynika, iż 66,7% badanych, którzy na tego typu urządzeniach mają ustawione domyślne hasło lub w ogóle nie mają hasła, uważa, że poprzez bezprzewodową sieć wi-fi można bezprawnie uzyskać dostęp do określonych informacji, natomiast aż 91,7% twierdzi, że są świadomi (58,4%) lub raczej są świadomi (33,3%) zagrożeń funkcjonujących w cyberprzestrzeni.

Niewiele ponad połowa respondentów (53,9%) przyznała, że ich hasła na urządzeniach oraz kontach są wystarczająco silne, a 33,1% wyraziło niewiedzę na ten temat. Następnie zapytani o to, z czego zazwyczaj składają się ich hasła, udzielili różnych odpowiedzi (tab. 3), przy czym dozwolony był wybór więcej niż jednego wariantu. Z tabeli wynika, że nadal stosuje się zbyt łatwe hasła, na które składają się m.in. tylko litery lub cyfry czy proste i znane słowa.

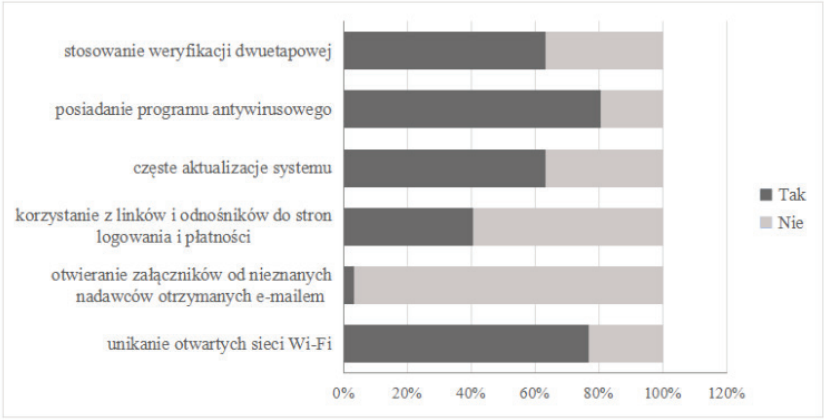
Tab. 3. Rodzaje haseł stosowanych przez respondentów

Rodzaj hasła	Procent respondentów stosujących tego typu hasło	Rodzaj hasła	Procent respondentów stosujących tego typu hasło
tylko małe litery	2	kombinacja cyfr i znaków specjalnych	8,4
tylko duże litery	2,6	kombinacja liter, cyfr i znaków specjalnych	46,8
kombinacja małych i dużych liter	36,4	słowa i liczby mające jakieś znaczenie	11,7
tylko cyfry	5,2	proste i znane ciągi cyfr	3,2
kombinacja liter i cyfr	26	proste i znane słowa	6,5
kombinacja liter i znaków specjalnych	11		

Źródło: opracowanie własne na podstawie przeprowadzonego badania.

Oprócz siły haseł respondentów sprawdzono także, czy stosują się oni do podstawowych zaleceń profilaktycznych pozwalających wzmocnić ich bezpieczeństwo w Internecie. Otóż należy pamiętać, że nawet odpowiednio dobre hasło nie daje stuprocentowej gwarancji uniknięcia ataku hackerskiego. Wyniki przedstawiają się następująco (ryc. 2).

Ryc. 2. Stosowanie przez respondentów profilaktyki przed zagrożeniami w obrębie Internetu



Źródło: opracowanie własne na podstawie przeprowadzonego badania.

Z wykresu przedstawionego na ryc. 2 wynika, że aż 96,8% badanych nie otwiera załączników otrzymanych e-mailem od nieznanych nadawców. Jeżeli chodzi o linki i załączniki, należy być wyjątkowo ostrożnym. Zdarzają się sytuacje, w których nadawcą co prawda jest osoba znajoma, ale wiadomość została wysłana bez jej wiedzy. Warto zatem najpierw upewnić się, czy jest to bezpieczne, a dopiero potem zapoznać się z zawartością.

Podsumowanie i wnioski

Podsumowując powyższe rozważania na temat bezprawnego uzyskania informacji, należy stwierdzić, że narażony na nie jest każdy człowiek. Niestety, wraz z postępem cywilizacyjnym udoskonalane są dotychczasowe oraz poszukiwane nowe metody popełniania przestępstw przeciwko informacji. Odpowiednie umiejętności oraz precyzja sprawcy potrafią spowodować, że ofiara może nie być niczego świadoma. Równocześnie ludzie też nie zawsze postępują właściwie, przez co stają się bardziej podatni na tego rodzaju zagrożenia.

Z badania wynika, że część respondentów (27,2% badanych) osobiście spotkała się chociaż raz z przestępstwem bezprawnego uzyskania informacji. Ponieważ zaś aż 48,1% badanych nie było pewnych, czy mogło dojść do takiej sytuacji, skala zjawiska może być większa. Według respondentów poważnym zagrożeniem dla społeczeństwa jest phishing. Styczność z nim miało aż 82,5% badanych. Wobec powyższego podstawowym filarem

dbania o bezpieczeństwo informacji jest wiedza merytoryczna na temat potencjalnych zagrożeń. Ogólnie rzecz biorąc, większość osób zna podstawowe zagadnienia czy sposoby związane z bezprawnym pozyskiwaniem informacji, tj. hacking czy wykorzystywanie bezprzewodowych sieci wi-fi. Bardziej problematyczny okazuje się jednak temat nagrywania rozmów – aż 64,3% respondentów nie potrafiło udzielić odpowiedzi na to, czy osoba, która bierze udział w rozmowie, może ją nagrywać. Jeżeli chodzi o cyberzagrożenia, to 92,9% badanych było ich świadomych w większym bądź mniejszym stopniu. W związku z tym stosowali odpowiednie rozwiązania, tj. silne hasła na kontach i urządzeniach, weryfikację dwuetapową czy unikanie otwartych (niezabezpieczanych hasłem) sieci wi-fi. Ogólny poziom ochrony można więc określić jako dobry.

Przeprowadzone badanie ankietowe umożliwiło określenie stosunku społeczeństwa wobec zjawiska bezprawnego pozyskiwania informacji. Tego typu badania przynoszą wiele korzyści, ponieważ pozwalają zobrazować skalę problemu i tym samym zwiększyć świadomość społeczeństwa, w efekcie prowadząc do wdrożenia i ulepszenia ochrony na różnych poziomach. Na podstawie analizy otrzymanych wyników stwierdza się, że udowodniono postawione hipotezy szczegółowe, w związku z czym potwierdzona została także hipoteza główna. Zakładała ona, że większa część społeczeństwa świadoma jest zjawiska, jakim jest bezprawne pozyskiwanie informacji, i podejmuje starania, aby się przed nim chronić.

Należy pamiętać, że na ochronę przed zjawiskiem bezprawnego uzyskania informacji w dużym stopniu oddziałuje profilaktyka oraz zachowanie ostrożności. Warto więc skupić się na ochronie przed nim, zarówno poprzez stosowanie indywidualnych rozwiązań (w tym także rozwiązań technicznych), jak i organizowanie wielu różnych przedsięwzięć (kampanie profilaktyczne, krótkie spoty nadawane za pomocą środków masowego przekazu, szkolenia), mających na celu uświadamianie jak największej części społeczeństwa. Im więcej ich będzie, tym większe prawdopodobieństwo, że trafią do szerszego grona odbiorców.

Bibliografia

Literatura

Bąkowicz K., *Wprowadzenie do definicji i klasyfikacji zjawiska fake newsa*, w: „Studia Medioznawcze" 2019, t. 20, nr 3(78).

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

Drogoń W., Mąka D., Skawina M., *Jak chronić tajemnice?*, Dom Wydawniczy Bellona, Warszawa 2004.
Gawroński M. (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Wolters Kluwer, Warszawa 2018.
Giezek J. (red.), *Kodeks karny: część szczególna. Komentarz*, Wolters Kluwer, Warszawa 2014.
Góralski A., *Techniczne środki inwigilacji oraz metody przeciwdziałania im*, „Wiedza Obronna" 2008, R. 35, nr 2.
Grabowski M., Zając A., *Dane, informacja, wiedza*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 798.
Gryszczyńska A., *Tajemnica korespondencji*, „Monitor Prawniczy" 2015, R. 23, nr 24.
Jarosz-Żukowska S., *Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w Internecie*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2008, t. 78.
Królikowski M., Zawłocki R. (red.), *Kodeks karny – część szczególna. Tom II. Komentarz, art. 222–316*, 4. wydanie, Wydawnictwo C.H. Beck, Warszawa 2017.
Kuczma E., *Cyber-dane osobowe jako dane osobowe nowej generacji*, „Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z nauk społecznych" 2017, nr 10.
Kwaśnik J., *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, „Annales Canonici" 2020, nr 16 [cz.] 1.
Lach A., *Karne prawo – poufność jako kryterium bezprawnego uzyskania informacji – posłużenie się urządzeniami utrwalającymi obraz lub dźwięk: Postanowienie SN – Izba Karna z dnia 27 kwietnia 2016 r., III KK 265/15. Glosa*, OSP 2017, nr 11.
Pączkowski T., *Słownik cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017.
Popescul D., *The confidentiality – integrity – accessibility triad into the knowledge security. A Reassessment from the point of view of the knowledge contribution to innovation*, w: *Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage)*, Kuala Lumpur 2011.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warszawa 2016.
Stefanowicz B., *Informacja*, Szkoła Główna Handlowa w Warszawie, Warszawa 2004.

Stefanowicz B., *Informacyjne systemy zarządzania. Przewodnik*, Szkoła Główna Handlowa w Warszawie, Warszawa 2007.
Stefanowicz B., *Koncepcja pojęcia informacji*, „Wiadomości Statystyczne" 2010, t. 55, nr 7.
Zych J., *Teleinformatyka dla bezpieczeństwa*, Wydawnictwo Naukowe FNCE, Poznań 2018.
Zawierucha K., *Personal data in the aspect of IT usage – the end of anonymity*, „Scientific Journal of the Military University of Land Forces" 2021, t. 53, nr 1.

Źródła prawa

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483, z 2001 r. Nr 28, poz. 319, z 2006 r. Nr 200, poz. 1471, z 2009 r., Nr 114, poz. 946).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2022 r., poz. 1138).
Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2022 r., poz. 1648).
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781).
Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2019 r., poz. 125, z 2022 r., poz. 1700).
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. Urz. UE L 119, ze zm.).
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218/8).

Wyroki i postanowienia sądów

Wyrok SA we Wrocławiu z 26 czerwca 2012 r., IACa 521/12, LEX nr 1238502.
Wyrok SA w Krakowie z 23 listopada 2018 r., I ACa 169/18, LEX nr 2699135.

Postanowienie SN z 27 listopada 2019 r., V KK 505/18, LEX nr 2966120.
Wyrok SA w Gdańsku z 04 marca 2020 r., I ACa 363/19, LEX nr 3036500.
Postanowienie SN z 27 kwietnia 2016 r., III KK 265/15, OSNKW 2016/8/54.
Sejm Rzeczypospolitej Polskiej, VI kadencja, Prezes Rady Ministrów RM 10-51-08, druk nr 458, Warszawa, 18 kwietnia 2008 r.

Źródła internetowe

https://cik.uke.gov.pl/gfx/cik/userfiles/jdubel/olsztyn/oeiizk/kodowanie_listopad/phishing.pdf (dostęp: 03.02.2022).
https://cert.pl/posts/2022/01/co-wycieki-danych-mowia-o-haslach/ (dostęp: 13.02.2022).
https://dictionary.cambridge.org/pl/dictionary/english-polish/hack (dostęp: 25.01.2022).
https://www.google.com/landing/2step/?hl=pl#tab=how-it-works (dostęp: 13.02.2022).
https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf (dostęp: 13.02.2022).

Konflikt interesów

Brak

Źródło finansowania

Brak