Włodzimierz Fehler
Uniwersytet Przyrodniczo-Humanistyczny
w Siedlcach
Marcin Górnikiewicz
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego

Studia Wschodnioeuropejskie
Publikacja w trybie ciągłym

Naruszenie ochrony danych osobowych - realne i potencjalne konsekwencje dla bezpieczeństwa informacyjnego jednostki

Istota i znaczenie informacyjnego bezpieczeństwa jednostki

W ogólnym ujęciu bezpieczeństwo jednostki można określić jako pewien stan i proces w ramach których jednostka ta funkcjonuje w sposób wolny od zagrożeń dla istotnych dla niej wartości takich jak: życie, zdrowie, wolność, nietykalność osoby i mienia, swoboda przekonań i głoszenia poglądów, prawo do pracy itp. oraz ma dostęp do środków i instrumentów pomocowych kiedy wartości te są zagrożone. Bezpieczeństwo jednostki budowane jest w każdym przypadku indywidualnie co wynika z autonomicznych w odniesieniu do każdego człowieka celów życiowych, systemu wartości czy zapatrywań na sposób życia. Istnieje jednak cała gama fundamentalnych warunków tego bezpieczeństwa obejmująca m.in.: zapewnienie nietykalności cielesnej oraz poszanowanie mienia oparte o prawo własności, ochronę godności i prywatności, istnienie możliwości zaspokajania potrzeb poprzez pracę, zagwarantowanie dobrych warunków dla zakładania rodzin i ich rozwoju, asekurację ze strony państwa w sytuacjach powstawania ryzyk socjalnych oraz utraty czy ograniczenia samodzielności np. związanej z procesem starzenia czy zakończenia aktywności pracowniczej. Przez długi czas personalny (jednostkowy) wymiar bezpieczeństwa był pomijany lub marginalizowany. Eksponowano bowiem tak w badaniach naukowych jak i w działalności praktycznej znaczenie innych podmiotowych wymiarów bezpieczeństwa a mianowicie bezpieczeństwa międzynarodowego oraz bezpieczeństwa państwa. Jak celnie wskazał Fen

Osler Hampson charakteryzując tę sytuację konwencjonalna, realistyczna szkoła myślenia o bezpieczeństwie pozostawała zamknięta na logikę bezpieczeństwa jednostki [1]. Istnienie takiego stanu rzeczy nie oznaczało całkowitego pomijania kwestii bezpieczeństwa personalnego. Jednak na co zwracają uwagę Kateryna Novikova i Anna Orzyłowska w rozważaniach dotyczących bezpieczeństwa indywidualnego akcentowano przede wszystkim problematykę nietykalności cielesnej oraz ochrony mienia przed aktami przemocy[2].Współcześnie zakres bezpieczeństwa jednostki oprócz wyliczonych wcześniej czynników a mianowicie nietykalności osoby i jej mienia oraz zapewnienia materialnych podstaw egzystencji, (w tym stabilności zatrudnienia) wyznaczany jest przez, swobodne i stabilne funkcjonowanie w sferze politycznej, kulturowej, ekonomicznej, społecznej, ekologicznej oraz informacyjnej. Jednocześnie na co zwraca uwagę m.in. Krzysztof Drabik jednostka staje się centralnym punktem odniesienia w procesach kształtowania i zabiegania o bezpieczeństwo podmiotów zbiorowych[3].

Dążąc do ustalenia istoty bezpieczeństwa informacyjnego jednostki we współczesnym kształcie należy dostrzec i podkreślić znaczenie faktu wytyczania jego ram przez regulacje prawne o charakterze międzynarodowym oraz narodowym. W pierwszej kolejności trzeba odwołać się do treści Powszechnej Deklaracja Praw Człowieka z 10 grudnia 1948 r. W artykule 12 przywoływanej Deklaracji umieszczono zapis mówiący o zakazie ingerowania w prywatną korespondencję, oraz prawie do ochrony przed taką ingerencją[4]. Z kolei w artykule 19 stwierdzono,, Każdy człowiek ma prawo do wolności poglądów i wypowiedzi; prawo to obejmuje nieskrępowaną swobodę posiadania poglądów oraz poszukiwania, otrzymywania oraz rozpowszechniania informacji i idei wszelkimi środkami, bez względu na granice”[5]. Podobne regulacje znalazły się w Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z 4 listopada 1950r. W artykule 8 wymienionej Konwencji zapisano, że każdy ma prawo do poszanowania swojej korespondencji zaznaczając, że ingerencja władzy publicznej

[1] Zob. F.O. Hampson, *Bezpieczeństwo jednostki* [w:] P. D. Williams (red.), *Studia bezpieczeństwa* , Kraków 2012, s. 237-238.

[2] Zob. K. Novikova, A. Orzyłowska, J*ednostka ludzka w obliczu zagrożeń współczesności: bezpieczeństwo indywidualne w Polsce. Implikacje metodologiczne* „Journal of Modern Science”2019 nr 1, s.319.

[3] Zob. K.Drabik, A. Pieczywok, *Bezpieczeństwo i natura człowieka wobec jego alienacji i kryzysu egzystencji,* Warszawa 2022, s.61.

[4] Zob. *Powszechna Deklaracja Praw Człowieka* , https://www.unic.un.org.pl/dokumenty/deklaracja.php [dostęp: 11.03.2023]

[5] *Powszechna Deklaracja Praw Człowieka* , https://www.unic.un.org.pl/dokumenty/deklaracja.php [dostęp: 11.03.2023]

w korzystanie z tego prawa jest niedopuszczalna poza sytuacjami określonymi przez ustawę, koniecznymi w demokratycznym społeczeństwie ze względu na zapewnienie: bezpieczeństwa państwowego, bezpieczeństwa publicznego, dobrobytu gospodarczego państwa, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności a także ochronę praw i wolności innych osób[6]. Z kolei w ustępie 1 art. 10. wspomnianej Konwencji stwierdzono, że każdy ma prawo do,, otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe"[7]. Zastrzeżono przy tym prawo państw do stosowania procedur udzielania zezwoleń na działalność przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych. W ustępie 2 przywoływanego artykułu 10 zaznaczono z kolei, że korzystanie z wymienionych w ustępie 1 wolności może podlegać wymogom formalnym, warunkom, ograniczeniom i sankcjom, na gruncie ustawowym ale tylko takim które są niezbędne w społeczeństwie demokratycznym ze względu na bezpieczeństwo państwowe, zapewnienie integralności terytorialnej lub bezpieczeństwa publicznego, ze względu na konieczność zapobiegania zakłóceniom porządku lub przestępstwom, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieganie ujawnianiu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej[8].

Tak zakreślone ramy bezpieczeństwa informacyjnego jednostki zostały potwierdzone w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych z 16 grudnia 1966 r. W artykule 17 tego Paktu zapisano nie tylko zakaz bezprawnej ingerencji w korespondencję ale także prawo do ochrony prawnej przed tego rodzaju działaniami. Natomiast w artykule 19 ujęto prawo do swobodnego poszukiwania, otrzymywania i rozpowszechniania informacji, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób. Jednocześnie w ustępie 3 wspomnianego wyżej artykułu stwierdzono że realizacja wymienionych w nim praw niesie ze sobą specjalne obowiązki i odpowiedzialność. Może zatem podlegać ograniczeniom (wyraźnie określonym przez ustawę)

[6] Zob. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2.* (Dz.U.z 1993r. nr 61,poz. 284).

[7] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2.* (Dz.U.z 1993r. nr 61,poz. 284).

[8] Zob. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2.* (Dz.U.z 1993r. nr 61,poz. 284).

niezbędnym dla zapewnienia: poszanowania praw i dobrego imienia innych, ochrony bezpieczeństwa państwowego lub porządku publicznego albo zdrowia lub moralności publicznej[9].

Kwestią bezpieczeństwa informacyjnego jednostki zajęto się również w Karcie Praw Podstawowych Unii Europejskiej ogłoszonej w Strasburgu 12 grudnia 2007 r. przez Parlament Europejski, Radę i Komisję. W artykule 7 Karty stwierdzono, że każdy ma prawo do poszanowania procesu komunikowania się. Następnie w artykule 8 określono, że ,,Każdy ma prawo do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania"[10]. Przywołać należy również artykuł 11 w którym zapisano prawo do wolności otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe[11]. Dla prowadzonych analiz ważny jest również artykuł 42 stanowiący że ,,Każdy obywatel Unii i każda osoba fizyczna lub prawna mająca miejsce zamieszkania lub statutową siedzibę w Państwie Członkowskim ma prawo dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy"[12]. Należy w tym miejscu zaznaczyć ,że szczegółowe rozstrzygnięcia w zakresie ochrony danych osobowych znalazły się w Rozporządzeniu 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[13].

Fundamenty informacyjnego bezpieczeństwa jednostki oprócz przywołanych wyżej aktów prawa międzynarodowego tworzą również przepisy prawa krajowego. W pierwszej kolejności dotyczy to aktualnie obowiązującej Konstytucji Rzeczypospolitej Polskiej uchwalonej 2 kwietnia 1997r przez Zgromadzenie Narodowe i zatwierdzonej w ogólnonarodowym referendum 25 maja 1997 r. W związku z prowadzoną analizą wskazać

[9] Zob. *Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 16 grudnia 1966 r.* (D z. U. z 1977 r. nr 38, poz. 167).

[10] *Karta Praw Podstawowych Unii Europejskiej*,(Dz.U.UE.C.2016.202.389).

[11] Zob. Tamże.

[12] *Karta Praw Podstawowych Unii Europejskiej,* (Dz.U.UE.C.2016.202.389).

[13] *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 poz. 119 nr 1).

trzeba na treść art.49 w którym zawarte są gwarancje dla wolności komunikowania się oraz jej ochrony. Bardzo ważne są także przepisy art. 51 zgodnie z którymi:

-wyłącznie w trybie ustawowym można zobowiązać jednostkę do ujawniania informacji na jej temat;

-prawo władz publicznych do pozyskiwania, gromadzenia i udostępniania informacje o obywatelach ogranicza się do takiego zakresu, który jest niezbędny dla demokratycznego państwa prawnego;

-każdemu przysługuje prawo dostępu do dokumentów urzędowych i zbiorów danych go dotyczących;

-każda osoba ma prawo do prostowania oraz usuwania informacji na jej temat o ile są one nieprawdziwe, niepełne lub zebrane w sposób sprzeczny z prawem [14].

Istotne dla bezpieczeństwa informacyjnego jednostki są również przepisy artykułu 54, stanowiące , że każdemu zapewnia się wolność pozyskiwania i rozpowszechniania informacji przy jednoczesnym zakazie stosowania cenzury prewencyjnej środków społecznego przekazu oraz koncesjonowania prasy [15]. Następnie w art.61 zapisano prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne a także dostępu do dokumentów oraz wstępu na posiedzenia kolegialnych organów władzy publicznej pochodzących z wyborów. Do regulacji konstytucyjnych dotyczących bezpieczeństwa informacyjnego jednostki należy także przepis art. 74 mówiący o tym, że „każdy ma prawo do informacji o stanie i ochronie środowiska”[16].

Kwestie dotyczące bezpieczeństwa informacyjnego jednostki regulują również ustawy zwykle. Najważniejsza grupa przepisów znajduje się w:

-ustawie z dnia 26 stycznia 1984 r. Prawo prasowe[17];

[14] Zob. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r*., (Dz.U.1997, nr 78, poz.483.).

[15] Zob. Tamże.

[16] Zob. Tamże.

[17] *Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe* (Dz. U. 1984 Nr 5 poz. 24). Art. 1. tej ustawy stanowi „Prasa, zgodnie z Konstytucją Rzeczypospolitej Polskiej, korzysta z wolności wypowiedzi i urzeczywistnia prawo obywateli do ich rzetelnego informowania, jawności życia publicznego oraz kontroli i krytyki społecznej”.

- ustawie z dnia 29 grudnia 1992 r. o radiofonii i telewizji[18];

-ustawie z dnia 6 września 2001r. o dostępie do informacji publicznej[19];

-ustawie z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko[20];

-ustawie z dnia 9 kwietnia 2010r.o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych[21];

- ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych [22];

-ustawie z dnia 10 maja 2018r.o ochronie danych osobowych[23];

- ustawie z dnia 6 czerwca 1997 r. - Kodeks karny (Rozdział XXXIII Przestępstwa przeciwko ochronie informacji oraz Rozdział XXXIV Przestępstwa przeciwko wiarygodności dokumentów,) [24].

W oparciu o przedstawione powyżej ustalenia można stwierdzić że obszar bezpieczeństwa informacyjnego jednostki wytyczają następujące składniki :

-zapewnienie swobody pozyskiwania, gromadzenia oraz transferu informacji;

-ochrona przed bezprawną ingerencją w sferę informacji dotyczących życia osobistego;

- prowadzenie racjonalnej polityki dotyczącej oznaczania informacji jako tajne, poufne czy zastrzeżone;

-zagwarantowanie wolności i tajemnicy komunikowania się;

---

[18] *Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji*(Dz. U. 1993 nr 7 poz. 34).

[19] *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej*, (Dz. U. 2001, nr 112, poz. 1198).

[20] *Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko*,(Dz. U. 2008, nr 199, poz. 1227).

[21] *Ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych* ,(Dz. U. 2010, nr 81, poz. 530).

[22] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, (Dz. U. 2010, nr 182, poz. 1228).

[23] *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. 2018 poz. 1000).

[24] *Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny* (Dz. U. 1997 nr 88 poz. 553).

-zapewnienie dostępu do informacji dobrej jakości (aktualnej, rzetelnej i integralnej);

-karne ściganie przestępstw przeciwko informacji i wiarygodności dokumentów.

W wyniku przeprowadzonych analiz można przyjąć że bezpieczeństwo informacyjne jednostki jest stanem i procesem w ramach których ma ona zapewnioną swobodę pozyskiwania, gromadzenia oraz wymiany wysokiej jakości informacji. Towarzyszy temu wyodrębnianie na gruncie prawnym informacji podlegających różnym formom reglamentacji i ochrony podyktowanych potrzebami zapewnienia bezpieczeństwa tej jednostce lub innym podmiotom [25].

Zapewnienie tak zdefiniowanego bezpieczeństwa informacyjne jednostki wiąże się zarówno z przestrzeganiem norm obowiązującego prawa jak i ze skutecznym zapobieganiem i zwalczaniem pojawiających się w tej sferze zagrożeń. Zważywszy na szczególne znaczenie danych osobowych dla funkcjonowania każdej jednostki ludzkiej skuteczna ich ochrona stanowi jedno z ważniejszych zadań w ramach zmagań o kształtowanie odpowiedniego poziomu informacyjnego wymiaru bezpieczeństwa tejże jednostki a tym samym także jej bezpieczeństwa personalnego.

Istota naruszenia ochrony danych osobowych

Jednym z wymogów dotyczących przetwarzania danych osobowych jest obowiązek realizowania tej czynności z wykorzystaniem odpowiednich środków technicznych i organizacyjnych, w taki sposób, aby zapewnić bezpieczeństwo tych danych i zagwarantować ochronę przed przetwarzaniem niedozwolonym lub niezgodnym z prawem oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem. Zgodnie z definicją zawartą w art. 4 , Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. naruszenie ochrony danych osobowych oznacza „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”[26]. W praktyce naruszenie

[25] Zob. W. Fehler, *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021,s.199.

[26] *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 poz. 119 nr 1).

oznacza zatem utratę określonych atrybutów danych osobowych, tj. ich poufności, integralności lub dostępności.

Poufność jest rozumiana jako ochrona informacji przed nieautoryzowanym ujawnieniem (odczytem) osobom do tego nieuprawnionym oraz przed nieautoryzowanym i nieuzasadnionym użyciem[27]. Naruszenie poufności oznacza niedozwolone lub przypadkowe ujawnienie, ale także umożliwienie nieuprawnionego dostępu do danych osobowych[28]. Integralność informacji to cecha oznaczająca jej dokładność, kompletność i merytoryczną poprawność w stosunku do oczekiwań odbiorcy. W kontekście ochrony danych osobowych jest rozumiana jako nienaruszalność, czyli skuteczna ochrona danych przed ich nieautoryzowaną zmianą (de facto więc dostępem do ich zapisu). Naruszeniem integralności danych osobowych jest zdarzenie, w wyniku którego dochodzi do ich nieuprawnionej, niedozwolonej, ale również przypadkowej modyfikacji. Dostępność informacji oznacza, że informacja jest dostępna i użyteczna na żądanie odbiorcy, zaś dostęp do niej jest niezakłócony – zarówno w chwili bieżącego żądania, jak i w dalszej perspektywie czasowej. Innymi słowy, jest to zapewnienie możliwości uzyskania terminowego i niezawodnego dostępu do informacji oraz korzystania z niej. Naruszenie dostępności należy rozumieć jako przypadkową lub niedozwoloną utratę dostępu do danych osobowych lub ich zniszczenie. Istotne jest również to, czy utrata miała charakter trwały. W tym kontekście należy podkreślić różnicę pomiędzy zniszczeniem a utratą danych. Zniszczenie oznacza, że dane przestają istnieć, zaś ich odzyskanie jest niemożliwe lub wymaga podjęcia bardzo skomplikowanych działań, co nierzadko wiąże się z koniecznością wysokich nakładów finansowych. Utrata danych to sytuacja, w której dane nadal istnieją i funkcjonują w obiegu , ale administrator przestaje mieć kontrolę zarówno nad nimi, jak i nad sposobem ich wykorzystywania. W tym przypadku naruszenie może oznaczać zarówno utratę dostępności, jak i poufności danych. W zależności od okoliczności zdarzenia, naruszenie może dotyczyć jednocześnie wszystkich trzech atrybutów bezpieczeństwa danych osobowych, ale zdarzają się również sytuacje, w których dochodzi do naruszeń w dowolnych ich konfiguracjach.

[27] Zob. IT Governance Institute, *COBIT 4.1. Metodyka. Cele kontrolne. Wytyczne zarządzania. Modele dojrzałości,* Rolling Meadows 2010, s. 3.

[28] Zob. *Wytyczne dotyczące zgłaszania naruszenia ochrony danych osobowych na mocy rozporządzenia 2016/679, Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.*, s. 7. https://iod.uj.edu.pl/documents/138774264/138805617/Wytyczne_dotycz%C4%85ce_zg%C5%82aszania_naruszenia_ochrony_danych_osobowych_na_mocy_RODO.pdf/f7fec666-8ba4-49d8-a9c0-f258cff67e50 [dostęp: 7.03.2023].

Konsekwencje naruszenia ochrony danych osobowych

Motyw 85 preambuły RODO wskazuje, że skutkiem braku odpowiedniej i szybkiej reakcji na naruszenie ochrony danych osobowych może być szkoda wyrządzona osobie fizycznej, nie tylko o charakterze majątkowym, ale również niemajątkowym, w postaci: utraty kontroli nad własnymi danymi osobowymi, ograniczenia praw, dyskryminacji, kradzieży lub sfałszowania tożsamości, straty finansowej, nieuprawnionego odwrócenie pseudonimizacji, naruszenia dobrego imienia, naruszenia poufności danych osobowych chronionych tajemnicą zawodową lub wszelkich innych „ znacznych szkód gospodarczych lub społecznych”[29]. Jeżeli chodzi o pierwszą, spośród wymienionych możliwych konsekwencji naruszenia ochrony danych osobowych czyli utratę kontroli nad własnymi danymi osobowymi to lista potencjalnych konsekwencji wynikających z braku sprawowania takiej kontroli w wyniku utraty poufności jest rozległa. Niewątpliwie trzeba na niej umieścić m.in. możliwość wykorzystania danych do założenia na osobę konta internetowego (np. w mediach społecznościowych), podszycia się pod osobę – lub instytucję – i podjęcie czynności w celu wyłudzenia dodatkowych informacji (np. szczegółów karty kredytowej, danych do logowania, danych wrażliwych), czy wykorzystania pozyskanych danych do zarejestrowania przedpłaconej karty telefonicznej, która może zostać użyta do celów niezgodnych z prawem. Warto podkreślić, że świadomość jednostki że nie ma ona pełnej kontroli nad własnymi danymi osobowymi, które teoretycznie mogą zostać wykorzystane w celach bezprawnych, może negatywnie oddziaływać jej stan zdrowia. Stres wywołany nawet pozornie mało istotnym naruszeniem może wpłynąć negatywnie nie tylko na bieżące samopoczucie ale w dalszej perspektywie także na zdrowie psychiczne, zwłaszcza, gdy dotyka on osób starszych lub bardzo wrażliwych emocjonalnie. W skrajnych przypadkach naruszenie może doprowadzić pośrednio nawet do samobójczej śmierci osoby, której ono dotknęło, np. w sytuacji nieradzenia sobie z poważną stratą finansową będącą konsekwencją kradzieży tożsamości. Dlatego tak istotne jest, aby z chwilą stwierdzenia wysokiego ryzyka naruszenia praw i wolności osób fizycznych w konsekwencji naruszenia, administrator niezwłocznie powiadomił o tym zdarzeniu osobę, której naruszenie dotyczy i przedstawił jej możliwości przeciwdziałania i minimalizacji negatywnych konsekwencji poprzez podjęcie działań zabezpieczających. Czynności

[29] Zob. *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 poz. 119 nr 1Dz.U.UE.L.2016 poz. 119 nr .

prewencyjne powinny być zawsze adekwatne do charakteru naruszenia oraz zakresu ujawnionych, zmienionych lub utraconych danych. Najczęściej zalecane w tego typu sytuacjach działania to: założenie konta w systemie informacji kredytowej lub gospodarczej i monitorowanie ewentualnych prób zaciągnięcia zobowiązań finansowych, zastrzeżenie i wymiana dokumentów potwierdzających tożsamość, ignorowanie nieoczekiwanej korespondencji od nieznanych nadawców, a także zachowanie szczególnej ostrożności w rozmowach telefonicznych i internetowych z osobami nieznajomymi lub podającymi się za przedstawicieli różnych instytucji - zwłaszcza gdy proszą one o podanie danych osobowych.

Konsekwencje utrudniające zachowanie kontroli nad własnymi danymi osobowymi mogą powstać także na gruncie ograniczenia przysługujących osobie praw wynikających z art. 15-22 RODO, tj. prawa dostępu do danych osobowych, ich sprostowania, usunięcia, przeniesienia, ograniczenia przetwarzania, zgłoszenia sprzeciwu wobec ich przetwarzaniu, a także niepodlegania decyzji wynikającej ze zautomatyzowanego przetwarzania jej danych.

Istotą prawa dostępu do danych jest uprawnienie osoby, której one dotyczą, do uzyskania od administratora potwierdzenia, czy przetwarza on dane osobowe jej dotyczące, dostępu do danych osobowych (w każdej formie) oraz informacji w zakresie obejmującym: cele przetwarzania, kategorie przetwarzanych danych osobowych, odbiorców, którym dane były lub mogą być ujawnione, planowany okres przechowywania danych osobowych (oraz w miarę możliwości kryteria ustalania tego okresu), informacje o prawie do żądania od administratora sprostowania, usunięcia, ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, informację o prawie złożenia skargi do organu nadzorczego, źródło pozyskania danych (jeśli nie zostały zebrane od osoby, której dane dotyczą), informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowania. Jednocześnie administrator powinien dostarczyć osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu[30].

Zgodnie z prawem do sprostowania danych, osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego sprostowania swoich danych, które są nieprawidłowe. Ponieważ zakres przetwarzanych danych musi być adekwatny do celu administratora, osoba może również żądać uzupełnienia niekompletnych danych jej dotyczących, pod warunkiem

[30] Zob. M. Szkutnik, *Realizacja praw osób których dane dotyczą zgodnie z RODO - praktyczne aspekty,* https://blog-daneosobowe.pl/wp-content/uploads/2019/02/2019.02.11-Realizacja-praw-os%C3%B3b-kt%C3%B3rych-dane-dotycz%C4%85-zgodnie-z-RODO-praktyczne-aspekty.pdf [dostęp 10.03.2023].

uwzględnienia celów przetwarzania. Prawo do usunięcia danych (tzw. prawo do bycia zapomnianym) polega na możliwości żądania przez osobę fizyczną niezwłocznego usunięcia dotyczących jej danych osobowych, przetwarzanych przez administratora. W art. 17 RODO wskazano konkretne okoliczności, w których żądanie to powinno zostać zrealizowane (np. dane nie są już niezbędne do celów, dla których zostały zebrane; osoba cofnęła zgodę na ich przetwarzanie i nie ma innej podstawy ich przetwarzania; osoba wnosi sprzeciw wobec przetwarzania; dane przetwarzano niezgodnie z prawem).

Prawo to nie przysługuje osobie, jeśli przetwarzanie jej danych jest niezbędne: do korzystania z prawa do wolności wypowiedzi i informacji; do realizacji obowiązku prawnego spoczywającego na administratorze; do ustalenia, dochodzenia lub obrony roszczeń; do celów archiwalnych, naukowych, historycznych lub statystycznych; ze względu na interes publiczny w dziedzinie zdrowia publicznego.

Prawo do przeniesienia danych osobowych polega na możliwości przeniesienia danych od jednego administratora do drugiego, co pomaga rozwijać konkurencyjność rynku. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie te dane, które dostarczyła administratorowi (tj. te, które sama podała) i ma prawo przesłać je innemu administratorowi. Jeśli jest to technicznie możliwe, to osoba może również zażądać, aby pierwotny administrator sam przesłał te dane innemu administratorowi. Warunkiem realizacji tego prawa jest przetwarzanie danych na podstawie zgody osoby lub umowy oraz przetwarzanie danych w sposób zautomatyzowany, tj. tylko w systemach informatycznych.

Istotą prawa do ograniczenia przetwarzania danych jest możliwość żądania od administratora oznaczenia przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Warunki realizacji tego prawa obejmują: kwestionowanie prawidłowości danych przez osobę fizyczną (ograniczenie następuje wówczas na czas ich weryfikacji); przetwarzanie niezgodnie z prawem; potrzebę zachowania danych do ustalenia, dochodzenia lub obrony roszczeń przez osobę; sprzeciw wobec przetwarzania danych (ograniczenie do czasu stwierdzenia zasadności podstaw przetwarzania). Administrator może wówczas czasowo przenieść wybrane dane do innego systemu przetwarzania, ograniczyć uprawnienia użytkowników do ich przetwarzania lub czasowo usunąć dane opublikowane na stronie internetowej.

Osoba, której dane dotyczą, ma również prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych, jeśli administrator przetwarza je na podstawie prawnie uzasadnionych interesów albo w celu wykonania zadania realizowanego w interesie publicznym lub w ramach powierzonej mu władzy publicznej. Warunkiem realizacji żądania jest wykazanie jej szczególnej sytuacji, w tym profilowania na podstawie tych przepisów. Administrator musi wówczas zaprzestać przetwarzania tych danych, chyba że wykaże, iż istnieją ważne i prawnie uzasadnione podstawy do ich przetwarzania, które będą nadrzędne wobec interesów, praw i wolności wnioskodawcy. Sprzeciw osoby będzie skuteczny również w sytuacji, w której jej dane są przetwarzane na potrzeby marketingu bezpośredniego.

Osobie fizycznej przysługuje także prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, jeśli decyzja taka ocenia jej czynniki osobowe i wywołuje wobec niej skutki prawne lub generuje podobny, istotny wpływ (np. powoduje automatyczne odrzucenie wniosku, wykluczenie z rekrutacji, itd.). Żądanie nie będzie zrealizowane, jeśli: owa decyzja jest niezbędna do zawarcia lub wykonania umowy osoby z administratorem; decyzja opiera się na zgodzie osoby; decyzja jest dozwolona prawem, któremu podlega administrator, a prawo to przewiduje właściwe środki ochrony praw, wolności i interesów osoby, której dane dotyczą.

Naruszenie integralności lub dostępności danych osoby fizycznej może spowodować, że administrator nie będzie w stanie prawidłowo zidentyfikować osoby, której dane dotyczą, a która wnioskuje o realizację przysługujących jej praw. W konsekwencji niemożliwa lub utrudniona będzie weryfikacja posiadanych przez administratora zbiorów pod kątem występowania w niej danych dotyczących wnioskodawcy.

Nie ulega wątpliwości, że utrata dostępu do danych osobowych przez określony czas stanowi naruszenie, ponieważ brak dostępu do nich może mieć istotny wpływ na prawa i wolności osób fizycznych. Przykładem jest ograniczenie możliwości realizacji przez osobę, której dane dotyczą, przysługujących jej praw wynikających z przepisów innych niż tylko te dotyczące danych osobowych**.** Należy w tym miejscu przypomnieć, że bardzo częstym warunkiem realizacji szeregu praw przysługujących konkretnemu człowiekowi jest możliwość potwierdzenia jego tożsamości. Podobnie jest w przypadku praw wynikających z RODO, naruszenie dostępności lub integralności danych osoby fizycznej może skutkować uniemożliwieniem realizacji jej praw wynikających z innych przepisów, utrudnieniami w ich przestrzeganiu lub wydłużeniem czasu ich wykonania. Skrajnym przypadkiem może być

sytuacja braku dostępu do danych medycznych w szpitalu i w konsekwencji np. odwołanie planowych zabiegów i operacji, co z kolei stwarza ryzyko zagrożenia dla zdrowia i życia .

Kolejnym negatywnym następstwem naruszenia może być dyskryminacja, rozumiana jako zjawisko polegające na niesprawiedliwym i nieobiektywnym różnicowaniu osób fizycznych lub grup społecznych. Aleksandra Winiarska i Witold Klaus wskazują, że dyskryminacja to forma nieusprawiedliwionego okolicznościami nierównego traktowania, które charakteryzuje się długotrwałością i celowością, zaś jego podstawą jest posiadanie określonej cechy przez daną osobę lub grupę[31]. Przepisy ustawy z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania wyróżniają dyskryminację bezpośrednią oraz pośrednią. Pierwsza z nich oznacza „sytuację, w której osoba fizyczna ze względu na płeć, rasę, pochodzenie etniczne, narodowość, religię, wyznanie, światopogląd, niepełnosprawność, wiek lub orientację seksualną jest traktowana mniej korzystnie niż jest, lub byłaby, traktowana inna osoba w porównywalnej sytuacji”[32]. Z kolei dyskryminacja pośrednia to sytuacja, w której dla osoby fizycznej ze względu na te same czynniki, „na skutek pozornie neutralnego postanowienia, zastosowanego kryterium lub podjętego działania występują, lub mogłyby wystąpić, niekorzystne dysproporcje lub szczególnie niekorzystna dla niej sytuacja, chyba że postanowienie, kryterium lub działanie jest obiektywnie uzasadnione ze względu na zgodny z prawem cel, który ma być osiągnięty, a środki służące osiągnięciu tego celu są właściwe i konieczne” [33] . Katalog czynników dyskryminacyjnych wskazany w art. 3 przywołanej ustawy pokrywa się w dużej mierze z katalogiem danych osobowych podlegających szczególnej ochronie, ujętym w art. 9 ust. 1. RODO, który co do zasady zabrania przetwarzania danych osobowych „ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby”[34],

[31] Zob. A. Winiarska, W. Klaus, *Dyskryminacja i nierówne traktowanie jako zjawisko społeczno-kulturowe,* „Studia BAS”, 2011, nr 2(26), s. 11.

[32] *Ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania,* (Dz.U.2020 poz. 2156).

[33] Ibidem.

[34] *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 poz. 119 nr 1).

wskazując jednocześnie przesłanki, kiedy przetwarzanie to jest dopuszczalne. Poważnymi i często spotkanymi czynnikami niedozwolonego zróżnicowanego traktowania są również płeć oraz wiek. Ujawnienie określonych danych, cech lub stanu zdrowia osoby, której dane dotyczą, może skutkować m.in. wyeliminowaniem jej np. z procesu rekrutacyjnego potencjalnego pracodawcy, obniżeniem pozycji na liście rekrutacyjnej uczelni, czy też ostracyzmem ze strony współpracowników. Należy również zauważyć, że rozwój nowych technologii, w tym coraz bardziej powszechne usprawnianie i wspieranie procesów decyzyjnych stosowaniem algorytmów i systemów automatycznego podejmowania decyzji, skutkuje pojawieniem się problemu tzw. dyskryminacji automatycznej, czyli nierównego traktowania jednostek należących do marginalizowanych grup społecznych w wyniku zautomatyzowanej decyzji. Ten rodzaj dyskryminacji nie stanowi jednak konsekwencji naruszenia ochrony danych osobowych, ale ich legalnego przetwarzania w określony sposób, a co za tym idzie – nie jest przedmiotem dalszej analizy.

Jedną z najpoważniejszych konsekwencji naruszenia danych osobowych może być kradzież lub sfałszowanie tożsamości. Biorąc pod uwagę, że tożsamość oznacza cechy i dane personalne konkretnej osoby, które pozwalają ją zidentyfikować, to kradzież tożsamości należy rozumieć jako bezprawne wejście w posiadanie danych osobowych innej osoby i wykorzystanie ich wbrew jej woli. Kradzież tożsamości została spenalizowana i wprowadzona do Kodeksu karnego w 2011 r. Zgodnie z art. 190a § 2 wspomnianego Kodeksu kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej podlega karze pozbawienia wolności do lat 3[35]. Kradzież tożsamości czy jej sfałszowania otwiera możliwości podjęcia licznych działań powodujących szkody materialne i niematerialne dla osoby, której dane zostały wykorzystane. Katalog możliwych konsekwencji w tym obszarze obejmuje m.in.: próby uzyskania dostępu do systemów obsługujących świadczenia medyczne i pozyskanie informacji o stanie zdrowia osoby; ukrywanie swojej tożsamości przy ponoszeniu konsekwencji nieuprawnionego działania (np. otrzymywaniu mandatu); sfałszowanie dokumentów (w formie tzw. „dokumentów kolekcjonerskich") i posługiwanie się podrobionymi egzemplarzami w czynnościach prawnych; założenie konta bankowego i używania go np. w procesie prania brudnych pieniędzy); zawarcie umowy z operatorem telekomunikacyjnym. Mniej dolegliwy charakter może mieć np. założenie fałszywego konta lub profilu internetowego. Osoba

[35] Zob. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*, (Dz. U. 2022 poz. 1726).

podszywająca się pod właściciela danych może np. zamieszczać w sieci obraźliwe, często nieprawdziwe informacje, opinie lub komentarze, szerzyć dezinformację, propagować nielegalne zachowania i treści czy naruszać dobre imię innych osób. Fałszywe konto może zostać również wykorzystane do wyłudzania pomocy materialnej i realizacji oszustw finansowych, za które odpowiedzialność – do momentu wyjaśnienia wszystkich okoliczności – będzie przypisywana prawdziwej osobie, której dane dotyczą.

Wymierną konsekwencją kradzieży tożsamości może być spowodowanie straty finansowej na szkodę właściciela danych. Katalog możliwych strat uzależniony jest od zakresu ujawnionych danych, jakości podrobionych dokumentów, kreatywności i zdolności socjotechnicznych osoby, która weszła w posiadanie danych oraz wiedzy i czujności instytucji umożliwiających stworzenie zobowiązania. Osoby nieuczciwe mogą m.in. podjąć próbę uzyskania na szkodę osoby pożyczek w instytucjach finansowych (głównie parabankowych), np. przez Internet lub telefonicznie, ale również osobiście – z wykorzystaniem „dowodu kolekcjonerskiego". Ujawnione dane mogą posłużyć również m.in. do: prób zakupu towarów w systemie ratalnym, wyłudzenia ubezpieczenia, prowadzenia fałszywej działalności biznesowej (i np. wyłudzenia zwrotu podatku), zawarcia umów cywilno-prawnych (np. najmu nieruchomości), wynajęcia mieszkania (lub pokoju hotelowego) i kradzieży jego wyposażenia, wypożyczenia sprzętu lub auta i ich kradzieży lub prób zbycia mienia (w tym również nieruchomości) należącego do osoby, której dane dotyczą.

Stosunkowo rzadko dostrzeganą i analizowaną konsekwencją naruszenia ochrony danych osobowych jest nieuprawnione odwrócenie pseudonimizacji. Dla celów prowadzonych analiz autorzy przyjęli że pseudonimizacja oznacza przetworzenie danych w taki sposób, aby bez użycia dodatkowych informacji nie można ich było już przypisać konkretnej osobie, której dane dotyczą. Dodatkowe informacje powinny być przechowywane osobno i zostać objęte środkami uniemożliwiającymi ich przypisanie do osoby fizycznej. W ujęciu bardziej technicznym, pseudonimizacja oznacza zbiór odwracalnych technik, które polegają na takim przetworzeniu danych osobowych, aby niemożliwe było ich przypisanie do konkretnej osoby. Należy odróżniać ten termin od anonimizacji, która oznacza nieodwracalne przetworzenie danych w taki sposób, aby w efekcie nie można ich było połączyć z żadną konkretną osobą. Pseudonimizacja ma zabezpieczać przed identyfikacją osoby, której dane są przetwarzane. Brak personaliów osoby nie uniemożliwia przypisania jej określonych atrybutów, parametrów czy innych informacji o niej – możliwe jest zatem stworzenie określonego zbioru danych lub ich grup bez wskazywania tożsamości osoby, której one dotyczą. Ponieważ pseudonimizacja

jest procesem odwracalnym, to objęte nią informacje – nawet po zaszyfrowaniu lub zniekształceniu w innej formie – są nadal traktowane jako dane osobowe, a zatem podlegają stosownym regulacjom w tym obszarze[36]. Najpopularniejsze techniki pseudonimizacji danych obejmują: szyfrowanie z kluczem tajnym (np. zamianę posiadanych danych na ciąg cyfr lub liter, możliwy do odszyfrowania wyłącznie na podstawie przechowywanego oddzielnie klucza); funkcję skrótu, w tym również z kluczem (funkcja hashująca, zamieniająca długi ciąg znaków na znacznie krótszy); szyfrowanie deterministyczne (przypisanie losowego numeru jako pseudonimu dla każdego atrybutu w bazie danych i usunięcie wszelkich korelacji) oraz tokenizację (zastąpienie fragmentów danych ciągiem losowych liczb, co sprawia, że informacje stają się bezużyteczne dla osób postronnych). Z uwagi na odwracalność pseudonimizacji, istnieje ryzyko dokonania tego odwrócenia przez osoby nieuprawnione. W zależności od sytuacji, odwrócenie może nastąpić zarówno w wyniku celowego działania, jak i mieć charakter przypadkowy. Wśród celowych działań umożliwiających odwrócenie pseudonimizacji wymienia się: wyodrębnienie (odseparowanie wszystkich lub części informacji pozwalających na identyfikację konkretnej osoby); tworzenie powiązań (zestawienia kilku rekordów dotyczących tej samej osoby – zarówno z jednej, jak i z kilku dostępnych baz danych) oraz wnioskowanie, czyli dedukowanie jednej cechy na podstawie cech opisanych w innym zbiorze[37]. Generalnie – poszczególnym technikom pseudonimizacji odpowiadają liczne zabiegi i narzędzia pozwalające na ich odwrócenie. Przypadkowe odwrócenie pseudonimizacji może nastąpić np. w sytuacji, w której osoba, której dane dotyczą, ma dostęp do zbioru spseudonimizowanych danych i na podstawie dostępnych informacji jest w stanie ustalić, które z nich dotyczą jej, a następnie wywnioskować stosowane kryteria i powiązać ze sobą informacje dotyczące innych osób. Niezależnie od zamiaru osoby, która dokonała odwrócenia pseudonimizacji danych osobowych, działanie to skutkuje możliwością zapoznania się z ich pełną treścią. To z kolei umożliwia wykorzystanie danych w celach nieuprawnionych.

Ujawnienie osobom nieupoważnionym danych osobowych w wyniku naruszenia ich ochrony może skutkować wyjawieniem cech osoby fizycznej lub czynników wpływających na jej sytuację osobistą, zdrowotną, rodzinną, majątkową, itd. Nie można wykluczyć, że udostępnione informacje zostaną wykorzystane do próby naruszenia dobrego imienia osoby,

[36] Zob. P. Jać, *Dane osobowe: szyfrowanie, anonimizacja, pseudonimizacja*, [on-line], LegalHut, 11.02.2020, https://legalhut.pl/blog/branze-nowych-technologii/dane-osobowe-szyfrowanie-anonimizacja-pseudonimizacja, [03.10.2022].

[37] Zob. Ibidem.

której dotyczą. Dobre imię określa się inaczej mianem czci zewnętrznej, która obejmuje m.in. opinię, jaką inne osoby mają o człowieku. Jako dobro osobiste, obejmujące wszystkie dziedziny życia człowieka (w tym w wymiarze osobistym, zawodowym, prywatnym i społecznym), dobre imię podlega ochronie cywilnoprawnej. Pojęcie naruszenia dobrego imienia oznacza zaś pomówienie innej osoby o takie postępowanie lub właściwości, które może poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego w określonym zawodzie, na danym stanowisku lub w konkretnym rodzaju działalności. Zazwyczaj naruszenie tego dobra przejawia się w sformułowaniu negatywnej wypowiedzi, odnoszącej się do danej osoby w związku z różnymi aspektami jej życia, przy czym wypowiedź ta powoduje utratę zaufania do niej. Przykładami naruszenia dobrego imienia mogą być: publikacja obraźliwego komentarza na temat określonej osoby, pomówienie lub wskazanie, że osoba ta dopuściła się takiego czynu, który sprawi, że straci ona zaufanie innych osób co do wykonywanego przez nią zawodu.

Skuteczne wykonywanie czynności w przypadku zawodów zaufania publicznego, np. w kancelariach notarialnych, radcowskich czy adwokackich, wiąże się ze stałym dostępem do pokaźnej bazy danych osobowych, w tym również o charakterze wrażliwym. Obowiązek strzeżenia tajemnicy zawodowej nieodłącznie wiąże się zatem w tym przypadku z zapewnianiem bezpieczeństwa przetwarzanych danych. Tajemnica zawodowa pozostaje pod ochroną przepisów wynikających z ustaw branżowych i odnosi się do dokumentów zawierających treści, o których pracownik dowiedział się w związku z realizowaniem zadań służbowych i które dotyczą przedmiotu świadczonej działalności. Utrata poufności danych osobowych, które są dodatkowo chronione tajemnicą zawodową, może skutkować odpowiedzialnością dyscyplinarną, karną i cywilną[38]. Art. 266 § 1 Kodeksu karnego wskazuje, że kto ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z wykonywaną pracą, pełnioną funkcją lub w ramach sprawowanej działalności publicznej, społecznej, gospodarczej lub naukowej, podlega karze ograniczenia wolności lub jej pozbawienia do dwóch lat[39]. Jeżeli natomiast niedochowanie tajemnicy doprowadziło do naruszenia czci, wizerunku lub innego dobra osobistego, to możliwe konsekwencje takiego działania obejmują również odpowiedzialność cywilną z tytułu bezprawnego naruszenia dobra osobistego[40].

[38] Zob. M. Bidziński, *Tajemnica danych i informacji*, „Edukacja Prawnicza", 2012, nr 11 (137), s. 20-21.
[39] Zob. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*, Dz.U.1997 nr 88 poz. 553, art. 266.
[40] Zob. *Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny*, Dz.U.1964 nr 16 poz. 93, art. 23, 24.

Roszczenia z zakresu ochrony danych osobowych są ściśle powiązane z dobrem osobistym w postaci prawa do prywatności. Trzeba mieć zatem na uwadze, że instytucjonalna ochrona dóbr osobistych jest realizowana poprzez wprowadzenie odpowiednich zakazów i nakazów prawnych, a o bezprawności rozstrzyga nie tyle naruszenie określonego dobra osobistego, co samo zachowanie sprzeczne z normą postępowania. Mimo, że art. 82 RODO nie wskazuje bezpośrednio dóbr osobistych ani rodzajów możliwych roszczeń, to należy przyjąć, że żądanie odszkodowania za doznaną krzywdę stanowi roszczenie majątkowe za szkodę niemajątkową[41].

Należy zauważyć, że naruszenie ochrony danych osobowych może mieć na osobę fizyczną zróżnicowany wpływ, obejmujący aspekty fizyczne, finansowe i emocjonalne[42]. W kategoriach możliwego oddziaływania fizycznego można rozpatrywać zarówno przejściowe dolegliwości wywołane stresem (np. ból głowy), jak również skutki prowadzące do chorób, wypadków czy poważnych dolegliwości powodujących długotrwałą szkodę w postaci pogorszenia zdrowia, zmianę wyglądu fizycznego (np. w wyniku napadu, rozboju, okaleczenia) lub – w skrajnych przypadkach – śmierć. Wpływ fizyczny obejmuje nie tylko dolegliwości zdrowotne, ale również związane z funkcjonowaniem człowieka w otoczeniu społecznym. Przykładem może być brak możliwości sprawowania odpowiedniej opieki wobec osoby zależnej, spowodowany pogorszeniem stanu zdrowia w wyniku stresu, który może być efektem dyskryminacji, naruszenia dobrego imienia, kradzieży tożsamości, itd. Zniesławienie może również skutkować dążeniem do psychologicznej lub fizycznej zemsty na osobie, która przyczyniła się do naruszenia lub wykorzystała w nieuprawnionych celach pozyskane w jego wyniku dane.

Negatywny wpływ finansowy może odnosić się zarówno do wymiernej straty materialnej, jak również do utraty czasu poświęconego np. na ponowne dopełnienie formalności urzędowych związanych z przetwarzaniem danych osobowych lub oczekiwaniem na ich realizację, usuwanie niechcianej korespondencji i wypisywaniem się z niepotrzebnych list mailingowych czy zniesienie blokady dostępu do serwisów internetowych wymagających autoryzacji.

Bezpośrednie konsekwencje finansowe mogą być dużo poważniejsze. Te związane z

[41] Zob. P. Wirska, *Prawo do odszkodowania za naruszenie RODO – tym też powinieneś się martwić, administratorze!*, [on-line], RODO Radar, 08.03.2021, https://rodoradar.pl/prawo-do-odszkodowania-za-naruszenie-rodo-tym-tez-powinienes-sie-martwic-administratorze/ [dostęp 26.02.2023].

[42] Zob. A. Czarnowski, M. Gawroński, *Analiza ryzyka i adekwatność środków czyli bezpieczeństwo danych w świetle RODO,* LEX/el. 2018.[dostęp:2.03.2023]

utrudnieniami z korzystaniu z własnych środków materialnych obejmują najczęściej: blokadę środków na rachunku bankowym, błędne działanie serwisów internetowych w wyniku przetwarzania nieprawidłowych danych (np. trudności w korzystaniu z usług bankowych) oraz ryzyko finansowe. Wyróżnić można także skutki związane z poniesieniem dodatkowych kosztów, takie jak: bezpośrednia utrata pieniędzy w wyniku oszustwa; nieprzewidziane płatności (np. błędnie nałożone kary, koszty sądowe, opłaty manipulacyjne); wzrost kosztów w wyniku podniesionych składek ubezpieczeniowych; sprzeniewierzenie wyłudzonych i niezwróconych pieniędzy; przedłużone problemy finansowe (np. spłata zobowiązań kredytowych); szkoda na mieniu czy znaczące długi. Dotkliwe dla osoby fizycznej skutki naruszenia mogą się również wiązać z materialnym aspektem funkcjonowania w społeczeństwie. W tym kontekście należy wymienić: utratę możliwości odpoczynku (np. konieczność rezygnacji z częściowo opłaconej wycieczki, zakupów, zakończenia użytkowania płatnego konta internetowego); utratę dedykowanych, unikatowych i niepowtarzalnych szans (np. w postaci odmowy udzielenia kredytu hipotecznego – skutkującej koniecznością ponoszenia długotrwałych opłat za wynajem lokalu, odmowy przystąpienia do egzaminu, odmowy przydzielenia praktyk lub stażu, odmowy przyjęcia na studia, do pracy, itd.); utratę możliwości awansu zawodowego; utratę pracy i/lub miejsca zamieszkania; brak możliwości podjęcia pracy; brak możliwości przemieszczania się; utratę dowodów w postępowaniu sądowym; utratę dostępu do strategicznej infrastruktury w postaci wody i elektryczności; separację lub rozwód, a także zakaz wjazdu do danego państwa.

Ostatnia kategoria możliwych negatywnych konsekwencji dla osób fizycznych odnosi się do sfery emocjonalnej. Podobnie jak w aspektach fizycznym i finansowym, wpływ emocjonalny jest zróżnicowany i zależy zarówno od poziomu samego naruszenia jak i profilu osobowości osoby poszkodowanej. W przypadku ograniczonego naruszenia, osoba może w ogóle nie odczuć jego wpływu lub zetknąć się z niewielką liczbą niedogodności, które może łatwo przezwyciężyć. Niedogodności te mogą obejmować w szczególności: irytację związaną otrzymywanymi informacjami lub żądaniem ich udzielenia; obawę przed utratą kontroli nad własnymi danymi osobowymi; poczucie ingerencji w sferę prywatności; poczucie straty czasu na rzecz ponownej konfiguracji danych; wątpliwości co do wolności Internetu spowodowane ograniczeniem dostępu do stron wymagających potwierdzenia wieku. W sytuacji szerszego naruszenia, osoba może napotkać znaczące niedogodności emocjonalne, które jednak powinna przezwyciężyć. Mogą one obejmować np. odmowę dalszego używania określonych systemów (np. w przypadku sygnalistów); niewielkie dolegliwości psychiczne związane ze

zniesławieniem, utratą reputacji, itd.; problemy w relacjach prywatnych lub służbowych (nadszarpnięcie wizerunku, utrata rozpoznawalności) oraz zastraszenie, przede wszystkim w kanałach społecznościowych. Znaczące naruszenie może spowodować, że osoba nim dotknięta będzie musiała borykać się z rozległymi konsekwencjami, którymi mogą być: poważne dolegliwości psychiczne (np. fobia, depresja, itp.); poczucie naruszenia sfery prywatności i poczynienia w niej nieodwracalnych szkód; zasłabnięcie w wyniku stresu spowodowanego otrzymaniem wezwania do sądu; poczucie naruszenia elementarnych praw człowieka (np. wolności wypowiedzi, zakazu dyskryminacji); różne formy szantażu, cyberprzemocy lub nękania. Przedstawiony podział konsekwencji emocjonalnych dla jasności wywodu oparto o pewien schemat. Jednak trzeba pamiętać (o czym już wspomniano) ,że istotne w tym kontekście są cechy osobowości i psychiki jednostki które powodują że nawet ograniczone naruszenia w przypadku osób wrażliwych i mało odpornych na stres mogą zrodzić poważne konsekwencje.

Wnioski

Przeprowadzone analizy dotyczące konsekwencji jakie dla bezpieczeństwa informacyjnego jednostki rodzą lub mogą rodzić naruszenia ochrony danych osobowych pozwalają sformułować wniosek, że obejmują one stosunkowo szeroki zakres negatywnych skutków . Co więcej ze względu na postępujące procesy digitalizacji i automatyzacji gromadzenia przesyłania i przetwarzania danych zwiększają się potencjalne możliwości pojawiania się negatywnych zdarzeń inicjowanych nie tylko intencjonalnymi działaniami ludzi ale także w wyniku niesprawności sprzętu i infrastruktury informatycznej. W związku z tym pojawia się kolejny wniosek mówiący o tym ,że każde negatywne zdarzenie w analizowanym obszarze powinno zawsze być dokładnie zbadane przez administratora pod kątem potencjalnego bezpośredniego i pośredniego wpływu na bezpieczeństwo osoby, której naruszenie ochrony danych dotyczyło. Należy podkreślić, że zaklasyfikowanie zdarzenia jako naruszenia wymaga spełnienia łącznie trzech przesłanek. Po pierwsze, naruszenie musi dotyczyć danych osobowych przetwarzanych przez podmiot. Po drugie, zdarzenie musi mieć konkretny skutek w postaci zniszczenia, utraty, zmiany, ujawnienia lub dostępu do danych osobowych. Ostatnim kryterium jest przyczyna naruszenia w postaci złamania zasad bezpieczeństwa danych. Prawidłowa ocena zdarzenia, z uwzględnieniem jego okoliczności, pozwoli podjąć skuteczne działania nie tylko w celu dopełnienia obowiązków formalnych związanych z poinformowaniem o naruszeniu organu nadzorczego, ale również na rzecz

zmniejszenia ryzyka materializacji tego naruszenia w przyszłości, minimalizacji skutków zdarzenia i ograniczenia negatywnego wpływu na osobę, której dane dotyczą.

Streszczenie:

Celem artykułu jest ustalenie i przedstawienie możliwych konsekwencji naruszenia ochrony danych osobowych na skutek zaistnienia czynów lub zdarzeń prowadzących do przypadkowego lub niezgodnego z prawem ich niszczenia, utraty, modyfikacji, nieuprawnionego ujawniania lub dostępu dla informacyjnego bezpieczeństwa jednostki. Zasadnicza hipoteza stanowiąca podstawę prowadzonych analiz zawiera sie w stwierdzeniu, że naruszenia ochrony danych osobowych generują w różnych aspektach zagrożenia dla informacyjnego wymiaru bezpieczeństwa jednostki a w konsekwencji także dla innych składników jej bezpieczeństwa. Podstawową metodą zastosowaną przez autorów jest metoda analizy prawnej. Jej użycie pozwoliło wyspecyfikować węzłowe kwestie dotyczące zakresu i znaczenia ochrony danych osobowych dla bezpieczeństwa informacyjnego jednostki oraz przedstawić ich postrzeganie z perspektywy obecnie obowiązujących przepisów prawa .W rezultacie przeprowadzonych analiz ustalono, że naruszenie ochrony danych osobowych tworzy szereg zagrożeń dla bezpieczeństwa informacyjnego jednostki które to zagrożenia przekładają się na wiele innych negatywnych skutków godzących w bezpieczną egzystencję i rozwój dotkniętych nimi osób.

W pierwszej części artykułu na tle syntetycznie scharakteryzowanej istoty bezpieczeństwa jednostki przedstawiono propozycję współczesnego pojmowania informacyjnego wymiaru jej bezpieczeństwa oraz sformułowano podstawowy katalog jego uwarunkowań. W dalszej części zawarte zostały analizy dotyczące płaszczyzn naruszeń ochrony danych osobowych. Zostały one ukazane w odniesieniu do takich atrybutów jak poufność, integralność i dostępność. W drugiej części tekstu przedstawiono rozważania dotyczące skutków jakie powstają lub mogą powstawać dla bezpieczeństwa jednostki wskutek naruszenie ochrony dotyczącej jej danych osobowych. Zostały one scharakteryzowane w kontekście: utraty kontroli nad własnymi danymi osobowymi, ograniczenia praw, dyskryminacji, kradzieży lub sfałszowania tożsamości, strat finansowych, nieuprawnionego odwrócenie pseudonimizacji, naruszenia dobrego imienia oraz naruszenia poufności danych osobowych chronionych tajemnicą zawodową. Artykuł zamykają syntetyczne wnioski

podkreślające nie tylko wagę i znaczenie skutecznej ochrony danych osobowych ale także nowe w tym zakresie wyzwania.

Słowa kluczowe:

Bezpieczeństwo jednostki, informacyjne bezpieczeństwo jednostki, ochrona danch osobowych, bezpieczeństwo danych osobowych

Keywords:

Individual security, individual information security, personal data protection, personal data security

Bibliografia:

1. Albert M. Bidziński M., *Tajemnica danych i informacji*, „Edukacja Prawnicza", 2012, nr 11
2. Czarnowski A., Gawroński M., *Analiza ryzyka i adekwatność środków czyli bezpieczeństwo danych w świetle RODO,* LEX/el. 2018. https://sip.lex.pl/komentarze-i-publikacje/komentarze-praktyczne/analiza-ryzyka-i-adekwatnosc-srodkow-czyli-470097897[dostęp 2.03.2023]
3. Drabik K., Pieczywok A., *Bezpieczeństwo i natura człowieka wobec jego alienacji i kryzysu egzystencji*, Warszawa 2022
4. Fehler W., *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021
5. Hampson F.O., *Bezpieczeństwo jednostki* [w:] P. D. Williams (red.) *Studia bezpieczeństwa* , Kraków 2012
6. IT Governance Institute, *COBIT 4.1. Metodyka. Cele kontrolne. Wytyczne zarządzania. Modele dojrzałości,* Rolling Meadows 2010
7. Jać P., *Dane osobowe: szyfrowanie, anonimizacja, pseudonimizacja*, [on-line], LegalHut, 11.02.2020, https://legalhut.pl/blog/branze-nowych-technologii/dane-osobowe-szyfrowanie-anonimizacja-pseudonimizacja, [03.10.2022].
8. Novikova K., Orzyłowska A., J*ednostka ludzka w obliczu zagrożeń współczesności: bezpieczeństwo indywidualne w Polsce. Implikacje metodologiczne* „Journal of Modern Science"2019 nr 1
9. Szkutnik M., *Realizacja praw osób których dane dotyczą zgodnie z RODO - praktyczne aspekty,* https://blog-daneosobowe.pl/wp-content/uploads/2019/02/2019.02.11-Realizacja-praw-os%C3%B3b-kt%C3%B3rych-dane-dotycz%C4%85-zgodnie-z-RODO-praktyczne-aspekty.pdf [dostęp 10.03.2023].
10. Winiarska A., Klaus W., *Dyskryminacja i nierówne traktowanie jako zjawisko społeczno-kulturowe*, „Studia BAS", 2011, nr 2

11. Wirska P., *Prawo do odszkodowania za naruszenie RODO – tym też powinieneś się martwić, administratorze!*, [on-line], RODO Radar, 08.03.2021, https://rodoradar.pl/prawo-do-odszkodowania-za-naruszenie-rodo-tym-tez-powinienes-sie-martwic-administratorze/ [dostęp 26.02.2023].
12. *Powszechna Deklaracja Praw Człowieka* , https://www.unic.un.org.pl/dokumenty/deklaracja.php [dostęp: 11.03.2023]
13. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2.* (Dz.U. 1993r. nr 61,poz. 284).
14. *Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 16 grudnia 1966 r.* (Dz. U. z 1977 r. nr 38, poz. 167).
15. *Karta Praw Podstawowych Unii Europejskiej*,(Dz.U.UE.C.2016.202.389)
16. *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 poz. 119 nr 1).
17. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r*., (Dz.U.1997, nr 78, poz.483.)
18. *Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny*, (Dz.U.1964 nr 16 poz. 93)
19. *Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe* (Dz. U. 1984 Nr 5 poz. 24)
20. *Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji*(Dz.U. 1993 nr 7 poz. 34).
21. *Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny* (Dz. U. 1997 nr 88 poz. 553).
22. *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej*, (Dz. U. 2001, nr 112, poz. 1198)
23. *Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko,*(Dz. U. 2008, nr 199, poz. 1227)
24. *Ustawa z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych* ,(Dz. U. 2010, nr 81, poz. 530).
25. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. 2018 poz. 1000).
26. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,* (Dz. U. 2010, nr 182, poz. 1228).
27. *Ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania,* (Dz.U.2020 poz. 2156).
28. *Wytyczne dotyczące zgłaszania naruszenia ochrony danych osobowych na mocy rozporządzenia 2016/679*, *Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.* https://iod.uj.edu.pl/documents/138774264/138805617/Wytyczne_dotycz%C4%85ce_zg%C5%82aszania_naruszenia_ochrony_danych_osobowych_na_mocy_RODO.pdf/f7fec666-8ba4-49d8-a9c0-f258cff67e50 [dostęp: 7.03.2023].