Agnieszka Stępień-Banach

Bezpieczeństwo danych osobowych w cyberprzestrzeni

Nr 89
Studia i Monografie
Łódź-Warszawa 2019

Społeczna Akademia Nauk
Łódź

Agnieszka Stępień-Banach

Bezpieczeństwo danych osobowych w cyberprzestrzeni

Nr 89
Studia i Monografie
Łódź-Warszawa 2019

Społeczna Akademia Nauk
Łódź

Agnieszka Stępień-Banach

Bezpieczeństwo danych osobowych w cyberprzestrzeni

Monografia recenzowana
dr hab. Weronika Jakubczak
dr hab. inż. Jerzy Zawisza, prof. SAN

Korekta językowa
Paulina Skoczylas

Skład i łamanie
Paweł Bednarek

Projekt okładki
Marcin Szadkowski

Studia i Monografie nr 89

ISBN 978-83-64971-59-4

Wydawnictwo Społecznej Akademii Nauk
Kilińskiego 109
90-011 Łódź
tel. (42)664 22 39
(42) 676 25 29 w. 339

Druk i oprawa
Mazowieckie Centrum Poligrafii
http://www.c-p.com.pl/
e-mail: biuro@c-p.com.pl

Spis treści

Wykaz skrótów

ABI – administrator bezpieczeństwa informacji
ADO – administrator danych osobowych
ASI – administrator systemu informatycznego
CEIDG – Centralna Ewidencja Działalności Gospodarczej
Dz.U. – Dziennik Ustaw
dyrektywa 95/46/WE – dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
EKPC– Europejska Konwencja Praw Człowieka
EOG – Europejski Obszar Gospodarczy
GIODO – Generalny Inspektor Ochrony Danych Osobowych
Grupa Robocza art. 29 – Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana na moc art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
IOD – inspektor ochrony danych osobowych
kc – ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny
KE – Komisja Europejska
kk – ustawa z dnia 6 czerwca 1997 r. – Kodeks karny
Konstytucja RP – Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r.
kp – ustawa z dnia 26 czerwca 1974 r. Kodeks pracy
kpa – ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego
KRS – Krajowy Rejestr Sądowy
OECD – Organizacja Współpracy Gospodarczej i Rozwoju
OchBazDanychU – ustawa z dnia 27 lipca 2001 r. o ochronie baz danych
ONZ – Organizacja Narodów Zjednoczonych
PDPC – Powszechna Deklaracja Praw Człowieka
NSA – Naczelny Sąd Administracyjny
rozporządzenie 2016/679 – 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
UODO – Urząd Ochrony Danych Osobowych
uodo – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
upapp – ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych

UE – Unia Europejska
ŚwiadUsłElektrU – ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną
SN – Sąd Najwyższy
TK – Trybunał Konstytucyjny
TSUE – Trybunał Sprawiedliwości Unii Europejskiej
WSA – Wojewódzki Sąd Administracyjny

Wstęp

Podjęta w niniejszej monografii problematyka bezpieczeństwa danych osobowych w cyberprzestrzeni wzbudza szerokie zainteresowanie zwłaszcza po 25 maja 2018 r., kiedy to zaczęliśmy stosować przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[1]. Cyberprzestrzeń stanowi nowy obszar aktywności człowieka. Chociaż jej powstanie datuje się na lata 60. XX wieku, to dynamiczny rozwój nastąpił w latach 90. XX wieku za sprawą rozpowszechnienia Internetu. Niewątpliwie wpływ na rozwój świata wirtualnego miało „internetowe" pokonanie przez człowieka bariery czasu i przestrzeni. Internet umożliwił komunikowanie się między jego użytkownikami niezależnie od miejsca, w którym bywają oraz pory dnia. Stał się platformą do wymiany myśli i poglądów. Za jego sprawą informacje zyskały zupełnie nowy wymiar, ich pozyskiwanie stało się szybkie i proste. Dostęp do nich przestał być ograniczony. Na tym tle szczególnie cenne okazały się informacje dotyczące poszczególnych osób.

Pojawienie się portali społecznościowych umożliwiło ich użytkownikom nie tylko zdobywanie nowych znajomości, ale także dzielenie się z innymi użytkownikami informacjami na temat życia prywatnego. Informacje, które dotychczas były uznawane za prywatne, przeznaczone dla wybranego wąskiego grona najbliższych członków rodziny, w cyberprzestrzeni udostępniane są z łatwością innym użytkownikom. Dzieje się tak między innymi dlatego, że wielu ludzi uważa cyberprzestrzeń za

1 Dz.Urz. UE L 119 z 04.05.2016.

bastion anonimowości. Tymczasem zbyt łatwe i pochopne dzielenie się w wirtualnym świecie informacjami dotyczącymi każdego aspektu życia użytkownika doprowadziło do redefinicji prawa do prywatności, które obecnie stanowi raczej przywilej, a nie prawo podstawowe. Nieprzemyślane i krótkowzroczne umieszczanie informacji na swój temat stworzyło natomiast wielu innym osobom szansę zysku z gromadzenia informacji na temat użytkowników sieci. Za sprawą Internetu możliwe stało się łączenie informacji o użytkownikach sieci z innymi informacjami, takimi jak odwiedzane strony internetowe, najczęściej wybierane towary czy produkty, tworząc w ten sposób wielkie zbiory danych. Te zaś, zbierane w różnych konfiguracjach prowadzą do powstania zupełnie nowych zestawów danych. Ten proces zdaje się nie mieć końca.

Rozwój technologiczny sprawił, że możliwe stało się także gromadzenia informacji na temat użytkowników bez ich wiedzy. Wykorzystywanie plików cookies, geolokalizacji czy telefonów to tylko nieliczne sposoby do osiągnięcia tego celu. Za sprawą zbieranych w ten sposób informacji można tworzyć profile użytkowników, zawierające informacje nie tylko na temat tego, co internauci oglądają, gdzie przebywają, ale także tego, co i gdzie jedzą, co czytają, w jakich sklepach się ubierają. Wszystkie tego rodzaju informacje, zgodnie z definicją danych osobowych, pozwalają na bezpośrednie lub pośrednie zidentyfikowanie osoby fizycznej, a co za tym idzie – podlegają ochronie prawnej.

Funkcjonowanie w cyberprzestrzeni uświadomiło międzynarodowej społeczności, że niezbędne jest zapewnienie bezpieczeństwa jej użytkownikom. W ocenie autora należy włożyć o wiele więcej wysiłku w działania ochronne w świecie wirtualnym niż realnym, pomimo swoistej równoległości obu tych obszarów naszej codziennej egzystencji. Dzieje się tak dlatego, że cyberprzestrzeń w radykalny sposób różni się od rzeczywistości. Stosowanie takich samych regulacji prawnych w świecie rzeczywistym i świecie wirtualnym może okazać się niewystarczające. Świadczy o tym chociażby fakt, że informacje zamieszczane w sieci nie przedawniają się – „Internet nie zapomina". Jest to zasadnicza różnica wobec konstrukcji zatarcia skazania stosowanej w prawie karnym.

Wychodząc naprzeciw oczekiwaniom użytkowników, podejmowane są działania legislacyjne dążące do zapewnienia jednostce jak największego bezpieczeństwa w świecie wirtualnym. Znaczącym krokiem w tym zakresie było wejście w życie rozporządzenia 2016/679. Chociaż problematyka ochrony danych osobowych jest równie młoda jak sam Internet, dopiero teraz udało się wypracować przepisy prawne gwarantujące jednostce ochronę w tym obszarze. Wydaje się to szczególnie ważne wobec faktu, że dane osobowe w XXI wieku są równie cenne jak pieniądze.

Rozporządzenie 2016/679 nakierowane jest na dążenie do zapewnienia osobom fizycznym bezpieczeństwa w zakresie przetwarzania ich danych osobowych.

Prawodawca unijny skupia się przede wszystkim na zapewnieniu transparentności procesu przetwarzania danych. W związku z tym osoba, której dane dotyczą, powinna mieć świadomość, w jakich procesach jej dane osobowe biorą udział, w jakim celu są wykorzystywane, jak długo będą przetwarzane oraz co się z nimi dzieje po zakończeniu procesu przetwarzania. W celu umożliwienia jednostce realizacji przysługujących jej praw wyposażono ją w instrumenty prawne pozwalające na weryfikowanie tego procesu, a na administratorów danych osobowych nałożono obowiązek rozliczenia się z procesu przetwarzania danych nie tylko przed osobą, której dane dotyczą, ale także przed organem nadzorczym. Niewłaściwe przetwarzanie danych osobowych lub działanie bez podstawy prawnej zagrożone jest bardzo wysokimi karami, które mają odstraszać ADO przed działaniami niezgodnymi z prawem.

Cyberprzestrzeń daje użytkownikom nieograniczone możliwości. Pozwala przełamywać bariery i ograniczenia. Staje się także obszarem aktywności nowych, nieznanych dotąd zagrożeń, które nie występowały dotychczas w świecie rzeczywistym. Te zaś, które zostały przeniesione ze świata realnego w cyberprzestrzeń mają zupełnie nowy, szerszy wymiar i spektrum oddziaływania. W ocenie autora szczególnie niebezpieczne są te zagrożenia, w których wykorzystywane są dane osobowe użytkowników. Dlatego też niezbędne jest wypracowanie mechanizmów prawnych zapewniających jednostce bezpieczeństwo.

Przedmiotem badań jest bezpieczeństwo jednostki w cyberprzestrzeni analizowane pod kątem ochrony jej danych osobowych. Jak zostało zauważone na wstępie, cyberprzestrzeń stała się nowym obszarem wymagającym zapewnienia bezpieczeństwa. W ostatnich latach pojęcie „bezpieczeństwo" bardzo się rozwinęło. Ma charakter interdyscyplinarny i przez przedstawicieli doktryny jest różnie definiowane. Podlega też licznym podziałom. Szczególnie widoczne jest to na płaszczyźnie podmiotowej i przedmiotowej, obejmuje nowe aspekty życia politycznego, gospodarczego i społecznego. Etymologicznie słowo bezpieczeństwo wywodzi się z języka łacińskiego (sine cura curia) i najczęściej tłumaczone jest jako stan beztroski, niepokoju, zmartwienia[2]. Chociaż w literaturze przedmiotu znajduje się wiele definicji tego pojęcia to najczęściej negatywne ujęcie bezpieczeństwa definiowane jest jako brak zagrożenia, pozytywne zaś uwzględnia: procesy trwania, przetrwania i rozwoju.

Bezpieczeństwo jest także podstawową potrzebą każdego człowieka gwarantującą jej niezależność, rozwój oraz samorealizację W naukach o bezpieczeństwie coraz częściej kładzie się nacisk na zapewnienie bezpieczeństwa pojedynczym

2 R. Rosicki, *O pojęciu i istocie bezpieczeństwa*, www.repozytorium.amu.edu.pl [dostęp: 06.03.2019].

jednostkom. Koncepcja bezpieczeństwa jednostki (human security) zyskała szczególnie na znaczeniu za sprawą Programu Narodów Zjednoczonych ds. Rozwoju Społecznego (United Nations Development Programme – UNDP)[3]. Kładzie ona nacisk na zapewnienie każdemu człowiekowi prawa do godnego życia oraz rozwoju. W dobie rozwoju technologicznego obszarem wymagającym zapewnienia bezpieczeństwa jednostce niewątpliwie stała się także cyberprzestrzeń. Jest to duże wyzwanie, bowiem obszar ten w znaczący sposób różni się od pozostałych przestrzeni wymagających zapewnienia bezpieczeństwa. Chociaż w literaturze przedmiotu znaleźć można wiele definicji cyberprzestrzeni, zgodnie z tą zaproponowaną w ustawie z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[4] jest to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[5] wraz z powiązaniami między nimi oraz relacjami z użytkownikami. Zapewnienie jednostce bezpieczeństwa w cyberprzestrzeni powinno stać się priorytetem każdego państwa, zwłaszcza gdy spojrzy się na statystyki, z których wynika, iż ponad 53% populacji ma stały dostęp do Internetu[6]. Nikt z nas chyba nie wyobraża sobie życia bez niego. Wykorzystywany jest na szeroką skalę zarówno w domu, jak i w pracy. Przeniesienie aktywności jednostki w cyberprzestrzeń w tak szerokim zakresie oraz na tak dużą skalę determinuje konieczność zapewnienia jednostce bezpieczeństwa w tym obszarze.

Przejawem tej aktywności jest m.in. przekazywanie przez jednostkę danych osobowych. Te rozumiane są jako „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową, społeczną tożsamość osoby fizycznej" (art. 4 ust. 1 rozporządzenia 2016/679). Katalog danych osobowych, które przetwarzane są w cyberprzestrzeni jest bardzo szeroki i dotyczy wielu aspektów aktywności

3 UNIC Warsaw Ośrodek Informacji ONZ w Warszawie, www.unic.un.org.pl [dostęp: 06.03.2019].

4 Dz.U. z 2011 r. nr 222, poz. 1323.

5 Tekst jedn. Dz.U. z 2017 r., poz. 570 ze zm.

6 W. Kulik, *Cztery miliardy internautów*, http://www.benchmark.pl/aktualnosci/ile-osob-ma-dostep-do-internetu-na-swiecie-juz-ponad-4-miliardy.html [dostęp: 07.02.2019].

człowieka w cyberprzestrzeni np. logowanie się do poczty elektronicznej, zakładanie kont na portalach społecznościowych czy robienie zakupów przez Internet.

Ochrona danych osobowych jest istotnym elementem bezpieczeństwa jednostki w cyberprzestrzeni. Jest to nowy problem badawczy, który często jest niedostrzegany lub pomijany zarówno na płaszczyźnie krajowej, jak i międzynarodowej, czego przejawem jest chociażby nieuwzględnienie tej problematyki w Polityce ochrony cyberprzestrzeni RP[7]. Tymczasem, zapewnienie bezpieczeństwa danych osobowych powinno być kluczowym aspektem bezpieczeństwa w cyberprzestrzeni. To zaś rozumiane jest jako „zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni"[8]. Już sama nazwa poruszanej problematyki „ochrona danych osobowych" nakierowana jest na zapewnienie jednostce warunków, by mogła bez żadnych przeszkód technicznych, prawnych i organizacyjnych bezpiecznie przetwarzać dane osobowe.

Problematyka podjęta w monografii ma charakter interdyscyplinarny. Jest ona niezwykle szeroka i obejmuje zagadnienia z zakresu bezpieczeństwa, prawa czy informatyki. Każdorazowo nakierowana jest jednak na zapewnienie ochrony danych osobowych jednostki w cyberprzestrzeni, czy to od strony prawnej (poprzez ustawodawstwo), rozwiązań informatycznych (stosowane zabezpieczenia), czy nauk o bezpieczeństwie (definiowania zagrożeń). W ocenie autora problematyka bezpieczeństwa danych osobowych w cyberprzestrzeni powinna stanowić istotny aspekt poznawczy nauk o bezpieczeństwie nie tylko ze względu na wykształcenie się nowych nieznanych dotąd zagrożeń w tym obszarze, ale także ze względu na wzmożoną aktywność człowieka w tej przestrzeni. Zarówno zagadnienia związane z funkcjonowaniem jednostki w cyberprzestrzeni, jak i bezpieczeństwo jej danych osobowych należą do nowych problemów badawczych wymagających szczegółowej analizy w kontekście dążenia do zapewnienia jednostce poczucia bezpieczeństwa w cyberprzestrzeni. W przeciwnym razie jednostka narażona jest na zagrożenia, które mogą wyrządzić jej poważną szkodę. Zagrożenia w cyberprzestrzeni charakteryzują się nie tylko znacznie większą siłą, ale także skalą oddziaływania niż tradycyjne zagrożenia. Warto mieć także na uwadze, iż w cyberprzestrzeni każdego dnia pojawiają się nowe, nieznane zagrożenia, które w istotny sposób wpływają na bezpieczeństwo jednostki w cyberprzestrzeni. Kradzież tożsamości, ataki phishingowe, pharming to tylko nieliczne z istniejących zagrożeń. Niezapewnienie jednostce

7 *Polityka Ochrony cyberprzestrzeni RP*, Warszawa 18 września 2012 r., www.mc.bip.gov.pl [dostęp: 06.03.2019].

8 Ibidem, s. 5.

bezpieczeństwa w tym obszarze może powodować negatywne konsekwencje nie tylko dla pojedynczych użytkowników, ale także mieć skutki prawne, społeczne, gospodarcze i polityczne dla poszczególnych państw oraz całej społeczności międzynarodowej.

Celem badań była ocena aktywności człowieka w cyberprzestrzeni w zakresie transferu swoich danych oraz bezpieczeństwo tego transferu. Głównym problemem badawczym było ustalenie, czy jednostki mają prawo czuć się bezpiecznie w cyberprzestrzeni w kontekście przetwarzania ich danych osobowych, a co za tym idzie – czy stosowane rozwiązania prawne i organizacyjne są wystarczające, by bezpieczeństwo to zapewnić.

Punktem wyjścia dla prowadzonych rozważań były pytania szczegółowe sformułowane w następujący sposób:

1. Czy pojęcie cyberprzestrzeni można ująć definicyjnie?
2. Czym różni się cyberprzestrzeń od rzeczywistości oraz jakie czynniki wpływają na rozwój cyberprzestrzeni?
3. Jakie dane osobowe są najczęściej przetwarzane w cyberprzestrzeni?
4. Jakie prawa i obowiązki mają administratorzy danych osobowych oraz osoby, których dane dotyczą w cyberprzestrzeni?
5. Jakie zagrożenia związane są z przetwarzaniem danych osobowych w cyberprzestrzeni?
6. Czy oraz w jaki sposób i w jakim zakresie państwa, organizacje międzynarodowe oraz inne podmioty prawa międzynarodowego dążą do zapewnienia bezpieczeństwa w cyberprzestrzeni?

W związku z podjętą analizą została sformułowana hipoteza badawcza, zgodnie z którą człowiek jest znacznie bardziej narażony na naruszenie danych osobowych w cyberprzestrzeni niż w świecie realnym. Szczególnie widoczne jest to przez pryzmat napływających każdego dnia informacji o nowych incydentach komputerowych, które w coraz szerszym zakresie zagrażają osobom fizycznym i przetwarzanym przez nie danym osobowym. Dzieje się tak z dwóch powodów. Po pierwsze mechanizmy prawne, znane nam z codzienności, w wirtualnym świecie okazują się niewystarczające lub nieskuteczne. Po drugie samo funkcjonowanie w cyberprzestrzeni w znaczący sposób różni się od funkcjonowania w świecie rzeczywistym. Tę różnicę dobrze obrazuje redefinicja prywatności oraz wizerunku w wirtualnym świecie czy wystąpienie zupełnie nowych rodzajów zagrożeń. W związku z tym niezbędne jest zapewnienie mechanizmów gwarantujących osobom, których dane dotyczą, bezpieczne przetwarzanie ich danych.

W badaniach zastosowano szereg metod badawczych. Jedną z nich była analiza historyczna wykorzystana na początku w celu prześledzenia etapów rozwoju

cyberprzestrzeni oraz związanych z tym konsekwencji. Przedstawienie tych zagadnień było konieczne do zrozumienia, jak szybko następują zmiany w tych obszarach, co je determinuje oraz jakie są ich konsekwencje. W pracy zastosowano także metodę porównawczą, na podstawie której analizie poddano wybrane regulacje prawne, w tym w szczególności dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz rozporządzenie 2016/679. Praca została wzbogacona o wyniki przeprowadzonego badania ankietowego. Wykorzystano przy tym technikę ankietowania poprzez zastosowanie kwestionariusza ankietowego składającego się z 24 pytań zamkniętych, wielokrotnego wyboru[9]. Pytania dotyczyły zachowań ankietowanych w cyberprzestrzeni, w tym w szczególności: rodzaju i zakresu przekazywanych danych osobowych, najczęściej stosowanych zabezpieczeń, wiedzy na temat zagrożeń w cyberprzestrzeni czy poziomu poczucia bezpieczeństwa. Podczas przeprowadzania badań zastosowano pisemną technikę wypełniania kwestionariusza. Badanie było przeprowadzone od kwietnia do listopada 2018 r. wśród 340 studentów studiów stacjonarnych i niestacjonarnych I i II stopnia kierunków: prawo, bezpieczeństwo i pedagogika, dwóch uczelni wyższych mających siedzibę w Warszawie. Za pomocą anonimowej ankiety przeprowadzono badania jakościowe i ilościowe. Miały one na celu wyjaśnienie motywów postępowania respondentów oraz sprawdzenia poziomu ich świadomości i wiedzy dotyczącej bezpieczeństwa procesu przetwarzania danych osobowych w cyberprzestrzeni. Wyniki badań ilościowych zostały przedstawione w formie wykresów. Badania jakościowe zostały przeprowadzone przy użyciu metod miękkich, które pozwoliły na określenie sposobu myślenia ankietowanych. Ponadto w pracy zaprezentowano wyniki analiz licznych dokumentów krajowych i międzynarodowych dotyczących przetwarzania danych osobowych w cyberprzestrzeni. Dokonano także przeglądu orzecznictwa i doktryny, które pozwoliły na poznanie ewolucji pojęć „wizerunek" czy „prywatność". Miało to na celu ukazanie luk prawnych w przepisach oraz braki w rozwiązaniach systemowych, które miały zapewnić użytkownikom bezpieczeństwo w cyberprzestrzeni.

Praca została podzielona na sześć rozdziałów. W pierwszym z nich omówiono pojęcie i genezę cyberprzestrzeni. Wyjaśniono przy tym trudności, jakie związane są w jej zdefiniowaniu. Przedstawiono także główne elementy wyróżniające cyberprzestrzeń oraz decydujące o odmienności w stosunku do świata rzeczywistego. Wyjaśniono, dlaczego przestrzeń ta stała się tak bardzo atrakcyjna dla

9 E. Krok, *Budowanie kwestionariusza ankietowego a wyniki badań, Zeszyty naukowe Uniwersytetu Szczecińskiego*, „Studia Informatica" 2015, nr 37, s. 61.

użytkowników. W rozdziale drugim zostały wymienione i scharakteryzowane te dane osobowe, które najczęściej są przetwarzane w cyberprzestrzeni, zwłaszcza nickname, adres e-mail, adres IP, wizerunek czy dane biometryczne. Ponadto zostały przybliżone najczęściej wykorzystywane metody przetwarzania danych osobowych w cyberprzestrzeni takie, jak big data czy cloud computing. Rozdział trzeci w całości został poświęcony ocenie obowiązków, jakie zostały nałożone na ADO przetwarzających dane w cyberprzestrzeni. Analiza ta obejmuje stan prawny po 25 maja 2018 r., kiedy to wraz z rozpoczęciem stosowania przepisów rozporządzenia 2016/679 zwiększono wymogi dotyczące transparentności i rozliczalności procesu przetwarzania danych. Przedstawiono także konsekwencje, jakie związane są z niezgodnym z prawem przetwarzaniem danych osobowych, szczególnie wysokim karom administracyjnym. Starając się przeanalizować proces przetwarzania danych w cyberprzestrzeni pod kątem zarówno ADO, jak i osób, których dane dotyczą, w rozdziale czwartym zostały przybliżone prawa, jakie przysługują użytkownikom w procesie zbierania i gromadzenia ich danych w cyberprzestrzeni, z podkreśleniem nowych uprawnień, które zostały wprowadzone rozporządzeniem 2016/679. Piąty rozdział został poświęcony analizie najczęściej występujących zagrożeń w cyberprzestrzeni, przybliżeniu skali zjawiska, charakterystyce tych zagrożeń oraz wskazaniu cech odróżniających cyberzagrożenia od tych występujących w realnym świecie. Dodatkowo przedstawione zostały wybrane metody ochrony danych osobowych oraz krytyczna ocena ich skuteczności.

Ostatni szósty rozdział został poświęcony badaniom empirycznym dotyczącym bezpieczeństwa procesu przetwarzania danych osobowych w cyberprzestrzeni. Przedstawione zostały wyniki badań, które zostały przeprowadzone wśród studentów studiów stacjonarnych i niestacjonarnych I i II stopnia dwóch warszawskich uczelni wyższych. Pytania kładły nacisk na zbadanie aktywności ankietowanych w cyberprzestrzeni pod kątem przekazywanych przez nich danych osobowych. Dotyczyły głównie zakresu przekazywanych danych osobowych, ustalenia komu, po co oraz jak często dane osobowe są przez respondentów przekazywane w cyberprzestrzeni. Celem ankiety było również zweryfikowanie, czy poczucie bezpieczeństwa ankietowanych w cyberprzestrzeni jest podobne do tego, jakie odczuwają w świecie realnym. Za pośrednictwem pytań zweryfikowano także odczucia ankietowanych dotyczące anonimowości i prywatności w cyberprzestrzeni. Przedmiotem badań były także stosowane przez ankietowanych zabezpieczenia w cyberprzestrzeni oraz częstotliwość ich zmiany. Istotną częścią ankiety były pytania dotyczące zagrożeń w cyberprzestrzeni, wiedzy ankietowanych na ich temat oraz stosowanych przez nich metod walki z zagrożeniami. Pytania te pozwolą ustalić poziom wiedzy i świadomości respondentów na temat przetwarzania danych

osobowych w cyberprzestrzeni oraz zakresu przetwarzanych danych osobowych. Wyniki badań empirycznych posłużą do potwierdzenia lub odrzucenia postawionej w pracy hipotezy.

Bezpieczeństwo danych osobowych w cyberprzestrzeni ma istotne znaczenie nie tylko dla poszczególnych osób, ale także państwa czy społeczności międzynarodowej. Zapewnienie bezpieczeństwa w cyberprzestrzeni jest procesem niezwykle trudnym i wymagającym podejmowania inicjatyw na różnych płaszczyznach.

Rozdział 1

Cyberprzestrzeń – rozwój i charakterystyka pojęć

Postęp technologiczny, który obserwujemy od początku lat 60. XX wieku miał istotny wpływ na rozwój cyberprzestrzeni. Bankowość elektroniczna, portale społecznościowe czy e-usługi to tylko nieliczne przykłady potwierdzające, że nowoczesne rozwiązania technologiczne na dobre zagościły w naszym życiu. Postęp w technologii doprowadził do wytworzenia społeczeństwa informacyjnego. To właśnie za sprawą Internetu informacja nabrała nowego wymiaru – stała się towarem posiadającym określoną wartość. W konsekwencji informacje zaczęły być rozróżniane na te bardziej lub mniej cenne. Internet stał się narzędziem umożliwiającym pozyskanie i przetworzenie wszelkich informacji. Bardzo szybko został wzbogacony o kolejne rozwiązania technologiczne umożliwiające użytkownikowi przeniesienie swojej aktywności ze świata realnego do wirtualnego praktycznie na każdej płaszczyźnie. Upowszechnienie komputerów doprowadziło także do podobnego przeniesienia aktywności u większości pracodawców. Bardzo szybko tradycyjne formy przetwarzania danych osobowych zostały zastąpione przez systemy informatyczne. Pozwoliło to niezliczonym podmiotom zaoszczędzić czas oraz pieniądze. Umożliwiło także przetwarzanie danych na dużą skalę.

Chociaż rozwój cyberprzestrzeni należy oceniać pozytywnie nie ulega wątpliwości, że funkcjonowanie w wirtualnym świecie niesie za sobą liczne zagrożenia. Takie określenia, jak „wojna", „terroryzm", „atak" poprzedzone przedrostkiem „cyber" i używane do opisania zagrożenia pokazują skalę tego zjawiska. Brak wykształconych mechanizmów prawnych w omawianym obszarze doprowadził bardzo szybko do wielu nadużyć, a w kolejnym kroku do licznych nieznanych dotąd naruszeń.

W niniejszym rozdziale autor stara się odpowiedzieć na podstawowe pytanie, czym jest cyberprzestrzeń oraz jakie cechy miały decydujący wpływ na jej dynamiczny i globalny rozwój.

1.1. Definicje cyberprzestrzeni

Samo pojęcie „cyberprzestrzeń" było znane już w latach 50. za sprawą rozwoju cybernetyki, ale rozwój tego obszaru nastąpił dekadę później[10]. W literaturze przedmiotu wskazuje się, że niewątpliwy wpływ na rozpowszechnienie pojęcia „cyberprzestrzeń" (cyberspace) miał William Gibson w powieści science fiction *Burning Chrome* z 1982 r., określając ją jako „królestwo przestrzennych paradoksów"[11]. Mimo że od tego czasu minęło zaledwie 37 lat, to zdarzenia opisane w książce, do niedawna wydające się mało realnym obszarem aktywności człowieka, bardzo szybko osadziły się w rzeczywistości. Przestrzeń zidentyfikowana przez autora była w późniejszym czasie wykorzystywana w filmach, kinie czy teatrze, czego najlepszym przykładem jest film Larry'ego oraz Andy'ego Wachowskich *Matrix*. Dziś wielu z nas z pewnością gotowa jest stwierdzić, że zdarzenia mające miejsce w filmach z gatunku science fiction są możliwe do zrealizowania. To, kiedy to nastąpi jest tylko kwestią czasu.

Społeczności międzynarodowej nie udało się dotychczas wypracować jednej spójnej definicji nowego obszaru aktywności człowieka, jakim stała się cyberprzestrzeń, mimo że pojęciem tym coraz częściej posługują się międzynarodowe organizacje (zarówno te o charakterze rządowym, jak i pozarządowym), państwa czy jednostki. Najczęściej jest ono wykorzystywane w kontekście definiowania i opisywania zagrożeń oraz wskazywania metod walki z nimi. Nie ulega wątpliwości, że cyberprzestrzeń wymaga takich samych wysiłków na rzecz zapewnienia bezpieczeństwa jak pozostałe obszary, na których państwa sprawują jurysdykcję. Brak wspólnej definicji niewątpliwie może rodzić pewne wątpliwości, czym w rzeczywistości jest owa przestrzeń, jakie elementy mieszczą się w jej pojęciu, a jakie wykraczają poza ramy definicji.

Słowo „cyberprzestrzeń" składa się z dwóch elementów: cyber oraz przestrzeń. Pojęcie przestrzeni nie budzi większych wątpliwości – słowo to używane jest na

10 Zgodnie z definicją *Słownika języka polskiego*: „cybernetyka jest nauką o procesach sterowania oraz przekazywania i przekształcania informacji w systemach takich jak np. maszyna, organizm żywy, społeczeństwo" za: *Cybernetyka*, [w:] *Słownik języka polskiego*, https://sjp.pwn.pl/sjp/cybernetyka [dostęp: 11.09.2018].

11 J. Wasilewski, *Zarys definicji cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5), s. 225, www.abw.gov.pl [dostęp: 11.09.2018].

określenie obszaru. W *Słowniku języka polskiego* znajdujemy także definicję wskazującą, że jest to rozległa, pusta powierzchnia bez wyraźnie oznaczonych, widocznych granic[12]. Słowo „cyber" nie znajduje zaś odzwierciedlenia w słowniku. Chociaż samo słowo nie zostało zdefiniowane wprost, to niewątpliwie wraz ze wzrostem znaczenia cyberprzestrzeni zaczęły powstawać nowe słowa, których elementem jest przedrostek cyber: cyberzagrożenia, cyberterroryzm, cyberspołeczeństwo, cyberatak czy cyberwojna. Każde z nich używane jest dla oznaczenia innego zagrożenia, niemniej każde z nich odnosi się do aktywności w cyberprzestrzeni.

Wśród licznych definicji określających ten obszar znajduje się ta zaproponowana przez Paulinę Tekielską i Łukasza Czekaja, którzy mianem cyberprzestrzeni określają „sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej, gazowej, czy ochrony zdrowia"[13].

W *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej* cyberprzestrzeń zdefiniowano jako „cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami oraz relacjami z użytkownikami"[14]. Cyberprzestrzeń Rzeczpospolitej zaś jako „przestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP"[15].

W ustawie z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[16] cyberprzestrzeń została zdefiniowana jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne określone w art. 3 pkt. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami między nimi oraz relacjami z użytkownikami". Zgodnie z definicją podaną w art. 3 pkt 3 wskazanej tu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności

12 *Przestrzeń*, [w:] *Słownik języka polskiego*, https://sjp.pwn.pl/szukaj/przestrzen [dostęp: 16.06.2018].

13 P. Tekielska, Ł. Czekaj, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI w.*, M. Górka, Warszawa 2014, s. 163.

14 Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*, 22 stycznia 2015 r., s. 7.

15 Ibidem.

16 Dz.U. z 2011 r. nr 222, poz. 1323.

podmiotów realizujących zadania publiczne[17] system teleinformatyczny jest to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)".

Trudność zamknięcia pojęcia cyberprzestrzeń w jedną uniwersalną definicję wynika z kilku powodów. Po pierwsze, jest to obszar nowy, który nie został jeszcze całkowicie zbadany. Pojęcie to ma charakter interdyscyplinarny i jest przedmiotem zainteresowania wielu różnych niezwiązanych ze sobą dyscyplin naukowych, które badają go pod każdym kątem oraz z różnych perspektyw. Po drugie jest to obszar bardzo dynamiczny, który podlega ciągłym zmianom. W literaturze przedmiotu zwraca się uwagę, że można wyodrębnić etapy rozwoju cyberprzestrzeni. Zdaniem Piotra Sienkiewicza można wykazać cztery etapy rozwoju cyberprzestrzeni (Cyberprzestrzeń-0, Cyberprzestrzeń-1, Cyberprzestrzeń-2, Cyberprzestrzeń-3). Każdy z nich charakteryzuje pojawienie się nowej, bardziej zaawansowanej formy aktywności człowieka[18].

W związku z tym warto się zastanowić nad zasadnością tworzenia definicji cyberprzestrzeni. Analiza przepisów prawnych z ostatnich 20 lat pod kątem ich aktualności pokazuje, że postęp technologiczny w znaczący sposób wyprzedza ustawodawstwa krajowe oraz wspólnotowe. Najlepszym tego przykładem jest chociażby unijna dyrektywa 95/46/WE, w której państwa członkowskie w 1997 r. nie przewidziały przepisów prawnych regulujących takie zagadnienia, jak monitoring wizyjny, biometrię, bankowość elektroniczną czy portale społecznościowe.

Z uwagi na fakt, że cyberprzestrzeń jest obszarem aktywności osób fizycznych, państw oraz międzyrządowych i pozarządowych organizacji, zasadne wydaje się chociażby ramowe określenie, czym ona jest, jakie są jej cechy charakterystyczne, a także prawa i obowiązki użytkowników korzystających z tego właśnie obszaru.

Warto zwrócić uwagę, że w ustawodawstwach krajowych innych państw europejskich pojęcie to nie jest zbyt często używane. Jak zauważa Marcin Mróz „żadnym z wewnętrznych aktów prawnych tych państw nie został użyty termin cyberprzestrzeń jako narzędzie opisu treści normatywnych dotyczących cyberprzestrzeni"[19].

---

17 Tekst jedn. Dz.U. z 2017 r., poz. 570 ze zm.

18 P. Sienkiewicz, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, vol. 9, s. 89.

19 M. Mróz, *Informacja nt. pojęcia cyberprzestrzeni oraz bezpieczeństwa i zagrożenia cyberprzestrzeni w prawie międzynarodowym i w ustawodawstwie wybranych państw demokratycznych*, 22.07.2011 r., www.orka.sejm.gov.pl [dostęp: 12.03.2018].

Nie oznacza to jednak, że omawiane pojęcie nie zostało zakorzenione w krajowych porządkach prawnych. W ocenie autora w celu zdefiniowania tej przestrzeni państwa posługują się definicjami wypracowanymi na szczeblu międzynarodowym, uznając tym samym, że regulacje we wspomnianym zakresie powinny być dorobkiem większej grupy państw. Potwierdzają w ten sposób przekonanie, że jest to obszar, w którym pojedyncze państwo nie jest w stanie zapewnić obywatelom odpowiedniego poziomu bezpieczeństwa. Zdaniem autora większość zagadnień związanych z cyberprzestrzenią powinno być dyskutowanych i opracowywanych na poziomie europejskim czy międzynarodowym. Niemniej jednak, jak zostanie to wykazane w późniejszych rozdziałach, starania społeczności międzynarodowej w tym zakresie są tylko jednym z etapów procesu mającego zapewnić bezpieczne przetwarzanie danych osobowych w cyberprzestrzeni. Każde z państw powinno podjąć wysiłki na rzecz rozpowszechniania wśród obywateli informacji na temat bezpiecznego poruszania się w wirtualnym świecie oraz promowania działań edukacyjnych podnoszących poziom ich wiedzy. Warto także przypominać, że nie jest to przestrzeń wolna od zagrożeń i każdy z użytkowników powinien mieć świadomość, iż może stać się ofiarą cyberprzestępstwa.

Problematyką cyberprzestrzeni zainteresowana jest cała społeczność międzynarodowa nie tylko z uwagi na dążenie państw do rozciągnięcia swojej jurysdykcji w tym obszarze, ale przede wszystkim z uwagi na rosnącą liczbę zagrożeń. Mimo że rezultat poszukiwań semantycznych dotyczących pojęcia cyberprzestrzeni wypracowany przez społeczność międzynarodową należy zaliczyć do bardzo bogatych, to wciąż nie została wypracowana jedna definicja określająca, czym jest cyberprzestrzeń. Znacznie częściej w dokumentach definiowane są konkretne zagrożenia występujące w tym obszarze takie, jak: przestępstwo nadużywania technologii informacyjnych[20], cyberprzestępczość, cyberterroryzm czy wojna cybernetyczna[21]. Podobne prawidłowości odnajdujemy w dokumentach Rady Europy czy Unii Europejskiej. Zapewnienie bezpieczeństwa w cyberprzestrzeni możliwe jest przede wszystkim poprzez podejmowanie inicjatyw na forach międzynarodowych. W ostatnich latach jest to widoczne coraz wyraźniej i coraz częściej. Mimo że zagadnienia związane z funkcjonowaniem i zapewnieniem bezpieczeństwa w cyberprzestrzeni są od lat podejmowane przez społeczność międzynarodową nie udało się stworzyć jednolitych standardów regulujących funkcjonowanie w tym obszarze.

20 Rezolucja Zgromadzenia Ogólnego ONZ ze stycznia 2002 r., nr 56/121, www.itu.int/ITU-D/cybcybersecurity [dostęp: 13.06.2018].

21 Rezolucja Zgromadzenia Ogólnego ONZ z grudnia 1998 r., nr 53/70, www.itu.int/ITU-D/cybcybersecurity [dostęp: 13.06.2018].

1.2. Internet

Jak wynika z przeprowadzonych badań pojęcia „Internet" i „cyberprzestrzeń" są w przekonaniu większości ankietowanych rozumiane jako tożsame. Wielu przedstawicieli doktryny również uważa podobnie, wskazując że „cyberprzestrzeń to po prostu Internet, jego zasoby i usługi oraz użytkownicy" lub „cyberprzestrzeń utożsamia się z wirtualną rzeczywistością generowaną przez komputer, sieć i Internet"[22]. Wydaje się, że jest to pewne uogólnienie, które w pewnym zakresie znajduje swoje uzasadnienie wynikające przede wszystkim z faktu, iż większość z nas jest czynnymi użytkownikami Internetu i doświadcza cyberprzestrzeni właśnie przez jego pryzmat. Zdaniem innych Internet jest najważniejszym, chociaż nie jedynym składnikiem cyberprzestrzeni[23]. Takie podejście jest reprezentowane m.in. przez Departament Obrony USA, gdzie cyberprzestrzeń jest zdefiniowana jako „Globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery"[24].

Dodatkowo w 2011 r. Kancelaria Premiera Wielkiej Brytanii wydała dokument *Strategia Cyberbezpieczeństwa Zjednoczonego Królestwa – ochrona oraz promocja Zjednoczonego Królestwa w cyfrowym świecie*, z którego wynika, że cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują nasz biznes, infrastrukturę oraz wspomagają świadczenie usług[25]. Cyfrowe sieci już dziś podbudowują proces zaopatrywania naszych domów w energię elektryczną oraz wodę, pomagają organizować dostawy żywności oraz innych dóbr do sklepów, a także służą za niezbędne narzędzie biznesowe w całym Zjednoczonym Królestwie. Ich zasięg ustawicznie się powiększa w miarę jak podłączamy do nich nasze telewizory, konsole do gier czy nawet urządzenia AGD[26].

Trudność w określeniu, czy cyberprzestrzeń oraz Internet są pojęciami tożsamymi, czy też cyberprzestrzeń jest jednak pojęciem szerszym wynika przede wszystkim z faktu, że oba pojęcia są definiowane w sposób niezwykle ogólny.

22 P. Sienkiewicz, *Ontologia...*, op. cit., s. 89.

23 R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4, www.pan.poznan.pl [dostęp: 20.10.2018].

24 J. Wasilewski, *Zarys...*, op. cit., , s. 225.

25 Ibidem.

26 Ibidem.

Dodatkowo oba są nierzeczywiste, trudne do wyobrażenia i *de facto* nie zostały jeszcze przez człowieka gruntownie zbadane.

W ocenie autora cyberprzestrzeń jest pojęciem znacznie szerszym niż Internet. Nie ulega wątpliwości, że Internet jest jej głównym składnikiem, stanowiącym łącznik pomiędzy światem rzeczywistym i wirtualnym. Rozszerzająca się każdego dnia cyberprzestrzeń domaga się spojrzenia wykraczającego poza ramy Internetu. W niniejszej pracy autor skupia się przede wszystkim na przetwarzaniu danych osobowych w Internecie z uwagi na fakt, że to jest właśnie obszar, w którym osoby, których dane dotyczą, są najbardziej aktywne. Niemniej jednak nie jest to wyłączna strefa aktywności ludzi, co zostało podkreślone podczas omawiania zagrożeń w cyberprzestrzeni.

W 1958 r. została powołana, w ramach Departamentu Obrony USA, agencja ARPA (Advanced Reseached Project Agency). Jej zadaniem było rozwijanie nauki i rozwijanie technik w zakresie obronności[27]. W 1969 r. powstała pierwsza sieć peer-to-peer APRANET (The Advanced Research Projects Agency Network)[28]. Bardzo szybko do sieci zaczęto podłączać lokalne sieci Wielkiej Brytanii czy Norwegii. Polska została podłączona do Internetu 12 września 1991 r. W literaturze przedmiotu wskazuje się, że rewolucja informatyczna jest czwartą tego rodzaju rewolucją w dziejach ludzkości po wynalezieniu druku, wynalezieniu książki i wynalezieniu maszyny drukarskiej[29].

W dzisiejszych czasach nie wyobrażamy sobie życia bez Internetu. Towarzyszy nam podczas jazdy samochodem, kiedy korzystamy z nawigacji w telefonie, w trakcie pracy, kiedy sprawdzamy informacje czy wysyłamy e-maile oraz w domu podczas oglądania naszych ulubionych seriali w serwisach internetowych. Internet jednak przede wszystkim służy nam do pozyskiwania informacji i komunikowania się ze sobą. Obecnie jest on ogólnodostępny w większości cywilizowanych miejsc na świecie, możemy się do niego przyłączyć za pomocą WI-FI, czyli sieci bezprzewodowej z praktycznie każdego miejsca na świecie. Internet jest wykorzystywany nie tylko przez osoby prywatne. Jest on nieodzownym elementem w świecie biznesu, nauki, a nawet w organizacjach rządowych.

Twórcą koncepcji Internetu był Paul Baran, amerykański informatyk urodzony w 1926 r. na terytorium II Rzeczypospolitej w polsko-żydowskiej rodzinie. Dwa lata później wraz z rodziną przeprowadził się do Ameryki, gdzie zdobył tytuł

---

27 K. Majgier, *Internet jako przestrzeń komunikacyjna*, „Przegląd psychologiczny" 2000, t. 43, nr 2, s. 157, www.kul.pl [dostęp: 16.09.2018].

28 Ibidem.

29 P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni państwa*, „Zeszyty naukowe Uniwersytetu Szczecińskiego" 2012, nr 88, *Ekonomiczne problemy usług*, s. 803, www.bazhum.muzhp.pl [dostęp: 17.09.2018].

Master of Science w dziedzinie inżynierii. W swojej karierze został odznaczony jednym z najwyższych wyróżnień przyznawanych przez Instytut Inżynierów Elektryków i Elektroników za osiągnięcia w telekomunikacji – IEEE Alexander Graham Bell Medal. Paul Baran był także odznaczony National Medal of Technology oraz znalazł się na liście National Inventors Hall of Fame. Był zatrudniony w RANND Corporation, amerykańskim think tank i organizacji badawczej non-profit, pierwotnie sformowanej dla potrzeb Sił Zbrojnych Stanów Zjednoczonych, która na zlecenie Amerykańskich Sił Zbrojnych realizowała projekt sieci cyfrowych transmisji danych[30].

Zadaniem agencji ARPA było także wspieranie inicjatyw powstających na uczelniach w USA i mających znaczenie dla obronności kraju. Przede wszystkim jednak ARPA miała wypracować przewagę technologiczną nad ZSRR w okresie tuż po wysłaniu przez Rosjan w kosmos Sputnika. Agencja miała zbudować sieć komunikacyjną, umożliwiającą przekazywanie informacji, a przede wszystkim rozkazów jednostkom wojskowym na wypadek zniszczenia tradycyjnych środków komunikacji[31]. Zespół ekspertów z ARPA stworzył tzw. Memorandum dla członków i oddziałów intergalaktycznej sieci komputerowej opisujące działanie Internetu. ARPANET na początku była eksperymentalną siecią łączącą komputery z kilku uniwersytetów, która stopniowo rozrastała się na coraz więcej uczelni. W 1971 r. ARPA zdecydowała się ujawnić protokół TCP/IP i zezwoliła na przyłączanie do ARPANET-u lokalnych sieci akademickich. Pierwszą siecią akademicką przyłączoną do ARPANET-u była sieć na kampusie Uniwersytetu Kalifornijskiego w Los Angeles. W latach 1972–1979 kolejne uczelnie USA przyłączały się do projektu ARPANET. Jednocześnie ARPA śledziła nowinki techniczne powstające na uczelniach i część z nich przekazywała na rzecz tajnych projektów wojskowych[32].

W 1980 r. zdecydowano się rozdzielić ARPANET na sieć tylko wojskową, która pozostała przy nazwie ARPANET i część cywilną, która zyskała miano INTERNET. Według definicji Słownika języka polskiego Internet to ogólnoświatowa sieć komputerowa, łącząca lokalne sieci, korzystające z pakietowego protokołu komunikacyjnego TCP/IP, mająca jednolite zasady adresowania i nazywania węzłów (komputerów włączonych do sieci) oraz protokoły udostępniania informacji[33].

---

30 *Historia Internetu*, [w:] *Wikipedia*, https://pl.wikipedia.org/wiki/Historia_Internetu [dostęp: 13.06.2018].

31 *Historia Internetu*, http://internet.arct.pl/historia_internetu.html [dostęp: 13.06.2018].

32 *ARPANET*, [w:] *Wikipedia*, https://pl.wikipedia.org/wiki/ARPANET [dostęp: 13.08.2018].

33 *Internet*, [w:] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/Internet;3915155.html [dostęp: 17.06.2018].

W 2018 r. z Internetu korzystało ponad 4 mld ludzi na całym świecie, a w samym 2017 r. przybyło aż 250 mln nowych użytkowników Internetu. W Polsce z Internetu korzysta ponad 78% ludności, co stanowi ok. 30 mln osób[34].

1.3. Czynniki wpływające na rozwój cyberprzestrzeni

Co miało decydujący wpływ na to, że ludzie zdecydowali się przenieść większą część swojej aktywności w świat wirtualny? Co sprawiło, że zdecydowaliśmy się zaryzykować i, nie znając wszystkich konsekwencji tego wyboru, przenieśliśmy całe aspekty naszego życia zawodowego i prywatnego w cyberprzestrzeń? Na te pytania nie ma jednej prostej odpowiedzi. Dla każdego z nas bowiem świat wirtualny jest atrakcyjny z innego powodu. Jedna osoba wskaże, że aktywność na tym polu pozwala jej zredukować koszty, inna osoba powie, że to oszczędność czasu, ktoś jeszcze wskaże na socjotwórczy aspekt Internetu – dzięki niemu poznał wielu nowych znajomych z całego świata, co nie byłoby możliwe w świecie realnym. Uogólniając powyższe opinie można stwierdzić, że atrakcyjność wirtualnego świata polega przede wszystkim na tym, iż nie ma on charakteru jednolitego i każdy z nas znajdzie tu coś dla siebie. Niemniej jednak, chcąc zdefiniować, czym jest to „coś" można wyróżnić kilka przedstawionych poniżej elementów.

1.3.1. Przestrzeń wirtualna

Z przeprowadzonych badań wynika, że większość ankietowanych kojarzy słowo „cyberprzestrzeń" z wirtualnym światem i Internetem. Niewątpliwie cyberprzestrzeń odnosi się do przestrzeni wirtualnej, nie zaś realnej. Jest to podstawowa różnica w stosunku do pozostałych obszarów, na których państwa sprawują jurysdykcję (przestrzeń lądowa, morska, powietrzna, kosmiczna). Jak zostało zdefiniowane w *Słowniku języka polskiego* „wirtualny" oznacza „stworzony w ludzkim umyśle, ale prawdopodobnie istniejący w rzeczywistości lub mogący zaistnieć"[35]. Słowo to pochodzi od łacińskiego *vitus* oznaczającego „mający moc sprawczą". Pojęcia tego używamy na określenie przestrzeni stworzonej przy wykorzystaniu technologii informatycznej.

Cyberprzestrzeń jest odrębna od przestrzeni realnej. Nie obowiązują w niej mechanizmy występujące w świecie realnym, dlatego też tak wiele osób nie rozumie mechanizmów i zasad funkcjonujących w świecie wirtualnym.

---

34 Ł. Majchrzyk, *Mobile i Digital w 2018 roku w Polsce i na świecie*, https://mobirank.pl/2018/02/02/mobile-i-digital-w-2018-roku-w-polsce-i-na-swiecie/ [dostęp: 21.10.2018].

35 *Wirtualny*, [w:] *Słownik Języka Polskiego*, https:sjp.pwn.pl [dostęp: 13.09.2018].

1.3.2. Zasięg globalny

Cyberprzestrzeń ma charakter globalny, co oznacza, że jest przestrzenią, która w przeciwieństwie np. do obszaru lądowego nie jest zmaterializowana i nie jesteśmy w stanie określić jej fizycznych granic. Nie ma w niej barier geograficznych ani czasowych. Jedyną granicą ograniczającą zakres cyberprzestrzeni jest zasięg sieci informatycznej, za pośrednictwem której istnieje możliwość połączenia się z wirtualnym światem.

Dzisiaj na całym świecie jest ponad 4 mld użytkowników Internetu, czyli 53% naszej populacji funkcjonuje w przestrzeni wirtualnej[36]. Jedna trzecia ludzkości korzysta z social media, z czego 34% wykorzystuje w tym celu urządzenia mobilne. W pierwszej piątce państw, w których występuje największy odsetek ludzi korzystających z Internetu w odniesieniu do całkowitej liczby mieszkańców w 2017 r. znalazły się: Zjednoczone Emiraty Arabskie (99%), Japonia (93%), Wielka Brytania (91%), Kanada (91%) oraz Korea Południowa (90%). Stany Zjednoczone znalazły się na miejscu szóstym ze wskaźnikiem 88% osób korzystających z Internetu. Polska zajęła 15. miejsce[37].

Z przeprowadzonych badań wynika, że pod koniec 2017 r. w Polsce z Internetu korzystało ponad 27,6 mln osób, to oznacza, że dostęp do Internetu ma ponad 81,9% gospodarstw domowych[38].

Badania wykazują, że z Internetu częściej korzystają mężczyźni niż kobiety w przedziale wiekowym 25–34 lata. Umiejętności komunikowania się w wirtualnym świecie, pozyskiwania i wymiany informacji uczymy się od najmłodszych lat. Dostęp do tych informacji jest tak skonstruowany, by był możliwy dla każdego użytkownika, niezależnie od wieku czy wykształcenia. Okazuje się też, że wiedza dostępna w wirtualnym świecie nigdy się nie kończy. Każdego bowiem dnia powstają nowe wpisy, dzielimy się nowymi informacjami. Są one dla nas dostępne bez względu na położenie geograficzne. Nie ma granic wiekowych, nie ma ograniczeń politycznych, wyznaniowych. Tak samo możliwości finansowe użytkowników nie mają większego wpływu na dostęp do informacji wirtualnych.

Wydawać by się mogło, że Internet daje nam możliwość selekcji wiadomości, które chcemy czytać. Czy jednak przekonanie to nie jest złudne? Czy rzeczywiście jest tak, że Internet daje użytkownikowi nieograniczony dostęp do

36 W. Kulik, *Cztery…*, op. cit.

37 Ł. Majchrzyk, *Mobile, digital i social media na świecie w 2017 roku*,https://mobirank.pl/2017/01/24/mobile-digital-social-media-na-swiecie-2017/ [dostęp: 17.07.2018].

38 IAB. Polska, *Raport strategiczny Internet 2017/2018*, 14.06.2018 r., https://iab.org.pl/badania-i-publikacje/raport-strategiczny-internet-20172018/ [dostęp: 17.07.2018].

informacji? Czy faktycznie to my decydujemy o tym, co chcemy czytać? Czy nasze wybory są rzeczywiście wolne? Dzięki rozwijającej się technologii możliwe stało się profilowanie, poprzez które wyszukiwanie informacji stało się zbyteczne. Na podstawie tego, jakie strony internetowe oglądamy, jakie produkty kupujemy, podsyłane są nam reklamy i informacje odpowiadające naszym potrzebom czy oczekiwaniom. Szybko okazało się, że informacja o użytkowniku jest kołem napędzającym zyski międzynarodowych korporacji, które swą siłę oddziaływania zawdzięczają Internetowi. Na podstawie odwiedzanych przez nas stron internetowych, dokonywanych wyborów, czasu spędzonego w sieci, rodzaju podejmowanych decyzji tworzone są profile użytkowników po to, żebyśmy szybko, tanio i w przystępny sposób otrzymali to, czego szukamy. Dodatkowo brak jakiejkolwiek kontroli nad umieszczanymi informacjami wpływa negatywnie na jakość publikacji. To do nas, odbiorców należy więc ocena, czy źródło informacji jest na tyle wiarygodne, by uznać je za prawdziwe. Niestety bardzo często o tym zapominamy.

1.3.3. Pozorna anonimowość

Wśród atutów wirtualnego świata wymienia się często anonimowość. W ocenie autora funkcjonowanie w Internecie daje użytkownikom tylko i wyłącznie złudne poczucie anonimowości. Większość użytkowników ma wrażenie, że wirtualny świat zapewnia im bycie „nierozpoznanym". Dzieje się tak dlatego, ponieważ w wirtualnym świecie mamy możliwość kreowania swojego wizerunku w dowolny sposób, czasami zupełnie różny od tego rzeczywistego. Jak zauważają Peter L. Berger i Thomas Luckmann z anonimowością mamy do czynienia „w miarę oddalania się od sytuacji, w której mamy bezpośredni kontakt z drugą osobą (...). Na jednym końcu tego kontinuum znajdują się ci inni, z którymi wchodzę w częste i intensywne interakcje w kontaktach osobistych, czyli «krąg moich bliskich». Na drugim końcu natomiast – anonimowe abstrakcje, które z samej natury nigdy nie mogą być mi dostępne w bezpośredniej interakcji"[39]. Co do zasady, posługując się powyższą definicją, należałoby uznać, iż Internet zapewnia użytkownikom anonimowość.

Ta natomiast zapewnia użytkownikowi jego nieidentyfikowalność. W ocenie autora teza, że Internet umożliwia jednostce pozostawanie anonimowym nie znajduje uzasadnienia w praktyce. Oczywiście osobom korzystającym z Internetu może się wydawać, że są w nim całkowicie *incognito*, niemożliwe lub trudne do

[39] Za: P. Mazurek, *Anatomia internetowej anonimowości, Społeczna przestrzeń Internetu*, red. D. Bartoszek, Warszawa 2006, s. 2.

zidentyfikowania. Na tym tle wyłoniło się wiele nowych, nieznanych dotąd zagrożeń w cyberprzestrzeni. Sprawcy bardzo długo żyli w przeświadczeniu, że nie postawiają po sobie żadnych śladów, a ich anonimowość umożliwia podszycie się pod kogoś innego; organ ścigania nie ustali ich prawdziwej tożsamości. Wynika to przede wszystkim z faktu, że kiedy powstawał Internet nie skupiano się nad zagadnieniem bezpieczeństwa. Szybko jednak okazało się, iż każdy użytkownik pozostawia po sobie ślad, który pozwala na jego zidentyfikowanie. Najlepszym przykładem potwierdzającym, że w cyberprzestrzeni nie jesteśmy anonimowi jest chociażby adres IP, na podstawie którego można (prawie zawsze) rozpoznać użytkownika.

Za brakiem anonimowości w Internecie przesądza także fakt, że coraz częściej powstają podmioty, których działalność polega na zbieraniu informacji o internautach. Na podstawie odwiedzanych stron czy kupowanych produktów tworzone są profile odwiedzających. Informacje te są następnie analizowane, tak by zaproponować użytkownikowi precyzyjnie dobrane do ich potrzeb towar lub usługę. Należy mieć świadomość, że każdego dnia powstają nowe rozwiązania, których celem jest lepsze dotarcie do użytkownika z konkretną usługą, informacją czy ofertą. Na tym tle pojawia się pytanie, gdzie leży granica ingerencji w naszą prywatność. Czy stosowana najczęściej praktyka śledzenia użytkowników bez ich wiedzy nie powinna zostać ograniczona, a w niektórych przypadkach wręcz zakazana?

Nieidentyfikowalność w Internecie pozwala także na podszycie się pod kogoś zupełnie innego. W tym celu można zarówno posłużyć się cudzymi danymi osobowymi, jak i użyć danych fikcyjnych. Dzieje się tak dlatego, ponieważ w wirtualnym świecie nie wchodzimy w bezpośrednie interakcje z innymi użytkownikami, tak jak robimy to w świecie rzeczywistym.

1.3.4. Brak ograniczeń czasu i przestrzeni

Cyberprzestrzeń jako nowy obszar aktywności człowieka stał się również terenem zainteresowania państw. Są one zorientowane nie tylko na bycie aktywnym uczestnikiem całego wirtualnego świata, ale także na sprawowanie na tym obszarze swoich jurysdykcji. Z pewnością kryteria, jakimi dotychczas posługiwano się na gruncie prawa międzynarodowego do wyznaczania granic czy sprawowania jurysdykcji na określonym terytorium nie będą miały zastosowania do cyberprzestrzeni. Prawo międzynarodowe jednak w znaczący sposób różni się od krajowych systemów prawnych i szczególną rolę zwraca się w nim na soft law, które w tym zakresie może mieć istotne znaczenie.

Trudno więc mówić o możliwości sprawowania władztwa przez określone państwa. Niezbędne wydaje się zatem przyjęcie innego kryterium. W dobie rosnącej skali zagrożeń w tym obszarze niezbędne jest podjęcie szybkich i zdecydowanych

kroków zmierzających do uregulowania sposobów funkcjonowania w cyberprzestrzeni oraz określenie zachowań, które nie tylko są nieakceptowane, ale również sankcjonowane. Zagadnienie to zostanie szczegółowo przeanalizowane w kolejnych rozdziałach pracy.

1.3.5. Cyberprzestrzeń jako platforma służąca do wymiany informacji

Chociaż Internet powstał jako sieć do przesyłania informacji o charakterze naukowym i wojskowym, jego szybka komercjalizacja doprowadziła do rozwoju społeczeństwa informacyjnego, a tym samym do wzrostu znaczenia informacji. Dodatkowo bardzo szybko okazało się, że Internet daje jej użytkownikom znacznie większe możliwości niż wyłącznie komunikowanie się. Dziś poza wymianą informacji wymieniamy się filmami, nagraniami, robimy zakupy, sprzedajemy swoje towary oraz usługi. Nikt z nas nie wie, jak będzie wyglądało funkcjonowanie w cyberprzestrzeni za kolejną dekadę. Jeżeli postęp technologiczny będzie rozwijać się w tak szybkim tempie jak ma to miejsce obecnie, filmy science fiction mogą okazać się realne.

Rozwój cyberprzestrzeni jest ściśle związany z rozwojem społeczeństwa informacyjnego na przełomie XX i XXI wieku. Dla jego członków informacja stanowi kluczową rolę w stosunkach społecznych i gospodarczych. Za twórcę określenia „społeczeństwo informacyjne" uważa się Daniela Bella, który w 1973 r. posłużył się tym terminem w swojej publikacji *The coming of post-industrial society*[40].

Rozwój społeczeństwa informacyjnego nie byłby możliwy, gdyby nie rozwój Internetu czy globalizacja. Jest ona zjawiskiem na tyle istotnym, że wskazuje się, iż informacja w XXI wieku jest dobrem cenniejszym niż złoto. Za prekursora powyższego określenia uważa się Tadeo Umesao japońskiego antropologa, który w 1963 r. posłużył się określeniem „społeczeństwo informujące się przez komputer"[41] w swojej pracy naukowej dotyczącej ewolucji teorii społeczeństwa opartego na informacji. W Europie pojęcie to zaczęło być stosowane znacznie później. W 1978 r. posłużyło się nim dwóch francuskich ekspertów w raporcie przedłożonym prezydentowi Francji.

Jak zauważają Tomasz Globan-Klas i Piotr Sienkiewicz społeczeństwo informacyjne to nie tylko społeczeństwo, które posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz przetwarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa[42].

---

40 Za: Z. Dobrowolski, *Koncepcja społeczeństwa informacyjnego Daniela Bella*, www.bbc.uw.edu.pl [dostęp: 21.09.2018].

41 Za: M. Golka, *Czym jest społeczeństwo informacyjne?*, „Ruch prawniczy, ekonomiczny i socjologiczny rok LXVII" 2005, nr z. 4, www.uj.edu.pl [dostęp:13.09.2018].

42 T. Globan-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999, s. 53.

Pojęcie to wykorzystywane jest także na forum międzynarodowym. W dokumentach Organizacji Współpracy Gospodarczej i Rozwoju zauważono, że społeczeństwo informacyjne może zostać odnalezione na przecięciu odrębnych kiedyś kierunków przemysłu: telekomunikacyjnego, mediów elektronicznych i informatycznego opartego na paradygmacie cyfrowej informacji. „Jedną z wiodących sił jest stale rosnąca moc obliczeniowa komputerów oferowanych na rynku, której towarzyszą spadające ceny. Innym elementem jest możliwość łączenia komputerów w sieci, pozwalająca im na dzielenie danych, aplikacji, a czasami samej mocy obliczeniowej, na odległości tak małe jak biuro i tak duże jak planeta. Ten podstawowy model rozproszonej mocy obliczeniowej i szybkich sieci jest sednem społeczeństwa informacyjnego”[43].

Społeczeństwo informacyjne dzięki Internetowi ma szybki i łatwy dostęp do informacji, możliwość szybkiego komunikowania się m.in. w celu wymiany informacji bez potrzeby wychodzenia z domu. Postęp technologiczny, a zwłaszcza powstanie Internetu, doprowadził także do zmiany stylu życia. Społeczeństwo informacyjne wytworzyło liczne narzędzia umożliwiające mu szybkie i łatwe zdobycie i przetworzenie potrzebnych informacji. Najlepszy tego przykład stanowią urządzenia multimedialne, w tym telefony komórkowe, smartfony czy laptopy. Dają one użytkownikowi możliwość szybkiego połączenia się z wirtualnym światem niezależnie od tego, w jakim miejscu się znajduje, o każdej porze dnia i nocy. Szybki rozwój cyberprzestrzeni doprowadził do tego, że pierwotny cel jej powstania – zdobycie informacji – stał się tylko jedną z wielu możliwości dostępnych do realizowania w tym obszarze.

W XXI wieku obecne rozwiązania technologiczne pozwalają na przeniesienie większości czynności wykonywanych w rzeczywistym świecie do świata wirtualnego, zaoszczędzając tym samym czas oraz pieniądze. Dodatkowo cyberprzestrzeń umożliwia dotarcie do znacznie większej liczby odbiorców, co w przypadku wielu usług ma znaczenie fundamentalne. Za sprawą Internetu pokonane zostały istniejące od wieków ograniczenia czasu i przestrzeni. Współcześnie Internet służy użytkownikom głównie jako narzędzie komunikacji pokonującej nieraz bardzo duże odległości. Jest to cecha mająca kluczowe znaczenie dla rozwoju tej formy porozumiewania się. W literaturze przedmiotu bardzo często podkreśla się, że ta forma komunikacji różni się od tradycyjnej komunikacji używanej w świecie rzeczywistym[44]. Przede wszystkim zwraca się uwagę, iż komunikacja internetowa

43 M. Goliński, *Społeczeństwo informacyjne- problemy definicyjne i problemy pomiaru*, [w:] *Dydaktyka informatyki problemy teorii*, s. 45, www.di.univ.rzeszow.pl [dostęp: 12.09.2018].

44 K. Majgier, *Internet jako przestrzeń komunikacji*, „Przegląd psychologiczny” 2000, t. 43, nr 2, s. 157.

odbywa się w przeważającej większości na płaszczyźnie tekstowej, chociaż coraz częściej użytkownicy posługują się wideokonferencjami.

Coraz częściej dostrzega się korzystny wpływ Internetu na gospodarkę światową. Z raportu, który przygotowała agencja McKinsey dla krajów należących do grupy G8 wynika, że Internet w 2015 r. wygenerował 3% światowego dochodu narodowego. Dostrzegając rosnące znaczenie Internetu w gospodarce na forum OECD wypracowano pojęcie „gospodarki Internetowej"[45]. Nie ulega wątpliwości, że Internet gwarantuje atrakcyjne warunki dla rozwoju różnych gałęzi gospodarki obecnych w świecie realnym. Doprowadził także do wyodrębnienia się nowych modeli biznesowych właściwych dla świata wirtualnego (e-bankowość, e-usługi). Internet doprowadził do powstania nowych nieznanych dotąd obszarów aktywności człowieka, których rozwój generuje określone wartości pieniężne (mowa przede wszystkim o portalach społecznościowych). Internet umożliwia szybsze i tańsze dotarcie do klienta, dostarczenie mu towaru lub usługi odpowiadających jego oczekiwaniom. Pozwala przedsiębiorstwom na obniżenie stałych kosztów związanych z prowadzeniem firmy. Dotychczasowe przeszkody takie, jak brak czasu, zbyt duża odległość czy niekorzystne warunki atmosferyczne zostają usunięte.

Możliwość zaoszczędzenia czasu stała się atrakcyjną zachętą zarówno dla wielkich międzynarodowych korporacji, jak i pojedynczych użytkowników sieci. Oszczędzamy czas, który stracilibyśmy, stojąc w korkach, lecz tracimy coś ważnego – możliwość obcowania z innymi ludźmi.

Oszczędność czasu oraz pieniędzy była istotnym czynnikiem wpływającym na przeniesienie większości procesów przetwarzania danych do systemów informatycznych. Kiedy w 1997 r. powstawała dyrektywa 95/46/WE przepisy kładły większy nacisk na przetwarzanie danych osobowych w formie papierowej niż elektronicznej, szybko jednak okazało się, iż zmiany technologiczne postępują dynamiczniej niż się tego spodziewano.

Rozwój cyberprzestrzeni niewątpliwe należy uznać za wielkie osiągnięcie XX wieku. Jej powstanie doprowadziło do ukształtowania się społeczeństwa informacyjnego, dla którego informacja stała się dobrem podstawowym. Upowszechnienie Internetu umożliwiło szybki, łatwy, a przede wszystkim tani dostęp do informacji. To z kolei przyczyniło się do podniesienia poziomu życia wielu osób, dla których dostęp do wybranych informacji i w innych warunkach nie byłby możliwy. Można więc wysunąć tezę, iż upowszechnienie Internetu doprowadziło do podniesienia poziomu życia jego użytkowników. I chociaż pojęcie jakości życia

45 S. Talar, *Obszary i sposoby oddziaływania Internetu na gospodarkę narodową*, „Przegląd Zachodniopomorski" 2013, t. XXVIII, z. 3, s. 326.

jest bardzo subiektywne, to z całą pewnością można przychylić się do twierdzenia, że w wirtualnym świecie każdy użytkownik ma prawo do samorealizacji[46].

O potrzebie dalszego rozwoju w tym obszarze świadczy chociażby Komunikat Komisji Europejskiej *Europa 2020*, w którym za jeden z priorytetów uznano „dążenie do upowszechnienia szybkiego Internetu i umożliwienie gospodarstwom domowym i przedsiębiorcom czerpanie korzyści z jednolitego rynku cyfrowego"[47]. W ramach UE tworzone są liczne ośrodki oraz inicjatywy skupiające się wokół nowoczesnych rozwiązań technologicznych. Bardzo często łączą one różne środowiska (biznes, szkolnictwo), by zaproponować użytkownikom nowe rozwiązania technologiczne.

W ocenie autora postęp technologiczny, którego jesteśmy świadkami, zmienił, zmienia i będzie zmieniać nasze życie każdego dnia. Niemniej jednak należy mieć na uwadze, że poza swoimi zaletami cyberprzestrzeń jest także obszarem, w którym upowszechniło się wiele nowych, nieznanych dotąd zagrożeń. Bardzo szybko okazało się, że cechy wyróżniające tę przestrzeń okazały się jej słabymi punktami. Dodatkowo, brak przepisów prawnych regulujących funkcjonowanie w cyberprzestrzeni miał decydujący wpływ na podjęcie starań zmierzających do zapewnienia bezpieczeństwa w tym obszarze.

46 A. Wassilew, *Technologia ICT a jakość życia*, „Roczniki Kolegium Analiz Ekonomicznych" 2009, z. 20, s. 139, www.researchgate.net [dostęp: 14.07.2018].

47 Komunikat Komisji Europejskiej, *Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu*, Bruksela 03.03.2010 r., www.ec.europa.eu [dostęp: 17.06.2018].

Rozdział 2

Przetwarzanie danych osobowych w cyberprzestrzeni

Powstanie oraz upowszechnienie Internetu doprowadziło do ukształtowania społeczeństwa informacyjnego, w którym informacja zyskała nowy wymiar – stała się dobrem równie cennym jak dobra materialne. Im jest ciekawsza, mało znana, tym bardziej wartościowa. Internet umożliwił szybkie i tanie pozyskiwanie, przetwarzanie i przechowywanie danych, stając się tym samym nieodzownym elementem naszego życia. Dostęp do wirtualnego świata stał się warunkiem umożliwiającym funkcjonowanie w świecie realnym. Za jego pośrednictwem użytkownicy mogą nie tylko przetwarzać zebrane informacje, ale i wyrażać opinie na ich temat.

W niniejszym rozdziale przybliżone zostanie zagadnienie przetwarzania danych w cyberprzestrzeni. Wyróżnione zostaną kategorie danych osobowych najczęściej przetwarzanych w świecie wirtualnym. Przedstawione zostaną również przepisy prawne regulujące przetwarzanie danych oraz ich skuteczność – czy jest taka sama w świecie realnym i wirtualnym.

2.1. Informacja a dane osobowe

Informacja w XX weku nabrała dużego znaczenia. Nie ulega wątpliwości, że od zawsze w dziejach ludzkości zajmowała istotne miejsce. Jednak dopiero powstanie Internetu pozwoliło na rozpowszechnianie informacji na niespotykaną dotąd skalę. Stało się to za sprawą przełamania dwóch najpoważniejszych dotąd przeszkód: bariery czasu i przestrzeni. Pojęcia „informacja" i „dane" (w tym dane osobowe) bardzo często stosowane są zamiennie. W praktyce jednak okazuje się, że precyzyjne

określenie obu pojęć ma istotne znaczenie dla procesu ich przetwarzania. Brak jednoznacznych definicji rodzi wątpliwości. Wraz z upowszechnieniem przetwarzania danych i informacji w wirtualnym świecie zyskały one nowe atrybuty, poszerzył się także zakres znaczeniowy tych pojęć. Dla przykładu, właściwe zdefiniowanie, czym są dane osobowe ma kluczowe znaczenie w zapewnieniu osobie, której dane dotyczą, przysługujących jej praw.

Pojęcie „informacja" ma charakter szerszy niż pojęcie „dane osobowe". Informacją jest to, co się zmienia i wspomaga zrozumienie, natomiast dane stanowią wejście do kanału komunikacji. Dane są materialne i składają się z numerów, słów, rozmów telefonicznych lub wydruków komputerowych wysyłanych lub otrzymywanych. Dane nie staną się informacją dopóki ludzie nie użyją ich do poprawy swojego zrozumienia[48]. W przeciwieństwie do danych, informacja ma charakter subiektywny. To od nas zależy, w jaki sposób informacja zostanie zinterpretowana. Jak zauważyli Mariusz Grabowski i Agnieszka Zając, aby dane stały się informacją, niezbędna jest aktywność odbiorcy, który decyduje, czy dane są dla niego zrozumiałe oraz czy chce je zinterpretować. W ocenie autorów kolejnym krokiem jest ustalenie, czy powstała w ten sposób wiadomość jest wyłącznie powtórzeniem czegoś, co już wie czy też stanowi dla niego element nowości. Jeżeli tak się dzieje, wówczas wiadomość staje się informacją[49]. Jednym z rodzajów danych przetwarzanych w cyberprzestrzeni są dane osobowe. Zalicza się do nich wszelkie informacje, które pozwalają na zidentyfikowanie osoby fizycznej.

Obecnie obowiązująca definicja danych osobowych zaproponowana w rozporządzeniu 2016/679 stanowi w dużej mierze powielenie obowiązującej dotychczas definicji zawartej w dyrektywie 95/46/WE. W myśl art. 4 rozporządzenia 2016/679 danymi osobowymi są informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego, jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Danymi osobowymi będą takie informacje, które pozwalają na ustalenie tożsamości osoby fizycznej bez nadzwyczajnego wysiłku i nakładów finansowych przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł[50].

---

48 M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, s. 3., www.uci.agh.edu.pl [dostęp: 12.06.2018].

49 Ibidem, s. 5.

50 *Czym są dane osobowe, jak interpretować art. 6.ust. 3 ustawy ochronie danych osobowych*, www.giodo.gov.pl [dostęp: 21.07.2018].

Obowiązująca definicja danych osobowych nie ma charakteru zamkniętego. W związku z tym pozwala odbiorcy danych ocenić na podstawie występujących kryteriów, czy w określonej sytuacji zachodzą przesłanki uzasadniające uznanie określonych danych za osobowe oraz czy na ich podstawie jesteśmy w stanie ustalić tożsamość osoby fizycznej. Jeżeli tak, podmiot zobowiązany jest stosować standardy określone w rozporządzeniu 2016/679, by zapewnić w najwyższym stopniu ich ochronę. Nie ma przy tym znaczenia obywatelstwo czy miejsce zamieszkania takiej osoby.

Przepisy rozporządzenia 2016/679 nie będą miały zastosowania w stosunku do danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw, w tym danych o firmie, jej formie prawnej oraz danych kontaktowych. Odnosić się to będzie również do osób fizycznych, których dane osobowe, ze względu na pełnione funkcje, są ujawnione w internetowym systemie Krajowego Rejestru Sądowego. Przy czym dotyczy to danych związanych z pełnieniem określonych funkcji, a nie w ogóle.

Przepisy rozporządzenia 2016/679 regulujące sposób przetwarzania danych osobowych mają zastosowanie wobec osób prowadzących działalność gospodarczą. Jest to istotna zmiana w stosunku do stanu prawnego obowiązującego przed 25 maja 2018 r., bowiem zgodnie z art. 39b ustawy z dnia 25 września 2015 r. o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw[51] do jawnych danych i informacji udostępnionych przez Centralną Ewidencję i Informację Działalności Gospodarczej nie stosuje się przepisów ochrony danych osobowych z wyjątkiem art. 14–19a i art. 21–22a oraz rozdziału 5. ustawy o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw. Wraz z wejściem w życie rozporządzenia 2016/679 zapis ten stracił na aktualności, co dodatkowo zostało podkreślone przez Komisję Europejską, która stanęła na stanowisku, że firmy, które znajdują się w CEIDG nie są osobami prawnymi, a co za tym idzie nie podlegają wyłączeniu stosowania przepisów rozporządzenia 2016/679[52]. Wynika z tego, że inne standardy będą stosowane do przetwarzania danych osobowych znajdujących się w jawnym rejestrze KRS, inne zaś w stosunku do CEIDG.

Dokonując charakterystyki danych osobowych nie można pominąć szczególnej kategorii danych osobowych. Katalog danych mieszczących się w tym pojęciu został poszerzony w stosunku do obowiązującego w dyrektywie 94/46/WE i obecnie zgodnie z art. 9 obejmuje przetwarzanie danych osobowych ujawniających pochodzenie rasowe, przynależność do związków zawodowych oraz przetwarzania danych

51 Dz.U. z 2015 r., poz. 1893.

52 I. Jackowska, *Firma Kowalski wyłączona z RODO*, www.pb.pl [dostęp: 15.07.2018].

genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności oraz orientacji seksualnej tej osoby. Wyodrębnienie powyższych danych jest celowe, bowiem, co do zasady, ich przetwarzanie jest zabronione, chyba że zachodzi jedna z przesłanek określonych w art. 9 ust. 2 rozporządzenia 2016/679. Przetwarzanie szczególnej kategorii danych osobowych wiąże się także z dodatkowymi obowiązkami ADO w zakresie zapewnienia ich bezpieczeństwa. Jest to szczególnie ważne w przypadku przetwarzania tego rodzaju danych osobowych w systemach informatycznych. Administrator danych osobowych, uwzględniając charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych powinien zastosować odpowiednie środki techniczne i organizacyjne (art. 24 rozporządzenia 2016/679).

2.2. Charakterystyka danych osobowych przetwarzanych w cyberprzestrzeni

Zapewnienie bezpieczeństwa danych osobowych przetwarzanych w cyberprzestrzeni wymaga właściwego określenia, którym z nich nadaje się status danych osobowych i jakie konsekwencje prawne przynosi ten wybór. Katalog danych osobowych podlegających standardom rozporządzenia 2016/679 uległ poszerzeniu w stosunku do katalogu danych przetwarzanych na podstawie dyrektywy 95/46/WE. Jest to szczególnie istotne w przypadku przetwarzania danych w cyberprzestrzeni, zwłaszcza, że bardzo długo nie było jednoznacznego stanowiska wskazującego, czy adres IP i adres e-mail stanowią dane osobowe.

2.2.1. Adres IP

Zgodnie z art. 2 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[53] IP to oznaczenie systemu teleinformatycznego umożliwiającego porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Każde urządzenie w sieci ma nadany adres IP (Internet Protocol), który służy jego identyfikacji. Adres IP nie występuje samodzielnie. Zazwyczaj odnoszą się do niego inne informacje, które stwarzają realną możliwość identyfikacji osoby korzystającej z sieci[54]. Jak zauważył Naczelny Sąd Administracyjny, IP jest informacją dotyczącą komputera, a nie konkretnej osoby fizycznej,

53 Tekst jedn. Dz.U. z 2017 r., poz. 1219 ze zm.

54 Wyrok WSA w Warszawie z 14 maja 2009 r., II SA/Wa 567/09.

zwłaszcza wtedy, gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej[55]. Tym samym IP jest informacją, która w tylko sposób pośredni pozwala zidentyfikować osobę posługującą się nim.

Do czasu wejścia w życie rozporządzenia 2016/679 to, czy adres IP należy do danych osobowych nie wynikało wprost z przepisów prawa. Grupa Robocza art. 29 w wydanej opinii w sprawie pojęcia danych osobowych uznała adres IP za dane osobowe[56]. W ocenie Grupy Roboczej art. 29 „dostawcy dostępu do Internetu, administratorzy sieci lokalnych mogą, używając sposobów, jakimi można się posłużyć, zidentyfikować użytkowników Internetu, którym przydzielili adresy IP, ponieważ systematycznie «rejestrują» oni w pliku datę, godzinę, czas trwania i dynamiczne adresy IP przydzielone użytkownikom Internetu. To samo można powiedzieć o dostawcach usług internetowych prowadzących rejestr na serwerze http. W takich przypadkach można niewątpliwie mówić o danych osobowych"[57]. Stanowisko to zostało następnie potwierdzone przez Wojewódzki Sąd Administracyjny w Warszawie, który uznał, że „adres IP stanowi dane osobowe, gdy jest na stałe przypisany do określonego urządzenia użytkowanego przez dany podmiot"[58].

Trudnością pojawiającą się przy pojęciu adresu IP jest sytuacja, w której z jednego urządzenia korzysta wielu użytkowników (np. kafejki internetowe). Adres IP nie jest wówczas w żaden sposób związany z użytkownikiem, co za tym idzie nie jesteśmy w stanie ustalić jego tożsamości[59]. Najnowsze stanowisko Trybunału Sprawiedliwości UE wskazuje, by uznać za dane osobowe dynamiczne adresy IP, czyli takie, które zmienią się za każdym połączeniem z Internetem. Będzie to jednak możliwe wówczas, gdy administrator prowadzący stronę będzie dysponował mechanizmami umożliwiającymi identyfikację osoby, której dane dotyczą[60].

Prawodawca unijny w rozporządzeniu 2016/679 wskazuje wprost identyfikator internetowy jako dane pozwalające na zidentyfikowanie osoby fizycznej. Identyfikatorem może być zarówno adres IP, jak i identyfikatory plików cookies (motyw 30 preambuły rozporządzenia 2016/679). W ocenie ustawodawcy mogą one bowiem pozostawić ślad, który w połączeniu z innymi informacjami może zostać wykorzystany do tworzenia profili i identyfikacji użytkowników.

---

55 Wyrok NSA z 19 maja 2011 r., I OSK 1079/10.

56 Grupa Robocza art. 29, Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta 20 czerwca 2007 r., WP 136, s. 16.

57 Ibidem.

58 Wyrok WSA w Warszawie z 3 lutego 2010 r., II SA/Wa 1598/09.

59 Ibidem.

60 Wyrok TSUE z 19 października 2016 r., Patric Breyer przeciwko Bundesrepublik Deutschland C-582/14, ECLI:EU:C:2016:779, http://curia.europa.eu/juris/liste.jsf?num=C-582/14&language=PL [dostęp: 12.06.2018].

Ustalenie, czy adres IP stanowi dane osobowe ma istotne znaczenie z punktu widzenia ADO w kontekście obowiązków nałożonych na niego przez obowiązujące przepisy prawa. Administrator danych osobowych może zostać poproszony o udostępnienie adresu IP innego użytkownika. W sytuacji, w której zostanie stwierdzone, że IP stanowi dane osobowe ADO powinien ocenić, czy istnieją przesłanki uzasadniające udostępnienie takiego adresu. Właściwą procedurą jest skierowanie do ADO pisemnego wniosku, na podstawie którego podejmie on właściwą decyzję. Należy jednak pamiętać, że udostępnienie danych wiąże się z utratą nad nimi kontroli i każdorazowa decyzja w tym zakresie powinna być poprzedzona wnikliwą analizą sytuacji przez ADO.

Przykład

Z podobnym wnioskiem wystąpiła do spółki X jedna z internautek. Wobec odmowy na prośbę o udostępnienie adresu IP innego internauty, skierowała sprawę do GIODO[61]. Organ orzekający na podstawie wydanej decyzji administracyjnej nakazał spółce X udostępnienie adresów IP osób, które w dniu wskazanym przez wnioskodawczynię zalogowały się i dokonywały wpisów na stronie internetowej administratora.

W odpowiedzi na decyzję GIODO spółka X stwierdziła, że nie jest w stanie sama tego fizycznie uczynić, wskazując dodatkowo, że udostępnienie adresów IP stanowiłoby naruszenie dóbr osobistych tych osób. Ponadto, spółka X podnosiła, iż „IP nie można było uznać za informację o osobie, a jedynie za «informację o numerze interfejsu lub sieci, przy wykorzystaniu którego lub której miała miejsce komunikacja polegająca na dokonaniu [...] kwestionowanych wpisów»". Spółka X zaskarżyła decyzję GIODO oraz wniosła o uchylenie decyzji w całości i oddalenie wniosku.

Na podstawie wydanej decyzji GIODO utrzymał w mocy zaskarżoną decyzję. W związku z tym spółka skierowała sprawę do WSA w Warszawie. W uzasadnieniu skargi pełnomocnicy spółki zwracali uwagę, że „wnioskodawczyni nie ma żadnej możliwości dokonania identyfikacji osób, które zalogowały się i dokonały wpisów na portalu, gdyż nie dysponuje jakimikolwiek informacjami, które taką identyfikację by jej umożliwiały, choćby nawet pośrednio"[62]. W ocenie pełnomocników „numery IP odnoszą się wyłącznie do oznaczenia urządzeń, a nie osób i same w sobie nie niosą informacji o konkretnej osobie. Zdaniem strony skarżącej powiązanie

61 Wyrok WSA w Warszawie z 3 lutego 2010 r., II SA/Wa 1598/09.

62 Ibidem.

przez wnioskodawczynię numerów IP, czyli informacji o urządzeniach, za pomocą których następowało logowanie i umieszczanie wpisów na forum serwisu [...] z konkretną osoba fizyczną nie jest technicznie możliwe". W uzasadnieniu sąd zauważył, że „adres IP stanowi dane osobowe, gdy jest na stałe przypisany do określonego urządzenia, użytkowanego przez określony podmiot"[63]. Co za tym idzie w określonych sytuacjach możliwa jest identyfikacja użytkownika. W ocenie sądu sam adres IP komputera nie wystarcza do wskazania osoby, która z niego korzystała, ale w zestawieniu z innymi informacjami pozwala na ustalenie tożsamości osoby fizycznej[64].

Naczelny Sąd Administracyjny w wyroku z 19 maja 2011 r. oddalił skargę kasacyjną, wskazując w sentencji wyroku, że „tam gdzie adres IP jest na dłuższy okres czasu lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacją umożliwiającą identyfikację konkretnej osoby fizycznej"[65].

Uznanie adresu IP za dane osobowe stanowi także potwierdzenie tezy głoszącej, że Internet zapewnia nam wyłącznie pozorną anonimowość. Na podstawie tego adresu jesteśmy w stanie (w większości przypadków) ustalić tożsamość użytkownika. Internet często pozornie, a czasami faktycznie zapewnia anonimowość jego użytkownikom. Stanowi medialne forum, na którym prezentowane są treści naruszające ludzką godność, cześć i dobre imię[66]. Dlatego też wszędzie tam, gdzie numer IP pozwala pośrednio na identyfikację konkretnej osoby fizycznej powinien on być uznany za dane osobowe.

2.2.2. Dane biometryczne

Dane biometryczne to dane zaliczane do szczególnej kategorii danych osobowych. Zgodnie z definicją przyjętą na gruncie rozporządzenia 2016/679 dane biometryczne są danymi osobowymi, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby i są to takie cechy, jak wizerunek twarzy lub dane daktyloskopijne. Typowymi przykładami danych biometrycznych są odciski palców, wzorzec siatkówki, struktura twarzy, głos, ale także geometria dłoni, układ żył. Technologia biometryczna jest wykorzystywana

63 Ibidem.
64 Ibidem.
65 Wyrok NSA z 19 maja 2011 r., I OSK 1079/10.
66 Ibidem.

przede wszystkim do weryfikacji i identyfikacji tożsamości osoby fizycznej[67]. Dane biometryczne pozwalają na bardzo precyzyjne ustalenie tożsamości osoby fizycznej. W literaturze przedmiotu wskazuje się, że granica błędu wynosi około 0,00001%[68]. Ten rodzaj danych jest wykorzystywany coraz częściej nie tylko jako „bezbłędny" identyfikator osoby fizycznej, ale także jako mechanizm uwierzytelnienia użytkownika telefonu czy komputera. Coraz chętniej pracodawcy używają ich w celu ewidencji czasu pracy pracowników oraz zapewnienia dostępu do wybranych pomieszczeń.

Przetwarzanie danych osobowych szczególnie chronionych powinno odbywać się z pełnym poszanowaniem przepisów prawa, w tym również zasadą celowości. Problem ten był rozstrzygany przy okazji sporu, jaki powstał w związku z pobieraniem odcisków palców pracowników w celu ewidencji czasu ich pracy. Generalny Inspektor Ochrony Danych Osobowych wskazał, że „gromadzenie przez pracodawcę odcisków linii papilarnych, obrazu tęczówki czy kodu DNA pracowników w celu kontroli czasu pracy jest zabronione"[69]. Podobne stanowisko prezentuje NSA, wskazując, że wykorzystywanie danych biometrycznych do kontroli czasu pracy pracowników zatrudnionych w Urzędzie Skarbowym jest nieproporcjonalne do zamierzonego celu ich przetwarzania.

Dane biometryczne uznajemy za dane osobowe wówczas, gdy za ich pośrednictwem jesteśmy w stanie ustalić tożsamość osoby fizycznej. Prawodawca unijny w rozporządzeniu 2016/679 zakazuje, co do zasady, przetwarzać dane biometryczne z wyjątkiem przypadków enumeratywnie wymienionych w art. 9 rozporządzenia 2016/679, wśród których wymienia się chociażby zgodę osoby, której dane dotyczą, oraz gdy przetwarzanie jest niezbędne do wypełniania obowiązków wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego, i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego. Dodatkowo, jeżeli przetwarzanie danych osobowych przy wykorzystaniu nowych technologii może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO jeszcze przed rozpoczęciem przetwarzania danych osobowych jest zobowiązany dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Dane biometryczne coraz częściej wykorzystywane są w wirtualnym świecie przez banki w celu uwierzytelnienia tożsamości klientów. Sektor bankowy posiada już w tym zakresie bogate doświadczenie. Jak zauważa Tomasz Brzostowski

---

67 W. Wiewiórowski, wystąpienie GIODO podczas konferencji naukowej *Bezpieczeństwo technologii biometrycznych – ochrona danych biometrycznych*, UKSW, Warszawa 09.12.2011 r.

68 GIODO o zagrożeniach płynących z upowszechniania danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi, www.giodo.gov.pl, s. 14 [dostęp: 23.11.2018].

69 Sprawozdanie z działalności GIODO w 2013 r., www.giodo.gov.pl [dostęp: 23.11.2018].

rozwiązania biometryczne wykorzystujące naczynia krwionośne klienta zostały po raz pierwszy wykorzystane we Francji w 2007 r.[70]. Zastosowane rozwiązanie nie wymagało użycia przez użytkownika karty. Coraz częściej wykorzystywane są skanery linii papilarnych czy też elektroniczna analiza głosu[71].

Przetwarzanie danych biometrycznych związane jest z obowiązkiem ADO zapewnienia odpowiednich środków technicznych i organizacyjnych chroniących je przed przypadkowym lub nielegalnym zniszczeniem lub utratą. Jest to szczególnie istotne, bowiem tego typu dane pozwalają na jednoznaczną identyfikację użytkownika.

Problem ten dostrzegła Grupa Robocza art. 29, podkreślając, że „im większa jest ilość wykorzystywanych danych biometrycznych, tym większe jest prawdopodobieństwo kradzieży tych danych"[72]. Istnieją poważne wątpliwości, co do tego, które z mechanizmów bezpieczeństwa należy stosować w celu bezpiecznego przechowywania danych biometrycznych oraz kto powinien mieć dostęp do tego rodzaju danych. Obawy te wynikają przede wszystkim z faktu, że kradzież takich danych może dawać niebezpiecznie nieograniczone możliwości ich nielegalnemu nabywcy. Z uwagi na fakt, że jest to najbardziej wiarygodna metoda uwierzytelnienia użytkownika, każda z pozostałych metod może okazać się wtórna. Dodatkowo przetwarzanie danych biometrycznych może powodować naruszenie prywatności osoby fizycznej. Dane te mogą być wykorzystywane w innym celu niż zostały zebrane. Pozwalają one nie tylko na precyzyjną identyfikację osoby fizycznej, ale także dostarczają szeregu innych informacji na jej temat[73].

W ocenie autora przetwarzanie danych biometrycznych jest nieuniknionym elementem naszego życia. Pozwala powiem na jednoznaczne określenie (potwierdzenie) tożsamości osoby fizycznej. Niemniej jednak z uwagi na szkody, jakie może nieść za sobą utrata lub dostęp do danych biometrycznych przez osobę do tego nieupoważnioną warto zastanowić się nad tym, czy nie decydować się na zastosowanie rozwiązań umożliwiających przetwarzanie danych biometrycznych dopiero wówczas, gdy nie ma innych metod zapewniających realizację założonego celu. Nick jest taką daną, która w zestawieniu z innymi danymi (np. IP) pozwoli w sposób pośredni lub bezpośredni na zidentyfikowanie osoby fizycznej.

---

70 T. Brzostowski, *Innowacje, technologie, zagrożenia w świecie XXI wieku – z perspektywy finansów*, www.alterum.pl, s. 18 [dostęp: 12.07.2018].

71 J. Mlaskawa, *Biometria w bankowości – szanse i zagrożenia Banku przyszłości*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2015, nr 3, www.cejsh.icm.edu.pl, s. 110 [dostęp: 26.10.2018].

72 Grupa Robocza art. 29, Opinia 3/2012 w sprawie zmiany sytuacji w dziedzinie technologii biometrycznej przyjęta 27 kwietnia 2012 r., WP 193, s.17, www.giodo.gov.pl [dostęp: 23.05.2018].

73 J. Mlaskawa, *Biometria*..., op. cit., s.117.

2.2.3. Nickname

Nickname oznacza przydomek, pseudonim użytkownika. Najczęściej wykorzystywany jest przez użytkownika, który nie chce w cyfrowym świecie posługiwać się swoimi prawdziwymi danymi. Nick składa się z wybranych przez użytkownika znaków graficznych, którymi użytkownik posługuje się w sieci. Nie ma przeszkód, by nickiem użytkownika były również jego imię i nazwisko. Co do zasady, użytkownicy identyfikują się z wybranym przez siebie nickiem i nie zmieniają go zbyt często. Mogą również, łącząc się za każdym razem z określonym serwisem internetowym posługiwać się innym nickiem.

W ocenie Sądu Najwyższego nick nawiązuje wprost do pojęcia pseudonimu, w związku z czym zasługuje na ochronę prawną. Co więcej, organ orzekający zauważył, że „w miarę zwiększania się ilości usług świadczonych Internetowo, może okazać się, że znaczenie nazwy użytkownika będzie dla poszczególnych osób równie ważne jak nazwisko”[74]. Tym samym nick został zrównany z innymi danymi pozwalającymi na ustalenie tożsamości osoby fizycznej.

W świetle omawianej problematyki istotne wydaje się ustalenie, czy nick może zostać uznany za dane osobowe. Jest to szczególnie ważne w związku z przetwarzaniem tego rodzaju danych w cyberprzestrzeni. Często sam nick nie pozwoli na ustalenie tożsamości osoby fizycznej, ale może stanowić jedną z informacji pośrednio pozwalających na ustalenie tożsamości użytkownika. Wówczas zestaw takich danych, wśród których znajduje się nick może być w określonych sytuacjach uznany za dane osobowe. Poprzez nick osoba fizyczna może zostać zidentyfikowana przez innych użytkowników, zwłaszcza jeżeli posługuje się nim stale. Tak więc „nick nie ma wyłącznie charakteru technicznego i służy do indywidualizacji operacji”[75].

2.2.4. Wizerunek

Podczas analizy pojęcia „wizerunek” należy stwierdzić, że wraz z rozwojem technologicznym ulegało ono systematycznemu rozszerzeniu. W przeszłości królowie, książęta, bogate mieszczaństwo zamawiało swoje portrety, by upamiętnić swój wizerunek. W późniejszych czasach wraz z upowszechnieniem aparatów fotograficznych wizerunek człowieka utrwalany był na kliszy dostępnej coraz szerszym masom. Pojawienie się aparatów cyfrowych rozpropagowało fotografię cyfrową. W końcu popularyzacja telefonów komórkowych umożliwiła szybkie i tanie utrwalanie wizerunku. Internet zaś stał się narzędziem umożliwiającym umieszczanie

74 Wyrok SN z 11 marca 2008 r., II CSK 539/07.

75 Ibidem.

zdjęć w wirtualnej przestrzeni, rozpowszechnianie wizerunku na szeroką skalę oraz jego modyfikację poprzez dedykowane programy komputerowe.

Dotychczas nie udało się wypracować jednej definicji określającej, czym jest wizerunek. Wynika to m.in. z tego, że ulega on ciągłemu rozwojowi, o czym świadczy fakt, iż coraz częściej wymienia się także głos, tatuaże, fryzurę czy ubiór jako elementy wizerunku[76].

Anna Wszołek, przybliżając to pojęcie podkreśla, że wizerunek jest rzeczywistym lub utrwalonym w jakiejś postaci zewnętrznym wyglądem fizycznym danej osoby mającym zindywidualizowany charakter[77]. Jan Błeszyński definiuje wizerunek jako cały obraz fizyczny umożliwiający zidentyfikowanie danej osoby[78]. Natomiast Janusz Barta i Ryszard Markiewicz opisują wizerunek znacznie szerzej, uznając, że jest to wytwór niematerialny, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby[79].

Wizerunek jest dobrem osobistym podlegającym reżimom nie tylko ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny[80], ale także ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[81]. Zgodnie z dyspozycją art. 23 kc stanowi on jedno z podstawowych dóbr osobistych człowieka obok zdrowia, wolności, czci, swobody sumienia, nazwiska lub pseudonimu, oraz tajemnicy korespondencji.

Zasady regulujące przetwarzanie wizerunku zostały uregulowane w prawie autorskim, gdzie w art. 81 upapp wskazano, że rozpowszechnianie wizerunku wymaga zgody osoby na nim przedstawionej. Z powodu braku wyraźnego zastrzeżenia zgoda nie jest wymagana, jeżeli ta osoba otrzymała umówioną zapłatę. Zgodnie zaś z art. 81 ust. 2 upapp zgoda nie jest wymaga przy rozpowszechnianiu wizerunku osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych czy zawodowych. Określenie wzajemnych relacji powyższych przepisów prawa jest takie, że prawo autorskie stanowi *lex specialis* do *lex generalis* prawa cywilnego.

Wraz z rozwojem techniki pojęcie wizerunku ulegało poszerzeniu. Sąd Najwyższy w jednym z wyroków wskazuje, że wizerunek to nie tylko „dostrzegalne dla

---

76 A. Wszołek, *Między Facebookiem a Instagramem. Wirtualny wizerunek czy prawo majątkowe? –analiza dóbr cyfrowych in concreto*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 3, s. 134.

77 Ibidem.

78 J. Błeszyński, *Prawo autorskie*, Warszawa 1988, s. 155.

79 J. Barta, R. Markiewicz, *Ochrona wizerunku, adresata korespondencji i tajemnicy źródeł informacji*, [w:] J. Barta i in., *Prawo autorskie i prawa pokrewne. Komentarz*, Kraków 2005, s. 628.

80 Tekst jedn. Dz.U. z 2018 r., poz. 1025 ze zm.

81 Tekst jedn. Dz.U. z 2018 r., poz. 1191 ze zm.

otoczenia cechy fizyczne ale także dodatkowe utrwalone elementy (...) jak ubiór, sposób poruszania się i kontaktowania z otoczeniem"[82].

Jakie są więc konsekwencje uznania wizerunku za dane osobowe? Najistotniejszą z nich jest fakt, że osoba, której wizerunek jest przetwarzany, podlega ochronie rozporządzenia 2016/679. Dodatkowo, upublicznianie nagrań, zdjęć na których został utrwalony wizerunek osoby fizycznej jest możliwe, co do zasady, za zgodą osoby, której dane dotyczą.

Przetwarzanie wizerunku w Internecie jest przede wszystkim związane z publikowaniem zdjęć na portalach społecznościowych. Za sprawą ich szybkiego rozwoju pojęcie wizerunku uległo kolejnemu rozszerzeniu. Nie jest to już tylko publikowanie zdjęć na naszym profilu, ale także wszelkie informacje związane z naszą osobą umieszczane w sieci[83]. Poprzez profil dowiadujemy się, co użytkownik lubi, jakie miejsca odwiedza, gdzie pracuje, a nawet gdzie mieszka. Inni użytkownicy dowiadują się o nas na podstawie naszych profili tego samego, co oznacza, że mamy wpływ na to, jak odbierają nas inni użytkownicy.

Chociaż umieszczanie zdjęć na portalach społecznościowych jest tylko jedną z form rozpowszechniania wizerunku, przetwarzanie go w ten sposób wzbudza wiele wątpliwości. W jednej z rozstrzyganych przed GIODO spraw, imię i nazwisko skarżącego zostały podane pod jego wizerunkiem sprzed wielu lat. W ocenie organu orzekającego zestawienie zdjęcia z dalekiej przeszłości wraz z imieniem i nazwiskiem określonej osoby oraz nazwa szkoły podstawowej, do której uczęszczał nie pozwala na identyfikację tej osoby bez nadmiernych kosztów i czasu, co za tym idzie nie może zostać uznane za dane osobowe[84].

Ze stanowiskiem tym nie zgodził się jednak WSA w Warszawie, który uznał, że wizerunek osoby fizycznej, wraz z jej imieniem i nazwiskiem stanowią dane osobowe[85]. Wobec powstałych wątpliwości prawnych, NSA zwrócił uwagę, że osoba, której dane osobowe zostały ujawnione w Internecie w postaci zdjęcia zamieszczonego na portalu społecznościowym jest możliwa do zidentyfikowania przez nieokreśloną liczbę osób. Sąd, rozstrzygając powyższe uznał, że zdjęcie zawierające wizerunek osoby fizycznej oraz jej imię i nazwisko stanowi dane osobowe. Naczelny Sąd Administracyjny zauważył także, że o zakwalifikowaniu danej informacji do kategorii danych osobowych decydują przede wszystkim obiektywne kryteria oceny, przy czym uwzględnić należy wszystkie informacje, w tym także pozajęzykowe, do jakich dostęp mają osoby trzecie. Dodatkowo

82 Wyrok SN z 20 maja 2004 r., II CK 330/03.

83 A. Wszołek, *Między...*, op. cit., , s. 134.

84 Wyrok NSA z 18 listopada 2009 r., I OSK 667/09.

85 Wyrok WSA w Warszawie z 3 marca 2009 r., II SA/Wa 1495/08.

w ocenie NSA, gdyby wizerunek skarżącego nie występował wraz z podpisem w postaci imienia i nazwiska, to bez wątpienia ustalenie jego tożsamości wymagałoby nadmiernych kosztów, czasu lub działań.

Warto mieć świadomość, że publikowanie wizerunku w Internecie naraża nas na rozpowszechnienie go na szeroką skalę. Jeżeli jednak publikujemy zdjęcia, na których utrwalone zostały także inne osoby (zdjęcie grupowe podczas wycieczki lub szkolenia) wówczas przed opublikowaniem takiego zdjęcia niezbędne jest uzyskanie zgody tych osób jako podstawy legalizującej przetwarzanie danych. Zgodą w świetle przepisów rozporządzenia 2016/679 jest dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych (art. 4 pkt 11 rozporządzenia 2016/679). Mimo że przepisy prawa nie wymagają od osoby, której dane dotyczą, złożenia oświadczenia w formie pisemnej, zalecane jest odebranie oświadczenia woli osoby, której dane dotyczą, w formie pisemnej, aby ochronić tę osobę przed mogącymi wystąpić w tym zakresie roszczeniami. Jeżeli nie jesteśmy w stanie zidentyfikować osób na zdjęciu lub stanowią one tło wydarzenia utrwalonego na fotografii wówczas zgoda takich osób nie jest wymagana.

Z przetwarzaniem wizerunku w wirtualnym świecie coraz częściej spotkamy się także w przypadku umieszczania przez pracodawców zdjęć pracowników na firmowej stronie internetowej. Na tym tle rodzą się wątpliwości, czy pracodawca może „zmusić" pracownika do zrobienia zdjęcia i umieścić je na firmowej stronie internetowej? Czy wizerunek pracownika utrwalony w formie fotografii może być wykorzystywany przez pracodawcę również po rozwiązaniu stosunku pracy? Co w sytuacji, w której pracownik odmawia umieszczenia zdjęcia na firmowej stronie internetowej?

Zgodnie z obowiązującymi przepisami prawa pracy, pracodawca może zbierać od pracownika informacje dotyczące imienia i nazwiska, daty urodzenia, danych kontaktowych wskazanych przez tę osobę, wykształcenia, kwalifikacji zawodowych, przebiegu dotychczasowego zatrudnienia, adresu zamieszkania, numeru PESEL, innych danych osobowych pracownika, jego dzieci i innych najbliższych członków rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Wśród tych danych nie wymienia się jednak wizerunku pracownika.

2.2.5. Adres poczty elektronicznej

Adres poczty elektronicznej – e-mail (electronic mail) – związany jest ze świadczeniem usług drogą elektroniczną polegającą na wysyłaniu i odbierani poczty. Po raz

pierwszy wiadomość e-mailowa została wysłana w 1971 r. przez Raya Tomlinsona[86]. Od tego czasu stała się podstawowym narzędziem komunikacji umożliwiającym wysyłanie nie tylko wiadomości tekstowej. W porównaniu z pocztą tradycyjną, posługiwanie się e-mailem jest szybsze i tańsze.

Zazwyczaj adres poczty elektronicznej składa się z określonego ciągu liter (najczęściej imię i nazwisko lub kombinacje liter imienia i nazwiska), znaku „@" oraz domeny internetowej, wskazującej dostawcę usługi internetowej. W świetle omawianej problematyki należy zastanowić się, czy takie zestawienie danych stanowi podstawę do uznania adresu poczty e-mail za dane osobowe. Analiza ta powinna być każdorazowo przeprowadzana indywidualnie z uwagi na fakt, iż nie jest możliwe jednoznaczne przesądzenie, że adres e-mail zawsze będzie stanowił dane osobowe. Adres taki będzie uznany za dane osobowe, jeżeli za jego pośrednictwem w sposób pośredni lub bezpośredni możliwe będzie ustalenie tożsamości jego użytkownika. W takiej sytuacji niezbędne jest ocenienie, czy za pośrednictwem wskazanego adresu jesteśmy w stanie ustalić tożsamość użytkownika poczty. Jeżeli tak, wówczas adres taki należy uznać za dane osobowe. Z taką właśnie sytuacją będziemy mieli do czynienia wówczas, gdy adres poczty użytkownika składa się z jego pełnego imienia i nazwiska oraz nazwy firmy, w której pracuje.

2.3. Wybrane metody przetwarzania danych osobowych w cyberprzestrzeni

2.3.1. Big data

Nie ulega wątpliwości, że powstanie Internetu pozwoliło na przetwarzanie danych na niespotykaną dotąd skalę. Dodatkowo pojawienie się przenośnych komputerów, powszechnie obecnych telefonów mobilnych, wpłynęło na zwiększenie ilości pojawiających się informacji. W konsekwencji powstały ogromne zbiory danych tzw. big data. Z uwagi na fakt, że ilość przetwarzanych danych w wirtualnym świecie jest ogromna i nie są one usuwane pojawiła się potrzeba wypracowania metod pozwalających na gromadzenie i przechowywanie takich zasobów.

Pojęcie „big data" nie doczekało się polskiego odpowiednika, chociaż polski ustawodawca nie pozostał całkowicie obojętny wobec poruszanej problematyki. Zgodnie z definicją zawartą w art. 2 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych[87] bazą danych jest zbiór danych lub jakichkolwiek innych materiałów i ele-

86 *Nie żyje wynalazca e-mail Ray Tomlinson*, www.forbes.pl [dostęp: 24.09.2018].

87 Dz.U. z 2001 r. nr 128, poz. 1402 ze zm.

mentów zgromadzonych według określonej systematyki lub metody indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości.

Badacze problematyki przetwarzania danych zwracają uwagę, że big data są zbiorami charakteryzującymi się dużą objętością (volume), wartością (value), zmiennością (variability) oraz szybkością (velocity) ich przetwarzania – tzw. model 4V[88]. Cechą charakterystyczną big data jest możliwość dokonywania analizy danych w czasie rzeczywistym[89]. Z uwagi na fakt, że znajduje się w nich ogromna ilość danych, powstaje problem związany nie tylko z ich przechowywaniem i zapewnieniem bezpieczeństwa, ale także sposobem ich przetwarzania. Big data nie tylko daje taką możliwość, ale także pozwala na ujawnienie nowych związków między danymi, przyczyniając się do dostarczenia nowych zasobów wiedzy[90]. Wśród gromadzonych danych znajdują się także dane osobowe. W bazach tych możemy znaleźć dane osobowe m.in. w postaci imienia, nazwiska, numeru PESEL, adresu zamieszkania, adresu e-mail, numeru telefonu czy wizerunku. Ponieważ informacja stała się towarem posiadającym określoną wartość pojawił się trend polegający na gromadzeniu danych osobowych oraz ich przetwarzaniu dla celów komercyjnych. Tu zaś z punktu widzenia ochrony danych osobowych rodzi się pytanie o metody pozyskiwania tych zasobów. Najczęściej bowiem proces ten odbywa się bez wiedzy użytkowników. Jest to szczególnie istotne wobec faktu, że stosowane metody pozyskiwania danych, a także ich zakres coraz bardziej wkraczają w prywatną sferę życia użytkownika.

Tempo pozyskiwania danych jest niezwykle dynamiczne, czego najlepszym przykładem są portale społecznościowe, z których korzysta dziś ponad 2 miliardy użytkowników[91]. Codziennie każdy z nich umieszcza nowe posty, dzieli się ważnymi lub interesującymi aspektami ze swojego życia. Chociaż aktywność na portalach społecznościowych służy przede wszystkim podtrzymaniu lub odnowieniu relacji koleżeńskich, coraz częściej portale społecznościowe wykorzystywane są do szerszych celów, jak chociażby wymiana informacji czy promowanie własnego biznesu. W tym kontekście zwraca się uwagę, że takie przetwarzanie

88 M. Tabakow, J. Korczak, B. Franczyk, *Big Data – definicje, wyzwania i technologie informatyczne*, „Informatyka ekonomiczna" 2014, nr 1, s. 140.

89 J. Wieczorkowski, *Zagadnienia społeczne i prawne w koncepcji big data*, „Nierówności Społeczne a Wzrost Gospodarczy" 2015, nr 4, s. 324.

90 M. Wójcik, *Big data w zarządzaniu informacją – przegląd wybranych zagadnień*, [w:] *Inspiracje i zarządzanie informacją w perspektywie bibliologii i informatologii*, www.ruj.uj.edu.pl, s. 62 [dostęp: 17.02.2018].

91 M. Kuchta, *Najnowsze dane na temat użytkowników mediów społecznościowych na świecie*, www.spocialpress.pl [dostęp: 08.09.2018].

danych wykracza poza działania o charakterze osobistym i domowym, które wyłączone jest spod reżimów rozporządzenia 2016/679. W ocenie Grupy Roboczej art. 29 „jeżeli użytkownik wykorzystuje serwis społecznościowy głównie jako platformę służącą do osiągania celów komercyjnych, politycznych lub charytatywnych wówczas wyłączenie to nie ma zastosowania. W takim przypadku użytkownik przejmuje pełnię obowiązków administratora danych ujawniającego dane osobowe innemu administratorowi danych lub osobom trzecim. W takich przypadkach użytkownik musi uzyskać zgodę osób zainteresowanych lub wskazać inną podstawę prawną"[92].

W założeniu twórców portali społecznościowych miały być one platformą umożliwiającą użytkownikom stworzenie indywidualnego konta. Za jego pośrednictwem użytkownicy łączą się w grupy, stwarzające możliwość wymiany informacji ze wszystkimi członkami lub tylko pojedynczymi osobami. Grupy tworzone są według różnego kryterium: znajomości, hobby, wykonywanego zawodu itp. Dostęp do danych użytkownika jest, co do zasady, ograniczony do określonego przez niego kręgu osób. Niemniej jednak możliwe jest przetwarzanie danych osobowych użytkownika przez osobę trzecią. Dane osobowe publikowane przez użytkowników na portalach społecznościowych mogą być wykorzystywane także przez inne osoby, co może prowadzić np. do kradzieży tożsamości. Nie ulega wątpliwości, że platforma ta umożliwia szybką i łatwą wymianę informacji, poznanie nowych osób oraz poszerzenie swoich zainteresowań bez potrzeby wychodzenia z domu. W ten sposób każdego dnia generowana jest ogromna ilość danych.

Tak zgromadzone zasoby big data podlegają analizom przez wyspecjalizowane podmioty[93]. Na podstawie profili użytkowników, udostępnianych linków, polubień, deklaracji zainteresowania określonym wydarzeniem lub każdej innej aktywności, przy wykorzystaniu odpowiedniego algorytmu podmioty te są w stanie określić np. poglądy polityczne użytkowników, ich płeć, a nawet orientację seksualną.

Z punktu widzenia problematyki przetwarzania danych osobowych, big data stwarza w ocenie autora zagrożenie dla prywatności osób, których dane dotyczą. Umiejętne wykorzystanie tych danych może umożliwić wpływanie zainteresowanych podmiotów na podejmowane przez nas decyzje. Najlepszym tego przykładem jest sprawa Cambridge Analytica – firmy, która za pośrednictwem Facebooka pozyskała informacje o 50 mln użytkowników bez ich wiedzy[94]. Dzięki analizie

92 Grupa Robocza art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta 12 czerwca 2009 r., WP 163, s. 7.

93 K. Polańska, A. Wassilew, *Analizy big data w serwisach społecznościowych*, „Nierówności Społeczne a Wzrost Gospodarczy" 2015, nr 4, s. 118.

94 *Afera Cambridge Analytica*, www.pcworld.pl [dostęp: 12.07.2018].

ich preferencji na podstawie zadeklarowanych polubień (od 10 do 300 polubień) możliwe stało się stworzenie profili psychologicznych użytkowników[95]. Umożliwiło to kierowanie do nich odpowiednio dopasowanych treści. Miało to miejsce zwłaszcza w stosunku do użytkowników niezdecydowanych. Istnieje duże prawdopodobieństwo, że w ten sposób możliwe było wpłynięcie na wynik ostatnich wyborów prezydenckich w USA czy Polsce.

Na tym tle rodzi się poważne zagrożenie, co do niezależności naszych wyborów, podejmowanych przecież na podstawie informacji, które znajdujemy (albo raczej one nas znajdują) w Internecie. Zagadnienie to zostało szczegółowo opisane w kolejnych rozdziałach publikacji. Duża część gromadzonych danych pochodzi z powszechnie dostępnych źródeł. Dzięki takim bazom użytkownicy mają możliwość ponownego wykorzystania danych oraz łączenia ich z danymi z innych źródeł[96]. Big data pozwala na ukazanie nowych, nieznanych dotąd relacji zachodzących pomiędzy danymi, łączenia ich w niewystępujących dotąd korelacjach. Na tej podstawie jesteśmy w stanie dowiedzieć się znacznie więcej o konkretnym użytkowniku. Dzięki big data możemy zaproponować użytkownikowi lepszą usługę czy produkt. Dostęp do dużych zasobów danych, a także przetwarzanie ich na dużą skalę rodzi poważne ryzyko naruszenia prywatności użytkowników cyberprzestrzeni. Ograniczenie prywatności poprzez wykorzystywanie koncepcji big data może się odbywać poprzez: monitorowanie i śledzenie, rozpowszechnianie i publikację oraz analizę i agregację[97]. Na tych wszystkich polach dochodzi do przetwarzania danych na dużą skalę oraz wykorzystywania mechanizmów ograniczających prywatność osoby fizycznej. Do ograniczenia prawa do prywatności dochodzi najczęściej bez naszej wiedzy m.in. poprzez metodę śledzenia. Coraz częściej też dochodzi do sytuacji, w której to osoba fizyczna sama decyduje się na ograniczenie prawa do prywatności. Jest to cena, którą płaci aktywny uczestnik wirtualnego świata za dostęp do określonych towarów lub usług. I chociaż cena ta jest bardzo wysoka większość z nas godzi się, by ją płacić. Do jak dalekich ograniczeń jesteśmy skłonni? Kiedy dojdziemy do wniosku, że wykorzystywane metody służące pozyskiwaniu informacji o jednostce są zbyt mocno ingerujące w naszą prywatność? Te pytania w ocenie autora długo jeszcze pozostaną bez odpowiedzi.

---

95 *Firma Cambigde Alanytica pomagała we wpływaniu na wyniki wyborów na świecie z wykorzystaniem nowego algorytmu Facebooka*, www.zmianynaziemi.pl [dostęp: 12.07.2018].

96 Warunki powtórnego wykorzystania danych są szczegółowo opisane w ustawie z dnia 25 lutego 2016 r. o ponownym wykorzystaniu informacji sektora publicznego, tekst jedn. Dz.U. z 2018 r., poz. 1243 ze zm. oraz ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej, tekst jedn. Dz.U. z 2018 r., poz. 1330 ze zm.

97 J. Wieczorkowski, *Akceptacja naruszenia prywatności w erze Big Data*, „Nierówności społeczne a Wzrost Gospodarczy" 2017, nr 4, s. 318.

Poza problemem związanym z poszanowaniem prawa do prywatności użytkownika, sprawa Cambridge Analytica ujawniła także inny problem związany z niezależnością i swobodnym wyborem treści przez użytkowników. Na podstawie uzyskanej wiedzy o użytkowniku, w tym przypadku o jego przekonaniach politycznych, poprzez właściwie sformułowane treści możliwe stało się wpływanie na decyzje użytkowników. To zaś rodzi zagrożenie dla prywatności użytkownika oraz podejmowania przez niego świadomej i swobodnej decyzji. Stanowi to prostą drogę do możliwości manipulowania użytkownikami[98]. Takim i podobnym praktykom w założeniu ma przeciwdziałać rozporządzenie 2016/679. Zgodnie z zawartą w nim zasadą transparentności danych, użytkownik powinien mieć pełną świadomość tego, kto oraz w jakim celu wykorzystuje jego dane. Dodatkowo zasada celowości wskazuje, że ADO może przetwarzać dane osobowe tylko i wyłącznie w tym celu, w jakim zostały zebrane. Jeżeli ADO zamierza zmienić cel przetwarzania powinien o tym każdorazowo poinformować osobę, której dane dotyczą. W analizowanej sprawie pozyskiwanie danych nie zawsze odbywało się na podstawie zgody użytkownika. Część z nich w ogóle nie wiedziała, że ich dane są przetwarzane, a to znaczy, iż odbywało się to bez właściwej podstawy prawnej. Warto także podkreślić, że w świetle obowiązujących przepisów prawa, dostawców aplikacji można uznać za samodzielnych ADO, jeżeli tworzą aplikacje, które funkcjonują obok serwisu społecznościowego[99]. Dane dotyczące preferencji politycznych zaliczane są do danych szczególnie chronionych, w związku z tym wymagają wyższych standardów ochrony.

Poza problemem związanym z ograniczeniem prywatności osoby, której dane dotyczą, przetwarzanie danych z zastosowaniem metody big data rodzić może także wątpliwości dotyczące jakości gromadzonych danych. Przetwarzanie danych na tak dużą skalę powoduje, że niemożliwym staje się weryfikowanie ich jakości. W dodatku są one bardzo często ponownie wykorzystane. Rodzi to wątpliwości wobec art. 5 ust. 1 lit. d rozporządzenia 2016/679, gdzie zwraca się uwagę, by dane były prawidłowe i w razie potrzeby uaktualniane. Prowadzi to do wniosku, że nikt nie zagwarantuje poprawności zgromadzonych danych. Przetwarzanie danych w modelu big data jest raczej ilościowe niż jakościowe, co może wpływać na obniżenie poziomu usług świadczonych przy wykorzystaniu danych zebranych w ten właśnie sposób. Powyższe praktyki niewątpliwie stanowią realne zagrożenie dla praw i wolności osób, których dane dotyczą. Chociaż okoliczności przytoczonej

98 Pismo RPO do GIODO w sprawie Cambridge Analytica, z 30.03.2018 r., VII.520.12.2018.AG, www.rpo.gov.pl [dostęp: 12.01.2019].

99 Grupa Robocza art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta 12 czerwca 2009 r., WP 163, s.6.

sprawy z udziałem Cambridge Analytica nie są wyjaśnione, najprawdopodobniej doszło w tym przypadku do naruszenia danych osobowych na dużą skalę.

2.3.2. Cloud computing

W ostatnich latach można zaobserwować zwiększone zainteresowanie użytkowników Internetu przetwarzaniem danych w chmurze obliczeniowej (cloud computing). Polega ono na prowadzeniu infrastruktury informatycznej przez wyspecjalizowane podmioty zewnętrzne. Obecnie na rynku usług informatycznych mamy do wyboru trzy rodzaje chmur:

- prywatną – do której dostęp ma wyłącznie użytkownik i tylko on z niej korzysta;
- publiczną – znajdującą się w przestrzeni publicznej, dostęp do niej ma znacznie większa liczba użytkowników;
- hybrydową – będącą połączeniem dwóch poprzednich.

Korzystanie z chmury stanowi niewątpliwie przyspieszenie i ułatwienie pracy wielu podmiotów. Użycie cloud computing generuje o wiele niższe koszty niż tradycyjne aplikacje. Dodatkowo przetwarzanie danych w ten sposób pozwala użytkownikowi na gromadzenie dużej ilości danych, co w przypadku komputerów lub innych nośników danych może rodzić trudności lub być wręcz niemożliwe. Niewątpliwą korzyścią cloud computing jest transgraniczny charakter usługi, pozwalający użytkownikowi na dostęp do danych niezależnie od miejsca, w którym się znajduje. Ponadto umożliwia korzystanie ze wszystkich potrzebnych nam aplikacji dostępnych w chmurze bez potrzeby generowania dodatkowych kosztów. Prowadzenie księgowości, wysyłanie e-maili, dokonywanie elektronicznych płatności to tylko nieliczne przykłady usług realizowanych za pośrednictwem cloud computing. Usługa ta bez wątpienia jest dogodnym rozwiązaniem nie tylko dla międzynarodowych koncernów handlowych, ale także dla małych i średnich przedsiębiorstw czy osób fizycznych, które nie muszą ponosić dodatkowych kosztów na rozwój infrastruktury informatycznej. Biorąc pod uwagę korzyści związane z wykorzystywaniem cloud computing należy prognozować, że zainteresowanie usługą będzie nadal mieć tendencję rosnącą zwłaszcza, iż coraz częściej dystrybutorzy chmur obliczeniowych proponują rozwiązania czy aplikacje, na które mikro i małe przedsiębiorstwa mogą sobie pozwolić.

Zanim jednak zdecydujemy się wykorzystać model cloud computingu warto przeanalizować, czy rozwiązanie to zapewnia bezpieczeństwo danych zwłaszcza pod kątem ochrony prawnej danych osobowych. Użytkownik usługi powinien mieć świadomość, że jest ADO odpowiedzialnym za proces ich przetwarzania. W związku z tym zanim zdecyduje się na skorzystanie z usługi powinien upewnić się, czy oferowana mu usługa chmurowa zapewnia adekwatny poziom bezpieczeństwa.

W związku z tym powinien nie tylko dysponować wiedzą o oferowanej usłudze, ale także uświadomić sobie potencjalne zagrożenia z nią związane. Powinien także szczegółowo przeanalizować oferowane warunki umowy oraz zwrócić uwagę na proponowane przez usługodawcę środki techniczne i organizacyjne. Na gruncie prawa polskiego brakuje przepisów kompleksowo regulujących to zagadnienie. Nic nie stoi jednak na przeszkodzie, by korzystać z tego rodzaju usług, o ile jest się świadomym konsekwencji związanych z wykorzystywaniem tego rodzaju rozwiązań.

Podstawą stosunku cywilno-prawnego regulującego przetwarzanie danych w chmurze jest umowa o świadczenie usług przetwarzania danych w chmurze obliczeniowej. Stronami umowy są użytkownik występujący w charakterze ADO oraz dostawca usług – podmiot przetwarzający. Administratorem danych osobowych jest użytkownik, ponieważ to on decyduje o celach i środkach przetwarzania danych. Jak podkreśla Grupa Robocza art. 29 „to administrator decyduje o powierzeniu przetwarzania danych i oddelegowaniu wszystkich lub części działań w zakresie przetwarzania zewnętrznej organizacji"[100]. To także ADO odpowiedzialny jest za zapewnienie bezpieczeństwa danych osobowych. Wobec powyższego dostawca usługi cloud computingu jest podmiotem przetwarzającym dane. Analiza prawna stosunku łączącego strony pozwala wysunąć tezę, że klasyczny podział na ADO oraz procesora w tym przypadku nie będzie miał zastosowania. To bowiem dostawca chmury obliczeniowej udostępnia ADO usługę (infrastrukturę i oprogramowanie). Bardzo często też ADO nie ma możliwości wpłynięcia na zastosowane rozwiązania w zakresie bezpieczeństwa. W związku z tym ocena relacji zachodzących pomiędzy podmiotami jest kluczowa dla ustalenia, czy wykorzystywanie tej metody jest bezpieczne z punktu widzenia przetwarzania danych osobowych.

Analizując relacje zachodzące pomiędzy stronami należy wskazać, że, co do zasady, mają one możliwość dowolnego kształtowania łączącego je stosunku prawnego, w zależności od wyboru metod przetwarzania danych w chmurze oraz zakresu świadczonych usług. W praktyce jednak trudno mówić tu o równorzędności i swobodzie obu stron, co widoczne jest zwłaszcza w przypadku świadczenia usług chmury publicznej. W przeważającej większości przypadków ADO są przedstawiane gotowe wzorce umowne narzucające konkretne rozwiązania prawne. Tak więc, ADO posiada ograniczone możliwości wpływania na treść łączącego ich stosunku prawnego, a tym samym umowy tego typu charakteryzują się stosunkowo niewielką elastycznością. Umowy regulujące kwestie cloud computing w większości przypadków cechuje niezwykła ogólność. Dla ADO, którzy nie mieli wcześniej do czynienia z tego typu usługami wiele trudności może sprawiać zrozumienie treści

100 Ibidem, s. 10.

umowy, choćby ze względu na zawiłość klauzul w niej zawartych. Bardzo często postanowienia umowy nie odnoszą się w ogóle do takich kwestii, jak: zakres odpowiedzialności usługodawców, stosowane środki bezpieczeństwa czy informacje o tym, co dzieje się z danymi po wypowiedzeniu lub rozwiązaniu przez strony umowy. Tymczasem brak tych elementów w umowie może stanowić podstawę do potencjalnych sporów pomiędzy stronami.

Analizując cloud computing z punktu widzenia bezpieczeństwa nie można pominąć zagadnienia związanego z transferem danych do państw trzecich, który w tym przypadku jest bardzo realny. Analiza rynku europejskiego pokazuje bowiem, że dostarczyciele usługi bardzo często pochodzą z USA czy Chin. W takiej sytuacji dochodzi do transferu danych poza Europejski Obszar Gospodarczy, co niewątpliwie wymaga nie tylko zastosowania dodatkowych mechanizmów prawnych, ale także zapewnienia wyższego poziomu ochrony przetwarzanych danych. Administrator danych osobowych, decydując się na skorzystanie z usługi cloud computingu powinien sprawdzić, czy istnieje ryzyko przekazania danych do państw trzecich.

Powyższe rozważania wskazują, że ADO nie ma całkowitej kontroli nad danymi przetwarzanymi w chmurze. Dodatkowo bardzo często w ogóle nie wie, gdzie są przechowywane dane osobowe. W związku z licznymi lukami w umowach, dotyczącymi kluczowych obszarów bezpieczeństwa, istnieje prawdopodobieństwo utraty kontroli nad przetwarzanymi danymi. Administrator danych osobowych nie ma możliwości zweryfikowania, czy rzeczywiście nikt poza nim nie ma dostępu do danych.

Przepisy rozporządzenia 2016/679 wymagają, by ADO korzystał z usług tylko takiego podmiotu przetwarzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Chociaż podmiot przetwarzający w tym przypadku może zapewnić o tym ADO poprzez odpowiednie zapisy umowne, w praktyce nie będzie miał możliwości ich zweryfikowania. Dodatkowo prawodawca unijny w przepisach rozporządzenia 2016/679 wymaga, by ADO wyraził pisemną zgodę na dalsze powierzenia danych osobowych. Jeżeli ADO nie wyrazi takiej zgody, do zawarcia umowy w ogóle może nie dojść, gdyż powyższa zgoda stanowi jeden z kluczowych elementów porozumienia. Powierzenie, czy też podpowierzenie danych osobowych nie zwalnia ADO z odpowiedzialności w zakresie właściwego zabezpieczenia danych, dlatego właściwe uregulowanie tego zagadnienia z punktu widzenia ADO wydaje się szczególnie istotne.

W art. 28 lit. g rozporządzenia 2016/679 jednoznacznie wskazuje się, że po zakończeniu świadczenia usług związanych z przetwarzaniem w zależności od decyzji ADO, podmiot przetwarzający zwraca lub usuwa wszelkie dane osobowe.

Tymczasem jak zauważa Grupa Robocza art. 29 w przypadku usługi cloud comutingu to ADO zobowiązany jest do usunięcia danych[101].

Z punktu widzenia bezpieczeństwa procesu przetwarzania danych w chmurze konieczne wydaje się wypracowanie wzorca umownego stanowiącego drogowskaz dla ADO. Analiza istotnych postanowień umowy zawartych w dostępnych wzorcach umownych uwidoczniła, że umowy tego typu mogą zawierać liczne „pułapki" dla ADO, narażając proces przetwarzania danych osobowych na niebezpieczeństwo. Nieznajomość problematyki jest także powodem, dla którego bardzo często ADO nie decydują się na korzystanie z cloud computing.

Jak zostało zauważone cloud computing jest atrakcyjną formą wspomagającą prowadzenie przedsiębiorstw. Oferowane aplikacje umożliwiają m.in. szybkie i sprawne przetwarzanie danych osobowych klientów, kontrahentów czy pracowników. Zanim jednak ADO zdecyduje się skorzystać z tego rozwiązania powinien zapoznać się i przeanalizować umowę, którą oferuje dostawca, by mieć pewność, że poza innowacyjnymi rozwiązaniami technologicznymi zapewnił sobie najwyższe standardy także w innych obszarach, w tym bezpieczeństwa.

Powyższa analiza pozwala stwierdzić, że chociaż cloud computing jest rozwiązaniem innowacyjnym i atrakcyjnym, jednak trudno jest jednoznacznie stwierdzić, że jest też przy tym rozwiązaniem bezpiecznym. Takim powinno być z punktu widzenia ADO. Dodatkowo brak właściwych regulacji prawnych determinuje to, że umowy adhezyjne w większości przypadków milczą w kluczowych dla ADO obszarach, w szczególności dotyczących stosowanych zabezpieczeń. Analiza wykazała także, że stosowanie chmury nie pozwala ADO na pełne realizowanie przysługujących mu praw na podstawie rozporządzenia 2016/679. Nie ulega wątpliwości, że zagadnienie to wymaga lepszych rozwiązań prawnych. Obecny stan pozwalający dostawcom usługi na kreowanie umowy nie jest zadawalający i budzi pewne obawy, że istotne z punktu widzenia ADO zagadnienia są celowo pomijane. Brak możliwości wpływania na treść umowy podważa równość stron stosunku prawnego, stawiając ADO na gorszej pozycji. Rozwiązania technologiczne dotyczące zabezpieczenia danych w chmurze są oceniane przez specjalistów pozytywnie. Bardzo często wskazują, że dostawca usługi może pozwolić sobie na inwestowanie dużych nakładów finansowych w celu właściwego zabezpieczenia usługi, którą dostarcza[102]. Chociaż oferowany model przetwarzania danych jest innowacyjnym rozwiązaniem, którego celem jest łatwy dostęp do danych, niski

101 Ibidem.

102 C. Ostrwalder, *Cloud computing. Przetwarzanie na dużą skalę i cloud computing*, [w:] *Cloud computing przetwarzanie w chmurze*, red. G. Szpor, Warszawa 2013, s. 13.

koszt utrzymania, a jednocześnie zapewnienie bezpieczeństwa przetwarzanych danych niezbędne są dalsze prace (przede wszystkim) legislacyjne gwarantujące ADO bezpieczeństwo. Przez bezpieczeństwo możemy tu rozumieć zapewnienie integralności, dostępności i poufności danych.

Rozdział 3

Obowiązki ADO związane z przetwarzaniem danych osobowych

Wejście w życie rozporządzenia 2016/679 rozszerzyło zakres obowiązków nałożonych na ADO. Ich realizacja zapewnia właściwy przebieg procesu przetwarzania danych osobowych oraz realizację praw osób, których dane dotyczą. Ustawodawca unijny położył ogromny nacisk na to, by przetwarzanie danych nie było przypadkowym działaniem, a dokładnie zaplanowanym i przemyślanym procesem od momentu zebrania danych do zakończenia procesu przetwarzania danych. W związku z tym, ochrona danych osobowych powinna zostać „zaszyta" we wszystkie procesy realizowane przez ADO. Dlatego też tak ważne jest, by wszyscy pracownicy ADO byli świadomi realizowanych działań, znali zasady ochrony danych osobowych oraz umieli reagować w sytuacji występującego zagrożenia. Wraz z wejściem w życie rozporządzenia 2016/679 nie tylko zmieniły się przepisy prawa, ale także samo myślenie o ochronie danych osobowych jako o trwającym procesie realizowanym przez całą jednostkę organizacyjną. Przed ADO pojawiło się więc wyzwanie dostosowania do nowych standardów. Jak podkreśla Grupa Robocza art. 29 zasada rozliczalności wymaga od ADO wykazania, jakie informacje osoba, której dane dotyczą, już posiada, w jaki sposób i kiedy je otrzymała oraz wykazania, że od tamtego czasu nie miały miejsca zmiany w tych informacjach, które powodowałyby ich nieaktualność[103]. Najlepszymi metodami zapewniającymi realizację obowiązków wynikających z rozporządzenia 2016/679 są m.in. audyty wewnętrzne oraz zewnętrzne. Zrozumienie przez ADO znaczenia ochrony danych osobowych,

[103] Grupa Robocza art. 29, Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679, WP 260, www.uodo.gov.pl [dostęp: 05.10.2018].

a także potrzeby dbania o najwyższe standardy bezpieczeństwa jest kluczem do zgodnego z prawem przetwarzania danych i uniknięcia odpowiedzialności przewidzianej w art. 82 rozporządzenia 2016/679.

Zapewnienie ochrony danych nie powinno być przypadkowym działaniem ADO, a rzetelnym, przemyślanym procesem. W związku z tym ustawodawca unijny wymaga, by ADO już na etapie planowania określonego procesu wiedział, w jaki sposób zostanie ona zapewniona.

Od momentu, w którym ADO planuje wdrożenie nowej usługi lub jakiegoś procesu biznesowego powinien zadbać o to, by zbierać tylko te dane, które są mu niezbędne do realizacji określonego celu. Stanowi to realizację zasady minimalizacji danych. W dalszym ciągu powinien przeanalizować, czy stosowane przez niego zabezpieczenia zapewniają należyty poziom ochrony, czy zamierza przekazywać innym podmiotom dane osobowe, a jeżeli tak, to na jakich zasadach. Niezwykle istotne jest także to, w jaki sposób realizowane są procesy wewnątrz organizacji. W szczególności, czy pracownicy są we właściwy sposób przeszkoleni, czy posiadają wiedzę na temat realizowanych procesów, czy wiedzą, jakie zagrożenia związane są z przetwarzaniem danych osobowych i w jaki sposób postępować, by ich uniknąć. Wśród części ADO zasady te stosowane są od dawna, niemniej jednak dla wielu z nich dopiero wejście w życie rozporządzenia 2016/679 przesądziło, iż zasady te stały się częścią obowiązującego prawa.

3.1. Uwzględnienie prywatności w fazie projektowania i domyślna ochrona danych

Uwzględnienie prywatności w fazie projektowania zakłada wbudowanie prywatności osoby, której dane dotyczą, w każdy projekt realizowany przez ADO. W ocenie autora obejmuje ona nie tylko etap planowania procesu, ale cały okres przetwarzania danych. Nie ulega wątpliwości, że właściwe zaplanowanie od samego początku procesu pozwoli na przewidzenie określonych konsekwencji i uniknięcie błędów. Sama koncepcja prywatności w fazie projektowania (privacy by desing) sformułowana została przez Ann Cavoukian, byłą rzeczniczkę do spraw informacji i prywatności kanadyjskiej prowincji Ontario[104].

Wspomniana zasada znalazła odzwierciedlenie w art. 25 ust. 1 rozporządzenia 2016/679, zgodnie z którym „uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw

104 Poradnik GIODO, *Czy jesteś gotowy na RODO?*, www.giodo.gov.pl [dostęp: 15.06.2018].

lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich chociażby jak minimalizacja danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą". Ustawodawca unijny w znaczący sposób zliberalizował przepisy, w stosunku do tych wynikających z dyrektywy 95/46/WE. W obecnym kształcie prawnym ADO sam decyduje, jakie środki zastosować, by zapewnić bezpieczeństwo procesu. Takie podejście wynika przede wszystkim z faktu, że nakładanie z góry ustalonych zabezpieczeń u każdego ADO niezależnie od rodzaju i zakresu przetwarzania danych nie spełniało swojej podstawowej funkcji, jaką jest zapewnienie bezpieczeństwa, które nie powinno być pojęciem abstrakcyjnym, ale faktycznie realizowanym przez ADO, który ze sposobu jego realizacji będzie musiał się rozliczyć.

Ustawodawca unijny uznał również, że ADO najlepiej wie, jakie procesy realizuje, jaki zakres danych przetwarza, kto ma do nich dostęp i jakie mogą być potencjalne zagrożenia związane z przetwarzaniem danych. Na tej podstawie sam powinien ocenić i wdrożyć odpowiednie mechanizmy gwarantujące bezpieczeństwo. Wychodząc naprzeciw oczekiwaniom ADO w rozporządzeniu 2016/679 zasugerowano niektóre z zabezpieczeń, które powinni oni wziąć pod uwagę. Wśród nich wymienia się m.in. pseudonimizację.

Innymi możliwymi do zastosowania rodzajami zabezpieczeń jest szyfrowanie danych czy wyznaczenie inspektora ochrony danych osobowych. Jak widać, wiele rozwiązań prawnych przewidzianych w całym rozporządzeniu 2016/679 składa się na zapewnienie ochrony prywatności osoby fizycznej w fazie projektowania, która wbrew nazwie rozciąga się na cały proces przetwarzania danych.

Z kolei domyślna ochrona danych (privacy by default) ma na celu zapewnić osobie, której dane dotyczą, prywatność bez potrzeby dokonywania jakichkolwiek ustawień. Ustawienia aplikacji czy systemów nie powinny być skonfigurowane w taki sposób, by umożliwiały zbieranie informacji o osobie bez jej wiedzy i zgody. Jest to szczególnie istotne w sytuacji, w której użytkownik w ogóle nie ma świadomości, że jego dane są zbierane przez zainteresowane podmioty bez jego wiedzy. W związku z tym rezygnacja z uprawnienia przysługującego osobie, której dane dotyczą, może nastąpić wyłącznie po jej aktywnym działaniu polegającym na odstąpieniu od tego prawa i zmianie ustawień. Jak wynika z art. 25 ust. 2 rozporządzenia 2016/679 ADO wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne do

osiągnięcia każdego konkretnego celu przetwarzania. Domyślna ochrona skupia się na ochronie tych użytkowników, którzy wykazywali swą bierną postawę wobec pozyskiwania danych bez ich wiedzy. Jak zauważa Michał Bienias konsekwencją tej zasady jest to, że ADO będzie musiał zminimalizować ilość zbieranych danych, zakres ich przetwarzania oraz okres ich przechowywania[105]. Domyślna ochrona danych stanowi wyraz realizacji zasad wynikających z art. 5 rozporządzenia 2016/679, do których zaliczamy: zasadę rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, rozliczalności, integralności i poufności. Obowiązkiem ADO jest więc zbieranie tylko tych danych, które są niezbędne do realizacji określonego celu. Dla wielu ADO będzie to zasadnicza zmiana, ponieważ przyzwyczajeni są do zbierania wszelkich informacji o swoich klientach i kontrahentach, wychodząc z założenia, że „dane te mogą się kiedyś przydać".

Przedstawione podejścia dotyczące ochrony prywatności osoby, której dane dotyczą, mają charakter *ex nunc* a nie *ex tunc*, co oznacza, że skupiają się na budowaniu rozwiązań zapobiegawczych a nie naprawczych. Jest to istotna zmiana, która nie była w tak wyraźny sposób wyartykułowana w dyrektywie 95/46/WE. To zaś przekładało się na sposób postępowania ADO, dla których ochrona danych osobowych niejednokrotnie była procesem wtórnym.

3.2. Ocena skutków dla ochrony danych

Z wymienionymi obowiązkami wiąże się potrzeba dokonania przez ADO oceny skutków dla ochrony danych (Data Protection Impact Assessment – DPIA) uregulowana w art. 35 rozporządzenia 2016/679. Jest to nowe zobowiązanie, które nie występowało pod rządami dyrektywy 95/46/WE. Ocena skutków dla ochrony danych powinna mieć miejsce wszędzie tam, gdzie istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Zgodnie z treścią cytowanego art. 35 rozporządzenia 2016/679, jeżeli dany rodzaj przetwarzania danych osobowych – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to ADO przed rozpoczęciem przetwarzania musi dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

105 M. Bienias, *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych*, [w:] *Ogólne rozporządzenie o ochronie danych – aktualne problemy prawnej ochrony danych osobowych*, red. G. Sibiga, Warszawa 2016, s. 52.

Proces ten należy przeprowadzić także w sytuacji:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu i jest podstawą decyzji wywołujących skutki wobec osoby fizycznej;
b) przetwarzania na dużą skalę danych wrażliwych, genetycznych, biometrycznych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Dodatkowo Prezes UODO podał do wiadomości publicznej wykaz 9 kategorii przetwarzania, dla których przeprowadzenie oceny jest obligatoryjne. Są nimi[106]:

a) ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych;
b) zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki;
c) systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni (do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa);
d) dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: liczby osób, których dane są przetwarzane, zakresu przetwarzania, okresu przechowywania danych oraz geograficznego zakresu przetwarzania;
e) przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych;
f) przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł;
g) przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i/lub oceniającymi;
h) innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych;
i) gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.

---

106 Komunikat Prezesa Urzędu Ochrony Danych Osobowych z 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, MP 2018 r., poz. 827, www.monitroposli.gov.pl [dostęp: 18.08.2018].

Nie ulega wątpliwości, że przetwarzanie danych na portalach społecznościowych, świadczenie usług marketingowych czy prowadzenie sklepów internetowych będzie wymagało przeprowadzenie oceny skutków dla ochrony danych. *A contratio*, ADO nie będzie musiał przeprowadzić oceny skutków dla ochrony danych, jeżeli dany rodzaj przetwarzania może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą. Przeprowadzenie procesu oceny skutków dla ochrony danych jest niezbędne wyłącznie w tych przypadkach, w których istnieje prawdopodobieństwo, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Grupa Robocza art. 29 podkreśla, że w sytuacji, w której ADO nie wie, czy wymagane jest przeprowadzenie oceny skutków czy też niezalecane jest wykonanie oceny jako elementu procesu przestrzegania przepisów o ochronie danych osobowych[107]. Jeżeli zaś ADO uzna, że nie musi przeprowadzać oceny skutków dla ochrony danych, wówczas powinien udokumentować swoją decyzję oraz poprzeć ją stanowiskiem IOD.

Ocena skutków dla ochrony danych powinna być przeprowadzona w formie pisemnej, chociaż ustawodawca unijny nie wskazał ani formy, ani metody, jaką powinien posłużyć się ADO do jej przeprowadzenia. Zachowanie jednak tej formy jest dobrym przykładem realizowania zasady rozliczalności danych. Osobą odpowiedzialną za przeprowadzenie tego procesu jest ADO. Jak wynika z obowiązujących przepisów prawa, przeprowadzając ją powinien konsultować się z IOD, o ile został powołany (art. 35 ust. 2 rozporządzenia 2016/679). W sytuacji, w której określony proces przetwarzania danych zostaje przejęty przez podmiot przetwarzający (outsourcing usług), wówczas powinien współpracować z ADO w przeprowadzeniu oceny skutków dla ochrony danych. W omawianą ocenę może być również zaangażowany organ nadzorczy w sytuacji, w której ADO nie może znaleźć środków ograniczających wysokie ryzyko do granic akceptowalnych.

Ocena powinna zawierać:

a) opis planowanych operacji przetwarzania i celów przetwarzania, w tym prawnie uzasadnionych interesów realizowanych przez ADO;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia 2016/679.

---

107 Grupa Robocza art. 29, Wytyczne z 4 kwietnia 2017 r. dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" dla celów rozporządzenia 2016/679 zmienione w dniu 4 października 2017 r., WP 248, www.uodo.gov.pl [dostęp: 01.11.2018].

Jeżeli ADO nie przeprowadzi oceny skutków dla ochrony danych, chociaż ciąży na nim taki obowiązek, lub przeprowadzi ją w sposób nieprawidłowy, musi liczyć się z odpowiedzialnością finansową w wysokości do 10 mln euro lub w przypadku przedsiębiorstwa – do 2% całkowitego rocznego obrotu w skali światowej za poprzedni rok budżetowy, w zależności od tego, która kwota jest wyższa zgodnie z art. 82 rozporządzenia 2016/679.

3.3. Analiza ryzyka

Wejście w życie rozporządzenia 2016/679 zmieniło sposób postrzegania problematyki ochrony danych osobowych. W ocenie autora i wbrew powszechnej opinii zmiany te należy oceniać z perspektywy ewolucji, a nie rewolucji. Wiele z przedstawionych mechanizmów funkcjonowało w praktyce od dawna, chociaż nie były wymagane prawem. Rozwiązania prawne zaproponowane w rozporządzeniu 2016/679 mogą wydawać się rewolucyjne, wyłącznie dla tych ADO, którzy dotychczas nie stosowali żadnej ochrony lub stosowali ją w minimalnym zakresie, czyniąc zadość wymaganiom prawnym, nie rozumiejąc jednak intencji, jaka przyświecała ustawodawcy. Podstawowym obowiązkiem ADO, jak zostało zauważone na wstępie tego rozdziału, jest zapewnienie danym osobowym odpowiedniego poziomu ochrony tak, by proces ich przetwarzania gwarantował osobie, której dane dotyczą, najwyższe standardy ochrony. Ustawodawca unijny odszedł od sztywnego określania, jakie działania powinien podjąć ADO na rzecz bardziej elastycznego rozwiązania pozwalającego mu na samodzielne podjęcie decyzji, jaki rodzaj zabezpieczeń wybrać. W art. 24 rozporządzenia 2016/679 wskazał, że „uwzględniając charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem". Jednak, aby mogło to nastąpić, niezbędne jest nie tylko określenie, jakie zagrożenia mogą wiązać się z przetwarzaniem danych osobowych, ale także dokonać właściwego wyboru zabezpieczeń.

W opinii Grupy Roboczej art. 29 ryzyko jest scenariuszem opisującym zdarzenia i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka[108].

Warto mieć na uwadze, że analiza ryzyka jest procesem ciągłym, a nie jednorazowym, co oznacza, że ADO muszą ciągle weryfikować proces przetwarzania

[108] Ibidem.

danych oraz ryzyko z nim związane, a także umiejętnie stosować odpowiednie mechanizmy zapobiegające wystąpieniu incydentu. Na gruncie rozporządzenia 2016/679 (art. 4 pkt 12) jest on definiowany jako „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".

Podstawowym celem analizy ryzyka jest ocena zagrożeń dla poprawnego przetwarzania danych oraz wybór i wdrożenie środków zmniejszających prawdopodobieństwo ich wystąpienia. Analiza polega na określeniu wielkości ryzyka, na zidentyfikowaniu grup informacji oraz obszarów ich przetwarzania, które wymagają zabezpieczenia. Jak zostało zauważone, dotychczas niewielu ADO dokonywało wyboru zabezpieczeń adekwatnie do skali zagrożeń. Podstawowym źródłem informacji o zabezpieczeniach były przepisy wykonawcze, które wskazywały – w dość ogólny sposób – możliwy do zastosowania katalog zabezpieczeń. Wraz z wejściem w życie rozporządzenia 2016/679 zliberalizowano przepisy regulujące rodzaj stosowanych zabezpieczeń, wskazując, iż ADO powinien sam wybierać i stosować te środki techniczne i organizacyjne, które są adekwatne do charakteru, zakresu, kontekstu, celu przetwarzania oraz ryzyka naruszenia praw i wolności osób fizycznych.

Administrator danych osobowych, oceniając, czy stopień bezpieczeństwa jest odpowiedni w stosunku do możliwego do wystąpienia zagrożenia powinien uwzględniać w szczególności ryzyko związane z przetwarzaniem danych osobowych, a w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 32 rozporządzenia 2016/679). Skuteczna realizacja tego procesu wymaga od ADO właściwego zidentyfikowania zagrożeń. Ustawodawca unijny podpowiada w tym zakresie, by prawdopodobieństwo i powagę ryzyka naruszenia praw wolności osoby, której dane dotyczą, określić poprzez odniesienie się do charakteru, zakresu, kontekstu celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko (motyw 76 preambuły rozporządzenia 2016/679).

Wśród możliwych do wystąpienia zagrożeń wymienia się przede wszystkim takie, które mogą skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie

tożsamości, stratę finansową, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne (motyw 85 preambuły rozporządzenia 2016/679).

3.4. Informowanie o naruszeniu ochrony danych osobowych

Właściwe zidentyfikowanie możliwych do wystąpienia zagrożeń, a także w konsekwencji zastosowanie odpowiednich środków technicznych i organizacyjnych jest kluczowym elementem zapewnienia prawidłowego funkcjonowania procesu ochrony danych osobowych.

Należy mieć przy tym świadomość, że ADO nie jest w stanie całkowicie wyeliminować możliwych do wystąpienia zagrożeń. Nie może także zakładać, że jeżeli dotychczas żaden incydent nie miał miejsca, to nigdy się on nie wydarzy. W związku z tym, jeżeli dojdzie do naruszenia, ADO oraz jego pracownicy powinni bez zbędnej zwłoki podjąć działania mające na celu minimalizowanie powstałych skutków. W związku z tym rozwijanie wśród osób przetwarzających dane osobowe świadomości, czym jest naruszenie i jakie niesie to za sobą konsekwencje jest niezwykle istotne. W praktyce okazuje się, iż pracownicy często nie mają świadomości, że doszło do naruszenia, nie mówiąc o podjęciu odpowiednich kroków w tym zakresie. Ustawodawca unijny wprowadził obowiązek informowania organu nadzorczego oraz osób, których dane dotyczą, o powstałym naruszeniu w sytuacji, w której istnieje prawdopodobieństwo, że mogło ono powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przewidział w tym zakresie ściśle określone ramy czasowe, dając ADO 72 godziny liczone od momentu stwierdzenia naruszenia. W praktyce oznacza to, że ADO powinien podjąć działania niezwłocznie po stwierdzeniu, że miało miejsce zdarzenie prowadzące do naruszenia[109]. W tym czasie ADO powinien podjąć działania zmierzające do zapobieżenia rozpowszechniania się naruszenia oraz określić jego skalę. Z tych względów tak ważne jest wdrożenie odpowiednich procedur postępowania na wypadek wystąpienia incydentu oraz zapoznanie z ich treścią wszystkich pracowników. Działania takie pozwolą na szybkie wykrycie powstałych naruszeń oraz podjęcie niezbędnych działań minimalizujących jego skutki.

---

109 Grupa Robocza art. 29, Wytyczne z 3 października 2017 r. w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679, WP 250, s. 9, www.giodo.gov.pl [dostęp: 03.03. 2018].

Jeżeli z jakichś względów ADO nie uda się zachować tego terminu, powinien dołączyć do zgłoszenia wyjaśnienia dotyczące przyczyn opóźnienia (art. 33 ust. 1 rozporządzenia 2016/679). Rozwiązanie to ma na celu ograniczenie możliwych do wystąpienia negatywnych skutków naruszenia. Administrator danych osobowych powinien podjąć stosowne działania natychmiast po stwierdzeniu naruszenia. Z związku z tym tak ważne jest wdrożenie odpowiednich procedur ułatwiających działanie ADO pod presją czasu i okoliczności, w jakich się znalazł.

Prawodawca unijny w art. 33 ust. 3 rozporządzenia 2016/679 wskazuje także okoliczności, jakie ADO powinien uwzględnić, dokonując zgłoszenia do organu nadzorczego. Przedstawiony katalog nie ma charakteru zamkniętego i ADO może wskazać także inne istotne okoliczności.

W związku z tym ADO powinien:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) dostarczyć imię i nazwisko oraz dane kontaktowe IOD lub oznaczyć inny punkt kontaktowy, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać lub proponować środki, które zastosuje w celu zaradzenia naruszeniom ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Poza tym, jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, ADO powinien bez zbędnej zwłoki poinformować osobę o naruszeniu (art. 34 ust. 1 rozporządzenia 2016/679). Celem wprowadzenia takiego rozwiązania jest zapewnienie osobom, których dane dotyczą, jak najwcześniejszego realizowania przysługujących im praw oraz podjęcie stosownych kroków, by uchronić ich przed możliwymi do wystąpienia konsekwencjami[110]. Zawiadomienie powinno mieć formę prostego i przystępnego komunikatu. Nie ma przeszkód, by poinformować osobę poprzez SMS czy umieścić taką informację w widocznym miejscu na stronie internetowej. Zawiadomienie osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 rozporządzenia 2016/679 nie jest wymagane, jeżeli:

a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

110 Ibidem.

b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

W sytuacji, w której ADO uzna, że nie zachodzą przesłanki uzasadniające poinformowanie osoby, której dane dotyczą, o naruszeniu zgodnie z zasadą rozliczalności powinien uzasadnić podjętą decyzję.

Z uwagi na fakt, iż niejednokrotnie ADO powierzają dane osobowe innym podmiotom. Ważne, żeby w umowie powierzenia przetwarzania danych zawrzeć odpowiednie zapisy zobowiązujące podmiot przetwarzający do powiadomienia ADO o powstaniu naruszenia przed upływem 72 godzin, tak by ADO miał możliwość podjęcia stosownych kroków.

Fakt zaistnienia naruszenia niezależnie od tego, czy wymaga poinformowania organu nadzorczego lub osoby, której dane dotyczą, czy też nie, zawsze powinien zostać przez ADO udokumentowany. Zgodnie z art. 33 ust. 5 rozporządzenia 2016/679 ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dzięki stworzeniu przejrzystej dokumentacji organ nadzorczy ma możliwość dokładnego poznania okoliczności naruszenia. Rekomendowanym rozwiązaniem jest prowadzenie rejestru naruszeń. Nierealizowanie przez ADO tego obowiązku może skutkować odpowiedzialnością na podstawie art. 83 rozporządzenia 2016/679.

3.5. Powołanie IOD

Jednym z obowiązków ADO jest powołanie IOD w ściśle określonych w rozporządzeniu 2016/679 sytuacjach. Funkcję tę powinna pełnić osoba posiadająca wiedzę, doświadczenie oraz odpowiednie kwalifikacje zawodowe. Jest to szczególnie istotne, gdyż w praktyce okazuje się, że tylko zapewnienie odpowiedniej osoby na tym stanowisku gwarantuje właściwe realizowanie praw osób, których dane dotyczą. Do 25 maja 2018 r. ADO miał pełną swobodę w decydowaniu, czy powoływać administratora bezpieczeństwa informacji czy też nie. Wraz z wejściem w życie rozporządzenia 2016/679 obowiązkowe jest wyznaczenie i zgłoszenie do organu nadzorczego IOD w sytuacji, w której:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) główna działalność ADO lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
c) główna działalność ADO lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rozporządzenia 2016/679.

W praktyce jednak okazuje się, że dużo trudności sprawia ADO określenie, czy wypełniają przesłanki uzasadniające powołanie przez nich IOD. Dzieje się tak m.in. dlatego, że wyrażenia takie, jak: „przetwarzanie na dużą skalę", „główna działalność" czy „regularne i systematyczne monitorowanie" są ogólne i niedookreślone. Pewne próby interpretacji powyższych pojęć zostały dokonane przez Grupę Roboczą art. 29, jednak w wielu przypadkach ADO nadal mają wątpliwości[111].

Administrator danych osobowych, decydując się na powołanie IOD powinien przede wszystkim kierować się prezentowanym przez niego poziomem wiedzy oraz kwalifikacjami zawodowymi. Jak wynika z motywu 97 preambuły rozporządzenia 2016/679 niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez ADO lub podmiot przetwarzający. W przepisach rozporządzenia 2016/679 oraz wytycznych Grupy Roboczej art. 29 kładzie się przede wszystkim nacisk na praktyczne przygotowanie do wykonywania powierzonych IOD zadań. Nie ulega wątpliwości, że dobranie właściwego IOD jest niezwykle ważne z punktu widzenia ADO, ponieważ to on ponosi odpowiedzialność za właściwy przebieg procesu przetwarzania danych.

Do podstawowych zadań IOD należy:
a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych,

111 Grupa Robocza art. 29, Wytyczne z 13 grudnia 2016 r. dotyczące Inspektorów Ochrony Danych, WP 243, www.giodo.gov.pl [dostęp: 15.02.2018].

w tym podziału obowiązków, działań zwiększających świadomość, prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Powyższy katalog obowiązków IOD określony w art. 39 rozporządzenia 2016/679 nie ma charakteru zamkniętego, co oznacza, że IOD może wykonywać także inne zadania związane z przetwarzaniem danych osobowych. Może do nich należeć chociażby wspieranie ADO przy wykonywaniu oceny skutków dla ochrony danych czy nawet prowadzenie rejestru czynności przetwarzania danych. W tym ostatnim przypadku ustawodawca unijny jasno wskazał, że czynność ta powinna być realizowana przez ADO. Dodatkowo na mocy art. 38 ust. 4 rozporządzenia 2016/679 osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach dotyczących przetwarzania ich danych. Warto także zaznaczyć, iż z przepisów rozporządzenia 2016/679 wynika jasno, że IOD nie może być odwoływany ani karany przez ADO, a także podmiot przetwarzający za wypełnianie swoich zadań. Jak zauważa Grupa Robocza art. 29 formą ukarania IOD może być brak lub opóźnienie awansu, utrudnienie rozwoju zawodowego[112].

Z punktu widzenia realizowanych przez IOD zadań nie ma znaczenia forma jego zatrudnienia. Administrator danych osobowych powinien za każdym razem samodzielnie ocenić, jakie są potrzeby jednostki organizacyjnej, jej wielkość, poziom wdrożenia przepisów ochrony danych czy ich znajomość przez pracowników. Ważne jest jednak właściwe umocowanie IOD w strukturze organizacyjnej jednostki. Zgodnie z obowiązującymi przepisami ADO zobowiązany jest do zgłoszenia IOD do organu nadzorczego w ciągu 14 dni od jego powołania. Wraz z wejściem z życie rozporządzenia 2016/679 nie nastąpiło automatyczne przekształcenie ABI w IOD, w związku z czym ABI zostali zmuszeni do dokonania ponownego zgłoszenia w terminie określonym przez Prezesa UODO. Dodatkowo ADO zobowiązany jest do opublikowania danych IOD chociażby na stronie internetowej tak, by osoba, której dane dotyczą, czy organ nadzorczy miały zapewnioną możliwość łatwego i bezpośredniego kontaktu z IOD.

112 Ibidem.

Nowością w przypadku wykonywania funkcji IOD jest możliwość powołania jednego IOD dla grupy przedsiębiorstw. Rozwiązanie to ma przede wszystkim ułatwić kontaktowanie się podmiotów działających w ramach jednej grupy oraz umożliwić lepsze sprawowanie funkcji przez IOD. Dotychczas każdy podmiot należący do grupy kapitałowej był zobowiązany do powoływania swojego ABI, co niewątpliwie utrudniało realizację powierzonych zadań. Umożliwienie w rozporządzeniu 2016/679 powierzenia realizacji zadań IOD jednej osobie niesie za sobą liczne korzyści, ale stanowi także zagrożenie. Skupienie wszystkich obowiązków w rękach jednego podmiotu będzie wymagało od niego nie tylko wiedzy na najwyższym poziomie, ale także dobrego przygotowania organizacyjnego.

3.6. Realizacja obowiązku informacyjnego

Konsekwencją prawa do informacji jest realizacja obowiązku informacyjnego, który przysługuje każdemu podmiotowi danych osobowych. Obowiązkiem ADO, zarówno pod rządami poprzednio obowiązującego stanu prawnego, jak i zgodnie z nowym rozporządzeniem 2016/679, jest poinformowanie osoby, której dane dotyczą, o procesie przetwarzania danych, jaki ma miejsce z udziałem zebranych danych osobowych. Ustawodawca unijny rozróżnia obowiązek informacyjny w zależności od tego, od kogo pochodzą dane osobowe: czy od osoby, której dane dotyczą (art. 13 rozporządzenia 2016/679) czy też z innego źródła (art. 14 rozporządzenia 2016/679). Ta sytuacja będzie najczęściej dotyczyła pozyskania danych osobowych od innych ADO czy z publicznie dostępnych źródeł. Dla osoby, której dane dotyczą, realizacja obowiązku informacyjnego stanowi źródło informacji o procesie przetwarzania danych oraz gwarancję, iż ADO przetwarza dane osobowe zgodnie z prawem. Dodatkowo dowiaduje się o wszystkich przysługujących tej osobie prawach oraz może przewidzieć, jakie wiążą się z tym konsekwencje. Na tej podstawie osoba może podjąć decyzję, czy chce by jej dane były przetwarzane przez ADO czy też nie.

Dokonując porównania obowiązku informacyjnego obowiązującego przed i po 25 maja 2018 r. należy uznać, że obowiązek informacyjny wynikający z art. 13 i 14 rozporządzenia 2016/679 został przez ustawodawcę unijnego w znaczący sposób rozszerzony w stosunku do obowiązku funkcjonującego pod rządami poprzednio obowiązującej uodo. Administrator danych osobowych został dodatkowo zobowiązany m.in. do poinformowania o fakcie wyznaczenia IOD, podstawie prawnej i okresie przetwarzania danych, informacji o zamiarze przekazywania danych do państwa trzeciego. Treść obowiązku informacyjnego realizowanego

wobec osoby, której dane dotyczą, w obecnie obowiązującym stanie prawnym kształtuje się następująco:

7. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
   a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
   b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
   c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
   d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
8. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
   a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   d) informacje o prawie wniesienia skargi do organu nadzorczego;
   e) informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Wszystkie informacje wymienione w art. 13 rozporządzenia 2016/679 są tak samo istotne i muszą zostać zrealizowane przez ADO. Oznacza to, iż niewłaściwą praktyką jest pomijanie niektórych z powyższych punktów.

Charakterystyczną cechą obowiązku informacyjnego realizowanego na gruncie art. 13 rozporządzenia 2016/679 jest to, że ma on zostać dostosowany do celu, w jakim zbierane są dane osobowe. Nie może być to jedna ogólna klauzula, która będzie powielana dla każdego procesu. Jeżeli ADO przetwarza dane z CV w celu przeprowadzenia rekrutacji, obowiązek ten powinien we właściwy sposób odzwierciedlać rzeczywiste zamiary ADO, co do realizacji wspomnianego procesu.

Aby jednak zapewnić, by osoba, której dane dotyczą, rozumiała informacje przekazane przez ADO, powinien on zadbać, by obowiązek został zrealizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, pisanej jasnym i prostym językiem (art. 12 rozporządzenia 2016/679). Chociaż samo pojęcie przejrzystości nie zostało zdefiniowane na gruncie rozporządzenia 2016/679, to jednak ustawodawca unijny w motywie 39 preambuły rozporządzenia 2016/679 podkreśla, że zasada przejrzystości wymaga, by wszystkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Oznacza to, że ADO powinien dostosować treść przekazu do przeciętnego odbiorcy tak, by był dla niego zrozumiały. W związku z tym, powinien unikać niezrozumiałych sformułowań, języka ściśle prawniczego i przesadnie rozbudowanych zdań.

Obowiązek informacyjny powinien zostać zrealizowany na etapie zbierania danych osobowych. Zgodnie z art. 13 rozporządzenia 2016/679 „jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje". Wymóg ten może jednak w praktyce okazać się problematyczny dla wielu ADO po 25 maja 2018 r. zwłaszcza, kiedy mając na uwadze obowiązek zapewniania rozliczalności decydowali się na zbieranie podpisów od osoby, której dane dotyczą, pod obowiązkiem informacyjnym. Zamieszanie związane ze sposobem realizacji tego obowiązku zostało jednak szybko usunięte. Nie ma potrzeby, by osoba potwierdzała ADO, że zapoznała się z obowiązkiem. Jego funkcja sprowadza się bowiem do poinformowania osoby o przysługujących jej prawach oraz wskazania kanału komunikacji, gdyby chciała z niego skorzystać.

Obowiązek informacyjny powinien zostać zrealizowany na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Ustawodawca unijny dał ADO możliwość wyboru metody realizacji obowiązku. Jeżeli osoba, której dane dotyczą, tego zażąda, obowiązek może zostać zrealizowany w formie ustnej. W tym jednak przypadku należy pamiętać, iż na ADO ciąży obowiązek udowodnienia realizacji obowiązku. Zdarza się, że ADO łączą obie formy. Przykładem tego są infolinie, gdzie ustnie realizowana jest skrócona forma obowiązku informacyjnego, a następnie osoba odsyłana jest do strony internetowej, na której znajduje się pełna klauzula.

W praktyce obowiązek ten realizowany jest pod formularzami kontaktowymi, w stopkach e-mailowych czy w umowach. Administrator danych osobowych ma pełną swobodę wyboru miejsca, w którym zamieści klauzulę informacyjną, pamiętając jednak o realizacji powyżej przedstawionych zasad. Rekomendowanym rozwiązaniem jest wykorzystywanie, w szczególności na stronach internetowych, warstwowych obowiązków informacyjnych. Oznacza to, że najpierw osoba, której dane dotyczą, otrzymuje zwięzłą informację, kto jest ADO oraz jaki jest cel ich przetwarzania, a dopiero po rozwinięciu linku pojawia się pełny komunikat. Takie rozwiązanie jest pomocne zwłaszcza, gdy dba się o łatwy dostęp do informacji na stronie internetowej.

Po wejściu w życie rozporządzenia 2016/679 wielu ADO zdecydowało się wobec osób, których danymi już dysponowali realizować ponownie obowiązek informacyjny na nowych zasadach. Podejmowanie takich działań mogło być spowodowane zapisem wynikającym z motywu 171 preambuły rozporządzenia 2016/679, z którego wynika, że przetwarzanie, które w dniu rozpoczęcia stosowania rozporządzenia 2016/679 już się toczy, powinno w terminie 2 lat od wejścia rozporządzenia 2016/679 w życie zostać dostosowane do jego przepisów. W ocenie autora do 25 maja 2018 r. obowiązywały art. 24 i 25 uodo i na tej podstawie ADO powinien realizować ten obowiązek. Po 25 maja 2018 r. nowy obowiązek informacyjny powinien być realizowany wobec procesów, które rozpoczęły się wraz z wejściem w życie rozporządzenia 2016/679. Wobec powyższego po 25 maja 2018 r. wbrew praktyce, wielu ADO nie było zobowiązanych do ponownego spełnienia obowiązku informacyjnego na podstawie art. 13 wobec toczących się procesów. Warto przy tej okazji przytoczyć treść art. 13 ust. 4, z którego wprost wynika, iż ADO nie jest zobowiązany do realizacji obowiązku informacyjnego w sytuacji i w zakresie, w jakim osoba, której dane dotyczą, dysponuje już tymi informacjami. W przypadku zbierania danych nie bezpośrednio od osoby, której dane dotyczą, zakres wyłączeń został w art. 14 ust. 5 dodatkowo rozszerzony.

Naruszenie obowiązku wynikającego z art. 13 i 14 rozporządzenia 2016/679 może powodować w stosunku do ADO konsekwencje przewidziane w art. 82 rozporządzenia 2016/679, tzn. może być podstawą do odpowiedzialności za szkodę majątkową i niemajątkową. Zwłaszcza w sytuacji, w której ADO w ogóle nie zrealizuje tego obowiązku wobec osoby, której dane dotyczą.

Warto pamiętać, że obowiązkiem ADO jest zapewnienie transparentności procesu przetwarzana danych, a właściwa realizacja obowiązku informacyjnego mu to zapewnia.

Przetwarzanie danych osobowych w Internecie wymaga, by ADO zadbał o właściwe poinformowanie osób, których dane dotyczą, o przysługujących im prawach. Jak zostało zauważone, obowiązek informacyjny należy zrealizować na etapie zbierania danych osobowych. W związku z tym, wszędzie tam, gdzie na stronie internetowej ADO zbiera dane osobowe poprzez formularze, zobowiązany jest wypełnić wobec podmiotu danych obowiązek informacyjny. Jest to szczególnie ważne, bowiem transakcje przy wykorzystaniu Internetu wymagają transparentności.

3.7. Dokumentacja ochrony danych osobowych

Po 25 maja 2018 r. ADO powinni prowadzić dokumentację ochrony danych osobowych zgodną z wytycznymi wynikającymi z rozporządzenia 2016/679. Podstawowymi dokumentami, którymi powinien legitymować się ADO jest rejestr czynności przetwarzania danych, rejestr kategorii czynności przetwarzania, rejestr naruszeń określony w art. 33 ust. 5 rozporządzenia 2016/679 oraz wyniki przeprowadzonej oceny skutków dla ochrony danych zgodnie z art. 35 ust. 7 rozporządzenia 2016/679. Niezależnie od tego, w ocenie autora, ADO powinien dokumentować znacznie więcej procesów przetwarzania danych. Wynika to przede wszystkim z obowiązku realizowania przez ADO zasady rozliczalności, która zobowiązuje go do gromadzenia dowodów potwierdzających określone postępowanie. Oznacza to, że powinien on zrealizować żądanie osoby, której dane dotyczą, czy organu nadzorczego dowodów potwierdzających, że działania przez niego podjęte są właściwe, przemyślane i nie wynikają z przypadku. Dlatego też tak ważne jest na każdym etapie procesu przetwarzania danych, niezależnie od tego, czy odbywa się on w systemie informatycznym czy też w formie papierowej, dokumentowanie przeprowadzanych czynności. Poprzez dokumentację ADO powinien wykazać, że przestrzega zasad przetwarzania danych, że zostały one zebrane w sposób legalny oraz, że stosuje właściwą podstawę prawną ich przetwarzania. Przepisy rozporządzenia 2016/679 dają ADO znacznie większą autonomię, niż wynikało to

z poprzednio obowiązującego stanu prawnego. Nie wymaga się, by dokumentacja ta miała określoną formę czy nazwę[113]. Jak wynika bowiem z motywu 78 preambuły rozporządzenia 2016/679 „aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych". Wielu ADO, dysponując dotychczasową dokumentacją zdecydowało się ją zatrzymać i dostosować do wymogów rozporządzenia 2016/679. W szczególności mowa tu o „polityce ochrony danych" oraz „instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych". Dokumenty te zostały wzbogacone o procedury zasady privacy by design, privacy by default czy sposób realizacji praw osób, których dane dotyczą.

Wspomniane wyżej dwa podstawowe dokumenty stanowią trzon procesu przetwarzania danych osobowych. Dlatego też powinny odzwierciedlać rzeczywisty stan jednostki organizacyjnej. Jak zostało zauważone ochrona danych osobowych powinna być uwzględniona we wszystkich procesach realizowanych przez jednostkę. Przygotowana dokumentacja powinna być aktualizowana wraz z dokonywanymi zmianami. Aby jednak, to co zawarte jest w dokumentacji ochrony danych osobowych było skuteczne, powinno zostać zakomunikowane oraz stosowane przez wszystkich pracowników jednostki organizacyjnej.

Administrator danych osobowych powinien dokumentować także pojedyncze procesy. Jak wynika z art. 24 ust. 2 rozporządzenia 2016/679 powinien on wdrożyć odpowiednie polityki ochrony danych, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania danych. W sytuacji, w której nie zachodzą przesłanki uzasadniające powołanie IOD powinien móc wykazać i uzasadnić podjętą decyzję. Podobnie fakt przeprowadzenia szkolenia powinien zostać udokumentowany poprzez przygotowanie planu szkolenia oraz listy obecności uczestników. Administrator danych osobowych powinien także umieć udokumentować realizację obowiązku informacyjnego czy sposób zbierania zgód. Podobnie, jeżeli ADO dopuszcza pracownika do przetwarzania danych, powinien nadać mu stosowne upoważnienie do przetwarzania danych osobowych. W przypadku podjęcia przez ADO decyzji o udostępnieniu lub powierzeniu przetwarzania danych osobowych, powinien na piśmie udokumentować oba procesy.

W rozporządzeniu 2016/679 kładzie się szczególny nacisk na wdrożenie przez ADO odpowiednich środków technicznych i organizacyjnych. Rodzaj stosowanych zabezpieczeń powinien być adekwatny do możliwego do wystąpienia zagrożenia.

113 *Dokumentacja przetwarzania danych osobowych zgodnie z RODO*, www.uodo.gov.pl [dostęp: 30.07.2018].

Nie muszą być one zawarte w jednym dokumencie. Równie dobrze mogą to być wyodrębnione regulaminy, procedury, polityki, które były dotychczas stosowane w jednostce organizacyjnej. Z uwagi na fakt, że przepisy rozporządzenia 2016/679 nie wskazują, jakie środki bezpieczeństwa ma zastosować ADO, wybór należy do niego. Każde z podjętych rozwiązań powinno być udokumentowane po to, by wykazać zasadność podjętych działań. Pozwoli to ocenić, czy ADO poprawnie ocenił ryzyko i zastosował odpowiednie mechanizmy postępowania z ryzykiem.

3.8. Dokumentowanie naruszeń ochrony danych

Jak wynika z art. 33 ust. 5 rozporządzenia 2016/679 ADO powinien dokumentować wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Wszystko po to, by organ nadzorczy mógł zweryfikować działania podejmowane przez ADO. Jak zostało zauważone w poprzednim rozdziale, rekomendowanym rozwiązaniem jest prowadzenie rejestru naruszeń. Chociaż przepisy rozporządzenia 2016/679 nie zawierają w tym zakresie żadnych wskazówek, ADO ma swobodę w wyborze zastosowanego rozwiązania. W dokumencie powinny znaleźć się informacje wskazujące, kto jest ADO, datę i godzinę wystąpienia incydentu, datę i godzinę stwierdzenia naruszenia, miejsce incydentu, charakter naruszenia, kategorie osób, których dotyczy naruszenie oraz skutki naruszenia. Administrator danych osobowych powinien także wskazać, czy naruszenie zostało zgłoszone organowi nadzorczemu oraz czy osoby, których dane dotyczą, zostały poinformowane o naruszeniu. Jeżeli nie zachodzą okoliczności uzasadniające poinformowanie wskazanych podmiotów, ADO powinien udokumentować i uzasadnić również podjętą w tym zakresie decyzję.

3.9. Rejestr czynności przetwarzania danych

Prowadzenie rejestru czynności przetwarzania danych jest nowym obowiązkiem ADO. Obowiązek ten zastąpił wymóg prowadzenia rejestrów zbiorów danych. Rejestr czynności przetwarzania danych, jak sama nazwa wskazuje, identyfikuje wszystkie procesy zachodzące u ADO. Jest to także narzędzie niezwykle pomocne w przypadku mapowania procesów przetwarzania danych osobowych. Na tej podstawie ADO uzyskuje wiedzę pozwalającą mu zweryfikować, w jaki sposób dane osobowe są pozyskiwane, w jakich działach są przetwarzane oraz komu są udostępniane, bądź powierzane. Jak zauważa UODO prowadzenie rejestru czynności

przetwarzania danych pozwala ADO podjąć decyzję, w jakim zakresie dotyczą ich obowiązki wynikające z rozporządzenia 2016/679, w tym, czy muszą przeprowadzić ocenę skutków dla ochrony danych[114]. Rejestr czynności przetwarzania danych jest dokumentem, który powinien być na bieżąco weryfikowany przez ADO, tak by był spójny z realizowanymi przez niego procesami.

Nie każdy ADO jest zobowiązany w świetle obowiązujących przepisów prawa do prowadzenia rejestru czynności przetwarzania danych. Jak wynika z art. 30 ust. 5 rozporządzenia 2016/679 obowiązek ten nie ma zastosowania do podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonuje, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego, lub obejmuje szczególne kategorie danych osobowych (dane szczególnie chronione) lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych.

Ustawodawca unijny wskazał informacje, jakie powinny znaleźć się w rejestrze. Do obligatoryjnych elementów rejestru zalicza się:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentację odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Przedstawiony katalog informacji nie ma charakteru zamkniętego, co oznacza, że ADO może ująć w nim także inne elementy.

Rejestr czynności powinien być prowadzony w formie pisemnej, co obejmuje również formę elektroniczną. Jest to szczególnie pomocne w sytuacji, w której często pojawiają się nowe procesy w jednostce organizacyjnej lub istniejące ulegają

114 UODO, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, www.uodo.gov.pl [dostęp: 23.10.2018].

zmianie. Wielu ADO ma problem dotyczący szczegółowości ewidencjonowania procesów. W ocenie UODO rejestr powinien zawierać opis zespołów operacji związanych zbiorczo z realizacją określonego celu[115]. Oznacza to, że ADO powinien skupić się na identyfikowaniu określonych procesów, a nie na pojedynczych czynnościach wykonywanych w ramach tych procesów.

Analogicznie do rejestru czynności przetwarzania danych, procesor zobowiązany jest prowadzić rejestr kategorii czynności przetwarzania prowadzonych w imieniu ADO. Zgodnie z art. 30 ust. 2 rejestr powinien zawierać:

a) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentację odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Wejście w życie rozporządzenia 2016/679 nałożyło na ADO wiele nowych obowiązków. Ich realizacja gwarantuje nie tylko zapewnienie zgodnego z prawem przetwarzania danych osobowych, ale także ochronę ADO przed odpowiedzialnością na gruncie art. 82 rozporządzenia 2016/679. Rola ADO w procesie przetwarzania danych jest szczególna, ponieważ to właśnie on odpowiada za zakres i cel przetwarzania danych. W przypadku przetwarzania danych w Internecie właściwe realizowanie obowiązków ADO jest szczególnie ważne, ponieważ nie dochodzi tu do bezpośredniego kontaktu podmiotu danych z ADO. Wejście w życie rozporządzenia 2016/679 nakierowane było m.in. na ograniczenie niezgodnego z prawem przetwarzania. Dochodziło do niego w przypadku, gdy ADO pozyskiwali dane osobowe bez wiedzy osoby, której dane dotyczą. W literaturze przedmiotu zwraca się uwagę na rolę prostych i zrozumiałych komunikatów, gwarantujących każdej osobie (niezależnie od wieku i wykształcenia) zrozumienie, w jakim celu ADO zbiera i przetwarza dane osobowe. Na tej podstawie zainteresowany może podjąć decyzję, czy chce brać udział w takim procesie. Dla tych ADO, którzy nie przestrzegają przepisów rozporządzenia 2016/679 lub realizują obowiązki w sposób niewłaściwy przewidziano odpowiedzialność w wysokości do 20 000 000 euro

115 Ibidem.

lub 4% wartości rocznego światowego obrotu przedsiębiorstwa. Oczywiście są to wartości maksymalne. Każdorazowo organ nadzorczy, analizując konkretny przypadek będzie brał pod uwagę charakter naruszenia, skutki naruszenia, stopień odpowiedzialności ADO, rodzaj zastosowanych środków zaradnych oraz kategorie osób, których dotyczyło naruszenie.

3.10. Odpowiedzialność ADO za naruszenie przepisów rozporządzenia 2016/679

Do najistotniejszych zmian, jakie nastąpiły wraz z wejściem w życie rozporządzenia 2016/679 należy zaliczyć możliwość nałożenia na ADO kar finansowych w wysokości do 20 000 000 euro lub 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego ADO. Zmiany te z punku widzenia polskich ADO są szczególnie istotne, bowiem dotychczas ADO nie ponosili odpowiedzialności finansowej za naruszenie, a wyłącznie odpowiedzialność administracyjną oraz karną. Ponieważ od rozpoczęcia stosowania przepisów rozporządzenia 2016/679 minęło już ponad 9 miesięcy organy nadzorcze państw członkowskich UE zdecydowały się skorzystać z uprawnień wynikających z art. 83 rozporządzenia 2016/679.

3.10.1. Odpowiedzialność cywilnoprawna

Każda osoba, której dane dotyczą, która poniosła szkodę majątkową (zarówno w postaci straty, jak i utraconych korzyści) lub niemajątkową w wyniku działania ADO może domagać się od niego lub podmiotu przetwarzającego odszkodowania zgodnie z art. 82 rozporządzenia 2016/679.

Zgodnie z motywem 146 preambuły rozporządzenia 2016/679 „pojęcie szkody na gruncie omawianego dokumentu należy interpretować możliwie szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego". Osobie, której dane dotyczą, przysługuje odszkodowanie zarówno za szkodę majątkową, jak i niemajątkową (krzywdę moralną). W konsekwencji, w przypadku szkody niemajątkowej osoba, której dane dotyczą, będzie zobowiązana wykazać poniesioną szkodę niemajątkową, która w przypadku przetwarzania danych osobowych może mieć charakter cierpienia psychicznego, poczucia braku bezpieczeństwa, poczucia zagrożenia, a nawet prześladowania w przypadku uciążliwego marketingu. W przeciwieństwie do szkody majątkowej, szkodę niemajątkową trudno jest wykazać, ponieważ każdy z nas w różny sposób reaguje na powstałe

sytuacje, różny też ma poziom wrażliwości. W świetle przytaczanych przepisów osoba, której dane dotyczą, powinna otrzymać pełne i skuteczne odszkodowanie za poniesione szkody. W pierwszym wyroku wydanym w świetle obowiązującego rozporządzenia 2016/679 sąd niemiecki zasądził na rzecz obywatela niemieckiego odszkodowanie za przesyłanie do niego przez jedną z firm niezamówionych informacji handlowych w wysokości 50 euro[116]. Sam poszkodowany wycenił poniesioną przez niego szkodę na kwotę 500 euro. Chociaż wysokość odszkodowania wydaje się niewielka to warto pamiętać, że dotyczyła tylko jednego e-maila wysyłanego przez jeden podmiot. Warto pamiętać, czemu ma służyć to odszkodowanie. Ma ono przede wszystkim charakter kompensacyjny, ma wynagrodzić poszkodowanemu poniesioną szkodę.

Niewątpliwie wyrok niemieckiego sądu będzie stanowił drogowskaz dla krajowych sądów innych państw europejskich, w jaki sposób mierzyć szkodę niemajątkową powstałą w wyniku naruszenia przez ADO. W przypadku podobnych spraw rozstrzyganych przez polskie organy orzekające sądem właściwym do rozpoznawania spraw jest sąd okręgowy, a zastosowanie znajdą przepisy kc. Sądy zostały na mocy ustawy zobowiązane do poinformowania Prezesa UODO o wniesionym przez osobę, której dane dotyczą, pozwie oraz o wynikach toczącego się postępowaniu.

3.10.2. Odpowiedzialność administracyjna

Odpowiedzialność ADO oraz podmiotu przetwarzającego oparta jest na zasadzie winy. Jest to konstrukcja odpowiedzialności deliktowej, w której podmiot, który wyrządził szkodę ponosi odpowiedzialność za jej naprawienie. Odpowiedzialność na zasadzie winy oznacza, że osoba, której dane dotyczą, musi wykazać, iż w skutek działania ADO jest winny określonemu działaniu. Pojęcie winy nie zostało jednak na gruncie rozporządzenia 2016/679 zdefiniowane. W literaturze przedmiotu wskazuje się, że „wina zachodzi wówczas, gdy sprawcy szkody można postawić zarzut obiektywnej lub subiektywnej niewłaściwości zachowania"[117]. Wina ADO lub podmiotu przetwarzającego może polegać na określonym działaniu, w przypadku administratora danych będzie to np. zbieranie danych bez podstawy prawnej, lub zaniechaniu. Natomiast w przypadku procesora będzie to niepodjęcie określonego działania na polecenie ADO.

Jak zostało podkreślone w art. 82 ust. 2 rozporządzenia 2016/679 „każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane

116 Germany: First court decision on claims for immaterial damages under GDPR, www.blogs.dlapiper.com [dostęp: 19.12.2018].

117 M. Serwach, *Wina jako zasada odpowiedzialności cywilnej oraz okoliczność zwalniająca z obowiązku naprawienia szkody*, „Wiadomości ubezpieczeniowe" 2009, nr 1, s. 86, www.piu.org.pl [dostęp: 28.01.2019].

przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom". W związku z tym, ważne jest właściwe uregulowanie w umowie powierzenia przetwarzania relacji łączących ADO oraz procesora. Pod kątem odpowiedzialności procesora ważne jest właściwe wypełnienie obowiązków wynikających z umowy, w tym w szczególności zapewnienie odpowiednich środków technicznych i organizacyjnych, nadanie upoważnień do przetwarzania danych. Umowa powierzenia przetwarzania danych powinna ponadto zawierać zgodnie z motywem 81 preambuły rozporządzenia 2016/679 przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Dodatkowo procesor zobowiązany jest do przetwarzania danych wyłącznie na udokumentowane polecenie ADO. W związku z tym możliwa jest odpowiedzialność procesora za naruszenia zarówno wobec ADO, jak i osoby, której dane dotyczą. Odpowiedzialność wobec ADO wynika ze stosunku umownego łączącego go z ADO na podstawie zawartej umowy. Strony, kierując się swobodą zawierania umów mają możliwość dowolnego ukształtowania odpowiedzialności procesora. Istotne jest jednak, by umowa powierzenia przetwarzania danych osobowych zawierała elementy, o których mowa w art. 28 rozporządzenia 2016/679.

Odpowiedzialność procesora została ograniczona do sytuacji, w której nie dopełnił obowiązków wynikających z rozporządzenia 2016/679 lub nie stosował się do instrukcji ADO. Dlatego też prawodawca unijny położył nacisk na to, by ADO wybierał takich procesorów, którzy gwarantują najwyższe standardy świadczonych usług, oraz odpowiednie standardy bezpieczeństwa. W przypadku podpowierzenia danych osobowych, gdy podmiot podpowierzający nie wywiąże się z ciążących na nim obowiązków związanych z zapewnieniem ochrony danych osobowych odpowiedzialność za jego działanie ponosi procesor, który podpowierzył dane osobowe zgodnie z art. 28 rozporządzenia 2016/679.

Każdy z podmiotów zaangażowanych w proces przetwarzania danych odpowiada w stosunku do osoby, której dane dotyczą, proporcjonalnie do poniesionej winy. W przypadku przetwarzania danych przez więcej niż jeden podmiot prawodawca unijny przewidział odpowiedzialność regresową, zgodnie z którą ADO, który wypłacił pełne odszkodowanie może dochodzić roszczeń regresowych wobec innych ADO lub podmiotów przetwarzających uczestniczących w tym

samym przetwarzaniu (motyw 146 preambuły rozporządzenia 2016/679). Odpowiedzialność administracyjna procesora jest niezależna wobec odpowiedzialności kontraktowej.

Zgodnie z art. 77 ust. 1 rozporządzenia 2016/679 „bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie".

Celem kar administracyjnych jest zapewnienie właściwego i zgodnego z prawem procesu przetwarzania danych osobowych. Prawodawca unijny jednoznacznie wskazał to w art. 83 rozporządzenia 2016/679, podkreślając, iż powinny być one „skuteczne, proporcjonalne i odstraszające". Ani na gruncie przepisów europejskich, ani krajowych nie został wypracowany żaden taryfikator kar. Jedynym drogowskazem dla krajowych organów nadzorczych są kryteria określone w art. 83 ust. 2 rozporządzenia 2016/679. Zgodnie z nimi przy określaniu wysokości administracyjnej kary pieniężnej należy brać pod uwagę:

a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
b) umyślny lub nieumyślny charakter naruszenia;
c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;
e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
g) kategorie danych osobowych, których dotyczyło naruszenie;
h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;
j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz

k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Prawodawca unijny dokonał swoistej klasyfikacji naruszeń na te o mniejszej oraz większej wadze ograniczając odpowiedzialność finansową tych pierwszych do wysokości 10 000 000 euro, a w przypadku przedsiębiorstwa do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Do naruszeń tych zgodnie z art. 83 ust. 3 rozporządzenia 2016/679 należą:

a) obowiązki administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 –39 oraz 42 i 43;
b) obowiązki podmiotu certyfikującego, o których mowa w art. 42 oraz 43;
c) obowiązki podmiotu monitorującego, o których mowa w art. 41 ust. 4;

Wyższa, bo do 20 000 000 euro, kara dotyczy naruszenia:

a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9;
b) praw osób, których dane dotyczą, o których mowa w art. 12–22;
c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49;
d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX;
e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.

Jak zostało podkreślone powyższe regulacje mają zastosowanie do podmiotów prywatnych. W przypadku kar nakładanych na podmioty i organy publiczne, państwa członkowskie zostały upoważnione do samodzielnego decydowania o wysokości kar administracyjnych nakładanych na nie. W związku z tym polski ustawodawca zdecydował, że maksymalna wysokość kary administracyjnej nałożonej przez Prezesa UODO w drodze decyzji administracyjnej na podmioty z sektora publicznego wynosi 10 000 złotych. Ta widoczna dysproporcja wysokości kary administracyjnej możliwej do nałożenia na podmioty publiczne i prywatne stała się podstawą do szerszej dyskusji oraz licznych sporów. W założeniu ustawodawcy kara administracyjna w przypadku podmiotów i organów publicznych nie ma mieć charakteru represyjnego, bowiem podmioty te są finansowane z budżetu państwa[118].

118 Uzasadnienie do ustawy o ochronie danych osobowych, druk nr 2410, www.orka.sejm.gov.pl, s. 40 [dostęp: 25.09.2018] .

3.10.3. Odpowiedzialność karna

Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych w znaczący sposób ograniczyły możliwość nakładania kar finansowych na ADO, głównie biorąc pod uwagę niską skuteczność przepisów pod rządami poprzednio obowiązującej ustawy o ochronie danych osobowych. Jak podkreślono w uzasadnieniu do ustawy odpowiedzialność karna ma być jednak wyjątkiem przewidzianym wyłącznie dla najcięższych naruszeń przepisów[119]. Niewątpliwie potwierdza to także założenie, zgodnie z którym dolegliwości finansowe mają lepiej motywować ADO do przestrzegania przepisów, niż widmo więzienia. Odpowiedzialność karna została ograniczona do sytuacji, w której ADO bądź procesor przetwarzają dane bez podstawy prawnej (art. 107 uodo). W innym przypadku odpowiedzialność karna przewidziana została za udaremnienie lub utrudnianie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych (art. 108 uodo).

Dotychczas Prezes UODO, pomimo ponad 40 przeprowadzonych kontroli, nie zdecydował się na nałożenie na ADO kar administracyjnych. Doświadczenie takie posiadają jednak organy nadzorcze innych państw, w tym w szczególności w Portugalii, Wielkiej Brytanii i Niemczech. Głównym powodem nałożenia kar w wysokości od 20 do 400 000 euro był brak różnicowania dostępu do danych osobowych, brak procedury przyznawania dostępu do danych osobowych w wersji cyfrowej, brak usuwania kont e-mail byłych pracowników czy też przenoszenie danych osobowych na pendrive, który nie był zaszyfrowany i został zagubiony.

119 Ibidem, s. 44.

Rozdział 4

Prawa osób, których dane dotyczą, w świetle przepisów rozporządzenia 2016/679

Przetwarzanie danych osobowych w cyberprzestrzeni wymaga zagwarantowania osobie, której dane dotyczą, najwyższych standardów ochrony. Wynika to przede wszystkim z faktu, iż w wirtualnym świecie dane są narażone na ryzyko naruszenia. Ponadto obowiązujące przepisy prawa nie gwarantują odpowiedniego poziomu ochrony prawnej. Chociaż prawo do ochrony danych osobowych wynika z licznych dokumentów międzynarodowych, to jednak dopiero wejście w życie rozporządzenia 2016/679 szczegółowo uregulowało omawianą problematykę. Już sama nazwa rozporządzenia 2016/679 „w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE" wskazuje, że jest to dokument skoncentrowany na zapewnieniu praw i bezpieczeństwa osobom, których dane dotyczą. Potwierdza to także art. 1 ust. 1 dokumentu, w którym podkreślono, że rozporządzenie 2016/679 chroni prawa i wolności osób fizycznych, w szczególności prawo do ochrony danych osobowych. Dodatkowo z motywu 14 preambuły rozporządzenia 2016/679 wynika, że ta ochrona powinna mieć zastosowanie do osób fizycznych niezależnie od ich obywatelstwa czy miejsca zamieszkania w związku z przetwarzaniem ich danych osobowych. Realizacja praw osób, których dane dotyczą, została szczegółowo opisana w rozdziale III rozporządzenia 2016/679 w art. od 12 do 23.

Nie ulega wątpliwości, że katalog praw osób, których dane dotyczą, wynikający z rozporządzenia 2016/679 jest znacznie szerszy niż ten przewidziany w dyrektywie 95/46/WE. Powodem tego jest fakt, że wraz z rozwojem nowych rozwiązań technologicznych pojawiły się także nowe zagrożenia. Konieczne stało się więc zapewnienie osobie, której dane dotyczą, nowych uprawnień. Prawodawca

unijny odwołuje się do kilkunastu praw, z których może korzystać osoba fizyczna w związku z przetwarzaniem jej danych osobowych. Część z nich jest powieleniem praw wynikających z wcześniejszych regulacji, część zaś stanowi przejaw nowych gwarancji. Bez wątpienia sposoby przetwarzania danych osobowych w wirtualnym świecie coraz bardziej ingerują w prawa podmiotów danych. Zostało także wykazane w poprzednich rozdziałach, że profilowanie czy wykorzystywanie plików cookies do śledzenia zachowań użytkownika to tylko nieliczne narzędzia, pozwalające na przetwarzanie danych osobowych bez wiedzy podmiotu danych. Mając na uwadze powyższe okoliczności oraz fakt, że podmiot danych „w walce o dane", która toczy się każdego dnia w wirtualnym świecie jest podmiotem słabszym, przedstawiciele państw członkowskich postanowili stworzyć przepisy gwarantujące takie same standardy prawne we wszystkich państwach należących do EOG. Jednakże aby skutecznie z nich korzystać i zapewnić sobie ochronę prawną w cyberprzestrzeni, ważne jest, by podmiot danych dobrze je poznał i zrozumiał ich wagę.

4.1. Prawo do wyrażenia zgody na przetwarzanie danych osobowych

Najczęściej realizowanym przez podmiot danych uprawnieniem jest prawo do wyrażenia zgody na przetwarzanie danych osobowych. Zgoda na przetwarzanie danych osobowych stanowi jedną z podstaw prawnych przetwarzania danych osobowych określoną w art. 6 rozporządzenia 2016/679. Wprawdzie jest ona najczęściej stosowaną podstawą, to jednak wszystkie podstawy przetwarzania danych określone w art. 6 mają równoważne zarówno charakter, jak i wartość.

Jak podkreśla KE „w środowisku internetowym, ze względu na niejasne reguły dotyczące prywatności, osoby fizyczne mają większe trudności z uzyskaniem informacji o przysługujących im prawach oraz wyrażeniem świadomej zgody. Sytuację komplikuje dodatkowo fakt, że w niektórych przypadkach nie jest nawet jasne, co stanowiłoby konkretną, świadomą i dobrowolną zgodę na przetwarzanie danych, tak jak w przypadku reklamy behawioralnej, kiedy to według stanowiska niektórych podmiotów, użytkownik wyraża zgodę przez same ustawienia przeglądarki internetowej"[120]. Przez pojęcie zgody należy rozumieć „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych" (art. 4 ust. 11 rozporządzenia

120 Grupa Robocza art. 29, Opinia 15/2011 w sprawie definicji zgody przyjęta 13 lipca 2011 r., WP 187, www.giodo.gov.pl, s. 8 [dostęp: 13.12.2018].

2016/679). W sytuacji przetwarzania danych w wirtualnym świecie zapewnienie dobrowolnego, świadomego i jednoznacznego okazania woli może być trudne do zrealizowania. Mowa tu zwłaszcza o elemencie dobrowolności zgody. Bardzo często ADO wymuszają na osobie, której dane dotyczą, złożenie oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych, warunkując tym samym możliwość przejścia do właściwej witryny internetowej. W takiej sytuacji osoba, której dane dotyczą, nie ma możliwości dokonania wyboru, czy chce udzielić zgody czy też nie. Administrator danych osobowych ogranicza jej wybór do scenariusza: albo wyrazisz zgodę na przetwarzanie twoich danych osobowych, albo nie będziesz mógł skorzystać z naszej usługi. Jest to klasyczne wyłudzanie danych i zmuszanie do wyrażania zgody. Tymczasem celem prawodawcy było zagwarantowanie osobie, której dane dotyczą, możliwości wyrażenia zgody, która byłaby bezwarunkowa.

Podmiot danych nie powinien ponosić żadnych negatywnych konsekwencji w związku z brakiem udzielenia zgody (poza sytuacją, w której uzyskanie zgody jest konieczne do przetwarzania jej danych). Zgody nie uważa się również za dobrowolną (zgodnie z motywem 42 preambuły rozporządzenia 2016/679), jeżeli osoba nie może jej wyrazić osobno na różne operacje przetwarzania danych osobowych. Częstą praktyką w cyberprzestrzeni jest łączenie zgód na różne cele w jednym oświadczeniu woli. W konsekwencji takiego działania osoba zostaje pozbawiona możliwości wyboru przedmiotu swojej zgody. W motywie 32 preambuły rozporządzenia 2016/679 prawodawca zwraca uwagę na to, że zgoda powinna dotyczyć wszystkich czynności przetwarzania danych w tym samym celu lub tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie z nich. Niezbędne w tym zakresie jest właściwe określenie celu przetwarzania danych, np. przeprowadzenia rekrutacji, wysłania newslettera. Niedopuszczalne jest zbieranie danych w jednym celu, a przetwarzanie ich w innym celu. O każdej zmianie celu ADO musi poinformować osobę, której dane dotyczą. Najczęściej niewłaściwe praktyki w tej materii stosowane są przez sklepy internetowe czy portale społecznościowe. Często wykonanie umowy warunkowane jest wyrażeniem zgody na przetwarzanie danych osobowych, mimo że do jej wykonania zgoda osoby, której dane dotyczą, nie jest potrzebna. Przejawem braku dobrowolności jest także zamieszczanie przez ADO na formularzach elektronicznych pola z uprzednio zaznaczonymi zgodami. Jeżeli osoba, której dane dotyczą, nie chce, by jej dane osobowe były przetwarzane we wskazanym celu, zobowiązana jest odhaczyć zaznaczoną zgodę. W ten sposób ADO wyraża wolę za osobę, której dane dotyczą, pozbawiając ją tym samym przysługujących jej praw. Praktyka ta bardzo często wykorzystywana w Internecie nakierowana była na pozyskanie zgód od tych osób, które nie czytają, na co wyrażają zgody lub nie są zainteresowane

celem przetwarzania danych. Zakaz ten wynika wprost z motywu 32 preambuły rozporządzenia 2016/679, gdzie zostało zauważone, iż „milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody". Chęć uzyskania dostępu do określonego towaru lub usługi jest tak duża, że skłonni jesteśmy udzielić zgody praktycznie na wszystko, byle tylko otrzymać spodziewany rezultat. Środowisko cyberprzestrzeni nacechowane jest mnogością informacji. Każdego dnia odwiedzamy nowe strony internetowe, gdzie zbierane są od nas zgody na przetwarzanie danych osobowych w różnych celach. Część z nas w ogóle nie przywiązuje uwagi do tego, na co właściwie wyrażamy zgodę. Zjawisko to zostało dostrzeżone przez Grupę Roboczą art. 29, która zauważa, że praktyki takie wykorzystywane są przez podmioty do nielegalnego zbierania zgód od użytkowników Internetu.

Brak dobrowolności zgody był wielokrotnie analizowany w kontekście stosunku pracy, gdzie podkreślano, że stosunek taki opiera się na podległości pracownika wobec pracodawcy. W związku z tym pracownik zawsze będzie musiał brać pod uwagę konsekwencje, jakie niesie za sobą niewyrażenie zgody[121]. Przykładem przetwarzania danych osobowych pracowników przez Internet jest publikowanie na stronie internetowej wizerunku pracownika. Administrator danych osobowych, zgodnie z zasadą rozliczalności, powinien wylegitymować się posiadaniem pisemnych zgód zainteresowanych na przetwarzanie ich wizerunku.

Każdy przypadek dotyczący sposobu wyrażenia zgody należy oceniać indywidualnie. Ciężar dowodowy w tym zakresie spoczywa na ADO, który będzie musiał wykazać, w jaki sposób odebrał zgodę na przetwarzanie danych osobowych. Dlatego tak ważne jest, by ADO mógł udowodnić, kiedy oraz w jakim celu została wyrażona zgoda przez osobę, której dane dotyczą. Przepisy milczą jednak, w jaki sposób ADO powinien realizować ten wymóg. Wymaga to od ADO dostosowania systemów informatycznych do przechowywania zgody oraz zapewnienia rozliczalności procesu poprzez wskazanie, na co osoba, której dane dotyczą, wyraziła zgodę, choćby poprzez stworzenie rejestru zgód. Z uwagi na fakt, że zgodą może być okazanie woli, np. poprzez podjęcie określonego działania, wówczas rekomendowane jest odebranie pisemnego potwierdzenia udzielenia przez osobę, której dane dotyczą, zgody. Administrator danych osobowych powinien przechowywać zgody tak długo, aż nie zostaną one cofnięte przez osobę, której dane dotyczą. Prawodawca unijny położył ogromny nacisk na zapewnienie możliwości szybkiego i łatwego cofnięcia zgody. Wiele osób uważało bowiem, że raz udzielonej zgody nie można cofnąć. W związku z tym przy każdym oświadczeniu o wyrażeniu zgody ADO musi

121 Wyrok NSA z 1 grudnia 2009 r., I OSK 249/09.

poinformować osobę o przysługującym jej prawie do wycofania zgody. Administrator danych osobowych powinien dodatkowo zapewnić możliwość wycofania zgody przez osobę, której dane dotyczą, tak samo łatwo jak jej udzielenia. Tak więc, jeżeli zgody zbierane są przez Internet w sposób, który polega na zaznaczeniu pola na formularzu, jej cofnięcie powinno odbyć się w podobnie prosty sposób. Zatem napisanie e-maila w celu odwołania zgody, gdy udzieleniem zgody było odznaczenie okienka na formularzu nie może być sposobem na cofnięcie zgody. Coraz częstszą praktyką jest zamieszczanie na stronie internetowej formularza cofnięcia zgody lub linku dedykowanego cofnięciu zgody.

Nie ulega wątpliwości, że standardy wprowadzone w rozporządzeniu 2016/679 nakierowane są na zapewnienie osobie, której dane dotyczą, szerszej ochrony. Jest to szczególnie widoczne w Internecie, gdzie ADO uciekają się do różnych metod, by pozyskać zgodę na przetwarzanie danych osobowych.

Udzielenie zgody wymaga od podmiotu danych okazania woli w formie oświadczenia lub wyraźnego działania potwierdzającego. W motywie 32 preambuły rozporządzenia 2016/679 podkreślono, że wyrażenie zgody może polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała sposób przetwarzania jej danych osobowych. Według opinii Grupy Roboczej art. 29 w przypadku zgody wyrażanej drogą elektroniczną działaniem potwierdzającym może być przesunięcie palcem po ekranie lub machnięcie przed inteligentną kamerą[122]. Należy podkreślić, iż ADO powinien uzyskać zgodę jeszcze przed rozpoczęciem procesu przetwarzania danych osobowych[123]. Ponadto każdorazowe udzielenie zgody na przetwarzanie danych osobowych powinno być poprzedzone pełną wiedzą osoby, której dane dotyczą, na temat realizowanego procesu. Najczęściej towarzyszyć temu będzie obowiązek wypełnienia przez ADO obowiązku informacyjnego.

4.2. Zgoda na przetwarzanie danych osobowych

Prawodawca unijny, mając na uwadze rozwijający się postęp technologiczny w przepisach rozporządzenia 2016/679 zwrócił także uwagę na potrzebę uregulowania

122 Grupa Robocza art. 29, Wytyczne z 28 listopada 2017 r. dotyczące zgody na mocy rozporządzenia 2016/679, WP 259, www.uodo.gov.pl, s. 17 [dostęp: 18.12.2018].

123 Ibidem, s. 22.

sposobu przetwarzania danych osobowych, które dotyczą małoletnich. Problematyka przetwarzania danych osobowych dzieci była już wcześniej podejmowana w dokumentach unijnych. Grupa Robocza art. 29, dostrzegając zagrożenie związane z korzystaniem przez dzieci z usług społeczeństwa informacyjnego wydała opinię 5/2009 w sprawie portali społecznościowych[124]. Rekomendacje wydawane przez Grupę Roboczą art. 29 nie mają charakteru wiążącego i stanowią jedynie opinie organu, niemniej jednak wnoszą istotny wkład w rozwój prawa do ochrony danych osobowych.

Na rozwój zainteresowania problematyką przetwarzania danych osobowych dzieci wpływ miały rozwijające się na niespotykaną wcześniej skalę portale społecznościowe. Powszechna dostępność, metody działania, a także niepożądane skutki, jakie coraz częściej pojawiają się wśród ich uczestników (uzależnienia, kradzież tożsamości) stały się podstawą do objęcia ochroną prawną osób poniżej 16. roku życia. Jednocześnie ustawodawca unijny dał państwom członkowskim możliwość obniżenia granicy wieku do 13 lat. Ustawodawca krajowy, przygotowując polską ustawę o ochronie danych osobowych z 2018 r. skorzystał z tej możliwości. W uzasadnieniu do unijnej propozycji wskazano, że sugerowana granica wieku będzie spójna z kc, a w szczególności z art. 15 kc, zgodnie z którym ograniczoną zdolność do czynności prawnych mają małoletni, którzy ukończyli lat 13 oraz osoby ubezwłasnowolnione częściowo. Ograniczona zdolność do czynności prawnych oznacza, że małoletni może składać oświadczenia woli, jednakże w pewnych sytuacjach do ich skuteczności wymagana jest zgoda przedstawiciela ustawowego[125]. Z uwagi na liczne protesty środowiska pedagogicznego, rodziców, a także samego UODO, nie zdecydowano się na utrzymanie obniżonej granicy wieku dzieci w Polsce[126]. Przepis ten należy interpretować jako wyraz troski prawodawcy unijnego o dzieci oraz świadomości zagrożeń związanych z ich funkcjonowaniem w wirtualnym świecie. Jak słusznie podkreślono w motywie 38 preambuły rozporządzenia 2016/679, dzieci są mniej świadome ryzyka, konsekwencji, sposobów zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych niż osoby dorosłe. W celu zapewnienia małoletnim odpowiedniego poziomu ochrony w cyberprzestrzeni niezbędne jest zapewnienie właściwych regulacji prawnych. Często jednak zwraca się uwagę na podejmowanie szerszych działań profilaktycznych,

124 Pojęcie usług społeczeństwa informacyjnego obejmuje umowy i inne usługi, które są zawierane i przekazywane online. Grupa Robocza art. 29, Wytyczne z 28 listopada 2017 r. dotyczące zgody na mocy rozporządzenia 2016/679., WP 259, s. 30. Definicja usług społeczeństwa informacyjnego została także zawarta w art. 4 ust. 25 rozporządzenia 2016/679.

125 Uzasadnienie do ustawy o ochronie danych osobowych, Druk nr 2410, s.10 [dostęp: 27.07.2018].

126 Uwagi GIODO do projektu nowych przepisów o ochronie danych osobowych, www.giodo.gov.pl, [dostęp: 12.08.2018].

jak na przykład prowadzenie akcji mających na celu zwiększenie świadomości dzieci oraz zachęcanie dostawców do przyjmowania kodeksów dobrych praktyk[127].

W przypadku przetwarzania danych osobowych dzieci zwraca się uwagę na to, by ADO używał prostego i czytelnego języka, nie konstruował długich, wielowątkowych zdań[128]. Administrator danych osobowych powinien mieć możliwość zweryfikowania wieku dziecka. Jak zauważa Grupa Robocza art. 29 „w przypadku gdy użytkownik stwierdzi, że jest poniżej wieku uprawniającego do wyrażenia zgody online, administrator danych może to oświadczenie zaakceptować bez dalszej kontroli, ale będzie musiał przejść do autoryzacji rodzicielskiej i weryfikacji, że osoba udzielająca takiej zgody sprawuje władzę rodzicielską"[129].

Odbieranie zgody od osób, których dane dotyczą, stało się także przedmiotem prac nad rozporządzeniem w sprawie prywatności i łączności elektronicznej, zwłaszcza pod kątem prawidłowości wyrażenia zgody przez użytkowników za pośrednictwem ustawień przeglądarek[130]. Zgodnie z propozycją użytkownik powinien mieć możliwość wyrażenia zgody na śledzenie aktywności na każdej odwiedzanej przez niego stronie internetowej. Łączenie zgód na śledzenie przez różnych dostawców byłoby możliwe wyłącznie w sytuacji, w której do tego samego ADO należy kilka stron. Podobnie przeglądarki powinny dawać użytkownikowi wybór akceptowanych przez niego plików cookies, zamiast akceptowania ich w całości[131]. Zgodnie z propozycjami odmowa wyrażenia zgody na śledzenie dotyczące całego Internetu przez konkretną organizację powinna uniemożliwiać jej ponowne zwrócenie się do wyrażenia zgody w ciągu kolejnych 6 miesięcy[132].

4.3. Prawo do usunięcia danych osobowych

Każdego dnia w Internecie pojawia się tysiące nowych informacji, które szybko ulegają dezaktualizacji. Szacuje się, że co sekundę powstaje 30 GB nowych informacji[133]. Rzadko kiedy weryfikujemy ich poprawność i jeszcze rzadziej aktualność.

127 Grupa Robocza art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta 12 czerwca 2009 r., WP 163.

128 Ibidem.

129 Grupa Robocza art. 29, Wytyczne z 28 listopada 2017 r. dotyczące zgody na mocy rozporządzenia 2016/679, WP 259, s.32.

130 Grupa Robocza art. 29, Opinia 1/2017 na temat proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej (2002/58/WE) przyjęta 4 kwietnia 2017 r., WP 247, www.uodo.gov.pl., s. 18 [dostęp: 13.09.2018].

131 Ibidem, s. 19.

132 Ibidem.

133 *Jak wygląda sekunda w Internecie?*, www.antyradio.pl [dostęp: 09.09.2018].

Informacje te nie są usuwane, co zaprzecza potocznemu przekonaniu, że Internet zapomina. W realnym świecie powszechnie stosowane są instrumenty prawne (zwłaszcza w prawie karnym i cywilnym) umożliwiające zatarcie skazania lub przedawnienia roszczeń, które po upływie określonego czasu pozwalają puścić w niepamięć zdarzenie z przeszłości. Okazuje się, że rozwiązanie to zostało pominięte w cyberprzestrzeni, która jest obszarem, gdzie publikujemy informacje, ale ich nie usuwamy. Na tym tle zaczęły pojawiać się zarzuty, iż użytkownicy wirtualnego świata nie mają zapewnionej ochrony na takim samym poziomie jak w rzeczywistości.

W 2014 r. TSUE wydał wyrok w sprawie Google[134]. W omawianej sprawie zostało skierowane pytanie prejudycjalne do TSUE w związku ze sporem pomiędzy Google i Google Spain a hiszpańskim organem ochrony danych (Agencia Española de Proteccion de Datos, AEPD) i obywatelem hiszpańskim – Mario Costeją Gonzalezem, który zażądał od Google i Google Spain usunięcia jego danych osobowych w zakresie imienia i nazwiska oraz informacji na swój temat zamieszczonych 19 stycznia i 9 marca 1988 r. w hiszpańskiej gazecie w związku z licytacją nieruchomości za niespłacone należności na rzecz zakładu zabezpieczeń społecznych. W ocenie skarżącego postępowanie zostało dawno zakończone i obecnie nie ma żadnego znaczenia. W związku tym Mario Costeja Gonzalez zwrócił się do Google Spain z prośbą o usunięcie jego danych osobowych w taki sposób, by nie były one ujawniane w wynikach wyszukiwania. Hiszpański organ ochrony danych – AEPD – przyjął skargę od poszkodowanego i zażądał od Google Spain SL oraz Google Inc. wycofania danych skarżącego ze swoich indeksów. Urząd uznał, iż publikacja rozpatrywanych danych była prawnie uzasadniona, gdyż nastąpiła na żądanie ministerstwa pracy i polityki społecznej, a jej celem było jak najszersze rozpowszechnienie informacji o licytacji, tak aby owa licytacja miała jak największą liczbę uczestników. W odpowiedzi na to Google i Google Spain wniosły dwa odwołania od decyzji organu orzekającego i zażądały jej usunięcia. Wobec rodzących się wątpliwości krajowy organ orzekający wystąpił do TSUE z pytaniami prejudycjalnymi odnoszącymi się do przedmiotu sporu w kontekście prawa do bycia zapomnianym – usunięcia danych.

Chociaż sama sprawa dotyczyła prawa do usunięcia danych, to jednak przy okazji poruszony został niezwykle ważny, z punktu widzenia przetwarzania danych osobowych w cyberprzestrzeni, problem dotyczący metod działania wyszukiwarek internetowych. Na tym obszarze istnieje ryzyko ograniczenia prawa do ochrony

134 Wyrok TSUE z 13 maja 2014 r., Google Spain SL, Google Inc. przeciwko Agencia Española de Proteccion de Datos, Mario Costeja Gonzalez, C-131/12, ECLI:EU:C:2014:317, www.curia.europa.eu [dostęp: 17.02.2018].

danych osobowych oraz prawa do prywatności użytkowników. Jak zauważono w omawianym wyroku, działania operatorów wyszukiwarek internetowych mogą mieć wpływ na podstawowe zasady poszanowania prywatności i ochrony danych osobowych w sytuacji, w której przeszukiwanie zasobów internetowych jest prowadzone począwszy od imienia i nazwiska osoby fizycznej. Umożliwia to bowiem wszystkim internautom otrzymanie listy wyników wszelkich informacji dotyczących tej osoby, jakie można znaleźć w Internecie. Mogą one obejmować cały szereg aspektów jej życia prywatnego. Gdyby nie wyszukiwarka to te informacje nie mogłyby zostać ze sobą powiązane lub też byłoby to bardzo utrudnione. Tym samym sporządzenie mniej lub bardziej szczegółowego profilu danej osoby, byłoby bardzo utrudnione lub wręcz niemożliwe. Dodatkowo w ocenie TSUE „skutki tej ingerencji w prawa osoby, której dane dotyczą, zostają zwielokrotnione ze względu na istotną rolę, jaką odgrywają Internet i wyszukiwarki internetowe we współczesnym społeczeństwie, nadając zawartej na takiej liście wyników informacji wszechobecny charakter”[135].

Trybunał Sprawiedliwości Unii Europejskiej uznał, że prowadzona przez wyszukiwarki internetowe działalność, która polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, stanowi przetwarzanie danych osobowych, a co za tym idzie operator wyszukiwarki internetowej został uznany za ADO, czyli podmiot decydujący o celach i sposobie przetwarzania danych. Trybunał Sprawiedliwości Unii Europejskiej, mając to na uwadze uznał „że operator wyszukiwarki internetowej jest zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania, mającego za punkt wyjścia imię i nazwisko danej osoby, linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje, również w przypadku gdy to imię czy nazwisko, czy też inne informacje nie zostały uprzednio, czy też jednocześnie usunięte z tych stron internetowych, i w odpowiednim przypadku, nawet jeśli ich publikacja na tych stronach jest zgodna z prawem”[136].

Usunięcie danych ze strony głównej (źródłowej) może okazać się niewystarczające wobec możliwości kopiowania i wtórnego wykorzystywania takich danych. W związku z tym ADO jest zobowiązany do poinformowania osób trzecich, które przetwarzają dane, o żądaniu podmiotu danych[137]. W myśl art. 17 ust. 2 rozporządzenia 2016/679 w przypadku żądania osoby o usunięcie jej danych osobowych ADO ma obowiązek usunąć je oraz podjąć działania, by poinformować innych ADO,

135 Ibidem.

136 Ibidem.

137 Grupa Robocza art. 29, Opinia 1/2012 o projektach reformy ochrony danych przyjęta 23 marca 2012 r., WP 191, www.giodo.gov.pl, s. 14 [dostęp:09.01.2019].

przetwarzających te dane, że osoba, której dane dotyczą, żąda, by ADO usunęli wszystkie łącza do tych danych, ich kopie lub replikacje. Dodatkowo w motywie 66 preambuły rozporządzenia 2016/679 zostało podkreślone, że „wzmocnienie prawa do «bycia zapomnianym» w Internecie, może mieć miejsce jeżeli prawo do usunięcia danych zostanie rozszerzone na zobowiązanie administratora, który upublicznił dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji". Administrator danych osobowych, spełniając ten obowiązek powinien podjąć racjonalne działania w celu poinformowania ADO, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą.

W omawianym wyroku organ orzekający przesądził, że prawo do prywatności oraz prawo do ochrony danych osobowych są nadrzędne w stosunku do celu gospodarczego, jaki przyświeca operatorom wyszukiwarek internetowych. W związku z tym osoba, której dane dotyczą, ma prawo żądać realizacji przysługujących jej praw. Zagwarantowane w art. 17 rozporządzenia 2016/679 prawo do usunięcia danych jest wyrazem wzmocnienia realizacji praw osób, których dane dotyczą, zwłaszcza w kontekście przetwarzania danych osobowych w Internecie. Prawo to było także zagwarantowane w przepisach dyrektywy 95/46/WE, chociaż wraz z wejściem w życie rozporządzenia 2016/679 uległo znacznemu wzmocnieniu.

W świetle obowiązujących przepisów osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia jej danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki je usunąć, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a rozporządzenia 2016/679 i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 rozporządzenia 2016/679 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 rozporządzenia 2016/679.

Żądanie usunięcia danych niesie po stronie ADO obowiązek podjęcia określonych działań. Po pierwsze zobowiązany jest zweryfikować tożsamość osoby, której dane dotyczą, a po drugie ustalić, czy zachodzą przesłanki uzasadniające usunięcie danych osobowych. Jeżeli tak (w praktyce najczęściej będą to dane przekazane na podstawie zgody osoby, której dane dotyczą), wówczas ADO powinien podjąć stosowne kroki w celu usunięcia danych. Zasada rozliczalności wymaga, aby pozostawić ślad pozwalający udowodnić przeprowadzoną operację.

4.4. Prawo do niepodlegania decyzjom podejmowanym w ramach zautomatyzowanego przetwarzania danych w tym profilowania

Dane osobowe przetwarzane przez ADO mogą być wykorzystywane w różny sposób i w różnych celach. Chcąc jak najlepiej dostosować towar lub usługę do oczekiwań klienta niezbędne jest dysponowanie wiedzą o jego potrzebach. Najnowsze rozwiązania technologiczne umożliwiają gromadzenie informacji o preferencjach i zachowaniach użytkowników, klientów. Najczęściej tego rodzaju informacje zbierane są bez wiedzy użytkowników, ingerując tym samym w ich prywatność. Problem ten został dostrzeżony już dawno, jednakże dopiero wejście w życie rozporządzenia 2016/679 pozwoliło na uregulowanie przepisów prawnych zapewniających jednostce bezpieczeństwo w tym obszarze. Profilowanie, w świetle omawianego dokumentu, jest zautomatyzowanym przetwarzaniem danych osobowych, które polega na wykorzystywaniu ich do oceny niektórych czynników osobowych osoby fizycznej, w szczególności analizy i prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się (art. 4 pkt 4 rozporządzenia 2016/679). Tworzenie profili oznacza przetwarzanie danych polegające na przypisaniu danej osobie „profilu" w celu podejmowania dotyczących jej decyzji, bądź analizy lub przewidywania jej preferencji, zachowań i postaw[138].

Na tym tle wyróżniamy dwa rodzaje profilowania:

- bezpośrednie – gdzie profil osoby tworzy się na podstawie dotyczących jej danych. W tym przypadku informacje o osobie zbierane są z różnych źródeł. Przykładem tego rodzaju profilowania jest dokonywanie oceny zdolności kredytowej klienta;

138 Komitet Ministrów Rady Europy, Rekomendacja CM/Rec (2010)13 przyjęta 23 listopada 2010 r. podczas 1099 posiedzenia Wiceministrów, www.giodo.gov.pl [dostęp:12.10.2018].

- pośrednie – gdy profil powstaje na podstawie danych o innych osobach. Jeżeli osoba przejawia zachowanie A to istnieje wysokie prawdopodobieństwo, że przejawia też zachowanie B i C – chociaż nie wiemy tego na pewno[139]. Przykładem tego rodzaju profilowania jest zbieranie danych z plików cookies[140].

W przypadku profilowania *sensu stricto* dochodzi wyłącznie do stworzenia profilu osoby fizycznej, bez jakiegokolwiek podejmowania decyzji[141]. W takim przypadku zastosowanie znajdują przepisy ogólne, a osobie, której dane dotyczą, przysługuje prawo wyrażenia sprzeciwu na podstawie art. 21 ust. 1 rozporządzenia 2016/679. Jeżeli proces przetwarzania danych odbywa się bez udziału czynnika ludzkiego, dochodzi wówczas do zautomatyzowanego przetwarzania danych. W tym przypadku człowiek nie ma wpływu na powstały wynik. Przykładem najlepiej obrazującym to zjawisko, zgodnie z motywem 71 preambuły rozporządzenia 2016/679, jest automatyczne odrzucenie wniosku kredytowego. W takiej sytuacji profil osoby tworzony jest na potrzeby automatycznego podejmowania decyzji[142]. W rozporządzeniu 2016/679 zostało mocno wyartykułowane, że osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa (art. 22 ust. 1 rozporządzenia 2016/679). Podejmowanie zautomatyzowanej decyzji na podstawie profilowania jest możliwe tylko w przypadku zaistnienia jednej z przesłanek określonych w rozporządzeniu 2016/679. Sytuacje określone w art. 22 ust. 2 stanowią wyjątek od ogólnej zasady określonej w art. 22 ust. 1 rozporządzenia 2016/679. Mowa tu przede wszystkim o sytuacji, w której jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO.

Podejmowanie zautomatyzowanej decyzji na podstawie profilowania jest możliwe również wówczas, gdy decyzja ta jest dozwolona prawem UE lub prawem państwa członkowskiego, któremu podlega ADO, i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, lub opiera się na wyraźnej zgodzie osoby, której dane dotyczą (art. 22 ust. 2 rozporządzenia 2016/679).

Jak zauważa Grupa Robocza art. 29, aby doszło do profilowania muszą zostać spełnione trzy przesłanki:

---

139 X. Konarski, *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce*, [w:] *Ogólne rozporządzenie o ochronie danych, aktualne problemy prawnej ochrony danych osobowych 2016 r.*, red. G. Sibiga, Warszawa 2016 r., s. 50.

140 E. Niezgódka, *Definicja i skutki profilowania w przepisach rodo*, „ABI Expert" 2018, nr 1, s. 15.

141 Ibidem.

142 X. Konarski, *Profilowanie…*, op. cit., s. 51.

- przetwarzanie danych musi mieć zautomatyzowaną formę;
- musi dotyczyć danych osobowych;
- celem profilowania musi być ocena niektórych czynników osobowych osób fizycznych[143].

Z uwagi na fakt, że profilowanie, co do zasady, (chociaż nie zawsze) będzie wiązało się z ustaleniem tożsamości osoby fizycznej, często będzie dochodziło na tym tle do przetwarzania danych osobowych, a co za tym idzie przepisy rozporządzenia 2016/679 znajdą zastosowanie w tym zakresie.

Informacje o użytkowniku rejestrowane są na podstawie odwiedzanych przez niego stron czy wyszukiwanych informacji. Określone treści, których szuka użytkownik podsyłane są na podstawie tego, co zostało dotychczas o nim zgromadzone (tzw. profil). To zaś w znaczący sposób ogranicza nam prawo dostępu do informacji, bowiem użytkownikowi zawęża się horyzont zainteresowań wyłącznie do informacji wyselekcjonowanych na podstawie stworzonego profilu. Przykładem są spersonalizowane reklamy. Jeżeli użytkownik szuka wybranego produktu, będzie otrzymywać w kolejnych dniach reklamy oferujące podobne produkty. Zjawisko to nazywane jest retargetingiem[144]. Informacje, jaki produkt ma zostać użytkownikowi przedstawiony zbierane są na podstawie odwiedzanych przez niego stron.

Profil użytkownika tworzony jest na podstawie jego aktywności w wirtualnym świecie, jego adresu IP, rodzaju odwiedzanych stron, urządzeń, z których się loguje oraz częstotliwości robionych zakupów przez Internet. Każda informacja pozwalająca na sprecyzowanie profilu użytkownika przyczynia się do zaproponowania mu lepszej informacji, usługi czy towaru. Profilowanie rodzi ryzyko powstania bańki filtrowej, która polega na zamykaniu się w świecie własnych poglądów poprzez brak dopływu informacji innych niż te, których szuka użytkownik[145].

Jako użytkownicy płacimy wysoką cenę za szybsze i łatwiejsze uzyskanie dostępu do informacji – utratę prywatności. Dopóki działania dostawców usług nie są dla nas uciążliwe, godzimy się na oferowane warunki. Czy jednak, kiedy uświadomimy sobie, na czym w rzeczywistości polegają te działania, nie będzie już zbyt późno?

Należy mieć świadomość, że część użytkowników nawet jeżeli zdaje sobie sprawę z faktu profilowania, nie zdaje sobie sprawy z ewentualnych konsekwencji.

---

143 Grupa Robocza art. 29, Wytyczne z 3 października 2017 r. dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, ostatnio zmienione i przyjęte 6 lutego 2018 r., WP 251, www.uodo.gov.pl., s. 7 [dostęp:12.09.2018].

144 K. Szymielewicz, *Profilowanie w marketingu*, „ABI Expert" 2018, nr 1, s. 17.

145 A. Dziekan-Łanucha, *Od personalizacji do profilowania. Opis konsekwencji korzystania z wyszukiwarki internetowej Google*, „Studia Socialia Cracoviensia" 2016, t. 8, nr 1, s. 123–136, http://dx.doi.org/10.15633/ssc.1897 [dostęp: 12.10.2018].

Warto więc edukować użytkowników od najmłodszych lat, jakie zagrożenia związane są z przetwarzaniem danych w cyberprzestrzeni, w jaki sposób zbierane są informacje o użytkownikach i do jakich celów mogą być wykorzystywane. Problem profilowania został dostrzeżony również przez Komitet Ministrów Rady Europy w 2010 r., który opublikował rekomendacje w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili[146]. Członkowie Rady Europy zwrócili uwagę na to, żeby przetwarzanie danych w związku z tworzeniem profili odbywało się zgodnie z poszanowaniem obowiązujących przepisów prawa, w sposób rzetelny, proporcjonalny i w uzasadnionym celu. Dodatkowo zbieranie danych osobowych powinno odbywać się na podstawie zgody osoby, której dane dotyczą. W ocenie członków Komitetu Ministrów Rady Europy ADO powinien realizować wobec osób, których dane dotyczą, obowiązek informacyjny, a osoba, której dane dotyczą, powinna mieć zapewniony dostęp do przysługujących jej praw, w tym w szczególności prawa dostępu do danych czy wyrażenia sprzeciwu. Dodatkowo ADO powinien zadbać, by dane przetwarzane były zgodnie z prawem, rzetelnie i w sposób przejrzysty. Jest to szczególnie ważne, ponieważ bardzo często osoba, której dane dotyczą, nie ma świadomości, że jest objęta procesem profilowania.

Poza zagrożeniem dla prywatności profilowanie może prowadzić do dyskryminacji oraz nierównego traktowania[147]. Najlepiej widoczne jest to w przypadku szukania ofert na wakacje. Jeżeli przeglądamy oferty hotelu dwugwiazdkowego istnieje wysokie prawdopodobieństwo, że nigdy nie otrzymamy oferty na pobyt w hotelu cztero- lub pięciogwiazdkowym. A przecież nie zawsze przeglądanie tańszych ofert związane jest ze stanem majątkowym i jeden tańszy wyjazd nie musi oznaczać, że zawsze wybieramy hotele niższego standardu. To właśnie profil pośredni rodzi ryzyko dyskryminacji, ponieważ tworzony jest jedynie na podstawie przewidywań. Oznacza to, że użytkownik Internetu może zostać niesłusznie zakwalifikowany do określonej grupy osób, co może przyczynić się do jego dyskryminacji[148]. Dodatkowo coraz częściej wskazuje się, że profilowanie może mieć charakter dyskryminujący poprzez ograniczanie użytkownikowi dostępu do określonych dóbr czy usług.

Jak zostało zauważone przepisy rozporządzenia 2016/679 w istotny sposób rozszerzają prawa osób, których dane dotyczą, skupiając się przede wszystkim na zapewnieniu osobie pełnej informacji na temat procesu przetwarzania danych.

146 Komitet Ministrów Rady Europy, Rekomendacja CM/Rec (2010)13 przyjęta 23 listopada 2010 r. podczas 1099 posiedzenia Wiceministrów, www.giodo.gov.pl [dostęp:17.09.2018].

147 Broszura RODO wersja 18.35, www.uodo.gov.pl [dostęp: 09.08.2018].

148 X. Konarski, *Profilowanie…*, op. cit., s.49.

W ramach realizowanego przez ADO obowiązku informacyjnego osoba, której dane dotyczą, powinna zostać poinformowana o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, zasadach podejmowania decyzji, a także o znaczeniu i możliwych do wystąpienia konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 13 ust. 2 lit. f rozporządzenia 2016/679). Przysługuje jej także prawo dostępu do danych (na podstawie art. 15 ust. 1 lit. h rozporządzenia 2016/679), prawo do sprostowania i usunięcia danych (art. 16 i 17 rozporządzenia 2016/679) czy prawo do ograniczenia przetwarzania danych (art. 18 rozporządzenia 2016/679). W celu zapewnienia rozliczalności procesu ADO powinien przeprowadzić ocenę skutków dla ochrony danych zgodnie z art. 35 rozporządzenia 2016/679. Jest to wymagane w przypadku systematycznej i kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym także profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływa na osobę fizyczną (art. 35 ust. 3 lit. a rozporządzenia 2016/679). Administrator danych osobowych powinien dodatkowo zadbać o stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych, a także uwzględniających poziom ryzyka związanego z profilowaniem.

4.5. Prawo do wniesienia skargi do organu nadzorczego

Prawo do wniesienia skargi do Prezesa UODO jest podstawowym uprawnieniem osoby, której dane dotyczą. Jego realizacja została zapewniona na podstawie art. 77 rozporządzenia 2016/679. Każdy organ nadzorczy, który został powołany w państwie członkowskim jest właściwy do wypełniania zadań i wykonywania uprawnień zgodnie z przepisami rozporządzenia 2016/679 na terytorium swojego państwa. Skargę do organu nadzorczego można wnieść w państwie członkowskim swojego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. W konsekwencji daje to osobie, której dane dotyczą, możliwość składania skargi praktycznie w każdym państwie członkowskim. W przypadku przetwarzania danych w cyberprzestrzeni ustalenie właściwego organu nadzorczego może rodzić jednak określone trudności.

Pomocne w tym zakresie mogą okazać się przepisy dotyczące transgranicznego przetwarzania danych osobowych. W przypadku, gdy ADO posiada jednostkę organizacyjną w więcej niż jednym państwie członkowskim za główną jednostkę organizacyjną uznaje się miejsce, w którym znajduje się centralna administracja w UE. Natomiast jeżeli decyzje odnośnie do celów i sposobów przetwarzania

danych osobowych zapadają w innej jednostce organizacyjnej tego ADO w UE i ta jednostka ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną, zgodnie z definicją zaproponowaną w art. 4 ust. 16 rozporządzenia 2016/679, uznaje się jednostkę organizacyjną, w której zapadają takie decyzje. W przypadku przetwarzania danych w cyberprzestrzeni może jednak zdarzyć się sytuacja, w której ADO nie będzie w ogóle posiadać jednostki organizacyjnej na terytorium UE. Wówczas, zgodnie z motywem 80 preambuły rozporządzenia 2016/679 ADO jednostki organizacyjnej poza UE, który przetwarza dane osobowe osób, których dane dotyczą, będących mieszkańcami UE, powinien wyznaczyć swojego przedstawiciela, który ma działać w jego imieniu i być adresatem ewentualnych działań organu nadzorczego.

Na podstawie przepisów rozporządzenia 2016/679 organ nadzorczy został zobowiązany do przeprowadzenia postępowania wyjaśniającego w zakresie odpowiadającym konkretnej sprawie. Organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga przeprowadzenia dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym poinformowana. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy został zobowiązany do przygotowania i opublikowania elektronicznego formularza skargi. Złożenie skargi w tej formie ma ułatwić osobie, której dane dotyczą, realizację przysługujących jej praw.

Prawo do wniesienia skargi do organu nadzorczego nie wyłącza możliwości dochodzenia swych praw przed sądami, co wyraźnie zostało podkreślone w rozporządzeniu 2016/679. Szczegółowa procedura postępowania przed Prezesem UODO została uregulowana w rozdziale VII ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[149]. Postępowanie prowadzone jest zgodnie ze standardami przewidzianymi w ustawie z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego[150]. Postępowanie prowadzone przed Prezesem UODO ma charakter jednoinstancyjny, co stanowi kluczową zmianę wobec dotychczasowych dwuinstancyjnych postępowań. W ocenie ustawodawcy za wprowadzeniem takiego rozwiązania przemawia konieczność zapewnienia osobie, której dane dotyczą, ostatecznego rozstrzygnięcia, które będzie skuteczne i szybko egzekwowalne[151]. Decyzja wydana przez Prezesa UODO będzie mogła być zgodnie z przepisami kpa zaskarżona do WSA, a następnie zgodnie z zasadą dwuinstancyjności – do NSA.

149 Dz.U. z 2018 r., poz. 1000 ze zm.

150 Tekst jedn. Dz.U. z 2018 r., poz. 2096 ze zm.

151 Sejm Rzeczypospolitej Polskiej VII Kadencja Prezesa Rady Ministrów RM10-49-18, *Uzasadnienie do ustawy o ochronie danych osobowych*, Druk nr 2410, www.sejm.gov.pl [dostęp: 15.05.2018].

4.6. Prawo do sprostowania danych

Prawo do sprostowania danych nie jest nowym uprawnieniem przysługującym osobie, której dane dotyczą, gdyż przewidziane było także w dyrektywie 95/46/WE. Na jego podstawie osoba, której dane dotyczą, może żądać sprostowania nieprawidłowych lub niekompletnych danych. Zgodnie z przyjętymi standardami osoba, której dane dotyczą, ma prawo wiedzieć, kto i w jakim celu przetwarza jej dane osobowe. Na tej podstawie może ocenić poprawność przetwarzanych danych. W przypadku, gdy dane te są błędne lub niekompletne ADO powinien zastosować się do żądań osoby, której dane dotyczą.

Prawodawca unijny nie określił, w jakiej formie osoba, której dane dotyczą, powinna zwrócić się do ADO z prośbą o sprostowanie danych, jednakże w ocenie autora powinna to uczynić w formie pisemnej, by nie doszło do kolejnych pomyłek. Podobnie jak w przypadku realizacji innych praw przysługujących osobie, której dane dotyczą, może nastąpić to poprzez złożenie wniosku. Prawodawca unijny, dążąc do ułatwienia osobie, której dane dotyczą, realizacji przysługujących jej praw, przewiduje również możliwość złożenia wniosku w formie elektronicznej.

Ciężar dowodowy, że dane osobowe są niekompletne lub błędne leży po stronie osoby, której dane dotyczą.

Administrator danych osobowych powinien rozpoznać wniosek niezwłocznie, co oznacza, że w terminie miesiąca od otrzymania żądania powinien poinformować osobę, której dane dotyczą, o czynnościach, jakie podjął w związku z realizacją żądania. W przypadku skomplikowanych spraw ustawodawca unijny wydłużył czas niezbędny ADO do 2 miesięcy, ale po upływie miesiąca ADO powinien poinformować podmiot danych o przyczynach opóźnienia. Jeżeli z określonych powodów ADO w ogóle nie ma zamiaru zrealizować żądania osoby, której dane dotyczą, również w ciągu miesiąca powinien poinformować osobę, której dane dotyczą, o powodach niepodjęcia działania oraz o przysługującym jej prawie do wniesienia skargi do organu nadzorczego (art. 12 ust. 3 i 4 rozporządzenia 2016/679).

Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, ADO w świetle art. 12 ust. 5 rozporządzenia 2016/679 może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo
b) odmówić podjęcia działań w związku z żądaniem.

Przy czym obowiązek wykazania, że żądanie jest nieuzasadnione lub nadmierne spoczywa na ADO.

W przypadku pozytywnego rozpatrzenia wniosku i podjęcia przez ADO decyzji o sprostowaniu danych, ADO powinien poinformować o tym także inne podmioty, którym dane zostały przekazane, chyba że jest to niemożliwe do zrealizowania lub było związane ze znacznymi kosztami finansowymi.

4.7. Prawo do przenoszenia danych osobowych

Do nowych uprawnień osoby, której dane dotyczą, należy także prawo do przenoszenia danych osobowych. Zgodnie z art. 20 rozporządzenia 2016/679 osoba, której dane dotyczą, ma prawo otrzymać do odczytu maszynowego dotyczące jej dane osobowe oraz przesłać je innemu ADO, jeżeli przetwarzanie odbywa się na podstawie jej zgody lub umowy oraz odbywa się w sposób zautomatyzowany. Chociaż przepisy prawa dotyczące przenoszenia danych po raz pierwszy pojawiły się w rozporządzeniu 2016/679, nie ulega wątpliwości, że praktyka ta stosowana była od dawna. Realizacja omawianego uprawnienia jest przejawem kontroli osoby, której dane dotyczą, nad jej danymi osobowymi oraz możliwości wpływania na proces przetwarzania danych. Dzięki niemu osoba, której dane dotyczą, ma możliwość łatwego i szybkiego przenoszenia danych osobowych, natomiast ADO ma obowiązek zapewnienia realizacji tego prawa. Prawo do przenoszenia danych zostało zaprojektowane po to, by umożliwić osobie, której dane dotyczą, ponowne wykorzystanie danych osobowych oraz zapewnić jej kontrolę nad danymi. Podobnie jak prawo do sprostowania danych, realizowane jest przez ADO na podstawie wniosku osoby, której dane dotyczą.

Jak zauważa Grupa Robocza art. 29 ADO odpowiadający na wniosek nie są zobowiązani do sprawdzenia jakości oraz aktualności danych osobowych[152]. Administrator danych osobowych zgodnie z art. 12 ust. 3 rozporządzenia 2016/679 powinien ustosunkować się do złożonego wniosku bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od otrzymania żądania. W przypadkach szczególnie skomplikowanych termin ten można wydłużyć do maksymalnie 3 miesięcy. W celu zapewnienia realizacji prawa do przenoszenia danych, ADO powinien stworzyć wewnętrzną procedurę umożliwiającą szybkie i łatwe przeniesienie danych.

Administrator danych osobowych, decydując się każdorazowo na realizację wniosku powinien zweryfikować tożsamość osoby, której dane dotyczą, zgodnie

152 Grupa Robocza art. 29, Opinia dotycząca prawa do przenoszenia danych przyjęta 13 grudnia 2016 r., WP 242, www.giodo.gov.pl [dostęp: 12.02.2018].

ze standardami przewidzianymi w art. 12 ust. 2 rozporządzenia 2016/679. Prawo do przenoszenia danych zostanie zrealizowane przez ADO, jeżeli podstawą przetwarzania jest zgoda osoby, której dane dotyczą, lub gdy przetwarzanie jest niezbędne do wykonania umowy. W przypadku przetwarzania danych na bazie innej podstawy prawnej, ADO nie może zrealizować prawa do przenoszenia danych osobowych. Dane osobowe powinny zostać przekazane osobie, której dotyczą, lub nowemu ADO w powszechnie używanym formacie nadającym się do odczytu maszynowego. Najlepszym przykładem obrazującym realizację tego prawa w Internecie jest możliwość przeniesienia swojej skrzynki e-mail do nowego dostawcy usług czy konta na portalu społecznościowym[153]. Prawo do przenoszenia danych nie może negatywnie wpływać na realizację innych praw przysługujących osobie, której dane dotyczą. Warto dodać, że jest ono zrealizowane tylko wówczas, gdy przeniesienie danych jest technicznie możliwe. Prawo to, jak wynika z motywu 68 preambuły rozporządzenia 2016/679, nie powinno nakładać na ADO obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania. Dlatego też, jeżeli istnieją jakiekolwiek przeszkody techniczne, prawne lub faktyczne uniemożliwiające przeniesienie danych, wówczas ADO powinien poinformować o tym fakcie osobę, której dane dotyczą. Realizacja tego prawa nie powoduje usunięcia danych z systemów ADO i nie wpływa na okres przechowywania danych przez ADO[154].

4.8. Prawo do ograniczenia przetwarzania danych osobowych

Prawo do ograniczenia przetwarzania danych osobowych jest nowym uprawnieniem przysługującym osobie, której dane dotyczą. Jest to kolejny przepis, potwierdzający realizację przez prawodawcę unijnego dążenia do wzmocnienia praw osób, których dane dotyczą. Zgodnie z art. 4 ust. 3 rozporządzenia 2016/679 ograniczenie przetwarzania danych osobowych faktycznie jest oznaczeniem przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Konsekwencją realizacji tego prawa jest obowiązek zaprzestania przetwarzania danych przez ADO. Osoba, której dane dotyczą, ma prawo ograniczenia przetwarzania danych w sytuacji, w której:

a) kwestionuje ona prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

153 Ibidem, s. 8.

154 Ibidem.

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 rozporządzenia 2016/679 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Po zrealizowaniu żądania osoby, której dane dotyczą, ADO może przetwarzać dane wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego UE lub państwa członkowskiego. Prawodawca unijny zaproponował przykładowe metody ograniczające przetwarzanie danych, wymieniając m.in.: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej (motyw 67 preambuły rozporządzenia 2016/679).

4.9. Prawo do wniesienia sprzeciwu

Prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych jest kolejnym uprawnieniem potwierdzającym wzmocnienie praw podmiotowych osób, których dane dotyczą. Administrator danych osobowych na etapie zbierania danych powinien poinformować osobę, której dane dotyczą, o przysługujących jej prawach, w tym prawie do złożenia sprzeciwu. Prawo to może zostać zrealizowane przez osobę, której dane dotyczą, w dwóch okolicznościach: z przyczyn związanych ze szczególną sytuacją podmiotu danych wobec przetwarzania dotyczących jej danych osobowych (w tym profilowanie) w interesie publicznym, bądź w ramach prawnie uzasadnionego interesu ADO oraz wobec przetwarzania danych na potrzeby marketingu bezpośredniego.

Mariusz Krzysztofek zwraca uwagę, że prawo do wniesienia sprzeciwu wobec przetwarzania danych ze względu na szczególną sytuację podmiotu danych nie ma charakteru bezwzględnego[155]. Podmiot danych powinien za każdym razem

[155] M. Krzysztofek, *Prawo do sprzeciwu wobec przetwarzania danych osobowych*, w: *Realizacja praw osób,*

uzasadnić wniesione żądanie. Dopiero po dokładnym przeanalizowaniu wszystkich okoliczności, ADO powinien podjąć stosowną decyzję. Jeżeli ADO uzna, iż nie zachodzą okoliczności uzasadniające realizację prawa osoby, której dane dotyczą, wówczas może odrzucić złożony sprzeciw.

W przypadku przetwarzania danych w cyberprzestrzeni znacznie częściej osoba, której dane dotyczą, będzie mogła powoływać się na drugą z wymienionych wyżej przesłanek, tzn. osoba, której dane dotyczą, wyraża sprzeciw wobec przetwarzania jej danych na potrzeby marketingu bezpośredniego, w tym również profilowania. W tym jednak przypadku decyzja osoby, której dane dotyczą, nie wymaga uzasadnienia[156]. W zależności od tego, czego dotyczy sprzeciw ADO, podobnie jak w przypadku prawa do bycia zapomnianym, powinien dysponować procedurą wewnętrzną zapewniającą realizację omawianego prawa[157]. Jeżeli więc podmiot danych wyraża sprzeciw na marketing bezpośrednio realizowany przez ADO za pośrednictwem wszystkich kanałów komunikacji, ADO powinien zrealizować prawo osoby, której dane dotyczą. Możliwe jest jednak, że osoba, której dane dotyczą, wyraża sprzeciw na przetwarzanie danych przekazywanych wyłącznie jednym określonym kanałem komunikacji.

4.10. Prawo do odszkodowania

Na gruncie prawa polskiego od dawna oczekiwano zmiany przepisów w zakresie możliwości dochodzenia roszczeń finansowych za szkodę spowodowaną naruszeniem przepisów ochrony danych osobowych. Nie oznacza to, że osoba, której dane dotyczą, była całkowicie pozbawiona możliwości dochodzenia roszczeń. Podstawą wówczas były art. 23 i 24 kc, na podstawie których dane osobowe były traktowane jako dobra osobiste. Dopiero wejście w życie rozporządzenia 2016/679 przyznało wprost osobie, której dane dotyczą, prawo do odszkodowania. Administrator danych osobowych może zostać pociągnięty do odpowiedzialności na podstawie art. 82 rozporządzenia 2016/679, jeżeli osoba, której dane dotyczą, poniesie szkodę majątkową lub niemajątkową wskutek przetwarzania jej danych osobowych. Podstawą odpowiedzialności ADO jest nie tylko naruszenie przepisów rozporządzenia 2016/679, ale także, zgodnie z motywem 146 preambuły rozporządzenia 2016/679, przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy

których dane dotyczą na podstawie rodo, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 292.

156 Ibidem, s. 295.

157 Grupa Robocza art. 29, Wytyczne z 2 października 2017 r. dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, WP 251.

niniejszego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące to rozporządzenie.

Administrator danych osobowych może zostać zwolniony z obowiązku naprawienia szkody, jeżeli wykaże, że nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody (art. 82 ust. 3 rozporządzenia 2016/679). Chociaż przepisy rozporządzenia 2016/679 nie definiują pojęcia szkody, wskazuje się, że pojęcie to powinno być definiowane szeroko, w świetle orzeczeń TSUE. Ciężar odpowiedzialności w tym zakresie leży po stronie ADO, który będzie musiał wykazać, iż nie ponosi winy za zaistniałą sytuację. Jeżeli w proces przetwarzania danych było zaangażowanych kilku ADO, zgodnie z art. 82 ust. 4 rozporządzenia 2016/679 podmioty te odpowiadają za szkodę solidarnie. W przypadku, gdy jeden z ADO zapłaci odszkodowanie osobie, której dane dotyczą, może wystąpić do pozostałych ADO z roszczeniem regresowym.

Wysokość kar – do 20 000 000 euro lub 4% całkowitego rocznego światowego obrotu ADO z poprzedniego roku obrotowego – podkreśla wagę, jaką prawodawca unijny przykłada do zgodnego z prawem przetwarzania danych. Kary te mają z jednej strony odstraszać przed niewłaściwymi praktykami stosowanymi przez ADO, z drugiej zaś zapewnić osobie, której dane dotyczą, zadośćuczynienie za poniesioną szkodę.

4.11. Prawo do prywatności w cyberprzestrzeni

W ocenie autora wszystkie wymienione w rozporządzeniu 2016/679 uprawnienia przysługujące osobie, której dane dotyczą, są bardzo ważne. Ich realizacja nigdy nie będzie skuteczna, jeżeli podmiotowi danych nie zapewni się podstawowego prawa wynikającego z norm prawa międzynarodowego – prawa do prywatności. Nie ulega wątpliwości, że zapewnienie jego realizacji w cyberprzestrzeni jest trudne. Jest jednak konieczne dla możliwości zapewnienia pozostałych praw wynikających z rozporządzenia 2016/679.

Celem pracy jest wykazanie, iż prawa osób, których dane dotyczą, nie są przestrzegane w taki sam sposób w świecie realnym i wirtualnym. Mimo że obie przestrzenie funkcjonują równolegle i państwa starają się wypracować mechanizmy gwarantujące jednostce korzystanie z przysługujących jej praw, w praktyce okazuje się, iż poziom ochrony w Internecie jest na znacznie niższym poziomie. Chociaż przepisy prawa teoretycznie umożliwiają jednostce realizację prawa do decydowania o tym, komu oraz w jakim zakresie przekazujemy informacje na swój temat, w praktyce okazuje się, iż korzystanie z autonomii informacyjnej

w Internecie nabiera zupełnie innego wymiaru i bardzo szybko tracimy kontrolę nad ujawnianymi danymi. Dlatego w ocenie autora realizacja prawa do prywatności w Internecie jest znacznie trudniejsza niż w rzeczywistości. Dzieje się tak nie tylko dlatego, że w wirtualnym świecie chętniej dzielimy się informacjami na swój temat, ale także dlatego, że wirtualny świat daje znacznie lepsze mechanizmy pozwalające na ingerencję w prywatność jednostki – często bez jej wiedzy. W związku z tym tak ważne jest zapewnienie jednostce możliwości korzystania z przysługujących jej praw w cyberprzestrzeni, gdzie znacznie częściej narażona jest na ich utratę.

4.11.1. Geneza prawa do prywatności

Wśród przedstawicieli doktryny nie ma konsensusu określającego początek kształtowania się prawa do prywatności. Niektórzy z nich odwołują się do czasów biblijnych, inni uważają, że prawo to zaczęło kształtować się znacznie później wraz z rozwojem myśli Thomasa Hobbesa, Charlesa de Montesquieu (Monteskiusza) czy Jean-Jacquesa Rousseau[158]. Natomiast Efstratios Stylianidis i Karl Popper głosili, że początki walki w obronie jednostki rozpoczęły się w antycznej Helladzie[159]. Już wtedy sądzono, iż człowiekowi przysługują te same prawa przyrodzone, których nikt nie może go pozbawić. Oczywiście należy zaznaczyć, że w tamtym czasie walka o prawo do prywatności nie mogła dotyczyć wszystkich klas społecznych[160]. Niezależnie od przyjętych koncepcji, nie ulega wątpliwości, że kluczowym dla rozwoju prawa do prywatności był wiek XIX, a dokładniej data 15 grudnia 1890 r., kiedy Samuel D. Warren i Louis D. Brandeis opublikowali w „Harvard Law Review" artykuł *Right to privacy*. Autorzy w swoich rozważaniach dotyczących kształtu prawa do prywatności podnosili, że powód powinien mieć możliwość dochodzenia naprawienia szkody w przypadku, gdy szkoda została wyrządzona na jego uczuciach, godności lub honorze[161]. W konsekwencji, po 15 latach od chwili ukazania się publikacji, zapadł pierwszy wyrok, w którym SN w Georgii wskazał wyraźnie naruszenie prawa do prywatności[162].

Omawiana problematyka zyskała na znaczeniu wraz z rozwojem techniki. Pojawienie się nowych metod komunikacji w tym telefonów, komputerów, rozwoju prasy przyczyniło się do wzrostu zainteresowania informacjami na temat poszczególnych jednostek. Poza postępującymi przemianami społecznymi i gospodarczymi

158 Za: J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych*, Wrocław 2014, s.153.

159 Za: T. Jurczyk, *Geneza rozwoju Praw Człowieka*, Wrocław 2009, s. 29.

160 Ibidem, s. 43.

161 Ibidem, s. 27.

162 J. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Kraków 2006, s. 28–29.

wpływ na zainteresowanie prawami człowieka, a co za tym idzie również prawem do prywatności, miały obie wojny światowe XX wieku. Szczególnie jednak tragiczna w skutkach druga wojna światowa wywarła duży wpływ na potrzeby zapewnienia ram prawnych gwarantujących jednostce poszanowanie przysługujących jej praw.

4.11.2. Rozwój prawa do prywatności po drugiej wojnie światowej

Prawo do prywatności chociaż znane od starożytności zyskało na znaczeniu po zakończeniu drugiej wojnie światowej w 1945 r. Wówczas uznano, że poza kwestiami gospodarczymi i politycznymi niezbędne jest odbudowanie podstawowych mechanizmów ochrony praw człowieka, w tym również prawa do prywatności. Po raz pierwszy zaczęto dyskutować nad powołaniem podmiotu, który byłby odpowiedzialny za zapewnienie międzynarodowego pokoju i bezpieczeństwa. Skutki wojny uświadomiły społeczności międzynarodowej, że zapewnienie pokoju i bezpieczeństwa jest możliwe tytko wówczas, gdy w dążenie do jego utrzymania zaangażują się wszyscy członkowie takiej organizacji. Kluczową dla realizacji założonego celu okazała się powołana na podstawie Karty Narodów Zjednoczonych – Organizacja Narodów Zjednoczonych[163]. Już w preambule podpisanego w 1946 r. dokumentu zwraca się uwagę, że państwa członkowskie za priorytet stawiają sobie „przywrócić wiarę w podstawowe prawa człowieka, godność i wartość jednostki, równość praw mężczyzn i kobiet oraz narodów wielkich i małych, stworzyć warunki umożliwiające utrzymanie sprawiedliwości i poszanowanie zobowiązań wynikających z umów międzynarodowych i innych źródeł prawa międzynarodowego, popierać postęp społeczny i poprawę warunków życia w większej wolności"[164]. Wraz z upływem czasu okazało się jednak, że działania państw w tym obszarze nie spełniają oczekiwanych skutków. Dlatego zdecydowano się na wyodrębnienie tego zagadnienia spośród licznych problemów poruszanych na forum ONZ i utworzenie niezależnego organu skupiającego się wyłącznie na problematyce praw człowieka. W 1948 r. podczas trzeciej sesji Zgromadzenia Ogólnego ONZ została uchwalona Powszechna Deklaracja Praw Człowieka, która w całości odnosi się do gwarancji zapewnienia jednostce poszanowania przysługujących jej praw[165]. Warto zwrócić uwagę na rangę dokumentu, który będąc rezolucją Zgromadzenia Ogólnego, stał się wyrazem woli i potrzeby podjęcia problematyki praw człowieka

163 Karta Narodów Zjednoczonych została podpisana 26 czerwca 1945 r., a weszła w życie 24 października 1945 r.

164 Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz.U. z 1947 r. nr 23, poz. 90.

165 Powszechna Deklaracja Praw Człowieka uchwalona podczas trzeciej sesji Zgromadzenia Ogólnego ONZ z 10 grudnia 1948 r., www.usesco.pl [dostęp: 05.09.2018].

na forum międzynarodowym. W art. 12 Powszechnej Deklaracji Praw Człowieka podkreślono, że „nikt nie będzie poddany arbitralnemu wkraczaniu w jego życie prywatne, rodzinę, mieszkanie lub korespondencję, ani też zamachom na jego honor i reputację". Minusem dokumentu jest to, iż nie ma on mocy powszechnie obowiązującej. Stał się jednak inspiracją do podjęcia dalszych prac nad prawnym uregulowaniem kwestii prywatności, których wynikiem było przyjęcie 19 grudnia 1966 r. Międzynarodowego Paktu Praw Obywatelskich i Politycznych[166]. Prawo do prywatności znalazło odzwierciedlenie w art. 17 dokumentu wskazującego, że „nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom, czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię". Dążenie do zapewnienia jednostce prawa do prywatności podejmowane było wielokrotnie przez społeczność międzynarodową, co podkreśla rangę i znaczenie tego prawa.

Istotnym dokumentem, który wywarł wpływ na rozwój praw jednostki w Europie była Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności zawarta 4 listopada 1950 r. w Rzymie przez państwa członkowskie Rady Europy, zwana Europejską Konwencją Praw Człowieka. Dokument, po uzyskaniu niezbędnych dziesięciu ratyfikacji, wszedł w życie 3 września 1953 r. Szczególnie istotny pod kątem analizowanej problematyki jest art. 8 EKPC stanowiący, że „każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji". Ponadto, zgodnie z cytowanym artykułem niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne oraz dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Na gruncie prawa europejskiego nie sposób nie wspomnieć o Karcie praw podstawowych Unii Europejskiej, gdzie w art. 7 wskazano, iż każdy ma prawo do poszanowania życia prywatnego rodzinnego, domu i komunikowania się[167].

4.11.3. Rozwój prawa do prywatności w Polsce

Rozwój prawa do prywatności w Polsce jest ściśle powiązany z nurtem europejskim, chociaż nie ulega wątpliwości, iż Polska posiada znacznie krótsze doświadczenie w tym zakresie. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.

166 Międzynarodowy Pakt Praw Obywatelskich i Politycznych podpisany 19 grudnia 1966 r. w Nowym Jorku, Dz. U. z 1977 r. nr 38, poz. 167.

167 Karta praw podstawowych Unii Europejskiej z 30 marca 2010 r., C83/389, www.bip.ms.gov.pl [dostęp: 03.05.2018].

wprost normuje prawo do prywatności w art. 47, gdzie zostało podkreślone, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym[168]. W przepisie tym prawo do prywatności zostało wyodrębnione oraz uznane za równie istotne jak prawo do życia rodzinnego oraz czci. Zostało zaliczone do kategorii wolności i praw osobistych zawartych w rozdziale I i II Konstytucji RP. Znalazło także odzwierciedlenie w art. 51 Konstytucji RP oraz wielu innych przepisach ustawy zasadniczej. Umiejscowienie prawa do prywatności w Konstytucji RP, a także potwierdzenie jego fundamentalnego znaczenia dla rozwoju praw podstawowych należy uznać za dojrzałość ustawodawcy krajowego dostrzegającego wagę oraz rangę tego prawa.

Rozwinięcie ogólnych zasad odnoszących się do prawa do prywatności znajduje rozwinięcie w licznych aktach rangi ustawy, w tym zarówno w kc, jak i uodo. Artykuł 23 kc odnosi się do ochrony dóbr osobistych osoby fizycznej. W przepisie został wymieniony przykładowy katalog dóbr osobistych. Prawo do prywatności należy uznać za prawo do dóbr osobistych określonych w cytowanym artykule. Jak podkreśla zaś Paweł Sobczyk za Markiem Safjanem, prawo do ochrony danych osobowych jest pochodną prawa do prywatności[169]. Prawo do ochrony danych osobowych gwarantuje jednostce możliwość decydowania o tym, komu oraz w jakim celu dane osobowe są przetwarzane. Ustawodawca przyznał jednostce daleko idącą ochronę prawną poprzez możliwość żądania zaprzestania przetwarzania jej danych osobowych, usuwania, poprawiania czy nawet żądania odszkodowania w przypadku naruszenia przysługujących jej praw. Każdy podmiot przetwarzający dane osobowe zobowiązany jest do spełnienia obowiązku informacyjnego po to, by zapewnić jednostce kontrolę nad procesem przetwarzania jej danych osobowych. Prawo do prywatności pozwala więc jednostce decydować o swoich danych osobowych. Nie ma jednak charakteru bezwzględnego, o czym świadczy art. 51 ust. 1 Konstytucji RP.

Warto zauważyć, że relacje zachodzące pomiędzy prawem do prywatności a ochroną danych osobowych nie są jednoznaczne. Świadczy o tym nie tylko stanowisko prezentowane w orzecznictwie, ale również wśród przedstawicieli doktryny. W ocenie SN imię i nazwisko uznawane są za dobra powszechne. Zatem „udostępnienie imion i nazwisk autorów opinii nie naruszy prywatności tychże osób ze względu na powszechne przyzwolenie na posługiwanie się tymi danymi i uznanie ich za tzw. dane powszechne, których ujawnienie nie spowoduje zagrożenia dla dóbr

168 Konstytucja RP z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r. nr 78, poz. 483, www.prawo.sejm.gov.pl [dostęp: 06.08.2018].

169 P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze UKSW" 2009, nr 1, s. 299.

osobistych osób, których te dane dotyczą, powołując się w swym stanowisku"[170]. Odmienne stanowisko prezentuje NSA, który uznał, że „dane osobowe takie jak imię, nazwisko, wiek, wykonywany zawód stanowią sferę prywatności, o jakiej mowa w art. 5 ust. 2 ustawy o ochronie danych osobowych"[171].

Nie ulega wątpliwości, że istnieje silny związek pomiędzy prawem do prywatności oraz prawem do ochrony danych osobowych. W ocenie autora należy uznać, że nie każda dana osobowa będzie podlegać ochronie prawa do prywatności, czego przykładem jest chociażby imię i nazwisko. Jednakże wielokrotne naruszenie danych osobowych będzie pociągało za sobą równoczesne naruszenie prawa do prywatności.

4.11.4. Definicja prawa do prywatności

Na gruncie prawa funkcjonuje wiele definicji prawa do prywatności. Dotychczas nie udało się wypracować jednej wspólnej formuły. Wśród polskich przedstawicieli doktryny podejmujących problematykę ochrony prawa do prywatności możemy wyróżnić Andrzeja Kopffa, który wskazuje, iż dobrem osobistym w postaci życia prywatnego jest uzasadnione odosobnienie się jednostki od ogółu, przyczyniające się do jej rozwoju fizycznego lub psychicznego osobowości oraz zachowania osiągniętej pozycji społecznej[172]. W ocenie autora życie prywatne podlega podziałowi na strefę intymnego życia osobistego oraz strefę prywatnego życia osobistego. Różnicujemy je poprzez krąg podmiotów mających dostęp do poszczególnych stref życia prywatnego[173]. Natomiast Joanna Braciak podkreśla, że prywatność jest ściśle związana z pojęciem interesu własnego jednostki oraz aktywnością podejmowaną przez jednostkę na rzecz ochrony tego dobra w przeciwieństwie do aktywności podejmowanej dla dobra wszystkich[174]. Niezależnie od tego, jaką definicję przyjmiemy za właściwą, ich wspólnym mianownikiem jest prawo jednostki do decydowania o sobie bez ingerencji podmiotów zewnętrznych. Prawo to gwarantuje jednostce również możliwość decydowania, komu oraz w jakim zakresie zostaną udostępnione informacje.

Z uwagi na fakt, że stworzenie jednej spójnej definicji prawa do prywatności należy uznać za bezcelowe – ze względu na szybko zmieniające się warunki, w jakich może dojść do naruszenia prawa – należy uznać, iż znacznie korzystniejszym

170 Wyrok SN z 19 listopada 2003 r., I PK 590/02.

171 Wyrok NSA z 13 stycznia 2011 r., I OSK 440/10.

172 A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego*, Studia Cywilistyczne t. XX, Kraków 1972, s. 72.

173 Ibidem.

174 J. Braciak, *Prawo do prywatności*, Warszawa 2004, s. 130.

rozwiązaniem jest określenie stref podlegających ochronie. Podejście to jest szczególnie widoczne w dokumentach i orzecznictwie międzynarodowym. Powszechnie wskazuje się, że prawo do prywatności dotyczy prawa do odosobnienia, poszanowania korespondencji, życia rodzinnego jednostki oraz do przemieszczania się.

Nie każde naruszenie danych osobowych będzie pociągało za sobą naruszenie prywatności. Prawodawca unijny w przepisach rozporządzenia 2016/679, chcąc zapewnić jednostce możliwie szeroką ochronę, nie posługuje się pojęciem prawa do prywatności, ale szerszym stwierdzeniem zapewnienia ochrony interesów i praw podstawowych jednostki. Prawo do prywatności jak najbardziej mieści się w tych standardach. Gwarantowana ochrona powinna być na tyle szeroka, by zapewniała jednostce bezpieczeństwo, z drugiej zaś strony powinna umożliwić jej realizację innych przysługujących jej praw, w tym autonomii informacyjnej. W związku z tym, z jednej strony poszerzony został katalog praw przysługujących osobie, której dane dotyczą, z drugiej zaś nałożono na ADO nowe obowiązki zapewniające większą transparentność procesu przetwarzania danych. Jak zauważa Bogusław Banaszak „zapewnienie jednostce prywatności najlepiej służyłoby zagwarantowaniu jednostce prawa do samookreślenia informacyjnego, czyli pozostawienia do jej wyłącznej decyzji sprecyzowania tego, kto, o czym, kiedy i w jaki sposób może się o niej dowiedzieć”[175].

Problem związany zapewnieniem jednostce prawa do prywatności w wirtualnym świecie dostrzegany jest od dawna. Nie tylko w rozporządzeniu 2016/679, ale także w proponowanym rozporządzeniu w sprawie prywatności i łączności elektronicznej dostrzega się potrzebę zapewnienia właściwego poziomu ochrony podmiotom danych. Tymczasem nie ulega wątpliwości, że nowe rozwiązania technologiczne umożliwiają ingerowanie w prywatność jednostki. Dotyczy to nie tylko sytuacji, w których zbierane są dane osobowe, ale także inne okoliczności podawania informacji bezpośrednio lub pośrednio ingerujących w prywatność jednostki. Najlepszym tego przykładem jest reklama behawioralna, która opiera się na obserwacji zachowania osób fizycznych przez określony czas. Dąży się przez to do zbadania charakterystyki zachowania poprzez analizę działań użytkowników w celu opracowania specjalnego profilu, a co za tym idzie zapewnienia osobom, których dane dotyczą, reklam dopasowanych do ich zainteresowań[176]. Dzieje się tak najczęściej za pomocą umieszczania plików cookies w urządzeniu końcowym użytkownika. Pliki te umożliwiają stworzenie profilu użytkownika, na podstawie

175 B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012, s. 296.

176 Grupa Robocza art. 29, Opinia 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta 22 czerwca 2010 r., WP 171, www.giodo.gov.pl [dostęp: 12.01.2019].

którego wyświetlana jest spersonalizowana reklama. Przy tej okazji najczęściej pobierane są także adresy IP użytkowników czy informacje dotyczące częstotliwości odwiedzanych stron lub inne zachowania użytkownika. Bardzo często wykorzystywanie reklamy behawioralnej będzie się wiązało z przetwarzaniem danych osobowych. Osoba, której dane dotyczą, najczęściej nie jest świadoma stosowanych technik.

Do naruszenia prawa do prywatności może dochodzić także podczas profilowania. Poprzez profilowanie dochodzi do ograniczenia wyborów użytkownika Internetu. Niejednokrotnie profilowanie może powodować dyskryminację jednostki. W opinii Grupy Roboczej art. 29 może prowadzić nawet do segregacji społecznej, podważając wolność wyboru[177]. Konsekwencją profilowania jest ograniczenie możliwości wyboru przez podmiot danych prawa do swobodnego podejmowania decyzji. Mając świadomość zagrożeń związanych z tym procesem, przepisy rozporządzenia 2016/679 dają osobie, której dane dotyczą, prawo decydowania, czy chce podlegać temu procesowi czy też nie, wyrażając w tym zakresie zgodę na podleganie profilowaniu.

W opinii autora rozwój nowoczesnej technologii spowodował zmianę pojęcia prywatności. Szczególnie widoczne jest to na portalach społecznościowych, gdzie dzielimy się z innymi użytkownikami znacznie szerszym zakresem informacji, niż miałoby to miejsce w rzeczywistości. Jak zostało zauważone cyberprzestrzeń zapewnia nam złudne przekonanie, że jesteśmy anonimowi, „nienamierzalni". Powszechnie zgadzamy się na formy ingerencji w naszą prywatność lub posługiwanie się naszymi danymi bez naszej wiedzy. Dobrze ilustruje to przykład przekazywania danych osobowych na różnego rodzaju formularzach. W przypadku wersji papierowej większość z nas zastanawia się, jakie dane udostępnia, komu oraz w jakim celu. Jeżeli odbywa się to na targach, w ramach konkursu, częstą praktyką jest dopytywanie o sposób zabezpieczenia danych czy długość ich przechowywania. Tymczasem w przypadku przekazywania danych osobowych za pośrednictwem formularzy elektronicznych nie zastanawiamy się nawet, czy strona, na którą weszliśmy nie została zhakowana, nie mówiąc już o zastanowieniu się, w jakim celu i przez kogo dane zostaną wykorzystane. Redefinicja prawa do prywatności polega więc na przesunięciu granicy informacji, jakie pozostają dla nas do wyłącznej wiadomości. Informacje na temat naszych przyzwyczajeń, odwiedzanych miejsc, ulubionych utworów muzycznych nie są zarezerwowane dla nas oraz naszych najbliższych. Granica ta przesuwa się także w zakresie danych szczególnie chronionych, w tym

177 Grupa Robocza art. 29, Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, WP 251, s. 6.

danych dotyczących stanu zdrowia. Co dziwniejsze w większości analizowanych przypadków osoba, której dane dotyczą, godzi się lub daje przyzwolenie na przesunięcie granicy. Można się zastanawiać, czy działanie to jest w pełni świadome oraz czy osoba ta jest w stanie przewidzieć konsekwencje swojego postępowania. Niemniej jednak w ocenie autora znacznie poważniejszym problemem jest wykorzystywanie nowoczesnych rozwiązań technologicznych w celu pozyskania informacji o jednostce bez jej wiedzy lub przy okazji jakiegoś procesu.

Najlepszym tego przykładem jest zagadnienie dużych zbiorów danych, czyli big data, za sprawą których możliwe jest tworzenie zupełnie nowych zestawów danych, przetwarzanie wizerunku przy wykorzystaniu monitoringu, powszechnie dostępnych jawnych rejestrów czy geolokalizacji. Za ich pośrednictwem następuje ingerencja w prywatność osoby fizycznej. Tymczasem, wciąż pojawiają się nowe rozwiązania technologiczne, które pozwalają na jeszcze szerszą ingerencję w życie prywatne jednostki. Przykład stanowią chociażby spammingi, czyli niezamówione informacje handlowe, na które użytkownik nie wyrażał zgody. Dopóki nie zostaną wypracowane mechanizmy prawne gwarantujące odpowiedni poziom ochrony powinniśmy liczyć się z tym, iż funkcjonowanie w cyberprzestrzeni, w znacznie szerszym zakresie niż ma to miejsce w świecie realnym, naraża nas na naruszenie lub utratę prywatności.

Realnym zagrożeniem dla prywatności osób fizycznych są także inteligentne urządzenia przenośne, takie jak telefony komórkowe. Funkcja tych urządzeń nie sprowadza się wyłącznie do prowadzenia rozmów telefonicznych, ale także wysyłania wiadomości e-mail, zarządzania zindywidualizowanymi aplikacjami, przechowywania zdjęć, łączenia się z wirtualnym światem. W ocenie Grupy Roboczej art. 29 za pośrednictwem tego typu urządzeń również możliwe jest stałe monitorowanie użytkownika[178]. Problem gromadzenia i przetwarzania danych bez wiedzy użytkowników został podjęty w związku z unijną reformą przepisów dotyczących ochrony danych osobowych oraz prac nad rozporządzeniem w sprawie prywatności i łączności elektronicznej. Pragnąc zalegalizować ten proces zdecydowano się zaostrzyć przepisy nakładające na ADO obowiązek zalegalizowania stosowanych praktyk oraz zapewnienia ich przejrzystości. W związku z tym wykorzystanie danych zgromadzonych bez wiedzy użytkownika możliwe jest wyłącznie za zgodą osoby, której dotyczą dane osobowe. Administratorzy danych osobowych przetwarzający dane osobowe w cyberprzestrzeni mają do dyspozycji wiele metod pozyskiwania zgód. Obecnie obowiązujące przepisy prawa wymagają, by operatorzy pozyskiwali

178 Grupa Robocza art. 29, Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych przyjęta 16 maja 2011 r., WP 185, www.giodo.gov.pl [dostęp: 12.09.2017].

zgody także na gromadzenie danych zebranych za pośrednictwem plików cookies[179]. Informacje o wykorzystywaniu plików cookies powinny pojawiać się bezpośrednio po wejściu na stronę internetową wraz z informacją, że korzystając ze strony użytkownik zgadza się na zapisywanie plików cookies przez stronę czy na śledzenie za pośrednictwem tych właśnie plików. Użytkownik powinien mieć także możliwość zmiany decyzji lub odwołania udzielonej zgody. Za pośrednictwem plików cookies możliwe jest nie tylko śledzenie użytkownika, ale także tworzenie profili. Niedopuszczalne są także praktyki polegające na odmowie dostępu do określonej strony lub usługi użytkownikowi, który nie wyraził zgody na ich śledzenie (cookie walls)[180]. Wraz z wejściem w życie rozporządzenia 2016/679 dokonano istotnych zmian w zakresie ustawień chroniących prywatność. Dostawcy usług powinni zagwarantować użytkownikom ustawienia domyślnie chroniące ich prywatność.

W przepisach rozporządzenia 2016/679 zostały zawarte przepisy wskazujące, że praktyki zbierania i gromadzenia informacji o jednostce powinny odbywać się na podstawie jasnej, konkretnej i świadomej zgody podmiotu danych. Administrator danych osobowych powinien poinformować go na przykład o stosowaniu plików cookies oraz o konsekwencjach z tym związanych. Realizacja praw wynikających z rozporządzenia 2016/679 powinna zapewniać użytkownikowi możliwość wycofania się z chęci otrzymywania spersonalizowanych reklam.

Dodatkowo ADO powinien zrealizować wobec osoby, której dane dotyczą, obowiązek informacyjny, wskazując, w jakim celu przetwarzane są jego dane osobowe, kto jest ADO i jak długo dane te będą przechowywane. Użytkownik powinien zostać poinformowany o przysługujących mu prawach. Administrator danych osobowych powinien także zadbać, by stosowane przez niego środki techniczne i organizacyjne były adekwatne do możliwego do wystąpienia zagrożenia.

4.11.5. Ograniczenia prawa do prywatności

Prawo do prywatności nie ma charakteru absolutnego, co oznacza, że podlega ograniczeniom wynikającym zarówno z przepisów krajowych, jak i międzynarodowych. Przesłanki ograniczające prawo do prywatności określone zostały chociażby w art. 8 ust. 2 EKPC czy art. 31 ust. 1 Konstytucji RP.

Ograniczenie korzystania z wolności i praw wynikających z Konstytucji RP możliwe jest wyłącznie wtedy, gdy jest to konieczne w demokratycznym państwie

179 Grupa Robocza art. 29, Wytyczne z 2 października 2013 r. w sprawie pozyskiwania zgody na zapisywanie plików cookies , WP 208, www.giodo.gov.pl [dostęp: 11.09.2018].

180 Grupa Robocza art. 29, Opinia 01/2017 na temat rozporządzenia w sprawie prywatności i łączności elektronicznej (2002/58/WE) przyjęta 4 kwietnia 2017 r., WP 247, www.giodo.gov.pl, s. 19 [dostęp: 13.02.2018].

prawa dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Podobne przesłanki umożliwiające ograniczenie prawa do prywatności wynikają z przepisów międzynarodowych. Jak chociażby art. 8 ust. 2 EKPC, gdzie do podstaw ograniczenia zalicza się interes bezpieczeństwa państwowego, publicznego i dobrobytu gospodarczego kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób.

Ograniczeniu podlega także prawo do ochrony danych osobowych na podstawie art. 51 ust. 2 Konstytucji RP. Ograniczenie wynika także z przepisów regulujących problematykę ochrony danych osobowych. Jak zauważył Trybunał Konstytucyjny ważne jest by ograniczenia były formułowane w sposób zgodny z obowiązującymi przepisami prawa. Oznacza to, że „ograniczenie prawa, bądź wolności może nastąpić tylko jeżeli przemawia za tym inna norma, zasada lub wartość konstytucyjna, a stopień tego ograniczenia musi pozostawać w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to ma służyć”[181].

Chęć zdobycia informacji stała się nieodłącznym elementem naszego życia. Nasze poszukiwania nie ograniczają się wyłącznie do informacji o nas i naszych najbliższych. Każdego dnia przetwarzamy bliżej nieokreśloną ilość informacji. Ograniczenie prawa do prywatności powinno stanowić wyjątek od ogólnej zasady prawa do poszanowania prywatności osoby fizycznej i być stosowane wyłącznie w wąskim zakresie, jasno określonym w przepisach prawa. Niebezpiecznym zabiegiem, z którym mamy do czynienia w ostatnim czasie coraz częściej, są nieuzasadnione przypadki ograniczania prawa do prywatności. Należy pamiętać, że prawo do prywatności jest jednym z przejawów demokratycznego państwa prawa i wszelkie próby ograniczania tego prawa są zabiegiem niebezpiecznym i mającym w dłuższej perspektywie daleko idące skutki. Zanim więc organy władzy państwowej zdecydują się na podjęcie takich kroków, powinny zastanowić się, czy nie istnieją inne metody mniej ingerujące w prywatność jednostki.

181 Wyrok TK z 19 maja 1998 r., U 5/97.

Rozdział 5

Bezpieczeństwo danych osobowych w cyberprzestrzeni

5.1. Zagrożenia związane z przetwarzaniem danych osobowych w cyberprzestrzeni

Zwiększona aktywność użytkowników w sieci oraz brak mechanizmów prawnych gwarantujących im bezpieczeństwo doprowadziły do powstania nowych, nieznanych dotąd przestępstw. Jak zostało zauważone w poprzednich rozdziałach, cyberprzestrzeń w znaczący sposób różni się od przestrzeni rzeczywistej. Złudne poczucie anonimowości, powszechny dostęp do informacji, brak granic czasowych czy terytorialnych to tylko nieliczne elementy zachęcające do aktywności w przestrzeni wirtualnej. Bardzo szybko okazało się, że obowiązujące dotąd normy prawne nie zawsze mają zastosowanie w cyberprzestrzeni. Nowatorski charakter cyberzagrożeń wynikał przede wszystkich ze specyfiki środowiska, w jakim się rozwijały. Zagrożenia w cyberprzestrzeni charakteryzują się przede wszystkim szerokim zasięgiem oraz szybkością działania sprawców, jak również trudnością w ich zidentyfikowaniu. W związku z tym należy uznać, że występowanie nowych zagrożeń wpływa nie tylko na proces przetwarzania danych osobowych, ale w ogóle na funkcjonowanie jednostek w wirtualnym świecie. Autor, zastanawiając się, w jaki sposób zapewnić bezpieczeństwo danych osobowych w cyberprzestrzeni ma na myśli zapewnienie bezpiecznego procesu przetwarzania danych z uwzględnieniem i poszanowaniem praw osób, których dane dotyczą.

Każdego dnia słyszymy o nowych atakach nakierowanych na pozyskanie danych osobowych. Co ciekawe w przeważającej większości przestępcy nakierowani są na uzyskanie w zamian za skradzione dane okupu, niż w rzeczywistości ich

wykorzystanie. Dlatego najczęstszymi ofiarami takich ataków są szpitale, przetwarzające dane osobowe szczególnej kategorii, banki czy firmy motoryzacyjne. Ataki hakerskie nie są zjawiskiem nowym, pierwsze pojawiły się już w czasie zimnej wojny, chociaż niewątpliwy ich rozwój miał miejsce na przełomie XX i XXI wieku[182]. Przełomowy w tym zakresie okazał się 2007 r., kiedy to hakerzy zaatakowali na dużą skalę administrację w Estonii. Wówczas hakerom udało się na kilka dni sparaliżować działanie całego państwa.

Od tego czasu, chociaż wiemy znacznie więcej o atakach w cyberprzestrzeni zagrożenie to jest tak samo realne. Od wielu lat bezpieczeństwo w cyberprzestrzeni budzi zainteresowanie zarówno polityków, jak i przedstawicieli nauki. W ostatnim czasie problematyka ta stała się kluczowym zagadnieniem w UE. Niemniej jednak analizując statystyki pokazujące liczbę skutecznie przeprowadzonych ataków hakerskich oraz sposób działania ich sprawców należy zastanowić się, czy, a jeżeli tak, to w jaki sposób zapewnić bezpieczeństwo w cyberprzestrzeni? Jest to szczególnie ważne w kontekście aktywności człowieka w tej przestrzeni oraz ilości przetwarzanych tam danych osobowych. Dopiero za sprawą rozpoczęcia stosowania przepisów rozporządzenia 2016/679 możliwe stanie się oszacowanie liczby incydentów, których ofiarą padli polscy ADO. Dotychczas bowiem przepisy prawa nie wymagały od nich zgłaszania incydentów do GIODO. Stała tendencja wzrostowa ataków hakerskich niewątpliwie wpływa na obniżone poczucie bezpieczeństwa użytkowników cyberprzestrzeni. Warto więc poznać najczęściej występujące techniki stosowane przez przestępców.

Pojęcie bezpieczeństwa informacji jest niezwykle szerokie. Najczęściej jednak wskazuje się, że zapewnienie bezpieczeństwa informacji sprowadza się do zapewnienia dostępności, poufności i integralności informacji. Standardy te wykorzystywane są także według normy ISO/IEC 27001[183]. Integralność definiowana jest jako właściwość polegająca na zapewnieniu dokładności i kompletności aktywów, dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu, a poufność – to właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.

Jak podkreślają J. Łuczak i M. Trybulski[184] poufność, integralność i dostępność informacji dla każdego podmiotu będzie oznaczać co innego. Są sektory, dla których zapewnienie tych trzech podstawowych elementów bezpieczeństwa informacji

182 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 9.

183 Norma międzynarodowa ISO/IEC 27001 ogłoszona 14 października 2005 r.

184 J. Łuczak, M. Trybulski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009, s. 12.

będzie kluczowe – mowa tu przede wszystkim o sektorze bankowym, służbie zdrowia i tych, dla których mają one mniejsze znaczenie.

5.1.1. Kradzież tożsamości

Wśród najczęściej występujących naruszeń związanych z przetwarzaniem danych osobowych w cyberprzestrzeni wymienia się kradzież tożsamości. Od kilku lat obserwujemy tendencję wzrostową tego przestępstwa, co znalazło odzwierciedlenie we właściwych regulacjach prawnych. Ustawą z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny[185] ustawodawca wprowadził w art. 190a kk nowy element – kradzież tożsamości, polegającą na podszywaniu się pod inną osobę, wykorzystaniu jej wizerunku lub innych danych osobowych w celu wyrządzenia szkody majątkowej lub osobistej. Kradzież tożsamości zaliczana jest do przestępstw tożsamościowych polegających na posłużeniu się przez sprawcę cudzą tożsamością[186]. Celem ustawodawcy była ochrona tożsamości danej osoby i wolności od zagrożeń wynikających z dzisiejszych sposobów komunikacji, w których inna osoba może działać na „rachunek" pokrzywdzonego[187]. Wśród przedstawicieli doktryny często wskazuje się, iż naruszenie to zostało zdefiniowane w nieprecyzyjny sposób, bowiem z punktu widzenia ochrony danych osobowych już samo posługiwanie się danymi osobowymi bez podstawy prawnej stanowi naruszenie[188]. Tymczasem na podstawie obowiązującego art. 190a kk posłużenie się nie swoimi danymi osobowymi w celu założenia konta na portalu społecznościowym może nie wyczerpywać znamion przestępstwa kradzieży tożsamości[189]. Wobec powyższego obecnie obowiązujące przepisy nie uwzględniają wielu sytuacji, w których w rzeczywistości dochodzi do kradzieży tożsamości.

Nie ulega wątpliwości, iż zachętą do popełniania tego rodzaju przestępstw stał się rozwój portali społecznościowych czy e-usług. Umieszczanie na stronach internetowych, które w większości przypadków mają zasięg globalny, danych osobowych stało się łatwym celem przestępców. Z punktu widzenia wykorzystywanych metod służących do kradzieży tożsamości należy stwierdzić, że każdy z nas może się stać ofiarą. Działanie przestępcy polega na podszywaniu się pod inną osobę w celu zdobycia określonych korzyści majątkowych. Może tego dokonać przez umieszczenie na stronie internetowej oferty z podpisem drugiej osoby. Takie działania muszą

185 Dz.U. z 2011 r. nr 72, poz. 381.

186 A. Lach, *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015, s. 34.

187 W. Wróbel, A. Zoll, *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, Warszawa 2017, s. 589.

188 J. Kuraś, *Dane osobowe: kradzież tożsamości w Internecie*, www.rp.pl [dostęp: 12.09.2018].

189 A. Lach, *Karnoprawna…*, op. cit., s. 92.

być podjęte bez wiedzy i zgody osoby, za którą sprawca się podaje. Przez podszywanie się pod inną osobę należy rozumieć zachowanie polegające na fałszywym podawaniu się za kogoś innego[190]. Do najczęstszych sposobów działania przestępcy w cyberprzestrzeni zalicza się posługiwanie się nie swoim adresem poczty internetowej[191], numerem IP (pod warunkiem, że na dłużej jest przyporządkowany do urządzenia przypisanego również na dłużej do konkretnej osoby), numerem PESEL oraz imieniem i nazwiskiem[192]. Niestety w cyberprzestrzeni przestępstwo to jest znacznie trudniejsze do wykrycia niż w świecie realnym i znacznie więcej czasu upływa zanim osoba zorientuje się, że padła ofiarą kradzieży tożsamości. O ile w przypadku kradzieży portfela z dokumentami wiemy, co robić, gdzie się zgłosić oraz jakie mogą być tego negatywne konsekwencje, to w przypadku podobnej kradzieży w Internecie w większości przypadków pozostajemy bierni, licząc, iż nikt nie posłuży się naszymi danymi osobowymi. Dzieje się tak nie tylko dlatego, że nie mamy świadomości wagi przestępstw, do jakich może dojść w cyberprzestrzeni, ale przede wszystkim dlatego, że w wirtualnym świecie znacznie trudniej jest odkryć, iż jest się ofiarą przestępstwa. W konsekwencji kradzież tożsamości może powodować dla pokrzywdzonego wielofalowe skutki. Są one związane nie tylko z utratą określonych korzyści majątkowych, ale także często dobrego imienia i reputacji. Fakt, że w cyberprzestrzeni znacznie później orientujemy się, iż ktoś nielegalnie posłużył się naszą tożsamością dodatkowo potęguje negatywne konsekwencje. Dzieje się to najczęściej, gdy za pośrednictwem skradzionych danych osobowych zaciągane są pożyczki lub inne zobowiązania, które nie zostają spłacane. Wiąże się to również z licznymi trudnościami administracyjnymi i prawnymi, na które napotka poszkodowany, który bardzo często, sam będąc ofiarą, musi udowadniać, że to nie on zaciągnął zobowiązania. Kradzież tożsamości może powodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Ryzyko w opinii Grupy Roboczej art. 29 jest obecne wówczas, gdy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osoby fizycznej[193].

Sprawcy posługują się coraz bardziej profesjonalnymi narzędziami i metodami służącymi zdobyciu danych, czego najlepszym przykładem jest umieszczanie fikcyjnych ogłoszeń o pracę. Zainteresowani kandydaci do pracy, skuszeni atrakcyjnymi warunkami rzadko sprawdzają wiarygodność firmy zamieszczającej ogłoszenie.

190 E. Sobol, *Mały słownik języka polskiego*, Warszawa 1999, s. 654.

191 Wyrok WSA w Krakowie z 11 października 2013 r., II SA/Kr 682/13.

192 Wyrok SA w Warszawie z 29 grudnia 2011 r., VI ACz 2212/11; wyrok NSA z 19 maja 2011 r., I OSK 1079/10.

193 Grupa Robocza art. 29, Wytyczne z 3 października 2017 r. w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679, WP 250, www.giodo.gov.pl [dostęp: 07.01.2019].

Na podany adres e-mail przesyłają swoje CV oraz list motywacyjny, w którym podają znacznie więcej informacji, niż te wymagane przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy[194], np. zdjęcia. W ten sposób przestępcy otrzymują cały pakiet informacji o osobie wraz z jej wizerunkiem. Dlatego tak ważne jest ograniczenie zakresu przekazywanych danych osobowych oraz weryfikowanie stron internetowych, na których się logujemy.

5.1.2. Phishing

Phishing, zgodnie z definicją zaproponowaną przez Komisję Nadzoru Finansowego, jest mechanizmem pozyskiwania danych. Jest to forma oszustwa, która może polegać m.in. na wysyłaniu fałszywych e-maili z prośbą o podanie danych autoryzacyjnych lub umieszczaniu w e-mailach linku z przekierowaniem do fałszywej strony internetowej[195]. Celem tego oszustwa jest pozyskanie informacji lub zainfekowanie komputera po to, aby przejąć nad nim kontrolę. Atak phishingowy polega na wysłaniu fałszywej wiadomości e-mailowej, w większości do przypadkowych użytkowników (zdarzają się również ataki celowe – imienne tzw. spear phishing), z informacją o niedopełnieniu przez nas jakiegoś obowiązku, jak chociażby braku zapłaty określonej kwoty, czy przesłaniu nam fałszywej faktury lub zablokowaniu konta lub usługi. W treści wiadomości umieszczony jest komunikat o potrzebie kliknięcia na podany link, który odsyła do strony, która jest kopią tej autentycznej i tam proszeni jesteśmy o podanie naszych danych osobowych czy loginów i haseł. Tym samym nasze dane osobowe zostają pozyskiwane przez podmioty do tego nieuprawnione[196]. Jeśli natomiast celem oszustów jest zainfekowanie naszego komputera, wówczas działanie sprawcy polega na wysłanej do nas wiadomości e-mailowej skłaniającej nas do kliknięcia w określony link czy otwarcia załącznika. Wykonanie tych czynności powoduje zainfekowanie naszego komputera. W dobie rosnącego znaczenia portali społecznościowych obserwuje się wzrost tego rodzaju zachowań. Bardzo często oszuści włamują się na konto użytkownika i za ich pomocą wysyłają do „naszych" znajomych określone zainfekowane linki, które zawierają szkodliwe oprogramowanie.

Ze względu na możliwe do osiągnięcia zyski, ofiarami ataków phishingowych są bardzo często banki. Aby uczulić na ten problem, powstają różne inicjatywy uświadamiające, czym jest phishing, jaką przybiera najczęściej postać i jak można

194 Tekst jedn. Dz.U. z 2018 r., poz. 917 ze zm.

195 Komisja Nadzoru Finansowego, Komunikat w sprawie „phishingu" danych, 13 listopada 2013 r., https://www.knf.gov.pl/?articleId=53085&p_id=18#1 [dostęp: 12.1.2019].

196 K. Czaplicki, *Przestępstwo phishingu i metody przeciwdziałania*, [w:] G. Szpor, A. Gryszczyńska, *Internet. Strategie bezpieczeństwa*, Warszawa 2017, s. 215.

się przed nim ustrzec. Komisja Nadzoru Finansowego 13 listopada 2013 r. na swojej stronie opublikowała komunikat w sprawie phisingu danych w brzmieniu:

> Do Urzędu Komisji Nadzoru Finansowego (dalej: UKNF) od pewnego czasu napływają sygnały wskazujące na znaczne ryzyko związane z zakładaniem rachunków bankowych, bądź uzyskiwaniem kredytów bankowych z wykorzystaniem informacji wyłudzonych od obywateli, głównie przez internet. Jednym z mechanizmów zgłaszanych przez poszkodowanych tym procederem jest gromadzenie podstawowych danych osobowych, adresów, numerów dowodów tożsamości w ramach procesu rzekomej rekrutacji do pracy „w domu". Potencjalnie nieuczciwi/fałszywi pracodawcy wymagają podania tych informacji i dokonania przelewu drobnej kwoty (np. 1 zł) na wskazany przez nich rachunek bankowy. Tym sposobem na podstawie wyłudzonych danych osobowych próbują założyć rachunki bankowe bądź pozyskać kredyty, a w niektórych przypadkach jako mechanizm weryfikacji tożsamości wykorzystywane są przez banki właśnie przelewy pochodzące z innego rachunku bankowego danej osoby. Pokrzywdzony staje się tym samym dłużnikiem banku z tytułu uzyskanego kredytu, a w przypadku założenia rachunku bankowego z wykorzystaniem jego danych osobowych, przez ten rachunek mogą być transferowane środki pochodzące z przestępstw.
>
> W związku z powyższym, niezmiernie istotne jest zwrócenie uwagi na konieczność nieujawniania w sytuacjach wzbudzających jakiekolwiek wątpliwości swoich danych, w szczególności tych zapisanych w dowodzie osobistym.
>
> Podkreślić należy również, że bardzo niebezpieczne może być przeprowadzanie na zlecenie nieznanych osób operacji przelewu środków z wykorzystaniem własnego rachunku bankowego (często w zamian za gratyfikację pieniężną). Osoba, która dokonuje takiej transakcji, nie wie, czy środki nie pochodzą z przestępstwa, ani tym bardziej w jakim celu są one przekazywane. Za szczególnie niebezpieczny należy uznać schemat działania, w którym jesteśmy proszeni o dokonanie wypłaty otrzymanej kwoty przelewu i następnie przekazanie jej za pośrednictwem banku lub instytucji płatniczej. W przypadku, gdyby rzeczywiście przekazywane środki pochodziły z przestępstwa, jakakolwiek styczność z nimi, a w szczególności przyjęcie ich na własny rachunek bankowy, może zostać uznane za samoistne przestępstwo bądź współudział w przestępstwie. Pamiętać należy również, że korzystanie z bankowości internetowej bez

> zachowania odpowiednich standardów bezpieczeństwa może stwarzać znaczne zagrożenia. Najpoważniejszym jest niebezpieczeństwo dostępu bez naszej wiedzy i zgody do rachunku przez nieuprawnione osoby. Zdarza się, że użytkownicy bankowości internetowej nieświadomie wchodzą na fałszywe strony bankowe lub reagują na prośby o podanie mailem danych osobowych i danych do logowania. Zastosowanie się do takich poleceń może spowodować nawet całkowitą utratę zgromadzonych na rachunku środków. W razie zaistnienia symptomów opisanych powyżej konieczne jest przekazanie szczegółowych informacji do banku bądź instytucji płatniczej prowadzącej rachunek, które są zobowiązane w zakresie swojej działalności do powiadamiania o przestępstwie odpowiednich organów państwa. W związku z powyższym UKNF sugeruje zachowanie daleko posuniętej ostrożności w powyższych sytuacjach i bezwzględne chronienie swoich danych osobowych[197].

Kaspersky Lab w opublikowanym raporcie dokonał podsumowania trendów występujących w pierwszym kwartale 2017 r., w którym zauważył, że łączna liczba załączników zawierających szkodliwe oprogramowanie w ruchu e-mailowym zmniejszyła się 2,4-krotnie w porównaniu z poprzednimi latami[198]. Celem ponad połowy wszystkich ataków phishingowych był sektor finansowy, w tym klienci banków (prawie 26%), systemów płatniczych (ponad 13%) oraz sklepów internetowych (prawie 11%)[199].

W drugiej połowie 2018 r. w ostatnich miesiącach tego rodzaju atak przeprowadzony został na klientów firmy kurierskiej DHL. Za pośrednictwem wiadomości e-mail klienci byli proszeni o kliknięcie linka dotyczącego informacji o statusie przesyłki. W ten sposób na komputerze użytkownika instalowane było złośliwe oprogramowanie wykradające dane użytkownika do logowania np. do portali społecznościowych czy bankowości elektronicznej[200]. Inny tego typu atak przeprowadzony został na klientów Banku PKO BP, gdzie poprzez wiadomości e-mail o treści „Potwierdzenie wpłaty", po kliknięciu na link również instalowane było złośliwe oprogramowanie[201]. W ostatnich miesiącach, w związku z rozpoczęciem stosowania rozporządzenia 2016/679 zwiększyła się liczba „oszustw na RODO".

197 Komisja Nadzoru Finansowego, Komunikat..., op. cit.

198 Kaspersky Lab, *Spam i phishing w I kwartale 2017 r. spadek liczby niechcianych e-maili pochodzących z największego na świecie botnetu spamowego*, https://www.kaspersky.pl [dostęp: 11.05.2018].

199 Ibidem.

200 Raport CERT Orange Polska 2017 r., www.cert.orange.pl [dostęp: 20.10.2018].

201 Ibidem.

W czerwcu 2017 r. został przeprowadzony atak phishingowy na środowisko prawnicze. W wiadomościach wysyłanych do kancelarii prawniczych przestępcy informowali o zbliżających się kontrolach GIODO. Wiadomość zawierała załącznik, którego otwarcie powodowało automatyczne blokowanie pracy komputera oraz utratę danych[202].

Chociaż skala phishingu systematycznie rośnie, niewiele państw zdecydowała się dotychczas uregulować prawnie tego rodzaju działania. Także w polskim ustawodawstwie nie znalazło ono odzwierciedlenia w konkretnych przepisach prawa, w związku z czym konieczne jest posiłkowanie się art. 269b kk oraz art. 190a § 2 kk. W ocenie autora niezwykle ważne jest informowanie opinii publicznej o tego rodzaju atakach oraz stałe edukowanie poprzez kampanie społecznościowe.

5.1.3. Pharming

Pharming jest zaawansowaną formą phisingu, jednak o wiele trudniejszą do wykrycia dla użytkownika. Pharming, jak publikuje na swojej stronie avast, to rodzaj oszustwa przypominający phishing, ale odwiedzający prawdziwą stronę są przekierowywani na podszywające się pod nią strony, które instalują na ich urządzeniach złośliwe oprogramowanie lub zbierają dane osobowe, np. hasła lub dane kont bankowych. Pharming jest szczególnie groźny, ponieważ w przypadku złamania zabezpieczeń serwera DNS (Domain Name Server) nawet dobrze zabezpieczeni użytkownicy z komputerami wolnymi od wirusów i złośliwego oprogramowania mogą paść ofiarami tego procederu[203].

Pharming występuje w dwóch postaciach. Pierwsza polega na zainstalowaniu wirusa na naszym komputerze, którego zadaniem jest przekierowanie nas na sfałszowaną stronę. Użytkownik nie dowiaduje się, że jest na fałszywej stronie, gdyż jest ona łudząco podobna do tej oryginalnej, a samo przekierowanie następuje automatycznie, bez jego wiedzy i zgody.

Druga postać polega na tym, iż zostaje zaatakowany cały serwer DNS, co znacznie poszerza krąg ofiar padających temu przestępstwu. Modyfikowanie DNS polega na zmianie ustawień protokołu TCP/IP lub pliku Imhost. Tym samym trafiamy na fałszywą stronę internetową, mimo naszego przekonania, iż przekierowanie następuje na stronę oryginalną. Najczęściej zaatakowane zostają strony banków czy sklepów internetowych, co ma związek z korzyściami finansowymi.

Cel tego przestępstwa jest taki sam, czyli zdobycie nielegalnie naszych haseł, loginów, kodów numerów kart kredytowych itp.

---

202 Ibidem.

203 *Pharming*, https://www.avast.com/pl-pl/c-pharming [dostęp: 12.10.2018].

5.1.4. Hacking

Celem przestępstwa hackingu jest uzyskanie informacji, w tym bardzo często danych osobowych, spowodowanie zniszczenia bądź uszkodzenia innych systemów informatycznych oraz pokonanie zabezpieczeń innych komputerów[204]. Zgodnie z art. 267 kk przestępstwo to polega na bezprawnym uzyskaniu przez sprawcę dostępu do informacji dla niego nieprzeznaczonej. Informacja, do której sprawca uzyskuje dostęp, może mieć postać zarówno utrwaloną na nośniku, jak i być przekazywana w sieci lub poza nią. Kodeks karny penalizuje sytuację, w której dostęp do informacji nieprzeznaczonej dla odbiorcy nastąpił w jeden z wymienionych w kk sposobów, tj. otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Chodzi zatem o zachowania polegające na przyłączeniu urządzenia odbiorczego do sieci kablowej (np. telefonicznej, komputerowej) lub innej infrastruktury (np. urządzenia radiowego), służącej do przekazywania informacji. Innymi słowy „podłączenie" oznacza wyłącznie połączenie fizyczne[205].

5.1.5. Niszczenie danych informatycznych

Przestępstwo niszczenia danych informatycznych zostało opisane w art. 268a kk. Odnosi się do danych informatycznych przetwarzanych zarówno w formie cyfrowej, jak i analogowej. Pojęcie to zostało zdefiniowane w konwencji o cyberprzestępczości jako „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"[206]. Polega ono na nieuprawnionym niszczeniu, uszkadzaniu, usuwaniu, zmianie lub utrudnianiu dostępu do danych informatycznych albo w istotnym stopniu zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Zachowanie sprawcy może polegać na zakłócaniu lub uniemożliwianiu działania procesu, którego skutkiem jest jego nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informacji. Uniemożliwienie natomiast oznacza zatrzymanie tych procesów lub niemożność ich podjęcia[207].

---

204 P. Bogacki, *Hacking w ujęciu art. 267 kk*, „Monitor Prawniczy" 2013, nr 17, s. 18. www.czasopisma.beck.pl/monitor-prawniczy [dostęp: 26.11.2018].

205 Wyrok WSA w Gdańsku z 28 września 2016 r., II Aka 111/16.

206 V. Konarska-Wrzosek, *Kodeks karny. Komentarz, wyd. II*, Warszawa 2016, s. 1142.

207 Wyrok SN z 30 września 2015 r., II K 115/15.

Tak jak każdego dnia pojawiają się w cyberprzestrzeni nowe rozwiązania technologiczne, tak samo rozwijają się nowe, nieznane nam zagrożenia. Wszystkie opisane działania sprawców nakierowane są na pozyskanie danych osobowych, po to, by za ich pośrednictwem uzyskać określoną korzyść majątkową. Działania sprawców są coraz bardziej śmiałe i pomysłowe. Gotowi są podjąć trud zmierzający do podstępnego wykradzenia danych osobowych, jak chociażby stworzyć odpowiedni program komputerowy służący do popełnienia przestępstwa lub innego oszustwa komputerowego. Przeciwdziałanie cyberzagrożeniom jest niezwykle trudne i wymaga wielopłaszczyznowych działań podejmowanych zarówno przez społeczność międzynarodową, jak i pojedynczych użytkowników.

Statystyki dotyczące liczby popełnianych przestępstw w cyberprzestrzeni od wielu lat wskazują tendencję wzrostową. W niedawno opublikowanym raporcie dotyczącym skali tego rodzaju zachowań w 2018 r. podkreśla się, iż systematycznie wzrasta liczba wysyłania „bezplikowych" złośliwych oprogramowań, wiadomości e-mail zawierających linki, które aktywowane infekują komputery[208]. Dodatkowo w Stanach Zjednoczonych zaobserwowano 16-procentowy wzrost liczby zgłaszanych naruszeń bezpieczeństwa polegających na niezamierzonym ujawnieniu danych[209]. Z opublikowanego raportu wynika także, że coraz częściej przestępcy wykorzystują innowacyjne metody pozyskiwania danych, (w tym także danych osobowych) polegające na instalowaniu w komputerach złośliwych plików czy też zdalne przejmowanie kontroli nad komputerem użytkownika. Innym gwałtownie rosnącym zagrożeniem jest włamywanie się na pocztę służbową pracowników[210]. Użytkownicy nadal bardzo często padają ofiarą ataków typu „wsparcie techniczne". Polega on na wyświetleniu na komputerze użytkownika informacji, że jego komputer został zainfekowany przez złośliwe oprogramowanie. W celu usunięcia wirusa proszony jest o zalogowanie się do bankowości internetowej i przelanie określonej sumy pomiędzy. W tym czasie przestępcy uzyskują dostęp do rachunku bankowego poszkodowanego[211].

Trendy światowe znajdują odzwierciedlenie także w Polsce. Z raportu opublikowanego przez CERT za 2017 r. wynika, że do najczęściej występujących incydentów zalicza się te związane z publikowaniem obraźliwych i nielegalnych treści, ataki na dostępność zasobów czy też próby włamań. Niestety nie mamy szczegółowych informacji o skali tego rodzaju zjawisk wśród podmiotów prywatnych. Wynika to przede wszystkim z faktu, że podmioty prywatne do czasu wejścia w życie

208 *Niedostrzegane zagrożenia, nieuchronne straty*, wwwtrendmicro.com [dostęp: 11.10.2018].
209 Ibidem.
210 Ibidem.
211 R. Janus, *Statystyki zagrożeń w pierwszej połowie 2018 r.*, wwwitfocus.pl [dostęp: 11.10.2018].

rozporządzenia 2016/679 nie były zobowiązane do zgłaszania występujących incydentów. Bardzo często informacja ta była pilnie strzeżona, w obawie przed kolejnymi atakami hakerskimi.

5.1.6. Złośliwe oprogramowanie ransomware

Słowo ransomware powstało w wyniku połączenia dwóch słów: ransom – okup, oraz software – oprogramowanie. W ten sposób otrzymujemy definicję oprogramowania, które wymusza na użytkowniku zapłatę okupu. Ofiara tego rodzaju ataku otrzymuje po włączeniu komputera komunikat, że pliki znajdujące się na komputerze zostały w wyniku ataku zablokowane, a jedyną drogą do ich odzyskania jest zapłacenie określonej kwoty pieniędzy. W przypadku banków czy też międzynarodowych korporacji kwota okupu może być naprawdę wysoka. Przestępcy stosują różne metody infekowania komputerów użytkowników tą metodą. Do najpopularniejszych należą wysyłanie spamów zawierających linki, których naciśnięcie powoduje powolne szyfrowanie plików czy wysyłanie zainfekowanych reklam. Bardzo często użytkownicy nie mają świadomości, iż otrzymują zainfekowane wiadomości, ponieważ są one łudząco podobne do tych prawdziwych. E-maile z fakturą za prąd, informacja statusu przesyłki kurierskiej to tylko wybrane przykłady stanowiące tego rodzaje ataki.

Jak wynika ze statystyk liczba ataków przy wykorzystaniu opisywanych metod sukcesywnie rośnie. Wiele firm, które stały się ofiarami złośliwego oprogramowania typu ransomware nie zawiadamia policji o tego typu zaistniałym ataku głównie w obawie przed utratą zaufania i dobrej reputacji wśród klientów, a co za tym idzie – spadkiem dochodów. To zaś stanowi dodatkowy bodziec zachęcający cyberprzestępców do popełniana kolejnych przestępstw, czują się w ten sposób bezkarni. W tym przypadku również świadomość użytkowników jest najlepszym mechanizmem pozwalającym na zminimalizowanie występowania ataków tego rodzaju. Warto także pamiętać o aktualnym programie komputerowym. Dla użytkowników, którzy nie wykonują regularnie kopii zapasowych takie ataki mogą przynieść nieodwracalne skutki w postaci utraty wszystkich danych. Wówczas, jedyną drogą do ich odzyskania jest zapłacenie okupu.

5.2. Metody ochrony danych osobowych w cyberprzestrzeni

5.2.1. Regulacje prawne zmierzające do zapewnienia bezpieczeństwa danych osobowych w cyberprzestrzeni

Zapewnienie bezpieczeństwa w cyberprzestrzeni w ocenie autora wymaga zaangażowania całej społeczności międzynarodowej. Nie zwalnia to jednak państw

z podejmowania wysiłku zmierzającego do zapewnienia swoim obywatelom poczucia bezpieczeństwa[212]. Chociaż w Polsce wielokrotnie podejmowano działania na rzecz zapewnienia bezpieczeństwa w cyberprzestrzeni poprzez różnego rodzaju dokumenty, w tym również akty prawne, powołując wyspecjalizowane w tym zakresie podmioty (CERT) czy też przyznając organom administracji publicznej określone w tym zakresie kompetencje, działania te należy ocenić za wysoce nieskuteczne, co zresztą zostało potwierdzone w 2015 r. w raporcie Najwyższej Izby Kontroli[213].

W ocenie autora pomimo podejmowanych inicjatyw nadal brakuje jednej spójnej koncepcji wskazującej, w jaki sposób zapewnić bezpieczeństwo obywateli Rzeczpospolitej Polskiej w cyberprzestrzeni. Z publikowanych dokumentów nie wynika także wprost, kto ma być odpowiedzialny za bezpieczeństwo w tym obszarze oraz jakie konkretnie działania mają je zapewnić. Dostępne materiały cechuje wysoka ogólnikowość, która z całą pewnością może stanowić wypadkową do dyskusji, ale nie jest wskazówką do realnych działań. Dużym problemem jest także rozproszenie kompetencji związanych z zapewnieniem bezpieczeństwa w cyberprzestrzeni pomiędzy wiele organów administracji publicznej[214]. Dziś kompetencje w tym obszarze posiada nie tylko Rada Ministrów, ale także m.in. Ministerstwo Cyfryzacji, Prezes UODO, Ministerstwo Sprawiedliwości. Działania przez nich podejmowane nie są w żaden sposób ujednolicone i zsynchronizowane. Pojedyncze inicjatywy, jak nowelizacja kk wprowadzająca postanowienia wynikające z Konwencji Rady Europy o cyberprzestępczości z całą pewnością nie są wystarczające[215]. Brakuje także przepisów prawnych kompleksowo regulujących bezpieczeństwo w cyberprzestrzeni. Co pewien czas pojawiają się ustawy dotyczące bardzo wąskich obszarów aktywności, jak ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[216]. Celem ustawy stało się „wzmocnienie mechanizmów koordynacji działań, doprecyzowanie zadań poszczególnych służb i organów oraz zasad współpracy pomiędzy nimi, zapewnienie możliwości skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym"[217]. Chociaż samo powstanie ustawy należy uznać za właściwe, to sposób i zakres zbieranych

212 M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 125.

213 Raport NIK, *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP* Warszawa 2015, s. 10, www.nik.gov.pl [dostęp: 07.09.2017].

214 P. Trąbiński, *Podział kompetencji w zapewnieniu cyberbezpieczeństwa*, [w:] G. Szpor, A. Gryszczyńska, *Internet…*, op. cit., s. 69.

215 Convention on Cybercrime, No185, www.ceo.int [dostęp: 17.12.2018].

216 Tekst jedn. Dz.U. z 2018 r., poz. 452 ze zm.

217 Uzasadnienie do ustawy o działaniach antyterrorystycznych, s. 1, www.sejm.gov.pl [dostęp: 12.10.2018].

danych osobowych osób podejrzanych o działania terrorystyczne w niej przewidziane budził liczne wątpliwości, w tym m.in. GIODO[218]. Głównym zarzutem organu nadzorczego stało się dążenie do nieadekwatnego i zbyt szerokiego zakresu gromadzonych danych osobowych.

Do źródeł prawa odnoszącego się do bezpieczeństwa w cyberprzestrzeni należy również Konstytucja RP. Mimo że nie znajdziemy w jej aktach bezpośrednio odesłania do tego obszaru, to jednak standardy wypracowane w ustawie zasadniczej jak najbardziej mają zastosowanie w stosunku do cyberprzestrzeni. Inną istotną z punktu widzenia bezpieczeństwa Polski w cyberprzestrzeni inicjatywą stała się podpisana 27 września 2011 r. nowelizacja ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[219]. Dokument ten nie tylko wprowadził do polskiego porządku prawnego definicję pojęcia cyberbezpieczeństwa, ale stał się także impulsem do dalszych prac w tym obszarze. W konsekwencji w 2014 r. w Strategii Bezpieczeństwa Narodowego RP założono jako cel podstawowy zapewnienie bezpieczeństwa Rzeczpospolitej Polskiej w tym obszarze[220].

Inną istotną i nową regulacją dążącą do zapewnienia bezpieczeństwa w cyberprzestrzeni (zwłaszcza w kontekście danych osobowych) jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[221], która weszła w życie 28 sierpnia 2018 r. Jej celem jest implementacja do krajowego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej[222]. Adresatami ustawy są przedsiębiorcy oraz podmioty publiczne w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[223], będący operatorami usług kluczowych w rozumieniu ustawy oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa, jednostki sektorów publicznych oraz inne podmioty wyszczególnione w art. 4 ustawy[224]. Na pod-

218 Uwagi GIODO z 12 maja 2016 r. do projektu ustawy o działaniach antyterrorystycznych. DOLiS-033-133/16, www.giodo.gov.pl [dostęp: 12.12.2018].

219 Dz.U. z 2011 r. nr 222, poz. 1323.

220 Biuro Bezpieczeństwa Narodowego, *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* Warszawa 2014.

221 Dz.U. z 2018 r., poz. 1560.

222 Dz.Urz. UE L 194 z 19.07.2016.

223 Tekst jedn. Dz.U. z 2017 r., poz. 570 ze zm.

224 Uzasadnienie do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, poz. 1560, www.sejm.gov.pl [dostęp: 15.11.2018].

mioty te zostały nałożone dodatkowe obowiązki, których celem jest podniesienie poziomu bezpieczeństwa w cyberprzestrzeni. Do najważniejszych należy zaliczyć wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniającego prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zarządzanie incydentami oraz stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

Dodatkowo, podmioty o których mowa w ustawie, zostały zobowiązane do zgłaszania każdego poważnego incydentu nie później niż w ciągu 24 godzin od momentu jego wykrycia do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. W ustawie zdefiniowano w sposób ogólny incydent jako każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Dostosowując przepisy do wymogów europejskich, podobnie jak ma to miejsce w rozporządzeniu 2016/679, ustawodawca przewidział wysokie kary za nieprzestrzeganie wymogów ustawy. Warto rozważyć wdrożenie niektórych rozwiązań zaproponowanych w ustawie wśród szerszej grupy podmiotów, zwłaszcza w zakresie obowiązku regularnego przeprowadzania audytów bezpieczeństwa systemów informatycznych co 2 lata.

Oba akty prawne są ze sobą ściśle powiązane. Na bezpieczeństwo w cyberprzestrzeni należy patrzeć znacznie szerzej niż z perspektywy tych aktów prawnych, niemniej jednak ich obecność stanowi drogowskaz, w jakim kierunku zmierza dążenie do zapewnienia bezpieczeństwa w cyberprzestrzeni nie tylko w kraju, ale również szerzej na terytorium państw należących do UE.

Nie ulega wątpliwości, że dopiero wejście w życie rozporządzenia 2016/679 w znaczący sposób przyczyniło się do poprawy bezpieczeństwa osób fizycznych w cyberprzestrzeni. Jak zostało wykazane w pracy, działania te mają charakter wielopłaszczyznowy. Z jednej strony nakłada się na ADO nowe, niewystępujące dotąd obowiązki względem osób, których dane dotyczą. Zobowiązuje się ich także do zapewnienia pełnej rozliczalności i transparentności realizowanych procesów zarówno przed osobą, której dane dotyczą, jak i przed organem nadzorczym. Z drugiej zaś strony osoba, której dane dotyczą, otrzymuje zupełnie nowe uprawnienia gwarantujące jej możliwość kontrolowania i weryfikowania działań podejmowanych przez ADO. Chociaż w literaturze przedmiotu można spotkać się z opiniami, że rozwiązania zaproponowane w rozporządzeniu 2016/679 należy uznać za

rewolucyjne, w ocenie autora stanowią one wyłącznie naturalną ewolucję. Jej brak naraziłby osobę, której dane dotyczą, na utratę kontroli nad danymi osobowymi, oraz związanymi z tym możliwymi do wystąpienia negatywnymi konsekwencjami.

Zapewnienie bezpieczeństwa danych osobowych w cyberprzestrzeni jest złożonym procesem, który wymaga podejmowania wielu różnych inicjatyw na różnych szczeblach. Bez wątpienia cyberprzestrzeń wymaga większego zainteresowania prawodawcy. Użytkownicy sieci mają prawo wiedzieć, że gwarancje konstytucyjne są stosowane wobec nich również w cyberprzestrzeni. Rozwiązania technologiczne w znaczący sposób wyprzedzają prawodawstwo, zatem funkcjonowanie w cyberprzestrzeni zmusza do innowacyjności i rozwoju, nie tylko użytkowników, ale także prawodawcę, który sprawując jurysdykcję także na tym obszarze powinien zapewnić warunki pozwalające na bezpieczne z niej korzystanie. Coraz powszechniejsze funkcjonowanie w cyberprzestrzeni zmusiło państwa UE do dostosowania dyrektywy 95/46/WE do współczesnych warunków oraz oczekiwań obywateli, że organizacja ta zapewni im należyte gwarancje ochrony. W podobny sposób powinien działać ustawodawca krajowy, dokonując przeglądu obowiązujących aktów prawnych i tam, gdzie to niezbędne, wprowadzić zmiany. W taki właśnie sposób postąpiono w Polsce, przygotowując projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, która przewiduje zmianę 168 ustaw krajowych. Reforma o tak szerokim zasięgu w Polsce nie była jeszcze przygotowywana. Pracę nad proponowanymi zmianami trwały od 2 lat, dążąc do zapewnienia obywatelom Rzeczpospolitej Polskiej realizowania praw wynikających z unijnego rozporządzenia 2016/678.

5.3. W jaki sposób zapewnić bezpieczeństwo danych osobowych w cyberprzestrzeni?

Większość zagrożeń w cyberprzestrzeni dotyczy bezpieczeństwa informacji. Część z nich to informacje dotyczące człowieka, których nie chce ujawniać osobom postronnym. Ich ujawnienie może nieść za sobą niepowetowane straty dla jednostki. Dlatego tak ważne jest zapewnienie tym danym odpowiedniego poziomu ochrony. Jak zostało już zauważone, zapewnienie bezpiecznego przetwarzania danych osobowych w cyberprzestrzeni wymaga podjęcia wysiłku przez wiele zaangażowanych w ten proces podmiotów[225]. Państwo powinno zapewnić ramy prawne, w których użytkownicy mogliby się bezpiecznie poruszać. Jest to niesłychanie ważne

225 J. Trubalska, Ł. Wojciechowski, *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017, s. 127.

w związku z przetwarzaniem danych osobowych w cyberprzestrzeni. W przeciwnym razie osoba, której dane dotyczą, będzie pozostawiona samej sobie. A samotna walka z cyberprzestępcami skazana jest na niepowodzenie przede wszystkim dlatego, że dysponują oni nowoczesnymi metodami łamania stosowanych zabezpieczeń, często dużymi zasobami finansowymi oraz zdolnością do ciągłego doskonalenia stosowanych metod. Właśnie przez to użytkownicy bardzo często nie zdają sobie w ogóle sprawy, w jaki sposób cyberprzestępcy mogą pozyskać dane z jego komputera.

Samo realizowanie obowiązków wynikających z rozporządzenia 2016/679 przez ADO również może okazać się niewystarczające. W wielu obszarach, zwłaszcza tych dotyczących środków technicznych i organizacyjnych, jakie powinien stosować, ADO otrzymał daleko idącą swobodę w wyborze metod i środków niezbędnych do zapewnienia bezpieczeństwa danych osobowych. Zastosowane przez ADO środki techniczne i organizacyjne powinny być adekwatne do możliwego do wystąpienia zagrożenia. Wśród takich środków technicznych najczęściej wykorzystywanych przez ADO zalicza się, m.in. stosowanie haseł BIOS, uwierzytelnianie użytkowników za pomocą haseł lub identyfikatorów, okresową zmianę haseł, środki uniemożliwiające wykonywanie niezautoryzowanych kopii zapasowych czy system rejestrowania dostępu do danych osobowych[226]. Bardzo ważnym elementem jest także zapewnienie aktualnego, legalnego programu antywirusowego (firewalla). Pozwala on chociaż w minimalnym zakresie uchronić przed powszechnie stosowanymi w sieci programami skierowanymi na pozyskanie lub przechwycenie danych.

Coraz częściej praktykowanym rozwiązaniem w przypadku przetwarzania danych osobowych w cyberprzestrzeni jest ich szyfrowanie. Powszechne dziś wykorzystywanie szyfrowanie komputerów czy telefonów coraz częściej też dotyczy szyfrowania wiadomości e-mail zawierających dane osobowe. Szyfrowanie jest jedną z metod chroniącą dane osobowe przed nieuprawnionym dostępem osób trzecich. Polega na wprowadzeniu dodatkowego zabezpieczenia w postaci hasła (najczęściej ciągu liczb). W przypadku wysłania wiadomości do niewłaściwego adresata nie ma on możliwości odczytania zaszyfrowanego pliku, bądź dokumentu bez znajomości klucza, który powinien zostać wysłany innym kanałem komunikacji niż wiadomość zawierająca dane osobowe. Inną metodą zabezpieczenia danych osobowych wymienianą w rozporządzeniu 2016/679, obok szyfrowania, jest pseudonimizacja. Chociaż metoda ta została rekomendowana jako jedna z możliwości zabezpieczenia danych już w 2010 r., Grupa Robocza art. 29 dostrzegała w tej

226 M. Szczęberek, K. Ułasiuk, *Bezpieczeństwo danych osobowych*, Wrocław 2017, s. 151.

metodzie pewne niedoskonałości, wskazując, iż pseudonimizowane informacje zamieszczane przez użytkowników na portalach społecznościowych można odczytać z grafów powiązań społecznościowych[227].

Pseudonimizacja polega na przetwarzaniu danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 5 rozporządzenia 2016/679). W motywie 28 preambuły rozporządzenia 2016/679 podkreślono, że rozwiązanie to zostało zaproponowane po to, by ograniczyć ryzyko osób, których dane dotyczą, oraz pomóc ADO wywiązać się z obowiązku ochrony danych. Warto w tym miejscu odnotować, iż pseudonimizacja i anonimizacja nie są pojęciami tożsamymi. W opinii Grupy Roboczej art. 29 „pseudonimizacja ogranicza możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą w związku z tym stanowi użyteczny środek bezpieczeństwa, ale nie metodę anonimizacji"[228]. Do najczęściej stosowanych metod pseudonimizacji zalicza się: szyfrowanie z kluczem tajnym, tokenizację czy też szyfrowanie deterministyczne[229]. Nie ulega wątpliwości, że w przypadku przetwarzania danych w systemach informatycznych niezwykle ważne jest zadbanie o tworzenie kopii zapasowych. Najczęściej częstotliwość ich dokonywania oraz miejsce i czas ich przechowywania są określone w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Regularne wykonywanie kopii zapasowych chroni przed zniszczeniem, uszkodzeniem lub inną formą utraty danych poprzez odtworzenie ich z kopii zapasowych.

Prawodawca unijny rekomenduje ADO także regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Najczęściej odbywa się to przez testy penetracyjne, które w ocenie wielu specjalistów uznawane są za skuteczną metodę wykrywania luk i błędów systemów informatycznych[230]. Ważne jest także, by ADO wdrażali i stosowali procedury ułatwiające realizację ciążących na nich obowiązków. Będą one jednak skuteczne dopiero wówczas, gdy pracownicy zrozumieją potrzebę ich stosowania. To zaś zostanie zapewnione, jeżeli ADO będzie dbał o poziom ich wiedzy fachowej związanej z przetwarzaniem danych osobowych.

---

227 Grupa Robocza art. 29, Opinia 05/2014 w sprawie technik anonimizacji przyjęta 10 kwietnia 2014 r., WP 216, www.giodo.gov.pl [dostęp: 12.04.2018].

228 Ibidem.

229 Ibidem.

230 J. Rowiński, *Testy penetracyjne*, „ABI Expert" 2018, nr 3, s. 24.

Regularne testowanie systemów informatycznych pozwala na wykrycie luk tam, gdzie się one pojawiają przed przestępcami. Należy mieć świadomość, że w przeciwnym razie hakerzy zrobią to za nas[231]. Dlatego tak ważne jest ciągłe szkolenie pracowników i promowanie przekonania, że cyberprzestrzeń zmienia się każdego dnia, więc muszą się z tym liczyć i mieć świadomość występowania nowych zagrożeń. Jeżeli ADO powołał IOD, wówczas obowiązek przeprowadzania szkoleń ciąży na nim, co wynika wprost z art. 39 ust. 1 lit. b rozporządzenia 2016/679, który stanowi, że do podstawowych zadań IOD należy między innymi działanie zwiększające świadomość oraz szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych. Wynika to między innymi z faktu, że ADO jest zobowiązany do zapewnienia każdemu, kto przetwarza dane osobowe, i kto decyduje o środkach i celach tego procesu, by przetwarzał je zgodnie z prawem oraz wyłącznie w zakresie jego polecenia. Dlatego równie ważne jest, by każdy pracownik posiadał aktualne upoważnienie do przetwarzania danych osobowych, z którego będzie jasno wynikało, do jakich operacji i na jakich danych jest upoważniony. Każdy ADO powinien zadbać także o aktualizowanie dokumentacji ochrony danych osobowych oraz regularne audytowanie procesu ich przetwarzania. Audyty te mogą być prowadzone zarówno przez ADO czy IOD, jak i przez profesjonalny podmiot zewnętrzny. Pozwoli on nie tylko na weryfikację istniejących zasobów, ale także na ocenę aktualności i przydatności dokumentacji oraz stosowanych procedur. Wyniki przeprowadzonego audytu powinny zostać następnie skonfrontowane z analizą ryzyka, aby ocenić, czy są obszary, które wymagają zmiany poziomu akceptacji przyjętego ryzyka. Warto pamiętać, że samo wykrycie luki w systemie jest niewystarczające. Działania zaradcze powinny być podejmowane niezwłocznie po ich wykryciu. Profilaktyka, ciągła praca nad dążeniem do zapewnienia bezpieczeństwa oraz praca całego zespołu ADO wydają się być jedynymi skutecznymi metodami walki z cyberprzestępcami.

Działania podejmowane przez państwo oraz ADO są niewystarczające dla zapewnienia bezpiecznego procesu przetwarzania danych, bowiem najczęściej ograniczają się wyłącznie do określenia ogólnych ram prawnych ochrony. Dlatego w dużej mierze ciężar związany z bezpiecznym przetwarzaniem danych osobowych w cyberprzestrzeni będzie spoczywał na osobie, której dane dotyczą. To zaś wiąże się nie tylko z potrzebą dysponowania wiedzy o tym, czym jest cyberprzestrzeń i jakie są zagrożenia związane z aktywnością w jej obszarze, ale przede wszystkim mądrym i świadomym poruszaniu się w tym środowisku. Tego rodzaju aktywność w wirtualnym świecie oznacza zaś dbanie o to, komu oraz w jakim celu

231 S. Gwoździewicz, K. Tomaszycki, *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warszawa 2017, s. 213.

przekazywane są dane osobowe. Jak zostało wykazane w pracy, w przypadku przekazywania danych w sieci rzadko zastanawiamy się, czy podmiot, który żąda od nas danych w rzeczywistości istnieje, czy nikt nie podszywa się pod kogoś realnego, stawiając fikcyjną witrynę internetową tylko po to, by nielegalnie pozyskać dane użytkownika. Obserwując ryzykowne zachowanie osób, których dane dotyczą, trudno jednoznacznie określić, czy wynika ono jedynie z braku wiedzy. Czy jeżeli osoba, której dane dotyczą, loguje się na stronie internetowej, gdzie wymusza się wyrażenie zgody na przetwarzanie danych, to ma świadomość konsekwencji prawnych swoich wyborów? Czy chęć skorzystania z usług oferowanych przez ADO jest tak wielka, że jej ceną będzie narażanie bezpieczeństwa danych osobowych? Wydawać by się mogło, że liczba godzin, którą dziennie spędzamy w cyberprzestrzeni (w Polsce 9 godzin tygodniowo[232]) powinna zobowiązywać do właściwych postaw w wirtualnym świecie. Tymczasem wciąż rośnie liczba ataków phishingowych, co świadczy o tym, że użytkownicy nawet w sytuacji, w której mają świadomość zagrożeń związanych z funkcjonowaniem w cyberprzestrzeni łatwo padają ofiarą tego rodzaju działań. Jak zauważają specjaliści, wynika to z faktu, że przestępcy bardzo często, by pozyskać dane osobowe posługują się różnymi metodami manipulacji[233]. Warto także mieć na względzie, że „Internet nie zapomina" i bardzo łatwo jest zebrać informacje o osobie, której dane dotyczą, z różnych źródeł, połączyć je oraz wykorzystać w celu popełnienia przestępstwa.

Warto się zastanowić, gdzie pozostawiamy ślady cyfrowe oraz w jakim celu inni mogą posłużyć się naszymi danymi osobowymi. Zgodnie z zasadą minimalizacji danych osobowych, dobrze jest przekazywać tylko te dane osobowe, które są niezbędne do realizacji określonego celu. Dodatkowo, ważne jest, by za każdym razem przed przekazaniem danych osobowych zapoznać się z klauzulą obowiązku informacyjnego. Wiedza ta wzbogaci osobę, której dane dotyczą, na temat procesu przetwarzania jej danych osobowych. Warto także korzystać z rozwiązań prawnych (policy by design, policy by default), gwarantujących użytkownikom prawo do prywatności. Dlatego każda zmiana ustawień urządzeń gromadzących i przetwarzających dane osobowe pozbawiająca tego prawa powinna być dokonana świadomie. Osoba, której dane dotyczą, powinna również umieć przewidzieć konsekwencje swoich zachowań w cyberprzestrzeni. Warto zwrócić uwagę na formę i treść zgód na przetwarzanie danych osobowych, które bardzo często są dołączane do formularzy elektronicznych, bowiem to one są miejscem, gdzie ADO narusza prawa osób, których dane dotyczą. Jak zostało zauważone w pracy, zgoda

232 Korzystanie z Internetu, Komunikat z Badań CBOS 49/2017 r., www. cbos.pl [dostęp: 12.09.2018].
233 Raport CERT Orange Polska 2017 r. www.cert.orange.pl [dostęp: 20.10.2018].

na przetwarzanie danych osobowych powinna być dobrowolnym i świadomym okazaniem woli. Osoba, której dane dotyczą, powinna zostać poinformowana o możliwości cofnięcia zgody w każdym czasie.

W ocenie autora największe zagrożenie dla bezpieczeństwa przetwarzania danych osobowych stwarzają portale społecznościowe. Tam też dochodzi do przetwarzania ogromnej ilości danych osobowych oraz najwyraźniej uwydatnia się konflikt wolności informacyjnej oraz bezpieczeństwa, które w przypadku cyberprzestrzeni są niezwykle trudne do pogodzenia. Oszuści chcący pozyskać dane osobowe mogą bez najmniejszych trudności stworzyć fikcyjne konto użytkownika, bądź przełamać zabezpieczenia stosowane przez dostarczyciela usługi. Taka sytuacja miała miejsce we wrześniu 2018 r., kiedy na Facebooku przestępcy uzyskali dostęp do 50 mln kont użytkowników. W związku z tym rekomendowane jest korzystanie z tego rodzaju usług w wąskim zakresie oraz ograniczenie zakresu udzielanych informacji. Warto też zadbać o korzystanie z prostych i sprawdzonych metod polegających na stosowaniu odpowiednich zabezpieczeń w postaci regularnie zmienianych haseł dostępu, nieudostępniania haseł osobom postronnym czy nieposługiwania się wszędzie tym samym hasłem. Warto także zabezpieczyć swój komputer w legalny program antywirusowy lub zaporę firewall.

Budowanie świadomości wśród użytkowników wirtualnego świata jest długim i trudnym procesem. W ocenie autora jest on jednak niezbędny w celu zapewnienia im odpowiedniego poziomu ochrony. Rozważne i przemyślane przekazywanie danych osobowych jest najlepszą metodą gwarantującą bezpieczne przetwarzanie danych osobowych w cyberprzestrzeni. Jednakże, aby wzbudzić i rozwijać tę świadomość wśród użytkowników wirtualnego świata, niezbędne jest regularne przeprowadzanie kampanii społecznych. Warto także skupić się na najmłodszych użytkownikach sieci, tak by od wczesnych lat uczyli się z rozwagą korzystać z Internetu. Edukacja tej grupy użytkowników sieci narażona jest dodatkowo na nowe zagrożenie uzależnienia od Internetu. Wielogodzinne przebywanie w wirtualnym świecie powoduje trudności w akomodacji w świecie realnym. Dzieci i młodzież niejednokrotnie przenoszą zachowania swoich wirtualnych bohaterów w świat realny. Z badań przeprowadzanych wśród uczniów szkół podstawowych i ponadpodstawowych wynika, iż pomimo licznych kampanii społecznych nie mają świadomości zagrożeń wiążących się z aktywnością w cyberprzestrzeni. Aż 32% ankietowanych nie dostrzega w ogóle żadnych zagrożeń związanych w funkcjonowaniem w wirtualnym świecie[234].

234 B. Komorowska, *Aktywność internetowa dzieci i młodzieży – wskazania dla praktyki pedagogicznej*, www.cejsh.icm.edu.pl, s. 7 [dostęp: 26.10.2018].

Zapewnienie bezpieczeństwa procesu przetwarzania danych osobowych w cyberprzestrzeni wymaga stosowania nowych, ulepszonych rozwiązań prawnych, technicznych i organizacyjnych. Ciężar ten spoczywa nie tylko na społeczności międzynarodowej czy państwie, ale także na każdym użytkowniku. Dane osobowe stanowią dobro, które ze względu na swoją wartość oraz znaczenie podlega ochronie, a w przypadku przetwarzania danych szczególnie chronionych, stosowania najwyższych standardów ochrony. Tymczasem z dostępnych informacji wynika, że to właśnie te dane są najczęściej wykradane[235].

Powstanie i upowszechnienie Internetu uznawane jest za odkrycie XXI wieku, które w istotny sposób zrewolucjonizowało życie ludzkości. W ocenie autora mimo licznych zalet cyberprzestrzeń pełna jest zagrożeń. Stosowane dziś rozwiązania prawne nie zapewniają jej użytkownikom należytej ochrony, a co za tym idzie państwo nie realizuje podstawowej wartości, jaką jest poczucie bezpieczeństwa.

235 *Niedostrzegane zagrożenia, nieuchronne straty*, wwwtrendmicro.com [dostęp: 11.10.2018]

Rozdział 6

Badania

6.1. Wprowadzenie i metodologia

Przetwarzanie danych osobowych stanowi istotny element aktywności człowieka w cyberprzestrzeni. Zapewnienie bezpieczeństwa danych osobowych gwarantuje użytkownikom swobodne i nieskrępowane poruszanie się w cyberprzestrzeni pozwalające na korzystanie z wybranych stron, bez potrzeby martwienia się, że przekazywane dane będą wykorzystane w celach przestępczych. Cyberprzestrzeń stała się miejscem podatnym na naruszenia danych osobowych. Dzieje się tak między innymi dlatego, że użytkownicy nie weryfikują ADO, którym przekazywane są dane osobowe, wyrażają „na wszystko" zgodę, byle tylko móc skorzystać z określonej usługi. Oszuści z kolei czerpią korzyści z nieświadomości i łatwowierności użytkowników, najczęściej w postaci ich danych osobowych. W konsekwencji do naruszeń dochodzi bardzo często nie tylko z winy użytkownika, który nierozważnie zamieszcza swoje dane, nie weryfikuje odbiorcy danych, ale także na skutek działań przestępczych, takich jak phishing, pharming. W opinii autora działania państwa zmierzające do zapewnienia bezpieczeństwa w cyberprzestrzeni są niewystarczające, w związku z tym na użytkownikach spoczywa większa odpowiedzialność i troska o zapewnienie swoim danym osobowym bezpieczeństwa. Użytkownicy, chcąc chronić własne dane osobowe powinni dysponować wiedzą nie tylko na temat praw, jakie przysługują im w cyberprzestrzeni, ale także metod ochrony przed naruszeniami. Za sprawą rozporządzenia 2016/679 ponownie podjęto dyskusję nad bezpieczeństwem w cyberprzestrzeni, głównie w kontekście stosowanych zabezpieczeń. Nowe przepisy wielu przedsiębiorcom uzmysłowiły, jak ważne jest

dbanie o dane osobowe klientów, a klientom, że mają prawo decydować, komu i w jakim zakresie udostępniają dane oraz to, że mają wpływ na proces przetwarzania ich danych. Czy wraz z wejściem w życie rozporządzenia 2016/679 wzrosła świadomość ludzi na temat zagrożeń w cyberprzestrzeni?

W badaniu wykorzystano kwestionariusz ankietowy w formie papierowej, składający się z 24 pytań zamkniętych wielokrotnego wyboru. Ankietowani pisemnie odpowiadali na pytania z kwestionariusza. Badanie zostały przeprowadzone wśród 340 studentów studiów stacjonarnych i niestacjonarnych I i II stopnia w dwóch uczelniach wyższych w Warszawie. Wśród ankietowanych jedną trzecią stanowiły kobiety. Kwestionariusze ankietowe były wypełniane w okresie od kwietnia do listopada 2018 r. przez studentów kierunków: prawo, pedagogika, bezpieczeństwo. Ankietowani to osoby, które na co dzień korzystają z Internetu nie tylko do celów zawodowych, ale i prywatnych. Wszyscy zadeklarowali, że posiadają własne urządzenie, za pomocą których logują się do Internetu.

Za pomocą ankiety przeprowadzono zarówno badania jakościowe, jak i ilościowe. Miały one na celu przybliżenie wiedzy na temat sposobu przetwarzania danych osobowych w cyberprzestrzeni oraz poziomu świadomości i wiedzy dotyczącej bezpieczeństwa tego procesu. Wyniki badań ilościowych zostały przedstawione w formie diagramów kołowych.

6.2. Cel badania

Podstawowym celem badania była diagnoza i analiza wiedzy, i świadomości wybranej grupy użytkowników na temat procesu przetwarzania danych osobowych w cyberprzestrzeni oraz metod, jakimi użytkownicy posługują się w celu zapewnienia bezpieczeństwa w tym obszarze. Wraz z rozwojem dostępu do Internetu użytkownicy coraz częściej korzystają nie tylko z komputerów, ale także laptopów, smartfonów czy tabletów. Badanie ma na celu zweryfikowanie za pośrednictwem, jakich urządzeń najczęściej przekazują dane osobowe. Istotne z punktu widzenia przeprowadzonego badania jest poznanie rodzaju stosowanych przez nich zabezpieczeń cyberprzestrzeni. Często zdarza się bowiem, że użytkownicy mają świadomość stosowania programów antywirusowych oraz firewalla na komputerach, ale zapominają o stosowaniu podobnych rozwiązań na telefonach czy tabletach.

6.2.1. Cele szczegółowe

1. Zbadanie, czym dla ankietowanych jest prywatność w cyberprzestrzeni oraz poznanie, w jaki sposób ją zachowują.

2. Poznanie, czy zdaniem ankietowanych możliwa jest anonimowość w cyberprzestrzeni.
3. Zdiagnozowanie poziomu wiedzy ankietowanych na temat zagrożeń w cyberprzestrzeni.
4. Poznanie okoliczności, w których najczęściej decydują się na przekazanie ADO danych osobowych w Internecie.
5. Zbadanie stopnia aktywności respondentów na portalach społecznościowych oraz poznanie zakresu przekazywanych tam danych osobowych.

Diagram 1. **Wielkość miasta, z którego pochodzą ankietowani**

Większość ankietowanych: 59% stanowiły osoby pochodzące z miast o zaludnieniu powyżej 100 tysięcy mieszkańców, 23,5% stanowiły osoby z miast od 21 tysięcy do 100 tysięcy mieszkańców, a 18% ankietowanych pochodziła z miast poniżej 20 tysięcy mieszkańców.

Diagram 2. **Płeć ankietowanych**
Wśród ankietowanych jedną trzecią stanowiły kobiety.

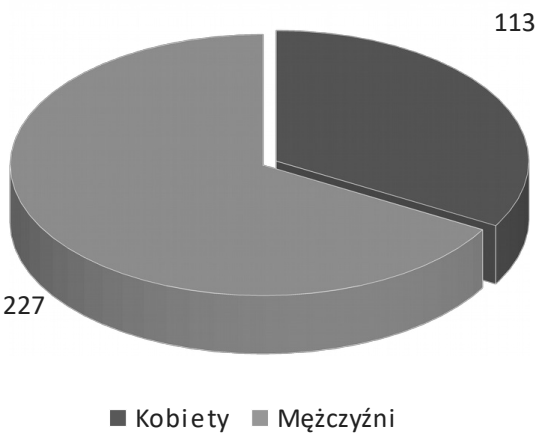


Diagram 3. **Wiek ankietowanych**
Największą grupę ankietowanych: 39% stanowiły osoby pomiędzy 20–30 rokiem życia, 32% to osoby w wieku 31–40 lat, 19% to osoby pomiędzy 41–50 rokiem życia, a tylko 9% stanowiły osoby powyżej 50 roku życia.

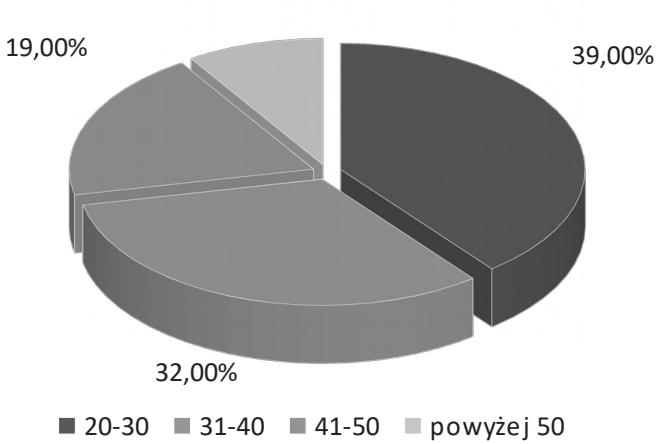
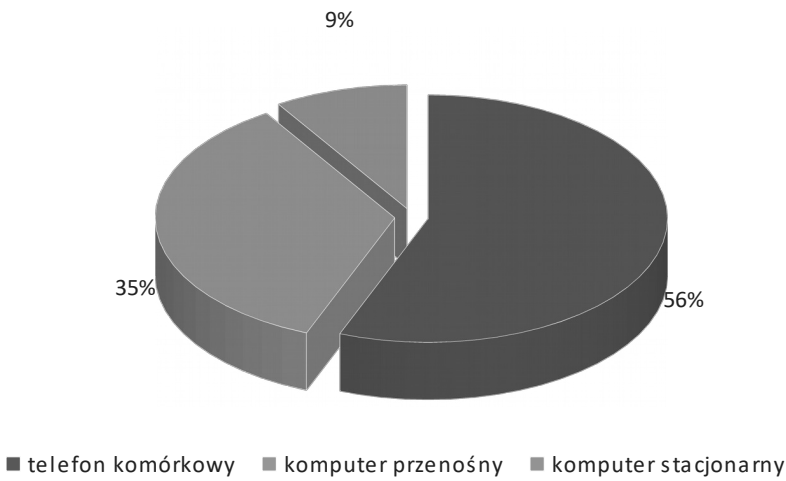


Diagram 4. **Za pomocą jakiego urządzenia najczęściej korzystasz, logując się do Internetu?**



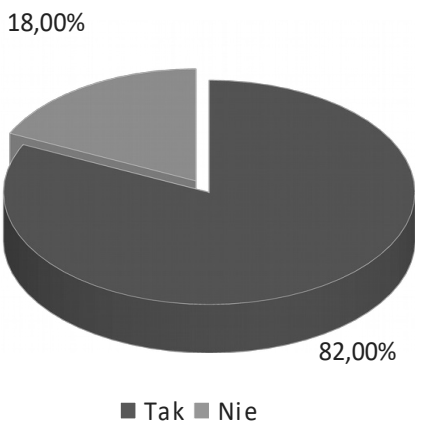
Postęp technologiczny umożliwia użytkownikom korzystanie z Internetu niezależenie od miejsca, w jakim się znajdują. Dzieje się tak, ponieważ logowanie możliwe jest nie tylko za pośrednictwem komputerów, ale także tabletów czy smartfonów. Te ostatnie coraz częściej wypierają tradycyjne komputery, przede wszystkim dlatego, że są znacznie mniejsze i praktyczniejsze, a dostawcy usług każdego dnia starają się uatrakcyjnić funkcjonalność tych urządzeń. Celem pytania było poznanie, za pomocą jakich urządzeń ankietowani najczęściej korzystają, logując się do Internetu. Pytanie to będzie istotne z punktu widzenia bezpieczeństwa przetwarzania danych osobowych za pośrednictwem tych urządzeń oraz wykorzystywanych w tych urządzeniach zabezpieczeniach.

Z przeprowadzonych badań wynika, że ankietowani są czynnymi użytkownikami Internetu. Najczęściej logują się do Internetu za pomocą telefonu komórkowego (56%) oraz komputerów przenośnych (35%). Znacznie rzadziej za pośrednictwem komputerów stacjonarnych (9%). Żaden z ankietowanych nie wskazał tabletu jako urządzenia, na którym najczęściej loguje się do Internetu. Telefony komórkowe są nieodłącznym elementem naszego życia. Już dawno przestały pełnić swoją podstawową funkcję, jaką jest odbieranie i wykonywanie połączeń telefonicznych. Za sprawą postępu technologicznego telefony komórkowe stały się nośnikiem wielu danych osobowych (książka telefoniczna, poczta e-mail, bankowość elektroniczna.

Ankietowani potwierdzili, że wielkość oraz możliwości technologiczne urządzenia są kluczowymi elementami przesądzającymi, o tym że telefony komórkowe (w tym w szczególności smartfony) stały się najpopularniejszym urządzeniem za pośrednictwem, którego pozostajemy aktywni w cyberprzestrzeni.

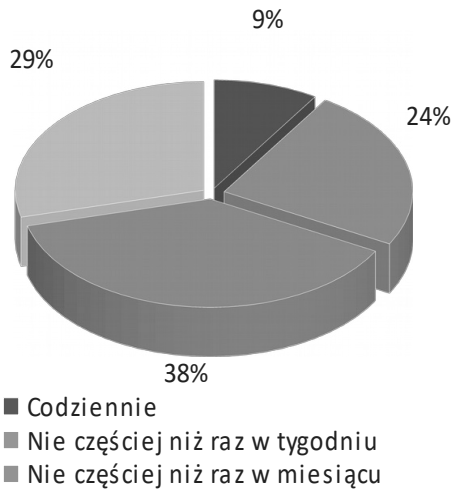
Diagram 5. **Czy jesteś czynnym użytkownikiem portali społecznościowych?**

Przeważająca większość ankietowanych, aż 82% zadeklarowała, iż jest użytkownikiem portali społecznościowych.



Powstanie portali społecznościowych miało istotne znaczenie z punktu widzenia przetwarzania danych osobowych w cyberprzestrzeni. Za ich sprawą nastąpiło bowiem udostępnianie na szeroką skalę nie tylko danych bezpośrednio identyfikujących osobę fizyczną, takich jak: imię i nazwisko, adres zamieszkania, numer telefonu, adres e-mail, wizerunek, ale także danych pośrednio identyfikujących osobę fizyczną, w tym jej zainteresowań, lokalizacji, powiązań z innymi osobami. Skupienie tak szerokiego zakresu danych osobowych w jednym miejscu może być poważnym zagrożeniem dla bezpieczeństwa tych danych. Ponadto za sprawą portali społecznościowych następuje udostępniane danych na szeroką skalę, co dodatkowo zwiększa ryzyko wystąpienia zagrożenia. Celem pytania było poznanie, czy ankietowani chętnie korzystają z portali społecznościowych oraz jaki zakres danych udostępniają za ich pośrednictwem.

Diagram 6. **Jak często zamieszczasz posty na portalach społecznościowych?**

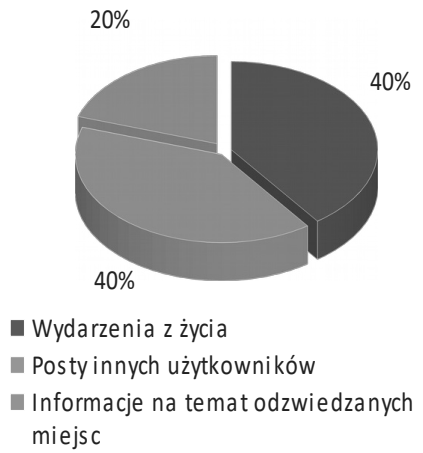


Wśród aktywnych użytkowników portali społecznościowych tylko 9% codziennie zamieszcza posty na swoim profilu. 38% ankietowanych zamieszcza posty nie częściej niż raz w miesiącu, a 29% zadeklarowało, że nigdy nie zamieszcza postów. Na podstawie tego można wnioskować, że chociaż ankietowani są częstymi użytkownikami portali społecznościowych, to jednak ich aktywność ma charakter bierny. Poprzez aktywne korzystanie z portali społecznościowych autor ma na myśli komentowanie, udostępnianie, lajkowanie postów innych użytkowników, zaś za biernego użytkownika uważa takiego, który wyłącznie obserwuje lub przegląda zamieszczane treści, nie wykazując żadnej innej czynności. Ankietowani znacznie częściej decydują się przeglądać informacje na temat innych użytkowników niż samodzielnie zamieszczać informacje na swój temat.

Diagram 7. **Jakiego typu posty zamieszczasz na portalach społecznościowych?**

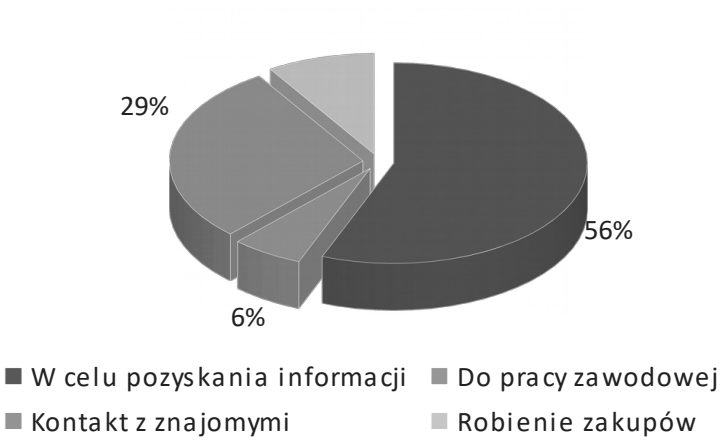
Portale społecznościowe zmieniły oblicze Internetu, który wykorzystywany był najczęściej jako źródło informacji. Dzięki portalom społecznościowym możliwe stało się dzielenie prywatnymi aspektami życia użytkowników z innymi. Ciekawość jest naturalną cechą człowieka, interesuje nas życie innych osób. Celem pytania było ustalenie, czy ankietowani chętnie dzielą się prywatnymi aspektami swojego życia z innymi

oraz jakie informacje na swój temat udostępniają ankietowani innym użytkownikom portali społecznościowych.



Wśród użytkowników, którzy zadeklarowali aktywność na portalach społecznościowych: 40% najczęściej zamieszcza posty dotyczące wydarzeń z ich życia, jak np. sukcesy dzieci, informacje o nowych zakupach, nowym wyglądzie; 40% użytkowników udostępnia posty innych użytkowników, a tylko 20% chętnie dzieli się informacjami na temat odwiedzanych przez siebie miejsc.

Diagram 8. **Do czego najczęściej wykorzystujesz Internet?**



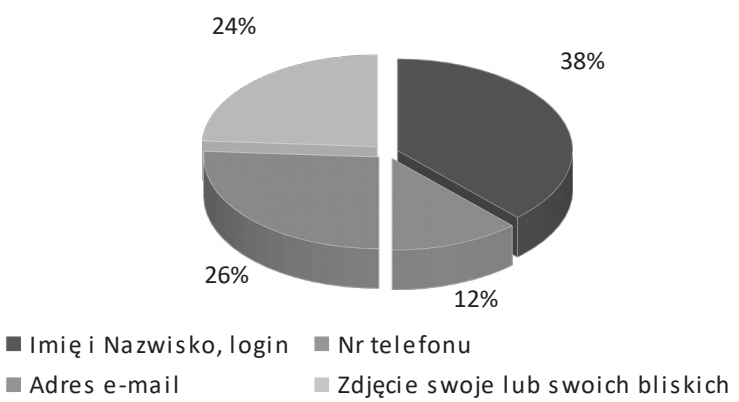
Różnorodność aplikacji, narzędzi, stron internetowych i informacji dostępnych w Internecie determinuje użytkowników do przenoszenia swojej

aktywności w cyberprzestrzeń. Umożliwia ona nawiązywanie kontaktów z nieograniczoną liczbą osób niezależnie od miejsca, w którym znajduje się dana osoba. Za sprawą nowoczesnych urządzeń możliwe stało się korzystanie w Internetu praktycznie z dowolnego miejsca o każdej porze dnia i nocy. Pytanie ma pomóc w poznaniu okoliczności i celu, w jakim ankietowani najczęściej sięgają do zasobów internetowych.

56% ankietowanych najczęściej wykorzystuje Internet w celu pozyskania interesujących go informacji, 29% ankietowanych w celu kontaktu ze znajomymi, 6% uznało, że Internet jest im najczęściej potrzebny w pracy zawodowej, 9% wykorzystuje go do robienia zakupów. Żaden z ankietowanych nie zadeklarował, że najczęściej korzysta z Internetu w celu udziału w różnego rodzaju forach internetowych.

Badania potwierdzają, że Internet nadal odgrywa istotną funkcję informacyjną, chociaż coraz częściej wykorzystywany jest także jako forma kontaktu ze znajomymi czy narzędzie ułatwiające poznanie nowych osób. Potwierdzają to także wyniki badania dotyczące liczby ankietowanych, który są uczestnikami portali społecznościowych. Internet wykorzystywany jest także chętnie przez ankietowanych do robienia zakupów lub pracy zawodowej, chociaż popularność tych dwóch ostatnich jest na znacznie niższym poziomie.

Diagram 9. **Jakie dane przekazujesz najczęściej przez Internet?**



Internet stał się narzędziem, które ułatwia i przyśpiesza pracę. Stanowi także źródło licznych zagrożeń, przez co wielu użytkowników niechętnie udostępnia dane osobowe przez Internet, bojąc się, komu je w rzeczywistości

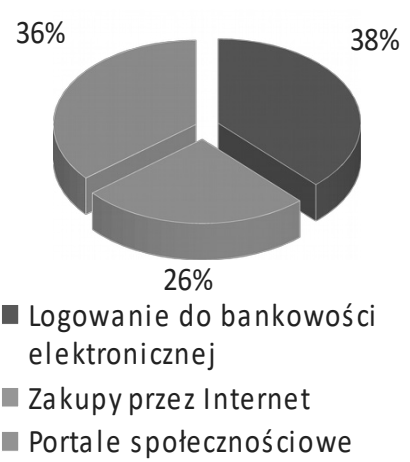
przekazuje. Celem pytania było ustalenie, jakie dane osobowe ankietowani najczęściej przekazują za pośrednictwem Internetu oraz w jakich okolicznościach.

Najczęściej ankietowani za pośrednictwem Internetu przekazują dane osobowe w zakresie: imienia i nazwiska lub loginu – 38%, adresu e-mail – 26%, zdjęć z wizerunkiem swoim lub swoich najbliższych – 24%, numeru telefonu – 12%.

Katalog udostępnianych danych należy zaliczyć do podstawowego, najczęściej wykorzystywanego zestawu danych osobowych. Podobnym zakresem danych posługujemy się w życiu zawodowym, wymieniając się wizytówkami czy zamieszczając informacje na swój temat w witrynach internetowych. Żadna z podanych danych nie stanowi szczególnej kategorii danych osobowych, których przekazanie wymagałoby od ADO zastosowania podwyższonych standardów bezpieczeństwa.

Diagram 10. **Przy jakiej okazji najczęściej przekazujesz swoje dane?**

Zakres udostępnianych danych osobowych jest ściśle związany z miejscem, gdzie dane osobowe przekazujemy. Ankietowani zadeklarowali, że najczęściej dane te przekazywane są przy okazji logowania się do bankowości elektronicznej – 38%, logowania się na portale społecznościowe – 36%, zakupów przez Internet – 26%.



Miejsce udostępniania danych osobowych jest spójne z tym, co ankietowani zadeklarowali we wcześniejszych pytaniach i w jakim celu w ogóle wykorzystują Internet. Żadna ze wskazanych form aktywności nie wymaga od ankietowanych przekazywania szczególnej kategorii danych. Niemniej

jednak zarówno przy logowaniu się do bankowości elektronicznej, jak i robieniu zakupów przez Internet dla ważności transakcji niezbędne jest podanie prawdziwych danych w przeciwieństwie do portali społecznościowych, gdzie istnieje możliwość posłużenia się nieprawdziwymi danymi.

Diagram 11. **Jak często robisz zakupy przez Internet?**

Przeniesienie aktywności użytkowników w cyberprzestrzeń znalazło również potwierdzenie wśród ankietowanych. Aż 47% ankietowanych zadeklarowało, iż robi zakupy przez Internet co najmniej raz w miesiącu, 29% nie częściej niż raz na pół roku, 15% ankietowanych nigdy nie robiło zakupów przez Internet, a 8% ankietowanych robi zakupy regularnie raz w tygodniu. Niewątpliwe ta forma jest atrakcyjna, ponieważ pozwala zaoszczędzić czas i pieniądze. Celem pytania było ustalenie częstotliwości robienia zakupów przez Internet, co wiąże się bezpośrednio z częstotliwością przekazywanych danych osobowych.

Robienie zakupów przez Internet jest atrakcyjną formą pozwalającą na zaoszczędzenie czasu oraz niejednokrotnie pieniędzy (często zakupy przez Internet są tańsze), niemniej jednak wymagają od kupującego przekazania pakietu danych osobowych, takich jak imię, nazwisko, adres zamieszkania, numer telefonu. Decydując się na zakupy online warto zweryfikować, czy ADO, któremu przekazujemy dane, wymusza udzielenie zgód lub czy na stronie internetowej w ogóle umieszcza informacje na temat sposobu przetwarzania danych osobowych.

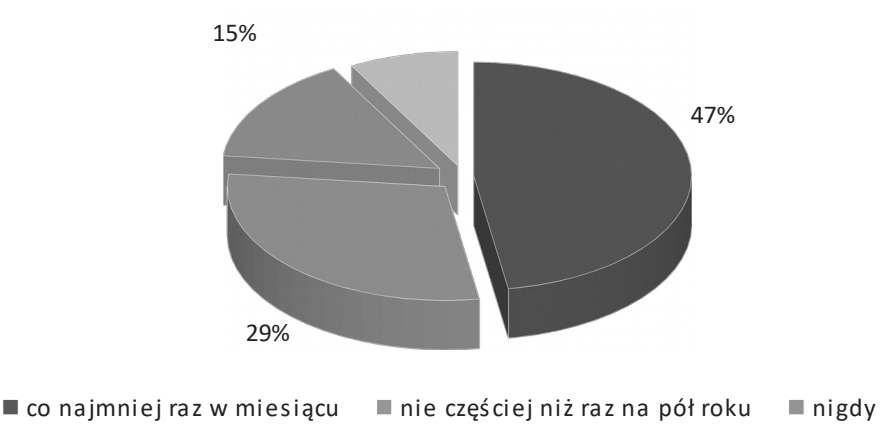
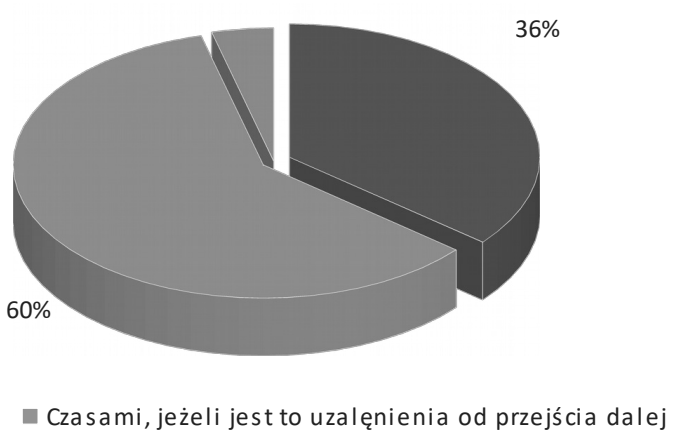


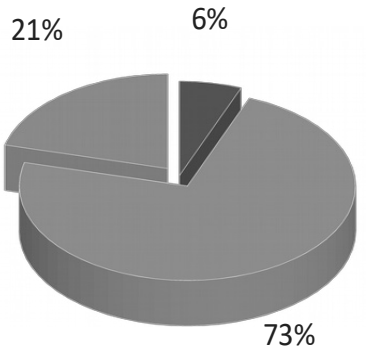
Diagram 12. **Czy wyrażasz zgodę na profilowanie?**



Od wielu lat ADO wykorzystują nowoczesne rozwiązania technologiczne, aby skuteczniej dotrzeć do klientów, oferując im towary i usługi dostosowane do ich potrzeb. W tym celu zbierają informacje na temat aktywności użytkowników w Internecie, odwiedzanych przez nich stron czy kupowanych produktów. Na podstawie zebranych informacji przygotowywane są reklamy dedykowane konkretnym potrzebom użytkowników. Celem pytania było ustalenie, czy ankietowani, robiąc zakupy przez Internet kierują się sugestiami reklam behawioralnych, jaki jest ich stosunek do tych reklam, czy traktują je pozytywnie jako podpowiedź, czy negatywnie jako ograniczające ich prawo do wyboru oraz prywatności.

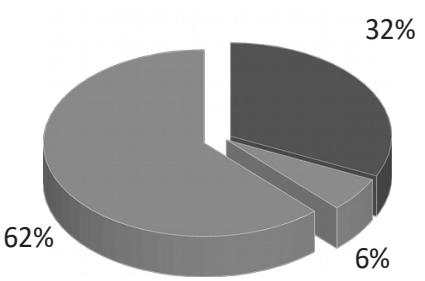
Większość ankietowanych, 60% zadeklarowała, że nie wyraża zgody na profilowanie. Na tej podstawie można uznać, że ankietowani nie akceptują zbierania informacji na ich temat przez dostawców usług. W tym kontekście wejście w życie rozporządzenia 2016/679 oraz przepisów dotyczących e-privacy należy uznać za właściwy krok, bowiem nakierowane są one na zwiększenia ochrony prawnej użytkowników w tym obszarze. Na podstawie kolejnego pytania można ponadto wnioskować, że ankietowani chcą samodzielnie decydować o wyborze towarów lub usług.

Diagram 13. **Jak oceniasz wyświetlanie reklam dedykowanych Twoim potrzebom?**



Na pytanie, w jaki sposób ankietowani oceniają wyświetlanie reklam dedykowanych ich potrzebom 73% wskazało, że nie korzysta z reklam podsyłających im produkty w ten sposób, 6% uznało, iż są one pomocne i nie przeszkadzają im, 21% ankietowanych przyznało się, że zastanawiają się, skąd reklamodawcy wiedzą, czego ankietowany szuka w sieci.

Diagram 14. **Wyrażanie zgody na przetwarzanie danych osobowych**



Wraz z wejściem w życie rozporządzenia 2016/679 wielu ADO zostało zmuszonych do zmiany sposobu zbierania zgód od osób, których dane dotyczą. Niejednokrotnie ich praktyki w tym zakresie były niezgodne z prawem. Wymuszanie zgód, blokowanie transakcji, umieszczanie oświadczeń woli na dole strony drobnym drukiem to tylko nieliczne niewłaściwe praktyki stosowane przez ADO. Proces przetwarzania danych odbywał się przez to niezgodnie z prawem. Wejście w życie rozporządzenia 2016/679 zmusiło ADO do zmiany tych praktyk. Teraz na każdy cel czy kanał komunikacji muszą zostać odebrane odrębne, niezależne zgody. To zaś zniechęca wielu użytkowników, ponieważ wydłuża proces dokonywania transakcji. Często klauzule zgód pisane są trudnym prawniczym językiem, co dodatkowo zniechęca użytkowników do składania oświadczeń woli. Celem pytania było poznanie opinii ankietowanych na temat składania oświadczeń woli elektronicznie.

Z przeprowadzonych badań wynika, że 32% dokładnie czyta, na co wyraża zgodę przez Internet, 62% ankietowanych kieruje się zasadą „na nic nie wyrażam zgody", chyba że muszę, a 6% ankietowanych odznacza zgody, w ogóle ich nie czytając.

Przedstawione wyniki wskazują, że ankietowani w przeważającej większości nie odznaczają fakultatywnych zgód na przetwarzanie danych osobowych. Te zaś najczęściej dotyczą ofert marketingowych i handlowych. Na tej podstawie można przypuszczać, że ankietowani nie chcą utrzymywać kontaktów z ADO w celu dowiedzenia się o nowych produktach i usługach przez nich oferowanych, co bardzo często wiąże się z dodatkową komunikacją przez telefon, e-mail czy SMS. Tylko 32% czyta dokładnie to, na co wyraża zgodę. Powodem tak niskiej aktywności ankietowanych w tym obszarze może być fakt rozbudowania po maju 2018 r. klauzul zgód. Wiąże się to z poświęceniem dodatkowego czasu na przeczytanie i odznaczenie kilku (najczęściej 3–6) checkboxów. Może też być oznaką niskiej świadomości i wiedzy ankietowanych w tym obszarze.

Diagram 15. **Jak często zmieniasz hasło do komputera?**

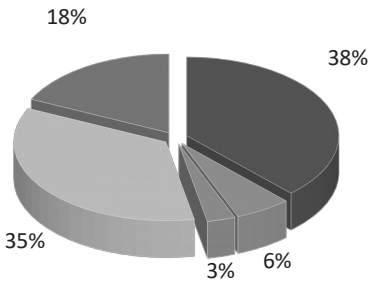
Pytanie dotyczące częstotliwości zmiany hasła w komputerze miało pokazać świadomość użytkowników na temat zagrożeń w cyberprzestrzeni. Chociaż nie ma wytycznych wskazujących, jak często należy zmieniać hasło logowania do komputera w literaturze przedmiotu podkreśla się, że częste jego zmienianie (co 3 miesiące w zależności od poziomu skomplikowania hasła) przyczynia się do podniesienia poziomu bezpieczeństwa użytkownika w cyberprzestrzeni. Celem pytania był ustalenie, jaka jest świadomość ankietowanych w tym zakresie.

W opinii autora największy wpływ na zapewnienie bezpieczeństwa w cyberprzestrzeni mają sami jej użytkownicy. Tymczasem z przeprowadzonych badań wynika, że 47% ankietowanych w ogóle nie zmienia hasła logowania do komputera, 41% robi to nie częściej niż co 3 miesiące, a tylko 12% ankietowanych zadeklarowało, że zmienia hasło logowania do komputera raz w miesiącu.

Nie ulega wątpliwości, iż ustawienie hasła dostępu do komputera stanowi podstawową metodę jego zabezpieczenia. Przed wejściem w życie rozporządzenia 2016/679 przepisy zobowiązywały do zmiany hasła co 30 dni. W konsekwencji wiele osób co miesiąc powielało to samo hasło, bądź stosowało dwa zamiennie. Zdarzały się także sytuacje, w których pracownicy zapisywali hasła na kartach przylepionych na ekranie komputera. Te praktyki przeczą idei stosowania haseł zabezpieczeń i w praktyce wywołują podobny skutek jak niestosowanie haseł dostępu. Prawodawca unijny w przepisach

rozporządzenia 2016/679 dał narzędzia do stosowania takiego rodzaju zabezpieczeń, jakie uznamy na najwłaściwsze i najlepsze, a nie ulega wątpliwości, że stosowanie haseł dostępu stanowi jedną z tych metod.

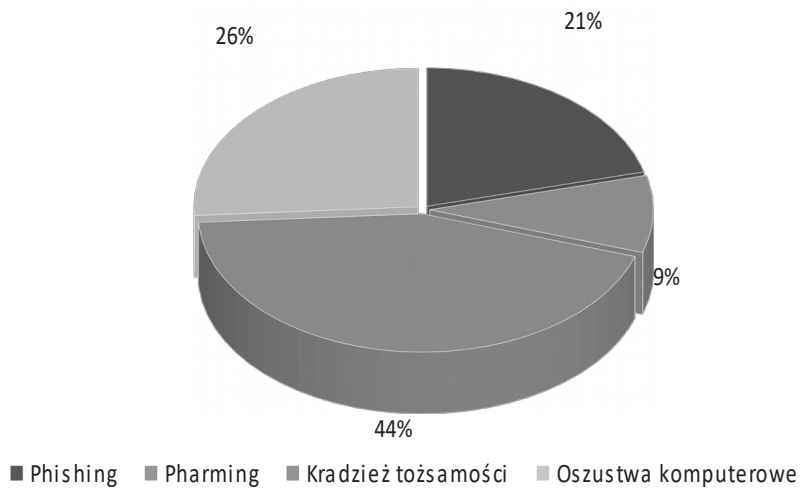
Diagram 16. **Poziom bezpieczeństwa w cyberprzestrzeni**



Wiele w ostatnim czasie mówi się w mediach na temat bezpieczeństwa w cyberprzestrzeni. Prowadzone kampanie społecznościowe mają przyczynić się do zwiększenia świadomości użytkowników na temat zagrożeń w tym obszarze. Tymczasem każdego dnia dowiadujemy się o nowych incydentach, których ofiarą padają nie tylko pojedyncze osoby fizyczne, ale także duże firmy czy państwa. Celem pytań dotyczących bezpieczeństwa w cyberprzestrzeni było ustalenie poziomu wiedzy ankietowanych na temat zagrożeń w cyberprzestrzeni, sposobów walki z zagrożeniami, poziomu poczucia bezpieczeństwa ankietowanych w cyberprzestrzeni.

Oceniając poziom bezpieczeństwa w cyberprzestrzeni 38% ankietowanych ma świadomość, że jesteśmy bardziej narażeni na zagrożenia w niej niż w świecie realnym. 18% ankietowanych uznało, że zagrożenia w cyberprzestrzeni są groźniejsze niż te w realnym świecie. Tylko 6% ankietowanych uważa, że zagrożenia w cyberprzestrzeni dotyczą państw, a nie jednostek. Zaledwie 3% ankietowanych uważa, że nasze państwo zapewnia wystarczające bezpieczeństwo obywateli w cyberprzestrzeni. Znacznie więcej ankietowanych, bo 35% uważa, że społeczeństwo międzynarodowe nie zapewnia wystarczającej ochrony w cyberprzestrzeni.

Diagram 17. **Które z zagrożeń Twoim zdaniem występują najczęściej w cyberprzestrzeni w kontekście przetwarzania danych osobowych?**



Ogólna wiedza na temat zagrożeń w cyberprzestrzeni może okazać się niewystarczająca w walce z nimi. Dlatego też zapytano ankietowanych, które zagrożenia występują ich zdaniem najczęściej.

Większość ankietowanych – 91% zadeklarowała, że nie padła ofiarą kradzieży tożsamości w cyberprzestrzeni, bądź nie jest tego świadoma. 9% ankietowanych przyznało, że padło ofiarą kradzieży tożsamości. Jednocześnie 44% ankietowanych uznało kradzież tożsamości za najczęściej występujące zagrożenie w cyberprzestrzeni. 21% ankietowanych uznało phishing za najczęściej występujące zagrożenie w cyberprzestrzeni, 26% – oszustwa komputerowe, a 9% – pharming.

Diagram 18. **Czy padłeś kiedyś ofiarą kradzieży tożsamości w kontekście przetwarzania danych osobowych?**

Chociaż kradzież tożsamości zaliczana jest do najczęstszych przestępstw w cyberprzestrzeni w kontekście przetwarzania danych osobowych użytkowników, aż 91% ankietowanych zadeklarowało, iż dotychczas nie padło ofiarą tego przestępstwa.

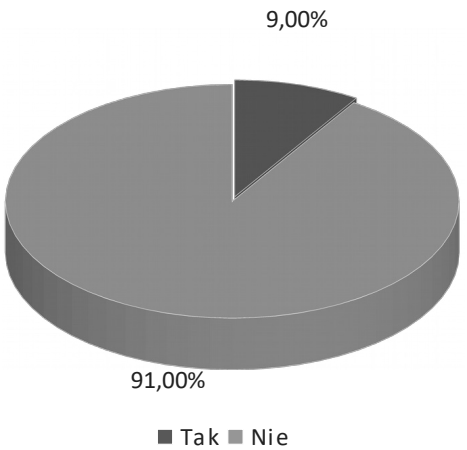
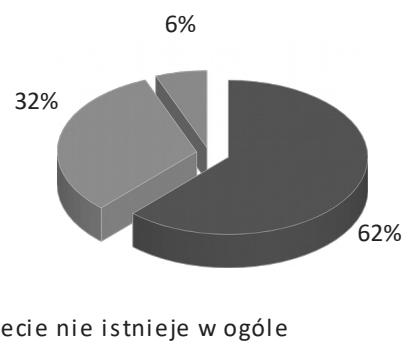


Diagram 19. **Prywatność w Internecie**



Często użytkownicy mają poczucie, że Internet zapewnia im anonimowość oraz prywatność. Sprzyja temu sam charakter wirtualnego świata, w którym w przeciwieństwie do świata rzeczywistego możemy posługiwać się

nieprawdziwym imieniem, nickiem czy pseudonimem. Wraz z rozwojem portali społecznościowych użytkownicy coraz chętniej dzielą się informacjami na temat prywatnych aspektów swojego życia. Tymczasem prywatność w sieci jest niezwykle ważnym elementem bezpieczeństwa w cyberprzestrzeni. Celem pytania było poznanie zdania ankietowanych na temat prywatności w Internecie w kontekście tego, czy w ogóle jest możliwa, co dla nich oznacza oraz w jaki sposób można ją zapewnić w cyberprzestrzeni.

Większość ankietowanych ma świadomość, że Internet nie zapewnia użytkownikom anonimowości, zaledwie 6% jest innego zdania. Jednocześnie na pytanie, czym jest dla ciebie prywatność w Internecie 62% uznało, że prywatność w Internecie w ogóle nie istnieje, 32% ankietowanych zaznaczyło, że prywatność utożsamiają z prawem decydowania o tym, co czytają i jakie informacje zamieszczają w Internecie, a tylko 6% uznało, iż prywatność w Internecie jest przywilejem.

Diagram 20. **Czy w Internecie możliwe jest zapewnienie sobie prywatności?**

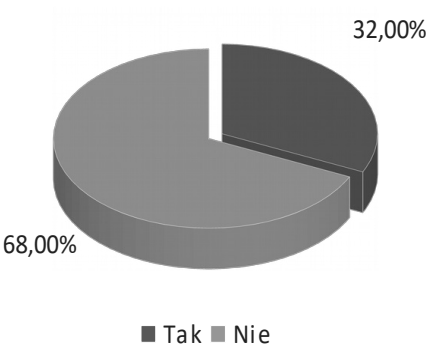
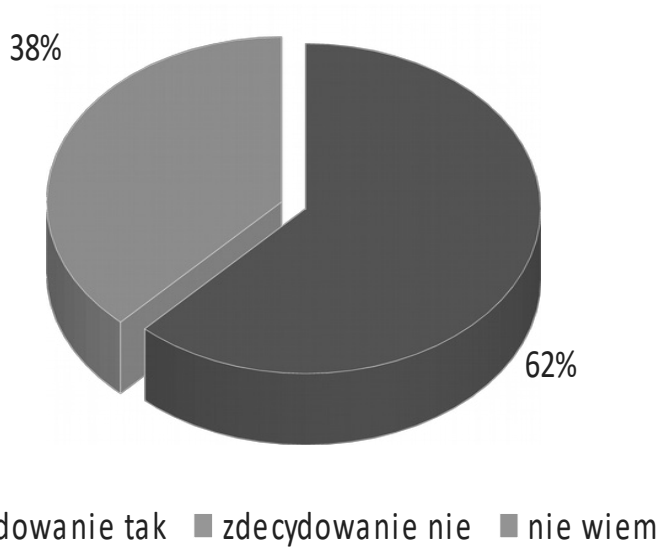


Diagram 21. **Czy wejście w życie rozporządzenia 2016/679 zwiększy bezpieczeństwo w Internecie?**

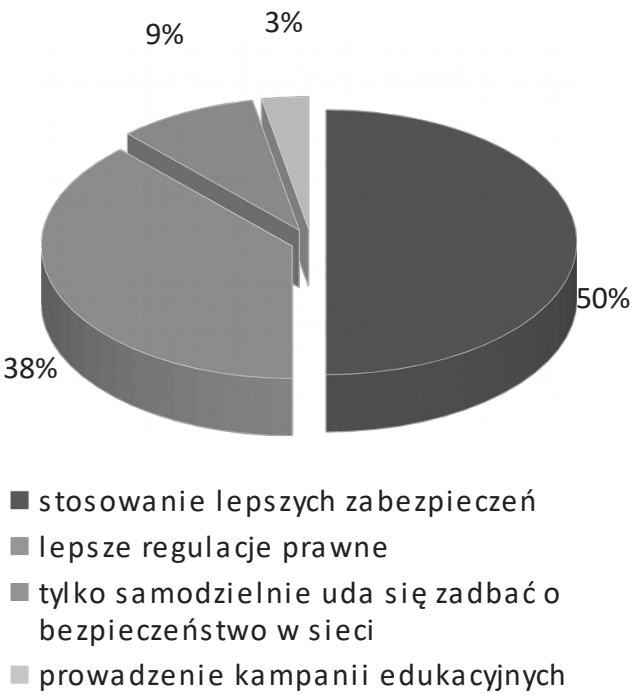


Podstawowym celem rozporządzenia 2016/679 było zapewnienie osobom, których dane dotyczą, ochrony prawnej w procesie przetwarzania danych osobowych w szczególności w cyberprzestrzeni. Poprzednio obowiązująca dyrektywa 95/46/WE nie gwarantowała należytej ochrony w tej przestrzeni ze względu na fakt, że w czasie, kiedy przygotowywano jej tekst rozwój technologiczny nie był na tak rozwiniętym poziomie. W związku z tym, przez dłuższy czas obowiązujące przepisy nie spełniały swojej funkcji, bowiem nie gwarantowały osobom, których dane dotyczą, odpowiedniego poziomu ochrony. Rozporządzenie 2016/679 w przeciwieństwie do dyrektywy 95/46/WE nakierowane jest w znacznie większym stopniu na zapewnienie ochrony prawnej osób fizycznych w cyberprzestrzeni. Chociaż rozporządzenie 2016/679 weszło w życie 25 maja 2018 r. wielu ADO przygotowywała się na zmiany znacznie wcześniej. Celem pytania było poznanie, czy ankietowani odczuli zmianę związaną z wejściem w życie nowych przepisów. Czy rozporządzenie 2016/679, zgodnie z tym co zapowiadał prawodawca unijny, rzeczywiście przyczyniło się do poprawy bezpieczeństwa procesu przetwarzania danych w Internecie.

Na pytanie, czy wejście w życie rozporządzenia 2016/679 zwiększy zdaniem ankietowanych bezpieczeństwo w Internecie: 62% uznało, że zdecydowanie tak, a 38% miało odmienne zdanie. Żaden z ankietowanych

nie odpowiedział, że nie wie, czy wejście w życie rozporządzenia 2016/679 wpłynie na poziom bezpieczeństwa w Internecie.

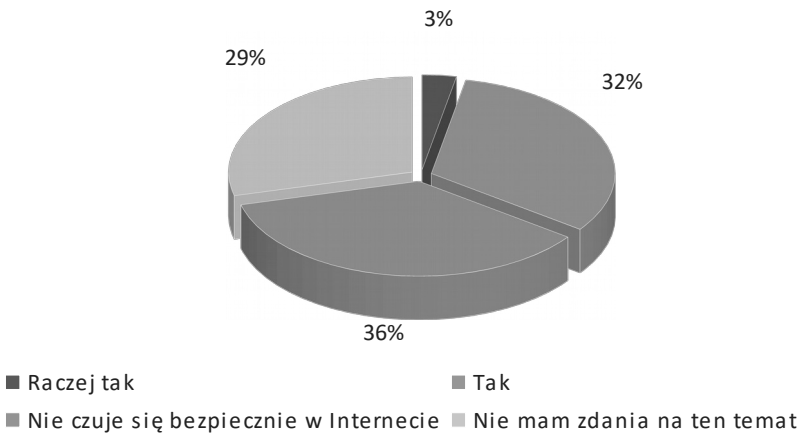
Diagram 22. **W jaki sposób zapewnić bezpieczeństwo w Internecie?**



Na pytanie, w jaki sposób zapewnić bezpieczeństwo w Internecie połowa ankietowanych uważa, że poprzez stosowanie lepszych zabezpieczeń, 38% wskazała, że należy stworzyć lepsze regulacje prawne, 9% twierdzi, że tylko samodzielnie uda się zadbać o swoje bezpieczeństwo w sieci, a 3% za najlepszą metodę zapewniania bezpieczeństwa w Internecie uważa prowadzenie kampanii edukacyjnych.

Wyniki badań wskazują, że ankietowani kładą większy nacisk na jakość zabezpieczeń oraz odpowiednie regulacje prawa niż samodzielne dbanie o bezpieczeństwo. Tylko nieliczna grupa ankietowanych uznała, że kampanie społeczne mogą przyczynić się do poprawy bezpieczeństwa.

Diagram 23. **Czy czujesz się bezpiecznie w Internecie?**



Tylko 3% ankietowanych uznało, ż czują się bezpieczni w Internecie, 32% wskazało, że raczej tak, 36% zadeklarowało, że nie czują się bezpiecznie w Internecie, a 29% nie ma zdania na ten temat.

Wyniki te pokazują, że wśród ankietowanych prawie taki sam odsetek jest tych, którzy czują się bezpiecznie w cyberprzestrzeni oraz tych którzy nie czują się bezpiecznie w cyberprzestrzeni. Wyniki te pokazują, jak bardzo ankietowani są podzieleni w tej kwestii i jak różnymi kryteriami kierują się, by bezpieczeństwo to zapewnić.

6.3. Podsumowanie i wnioski z badania

W badaniu wzięło udział 340 respondentów pochodzących w większości (58%) z miast powyżej 100 tysięcy mieszkańców, 23,5% stanowiły osoby z miast od 21 tysięcy do 100 tysięcy mieszkańców, a 18% ankietowanych pochodziła z miast poniżej 20 tysięcy mieszkańców. Wśród ankietowanych jedną trzecią stanowiły kobiety. Większość ankietowanych to osoby w wieku 20–30 lat. Wszyscy ankietowani są czynnymi użytkownikami Internetu. Każdy z nich w trakcie badania dysponował własnym urządzeniem, za pośrednictwem którego mógł się logować do Internetu. Ankietowani w większości (56%) zadeklarowali, że najczęściej logują się do Internetu za pośrednictwem telefonu komórkowego. Warto przy tym zaznaczyć, że żaden z ankietowanych nie wskazał, iż loguje się do Internetu za pośrednictwem tabletu. Może to oznaczać, że tak modne kiedyś urządzenia zostały zastąpione przez znacznie mniejsze i poręczniejsze smartfony.

Aż 82% ankietowanych zadeklarowało, że korzysta z portali społecznościowych. Przedmiotem badania była chęć poznania aktywności ankietowanych w tym obszarze, nie wskazując jednak nazwy żadnego konkretnego portalu, z którego korzystają. Badania wykazały, iż aktywność ankietowanych ma charakter bierny, bowiem 29% ankietowanych zadeklarowała, że w ogóle nie zamieszcza tam żadnych postów, 38% ankietowanych robi to nie częściej niż raz w miesiącu, co należy uznać za sporadyczne, a tylko 9% zadeklarowała, że zamieszcza posty codziennie. Te zaś najczęściej dotyczą wydarzeń z ich życia codziennego (tak zadeklarowało 40% ankietowanych, którzy wskazali, że zamieszczają posty na portalach społecznościowych) lub informacji na temat odwiedzanych przez nich miejsc.

Internet przez większość ankietowanych (tak zadeklarowało 56% ankietowanych) wykorzystywany jest jako źródło informacji. 29% ankietowanych zadeklarowało, iż Internet jest im potrzebny w celu komunikacji ze znajomymi. Znacznie rzadziej niezbędny im jest do robienia zakupów lub w pracy zawodowej. Na tej podstawie można uznać, iż Internet częściej wykorzystywany jest przez ankietowanych jako źródło wiedzy lub formę komunikacji niż narzędzie do pracy.

Aktywność ankietowanych w cyberprzestrzeni przekłada się także na zakres przekazywanych przez nich danych osobowych. Z przeprowadzonych badań wynika, że ankietowani najczęściej przekazują dane osobowe w zakresie: imienia i nazwiska, adresu e-mail, numeru telefonu i wizerunku. Jest to podstawowy zakres danych osobowych, którym zazwyczaj się posługujemy. Żadna z tych danych nie jest zaliczana do szczególnej kategorii danych osobowych. Wart uwagi jest fakt, że 24% ankietowanych wskazało, że za pośrednictwem Internetu przekazuje swój wizerunek. Można przypuszczać, iż jest to związane z ich aktywnością na portalach społecznościowych, gdzie bardzo często podczas zakładania konta ADO zamieszcza informację o możliwości dołączenia swojego zdjęcia.

Zakres udostępnianych przez ankietowanych danych osobowych jest spójny z miejscem zadeklarowanym przez ankietowanych ich przekazywania. Najczęściej dane te przekazywane są przy okazji logowania się do bankowości elektronicznej – 38%, logowania się na portale społecznościowe – 36%, zakupów przez Internet – 26%. Ani przy logowaniu się do bankowości elektronicznej, ani robieniu zakupów nie jest wymagane podawanie takich danych jak PESEL, płeć czy stan zdrowia.

Chociaż robienie zakupów przez Internet zadeklarowało tylko 9% ankietowanych jako najczęstszą czynność, którą wykonują w Internecie, niemniej jednak należy uznać, że jest to atrakcyjna alternatywna dla tradycyjnej wizyty w sklepie. 47% ankietowanych zadeklarowało, iż robi zakupy raz w miesiącu, 29% nie częściej niż raz na pół roku, tylko 8% robi zakupy raz w tygodniu, a 15% nigdy nie robiło

zakupów przez Internet. Pytanie dotyczące częstotliwości robienia zakupów przez Internet jest ściśle związane z zakresem udostępnianych tam danych osobowych. Im częściej robimy zakupy za pośrednictwem Internetu, tym częściej przekazujemy swoje dane osobowe. Jeżeli robimy zakupy w sklepie internetowym po raz pierwszy, dodatkowo nie znamy wyglądu witryny internetowej może okazać się, że strona ta powstała wyłącznie po to, by pozyskiwać dane osobowe klientów, które wykorzystane zostaną w celu popełnienia przestępstwa. Warto więc, decydując się na taką formę aktywności w cyberprzestrzeni dokładnie wiedzieć, kim jest ADO oraz pamiętać o zasadzie minimalizacji danych, która w przypadku zakupów online powinna ograniczyć się do zebrania przez ADO podstawowych danych osobowych niezbędnych do ważności transakcji i wysłania produktu.

Badania wykazały, że aktywność ankietowanych w Internecie nie oznacza godzenia się na wszystkie rozwiązania technologiczne, które są tam dostępne. Większość ankietowanych zadeklarowała, że nie wyraża zgody na profilowanie. Warto w tym miejscu zwrócić uwagę na fakt, że do dnia wejścia w życie rozporządzenia 2016/679 ADO zbyt często nie pytali użytkowników o to, czy wyrażają zgodę na profilowanie, co oznacza, że większość użytkowników mogła nie mieć wiedzy, iż podlega profilowaniu. Dopiero od maja 2018 r. użytkownicy na szeroką skalę zaczęli być pytani o to, czy chcą podlegać procesom profilowania. Jak wynika z przeprowadzonego badania większość ankietowanych jednak zadeklarowała, że nie. Oznacza to, że nie chcą by towary i usługi były dostosowywane do ich profili i chcą mieć prawo samodzielnego decydowania o produktach dostarczanych im w Internecie. Potwierdziło to dodatkowo inne pytanie, z którego wynika, iż aż 73% ankietowanych nie korzysta z reklam behawioralnych.

Przetwarzanie danych osobowych związane jest z wyrażeniem zgód na przetwarzanie danych osobowych w różnych celach. Bardzo często przy tej okazji ADO chcą nawiązywać stałe relacje z klientami, oferując im dodatkowe towary i usługi. Wraz z wejściem w życie rozporządzenia 2016/679 wielu ADO zostało zmuszonych do zmiany dotychczasowych klauzul zgód na bardziej przystępne. Dodatkowo przepisy prawa wymusiły na nich zbieranie oddzielnych zgód w zależności od celu zbierania danych osobowych czy kanału komunikacji. To zaś spowodowało, że użytkownik musi zapoznać się z wieloma różnymi zgodami. Z przeprowadzonego badania wynika, że ankietowani negatywnie podchodzą do tej formy zbierania oświadczeń woli. 62% ankietowanych zadeklarowało, że w ogóle nie czyta zgód, kierując się zasadą „na nic nie wyrażam zgody". Tylko 32% ankietowanych wskazała, że dokładnie czyta, na co wyraża zgodę, a 6% odznacza zgodę na wszystko. Wyniki te mogą świadczyć o niskim poziomie wiedzy na temat procesu przetwarzania danych oraz praw przysługujących użytkownikom w cyberprzestrzeni.

Celem ankiety były zbadanie aktywności ankietowanych w cyberprzestrzeni oraz zbadania poziomu ich wiedzy na temat bezpieczeństwa procesu przetwarzania danych w Internecie. W związku z tym część pytań dotyczyła bezpośrednio metod, jakie stosują ankietowani w celu zapewnienia bezpieczeństwa w tym obszarze. Wśród nich znalazło się pytanie dotyczące częstotliwości zmiany hasła w komputerze. 47% ankietowanych zadeklarowało, iż w ogóle nie zmienia hasła logowania do komputera, 41% ankietowanych robi to nie częściej niż raz na 3 miesiąca, a tylko 12% zadeklarowało, że zmienia hasło logowania do komputera raz w miesiącu. Wyniki te wskazują, iż użytkownicy nie mają wiedzy lub świadomości, że ciągłe posługiwanie się tym samym hasłem logowania się do komputera nie zapewnia odpowiedniego poziomu ochrony, a rekomendowanym rozwiązaniem jest stosowanie częstszej zmiany hasła.

38% ankietowanych, dokonując oceny bezpieczeństwa ma świadomość, że w cyberprzestrzeni są bardziej narażeni na zagrożenia niż w świecie realnym. 35% ankietowanych uznało, iż społeczność międzynarodowa nie zapewnia im wystarczającej ochrony w tym obszarze, a 6% żyje w przeświadczeniu, że na zagrożenia są narażone państwa, a nie jednostki. Zaledwie 3% ankietowanych uznało, że państwo zapewnia wystarczający poziom bezpieczeństwa w cyberprzestrzeni. Te wyniki pokazują, że mimo wiedzy użytkowników na temat zagrożeń czyhających na nich w cyberprzestrzeni, nie mają oni wystarczającej świadomości, że sami też mogą stać się ofiarami naruszeń przez niewłaściwe postępowanie w Internecie. Ogólna wiedza na temat zagrożeń jest jednak niewystarczająca do skutecznej z nimi walki. W związku z tym ankietowani zostali poproszeni o wskazanie tych zagrożeń, które ich zdaniem występują najczęściej w związku z przetwarzaniem danych osobowych: 44% ankietowanych wskazało, iż najczęściej narażeni jesteśmy na kradzież tożsamości, 26% wskazało, że są to oszustwa komputerowe, 21% – phishing, a 9% – pharming. Na podstawie tego można wnioskować, że ankietowani mają wiedzę na temat rodzaju możliwych do wystąpienia w cyberprzestrzeni zagrożeń, mają także wiedzę na temat skali tych zjawisk. Jednocześnie 91% ankietowanych zadeklarowało, że nie padło ofiarą kradzieży tożsamości.

Istotna, jeżeli chodzi o zapewnienie bezpieczeństwa w cyberprzestrzeni, jest kwestia ich prywatności. Jak zostało zauważone w pracy wraz z upowszechnieniem się portali społecznościowych pojęcie prywatności uległo redefinicji. Chociaż badania pokazały, że większość ankietowanych jest biernym uczestnikiem portali społecznościowych i niechętnie dzieli się informacjami na swój temat, to jednak aż 62% ankietowanych uważa, że prywatność w Internecie w ogóle nie istnieje. Ci zaś, którzy myślą inaczej, prawo do prywatności utożsamiają z prawem decydowania o tym, co czytamy i jakie informacje zamieszczamy w Internecie, co powoduje

niezwykłe spłycenie wręcz bagatelizowanie problematyki prywatności. 6% ankietowanych traktuje zaś prywatność nie jako prawo, jakie im przysługuje, lecz jako przywilej, nadając mu tym samym rangę czegoś wyjątkowego.

Wejście w życie rozporządzenia 2016/679 miało zwiększyć ochronę prawną osób, których dane dotyczą, zapewniając im większy wachlarz uprawnień oraz gwarancji bezpieczeństwa w procesie przetwarzania danych osobowych. Jak wynika z przeprowadzonych badań, chociaż od wejścia w życie dokumentu nie minął jeszcze rok, ankietowani uznali, że zmiany, jakie nastąpiły po maju 2018 r. nie przyczyniły się do poprawy poziomu ich bezpieczeństwa. Tylko 32% ankietowanych uznało, że wejście w życie rozporządzenia 2016/679 przyczyniło się do poprawy poziomu ich bezpieczeństwa w procesie przetwarzania danych. Na pytanie, w jaki sposób więc zapewnić bezpieczeństwo w cyberprzestrzeni większość ankietowanych odpowiedziała, że należy stosować lepsze zabezpieczenia oraz wprowadzać lepsze regulacje prawne. 9% uznało, że tylko samodzielnie można najlepiej zadbać o swoje bezpieczeństwo. Zaledwie 3% ankietowanych twierdzi, że prowadzenie kampanii edukacyjnych może pomóc w zwiększeniu bezpieczeństwa w sieci.

Chociaż większość ankietowanych zadeklarowała swoją aktywność w Internecie, to jednak ich odczucia odnośnie do bezpieczeństwa są różne, bowiem 36% ankietowanych zadeklarowało, że nie czuje się tam bezpiecznie, jednocześnie 32% ankietowanych zadeklarowało, że czują się bezpiecznie w cyberprzestrzeni. 29% ankietowanych nie ma w ogóle zdania na ten temat.

Ankieta dotycząca bezpieczeństwa w cyberprzestrzeni

Płeć
□ kobieta
□ mężczyzna

Miejsce zamieszkania
□ miasto poniżej 20 tysięcy mieszkańców
□ miasto od 21 tysięcy do 100 tysięcy mieszkańców
□ miasto powyżej 100 tysięcy mieszkańców

Wiek
□ 20–30 lat
□ 31–40 lat
□ 41–50 lat
□ powyżej 50 lat

Z jakiego urządzenia najczęściej korzystasz, logując się do Internetu?
□ telefon
□ komputer stacjonarny
□ komputer przenośny
□ tablet

Czy jesteś czynnym użytkownikiem portali społecznościowych?
□ TAK
□ NIE

Jak często zamieszczasz posty na portalach społecznościowych?
□ codziennie
□ nie częściej niż raz w tygodniu
□ nie częściej niż raz na miesiąc
□ nigdy

Czego dotyczą zamieszczane posty?
□ wydarzeń z mojego życia, np. sukcesy dzieci, nowe ubranie, fryzura, nowe mieszkanie
□ odwiedzanych miejsc, np. restauracja, kino, teatr
□ ważnych wydarzeń społecznych, np. zaginęła osoba, zaginął pies
□ promowania własnej firmy

Jakie dane osobowe najczęściej przekazujesz przez Internet?
□ imię i nazwisko
□ numer telefonu
□ adres e-mail
□ zdjęcia ze swoim wizerunkiem lub wizerunkiem bliskich

Przy jakiej okazji najczęściej przekazujesz swoje dane przez Internet?
□ logowanie do banku
□ zakupy przez Internet
□ portale społecznościowe

Jak często robisz zakupy przez Internet?
□ częściej niż raz w tygodniu
□ co najmniej raz w miesiącu
□ nie częściej niż raz na pół roku
□ nigdy

Jak często zmieniasz hasło logowania do komputera?
□ nigdy
□ nie częściej niż co 3 miesiące
□ raz w miesiącu

Czy wyrażasz zgodę na profilowanie?
□ TAK
□ NIE
□ czasami, jeżeli jest to uzależnione od przejścia dalej

Czy wyrażając zgodę na przetwarzanie danych osobowych:
□ dokładnie czytam, na co wyrażam zgodę
□ odhaczam zgodę na wszystko bez zastanowienia
□ kieruję się zasadą „nie wyrażam na nic zgody", chyba że muszę

Czy padłeś kiedyś ofiarą kradzieży tożsamości w kontekście przetwarzania danych osobowych?
□ TAK
□ NIE

Twoim zdaniem...
□ jesteśmy bardziej narażeni na zagrożenia w cyberprzestrzeni niż w realnym świecie
□ zagrożenia w cyberprzestrzeni dotyczą państw nie jednostki
□ nasze państwo zapewnia wystarczające bezpieczeństwo obywateli w cyberprzestrzeni
□ społeczność międzynarodowa nie zapewnia wystarczającej ochrony w cyberprzestrzeni
□ zagrożenia w cyberprzestrzeni są groźniejsze niż te w rzeczywistym świecie

Które z zagrożeń Twoim zdaniem występują najczęściej w cyberprzestrzeni w kontekście przetwarzania danych osobowych?
□ phishing
□ pharming
□ kradzież tożsamości
□ oszustwa komputerowe

Czy uważasz, że w Internecie jesteś anonimowy?
□ TAK
□ NIE

W jakim celu najczęściej korzystasz z Internetu?
□ szukam informacji
□ kontakt ze znajomymi
□ jest mi potrzebny do pracy zawodowej
□ przeglądanie lub udział w forach internetowych
□ robienie zakupów

Jak oceniasz wyświetlanie reklam dedykowanych Twoim potrzebom?
□ są pomocne i nie przeszkadzają mi
□ nie korzystam z reklam podsyłających produkty w ten sposób
□ często zastanawiam się skąd reklamodawcy wiedzą, czego szukam

Czy Twoim zdaniem wejście w życie rozporządzenia 2016/679 zwiększy bezpieczeństwo w Internecie?
□ TAK
□ NIE

Czy w Internecie możliwe jest zapewnienie sobie prywatności?
□ TAK
□ NIE

Czym jest dla Ciebie prywatność w Internecie?
□ przywilejem
□ prawem decydowania o tym, co czytam i zamieszczam w Internecie
□ prywatność w Internecie nie istnieje

W jaki sposób zapewnić bezpieczeństwo w Internecie?
□ stworzyć lepsze regulacje prawne
□ stosować lepsze zabezpieczenia
□ prowadzić kampanie edukacyjne
□ samemu zadbać o swoje bezpieczeństwo w sieci

Czy czujesz się bezpieczny w sieci?
□ tak
□ raczej tak
□ nie
□ nie mam zdania

Zakończenie

Celem pracy było ocena aktywności człowieka w cyberprzestrzeni w zakresie przekazywanych danych oraz zbadanie poziomu bezpieczeństwa przetwarzanych tam danych osobowych. Umieszczane z łatwością w Internecie dane osobowe narażone są na różnego rodzaju naruszenia ze strony ADO oraz ataki cyberprzestępców. Wszystko przez różnice między światem wirtualnym a realnym.

Wraz z rozpowszechnieniem Internetu ludzie przenieśli większą część swojego życia w cyberprzestrzeń, która stała się atrakcyjna z uwagi na płynność i łatwość komunikacji. Szybko jednak okazało się, że standardy zachowania użytkowników w świecie realnym w znaczący sposób różnią się od tych występujących w świecie wirtualnym. Funkcjonowanie w cyberprzestrzeni powoduje, że nie tylko czujemy się bardziej anonimowi, ale znacznie chętniej dzielimy się informacjami na nasz temat. Cyberprzestrzeń pozwala nam na możliwość kreowania swojego wizerunku w znacznie szerszym zakresie niż dzieje się to w świecie realnym.

W cyberprzestrzeni występuje znacznie więcej danych pozwalających zidentyfikować bezpośrednio lub pośrednio osobę fizyczną niż w świecie realnym. W wirtualnym świecie, podobnie jak w świecie realnym, dochodzi do przetwarzania danych osobowych, które pozwalają na zidentyfikowanie osoby fizycznej. Dodatkowo za sprawą postępującego rozwoju technologicznego, możliwe stało się wykorzystywanie metod umożliwiających pozyskiwanie informacji na temat osób, których dane dotyczą, bez ich wiedzy, jak np. za pomocą plików cookies. Stało się tak dlatego, że bardzo długo stosowane mechanizmy prawne nie gwarantowały osobie, której dane dotyczą, skutecznej ochrony. W konsekwencji pojawiło się wiele nowych i niezwykle groźnych przestępstw, których podstawowym celem jest zebranie i niezgodne z prawem wykorzystanie danych osobowych użytkowników,

takich jak phishing czy pharming. Dzięki nim możliwa jest nie tylko kradzież tożsamości, ale także posłużenie się nią w celu popełnienia przestępstwa. Ściganie takich przestępstw jest jednak znacznie trudniejsze niż w świecie realnym, co zostało potwierdzone na podstawie przedstawionych statystyk policyjnych. Liczba cyberprzestępstw z wykorzystaniem danych osobowych wzrasta każdego roku. Jest to wynikiem zarówno niedopasowania dotychczasowych regulacji prawnych, jak i braku świadomości użytkowników sieci na temat konsekwencji związanych ze zbyt łatwym i szybkim udzielaniem informacji na swój temat.

Cyberprzestrzeń nie została przez człowieka jeszcze w pełni zbadana. Nie wiemy, czy w ogóle jest to możliwe. Nie ulega wątpliwości, iż urzekła nas swą innowacyjnością, a zarazem prostotą. W wielu przypadkach poprzez sposób funkcjonowania w cyberprzestrzeni sami narażamy się na zagrożenie. Bardzo często nie jesteśmy świadomi konsekwencji naszych zachowań. Wszystko przez to, że nie mamy pełnej wiedzy, w jakim zakresie przestrzeń ta różni się od przestrzeni rzeczywistej. Znacznie częściej narażeni jesteśmy na naruszenie danych osobowych, ponieważ cyberprzestrzeń daje przestępcom możliwość stosowania nowych, niewystępujących w realnym świecie metod pozyskiwania i gromadzenia informacji.

Z przeprowadzonych badań wynika, że przetwarzanie danych osobowych stanowi istotny element aktywności człowieka w cyberprzestrzeni, czy to na portalach społecznościowych, podczas robienia zakupów czy też logowania się do bankowości elektronicznej. Najchętniej korzystamy z Internetu za pośrednictwem smartfonów, które stały się popularniejsze od komputerów czy tabletów. W ten sposób najczęściej przekazujemy dane osobowe w zakresie imienia i nazwiska, numeru telefonu czy adresu e-mail. Rzadko decydujemy się na przekazanie za pośrednictwem Internetu takich danych, jak PESEL, adres zamieszkania czy płeć. Wyniki badań potwierdziły, że użytkownicy chętnie korzystają z usług portali społecznościowych, jednak znacznie częściej pozostają biernymi użytkownikami obserwującymi profile innych użytkowników, niż decydują się udostępniać dane dotyczące ich życia prywatnego. Ci, którzy decydują się na zamieszczanie informacji na swój temat ograniczają się najczęściej do umieszczania informacji ogólnych, np. o odwiedzanych miejscach. Chociaż popularność portali społecznościowych jest niekwestionowana – korzystanie z nich zadeklarowało 82% ankietowanych – to jednak badania ujawniły, iż najczęściej Internet wykorzystujemy jako źródło informacji o interesujących nas zagadnieniach.

Aktywność użytkowników w Internecie niestety nie przekłada się na poziom ich wiedzy na temat bezpieczeństwa w tym obszarze. Świadomość użytkowników na temat procesu przetwarzania danych osobowych w cyberprzestrzeni na podstawie przeprowadzonego badania należy ocenić negatywnie. Chociaż na podstawie

wyników badania ankietowego można wysunąć tezę, iż użytkownicy mają świadomość, że w cyberprzestrzeni są bardziej narażeni na zagrożenia niż w świecie realnym, potrafią wymienić podstawowe przestępstwa związane z niezgodnym z prawem przetwarzaniem danych osobowych, to jednak większość z nich nie ma świadomości, iż własnym (często niewłaściwym) postępowaniem mogą przyczynić się do powstania incydentu, m.in. poprzez posługiwanie się ciągle tym samym hasłem logowania się do komputera.

Niska świadomość użytkowników na temat bezpieczeństwa danych osobowych w cyberprzestrzeni widoczna jest także w zakresie udzielanych przez nich zgód na przetwarzanie danych osobowych. Z przeprowadzonego badania wynika, że większość użytkowników w ogóle nie czyta klauzul zgód i nie zaznacza checkboxów. A przecież ich obecność jest najlepszym przejawem realizacji uprawnień przysługujących na podstawie rozporządzenia 2016/679. Dodatkowo część użytkowników jest zupełnie nieświadoma, że może stać się ofiarą cyberataku, uznając, iż narażone na nie są wyłącznie państwa. Przeprowadzone badania uwidoczniły także inny istotny z punktu widzenia bezpieczeństwa problem dotyczący prywatności w cyberprzestrzeni. Aż 62% ankietowanych zadeklarowało, że ich zdaniem prywatność w Internecie w ogóle nie istnieje, a 6% traktuje ją w jako przywilej. Takie podejście może narazić nie tylko pojedynczych użytkowników, ale także administrację rządową na incydenty, które mogą stanowić istotne zagrożenie dla bezpieczeństwa informacyjnego państwa, stanowiącego integralną część bezpieczeństwa narodowego. Powszechnie wiadomo, że informacje stanowią istotny zasób każdego państwa. Te zaś dotyczące jednostek (w tym dane osobowe) są szczególnie ważne, bowiem za ich pośrednictwem jesteśmy w stanie wpłynąć na tok myślenia jednostek, manipulować opinią publiczną, wpływając na sposób jej postępowania. Działania te mogą wpłynąć na destabilizację infrastruktury krytycznej czy bezpieczeństwo gospodarcze, polityczne, bądź społeczne. Wyniki przeprowadzonego badania były podstawą do potwierdzenia postawionej w pracy hipotezy, zgodnie z którą człowiek jest znacznie bardziej narażony na naruszenie danych osobowych w cyberprzestrzeni niż w świecie realnym.

Wejście w życie rozporządzenia 2016/679 miało w znaczący sposób wpłynąć na poprawę bezpieczeństwa danych przetwarzanych w cyberprzestrzeni. Dotychczasowe rozwiązania prawne (w szczególności dyrektywa 95/46/WE) w ogóle nie przewidywały takich metod zbierania danych, jak monitoring, biometria, portale społecznościowe czy pliki cookies. Rozporządzenie 2016/679 w znaczący sposób poszerzyło także katalog praw osób, których dane dotyczą. W związku z tym zagwarantowane zostały im mechanizmy umożliwiające szybkie i łatwe dochodzenie przysługujących im praw. Na ADO nałożono obowiązek zgodnego z prawem

i legalnego przetwarzania danych osobowych. Żadne procesy gromadzenia i przetwarzania danych nie mogą odbywać się bez wiedzy i zgody osoby fizycznej, która ma mieć możliwość wyrażania jej w sposób świadomy, swobodny i dobrowolny. Wszelkie działania zmierzające do niezgodnego z prawem przetwarzania danych zagrożone są karą do 20 mln euro co z jednej strony ma być bodźcem odstraszającym, z drugiej zaś pokazuje jak cennym dobrem są dane osobowe. Niemniej jednak wszystkie te działania należy uznać za niewystarczające, bowiem z badania wynika, iż użytkownicy uważają, że wejście w życie rozporządzenia 2016/679 nie przyczyniło się w istotny sposób do poprawy bezpieczeństwa w odniesieniu do procesu przetwarzania danych osobowych w cyberprzestrzeni.

W ocenie autora dążenie do zapewnienia bezpieczeństwa w cyberprzestrzeni jest możliwe wyłącznie wówczas, gdy cała społeczność międzynarodowa zaangażuje się w tę sprawę. Jak zostało wykazane w pracy, każdego dnia w wirtualnym świecie powstają nowe zagrożenia. Oczywiście działania państw zmierzające do zapewnienia bezpieczeństwa poprzez właściwe przepisy umożliwiające ściganie i osądzenie sprawców są niezbędne, niemniej jednak w ocenie autora równie ważne są działania zmierzające do podniesienia świadomości o zagrożeniach związanych z funkcjonowaniem w cyberprzestrzeni. Mowa tu nie tylko o kampaniach społecznych, ale także o edukowaniu od najmłodszych lat dzieci, które coraz częściej stają się czynnymi użytkownikami wirtualnego świata. Wysiłki zmierzające do podniesienia wiedzy oraz świadomości wagi problemu przetwarzania danych osobowych w cyberprzestrzeni mają kluczowe znaczenie dla zapewnienia bezpieczeństwa w tym obszarze. Kampanie społeczne powinny być przeprowadzane tak, by dotrzeć do różnych grup odbiorców (dzieci, młodzieży czy osób starszych). Rosnące zaangażowanie dzieci w sieci i związane z tym zagrożenia zostały dostrzeżone, co zaowocowało ochroną prawną w przepisach rozporządzenia 2016/679. Badania ujawniły, że wiedza na temat procesu przetwarzania danych osobowych w cyberprzestrzeni nie jest na zadawalającym poziomie. Większość użytkowników Internetu posiada wyłącznie ogólną wiedzę na temat bezpieczeństwa w tym obszarze, uważając, iż państwo lub społeczność międzynarodowa są tymi, którzy w pierwszej kolejności powinni zapewniać im bezpieczeństwo.

Diagnozowana w pracy problematyka stanowi istotny wkład w rozwój nauk o bezpieczeństwie, ponieważ wskazuje, że zapewnienie bezpieczeństwa procesu przetwarzania danych osobowych w cyberprzestrzeni ma istotne znaczenie nie tylko w kontekście wobec bezpieczeństwa jednostki, ale także dla bezpieczeństwa informacyjnego państwa.

Przeprowadzone badania pokazały, że niezbędne są wielopłaszczyznowe działania, z jednej strony zmierzające do podnoszenia wiedzy użytkowników,

zapewnienia lepszej ochrony prawnej poprzez nowe rozwiązania prawne, a z drugiej przez wprowadzanie nowych rozwiązań technologicznych po ty, by proces przetwarzania danych osobowych w cyberprzestrzeni można było uznać za bezpieczny. Nikt z nas nie wyobraża sobie współcześnie funkcjonowania bez cyberprzestrzeni. Warto jednak pamiętać, że jest to przestrzeń tak samo podatna na zagrożenia jak otaczający nas świat rzeczywisty. Wydaje się, że najskuteczniejszą metodą gwarantującą człowiekowi bezpieczeństwo w świecie wirtualnym jest mądre i rozważne dysponowanie swoimi danymi, używanie dostępnych zabezpieczeń i ciągłe doskonalenie wiedzy na temat, czym jest cyberprzestrzeń i jak się w niej bezpiecznie poruszać. Relacja cyberprzestrzeń – ochrona danych osobowych jest już źródłem zagrożeń bezpieczeństwa ludzi, ale jest przede wszystkim szczególnym wyzwaniem dla jej systematycznego diagnozowania i projektowania zmian pozwalających uniknąć ludzkich tragedii. Jest to w dużej mierze wyzwanie dla interdyscyplinarnych badań naukowych, w których nie może zabraknąć wyraźnej obecności nauk o bezpieczeństwie.

Bibliografia

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012.

Barta J., Markiewicz R., *Ochrona wizerunku, adresata korespondencji i tajemnicy źródeł informacji*, [w:] J. Barta i in., *Prawo autorskie i prawa pokrewne. Komentarz*, Kraków 2005.

Bienias M., *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych*, [w:] *Ogólne rozporządzenie o ochronie danych – aktualne problemy prawnej ochrony danych osobowych*, red. G. Sibiga, Warszawa 2016.

Błeszyński J., *Prawo autorskie*, Warszawa 1988.

Bogacki P., *Hacking w ujęciu art. 267 kk*, „Monitor Prawniczy" 2013, nr 17.

Braciak J., *Prawo do prywatności*, Warszawa 2004

Czaplicki K., *Przestępstwo phishingu i metody przeciwdziałania*, [w:] G. Szpor, A. Gryszczyńska, *Internet strategie bezpieczeństwa*, Warszawa 2017.

Dziekan-Łanucha A., *Od personalizacji do profilowania. Opis konsekwencji korzystania z wyszukiwarki internetowej Google*, „Studia Socialia Cracoviensia" 2016, t. 8, nr 1.

Globan-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999.

Golka M., *Czym jest społeczeństwo informacyjne*, „Ruch prawnicy, ekonomiczny i socjologiczny", 2005, z. 4.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.

Gwoździewicz S., Tomaszycki K., *Prawne i społeczne aspekty cyberbezpieczeństwa*, Warszawa 2017.

Jurczyk T., *Geneza rozwoju Praw Człowieka*, Wrocław 2009.

Konarska-Wrzosek V., *Kodeks karny. Komentarz, wyd. II*, Warszawa 2016.

Konarski X., *Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce*, [w:] *Ogólne rozporządzenie o ochronie danych, aktualne problemy prawnej ochrony danych osobowych 2016 r.*, red. G. Sibiga, Warszawa 2016.

Kopff A., *Koncepcja prawa do intymności i do prywatności życia osobistego*, „Studia Cywilistyczne", Kraków 1972, t. XX.

Krok E., *Budowanie kwestionariusza ankietowego a wyniki badań, Zeszyty naukowe Uniwersytetu Szczecińskiego*, „Studia Informatica" 2015, nr 37.

Krzysztofek M., *Prawo do sprzeciwu wobec przetwarzania danych osobowych*, [w:] B. Fischer, M. Sakowska-Baryła, *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, Warszawa 2017.

Lach A., *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Warszawa 2015.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Łuczak J., Trybulski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009.

Majgier K., *Internet jako przestrzeń komunikacyjna*, „Przegląd psychologiczny" 2000, t. 43, nr 2.

Mazurek P., *Anatomia internetowej anonimowości, Społeczna przestrzeń Internetu*, red. D. Bartoszek, Warszawa 2006.

Mlaskawa J., *Biometria w bankowości – szanse i zagrożenia Banku przyszłości*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2015, nr 3.

Mróz M., *Informacja nt. pojęcia cyberprzestrzeni oraz bezpieczeństwa i zagrożenia cyberprzestrzeni w prawie międzynarodowym i w ustawodawstwie wybranych państw demokratycznych*, Warszawa 2011.

Niezgódka E., *Definicja i skutki profilowania w przepisach rodo*, „ABI Expert" 2018, nr 1.

Ostrwalder C., *Cloud computing. Przetwarzanie na dużą skalę i cloud computing*, [w:] Cloud computing przetwarzanie w chmurze, red. G. Szpor, Warszawa 2013.

Polańska K., Wassilew A., *Analizy big data w serwisach społecznościowych*, „Nierówności Społeczne a Wzrost Gospodarczy" 2015, nr 4.

Rowiński J., *Testy penetracyjne*, „ABI Expert" 2018, nr 3.

Rzucidło J., *Prawo do prywatności i ochrona danych osobowych*, Wrocław 2014.

Serwach M., *Wina jako zasada odpowiedzialności cywilnej oraz okoliczność zwalniająca z obowiązku naprawienia szkody*, „Wiadomości ubezpieczeniowe" 2009, nr 1.

Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni państwa*, „Zeszyty naukowe Uniwersytetu Szczecińskiego" 2012, nr 88, *Ekonomiczne problemy usług*.

Sienkiewicz P., *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, vol. 9.

Sieńczyło-Chlabicz J., *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Kraków 2006.

Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze UKSW" 2009, nr 1.

Sobol E., *Mały słownik języka polskiego*, Warszawa 1999.

Szczęberek M., Ułasiuk K., *Bezpieczeństwo danych osobowych*, Wrocław 2017.

Szymielewicz K., *Profilowanie w marketingu*, „ABI Expert" 2018, nr 1.

Tabakow M., Korczak J., Franczyk B., *Big Data – definicje, wyzwania i technologie informatyczne*, „Informatyka ekonomiczna" 2014, nr 1.

Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4.

Talar S., *Obszary i sposoby oddziaływania Internetu na gospodarkę narodową*, „Przegląd Zachodniopomorski" 2013, t. XXVIII, z. 3.

Tekielska P., Czekaj Ł, *Działania służ w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI w.*, red. M. Górka Warszawa 2014.

Trąbiński P., *Podział kompetencji w zapewnieniu cyberbezpieczeństwa*, [w:] G. Szpor, A. Gryszczyńska, *Internet strategia bezpieczeństwa*, Warszawa 2017.

Trubalska J., Wojciechowski Ł., *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017.

Wasilewski J., *Zarys definicji cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Wassilew A., *Technologia ICT a jakość życia*, „Roczniki Kolegium Analiz Ekonomicznych" 2009, z. 20.

Wieczorkowski J., *Akceptacja naruszenia prywatności w erze Big Data*, „Nierówności społeczne a Wzrost Gospodarczy" 2017, nr 4.

Wieczorkowski J., *Zagadnienia społeczne i prawne w koncepcji big data*, „Nierówności Społeczne a Wzrost Gospodarczy" 2015, nr 4.

Wróbel W., Zoll A., *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, Warszawa 2017.

Wszołek A., *Między Facebookiem a Instagramem. Wirtualny wizerunek czy prawo majątkowe? –analiza dóbr cyfrowych in concreto*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 3.

Raporty, sprawozdania, komunikaty i poradniki

Broszura RODO wer. 18.35, www.uodo.gov.pl.

Janus R., *Statystyki zagrożeń w pierwszej połowie 2018 r.*, wwwitfocus.pl.

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, MP 2018 r., poz. 827.

Korzystanie z Internetu, Komunikat z Badań CBOS 49/2017 r., www. cbos.pl.

Pismo RPO do GIODO w sprawie Cambridge Analytica, VII.520.12.2018.AG.

Polityka Ochrony cyberprzestrzeni RP, Warszawa 18 września 2012 r., www.mc.bip.gov.pl.

Poradnik GIODO, *Czy jesteś gotowy na RODO?*, www.giodo.gov.pl.

Raport CERT Orange Polska 2017 r. www.cert.orange.pl.

Raport dotyczący stanu Internetu w roku 2017, www.mobirank.pl.

Raport NIK, *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Warszawa 2015, www.nik.gov.pl.
Raport strategiczny, Internet 2017/2018r., www.iab.org.pl.
Sprawozdanie z działalności GIODO w 2013 r., www.giodo.gov.pl.
Urząd Ochrony Danych Osobowych, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, www.uodo.gov.pl.

Źródła internetowe

Afera Cambridge Analytica, www.pcworld.pl.
ARPANET, [w:] *Wikipedia*, https://pl.wikipedia.org/wiki/ARPANET.
Brzostowski T., *Innowacje, technologie, zagrożenia w świecie XXI wieku – z perspektywy finansów*, www.alterum.pl.
Dobrowolski Z., *Koncepcja społeczeństwa informacyjnego Daniela Bella*, www.bbc.uw.edu.pl.
Dokumentacja przetwarzania danych osobowych zgodnie z RODO, www.uodo.gov.pl.
Firma Cambrigde Alanytica pomagała we wpływaniu na wyniki wyborów na świecie z wykorzystaniem nowego algorytmu Facebooka, www.zmianynaziemi.pl.
Germany: First court decision on claims for immaterial damages under GDPR, www.blogs.dlapiper.com.
GIODO o zagrożeniach płynących z upowszechniania danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi, www.giodo.gov.pl.
Goliński M., *Społeczeństwo informacyjne- problemy definicyjne i problemy pomiaru, w Dydaktyka informatyki problemy teorii*, www.di.univ.rzeszow.pl.
Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, www.uci.agh.edu.pl.
Historia Internetu, [w:] *Wikipedia*, https://pl.wikipedia.org/wiki/Historia_Internetu.
Historia Internetu, http://internet.arct.pl/historia_internetu.html.
Internet, [w:] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/Internet;3915155.html.
Jackowska I., *Firma Kowalski wyłączona z RODO*, www.pb.pl.
Kaspersky Lab, *Spam i phishing w I kwartale 2017 r. spadek liczby niechcianych e-maili pochodzących z największego na świcie botnetu spamowego*, https://www.kaspersky.pl.
Komisja Nadzoru Finansowego, Komunikat w sprawie „phishingu" danych, 13 listopada 2013 r., https://www.knf.gov.pl.
Komorowska B., *Aktywność internetowa dzieci i młodzieży – wskazania dla praktyki pedagogicznej*, www.cejsh.icm.edu.pl.

Kuchta M., *Najnowsze dane na temat użytkowników mediów społecznościowych na świecie*, www.spocialpress.pl.

Kulik W., *Cztery miliardy internautów*, 30 stycznia 2018 r., http://www.benchmark.pl/aktualnosci/ile-osob-ma-dostep-do-internetu-na-swiecie-juz-ponad-4-miliardy.html.

Kuraś J., *Dane osobowe: kradzież tożsamości w Internecie*, www.rp.pl.

Majchrzyk Ł., *Mobile, digital i social media na świecie w 2017 roku*, https://mobirank.pl/2017/01/24/mobile-digital-social-media-na-swiecie-2017/.

Majchrzyk Ł., *Mobile i Digital w 2018 roku w Polsce i na świecie*, https://mobirank.pl/2018/02/02/mobile-i-digital-w-2018-roku-w-polsce-i-na-swiecie/.

Nie żyje wynalazca e-mail Ray Tomlinson, www.forbes.pl.

Pharming, https://www.avast.com/pl-pl/c-pharming.

Rekomendacja CM/Rec (2010)13, przyjęta przez Komitet Ministrów 23 listopada 2010 r. podczas 1099 posiedzenia Wiceministrów www.giodo.gov.pl.

Rosicki R., *O pojęciu i istocie bezpieczeństwa*, www.repozytorium.amu.edu.pl.

Uwagi GIODO z dnia 12 maja 2016 r. do projektu ustawy o działaniach antyterrorystycznych DOLiS-033-133/16, www.giodo.gov.pl.

Uwagi GIODO z dnia 20 października 2017 r. do projektu ustawy o ochronie danych osobowych, www.giodo.gov.pl.

Wiewiórowski W., wystąpienie GIODO podczas konferencji naukowej *Bezpieczeństwo technologii biometrycznych – ochrona danych biometrycznych*, UKSW, Warszawa 09.12.2011, www.giodo.gov.pl.

Wójcik M., *Big data w zarządzaniu informacją – przegląd wybranych zagadnień*, [w:] *Inspiracje i zarządzanie informacją w perspektywie bibliologii i informatologii*, www.ruj.uj.edu.pl.

Dokumenty Grupy Roboczej art. 29

Grupa Robocza art. 29, Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta 20 czerwca 2007 r., WP 136.

Grupa Robocza art. 29, Opinia 5/2009 w sprawie portali społecznościowych przyjęta 12 czerwca 2009 r., WP 163.

Grupa Robocza art. 29, Opinia 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta 22 czerwca 2010 r., WP 171.

Grupa Robocza art. 29, Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych przyjęta 16 maja 2011 r., WP 185.

Grupa Robocza art. 29, Opinia 15/2011 w sprawie definicji zgody przyjęta 13 lipca 2011 r., WP 187.

Grupa Robocza art. 29, Opinia 1/2012 o projektach reformy ochrony danych przyjęta 23 marca 2012 r., WP 191.

Grupa Robocza art. 29, Opinia 3/2012 w sprawie zmiany sytuacji w dziedzinie technologii biometrycznej przyjęta 27 kwietnia 2012 r., WP 193.

Grupa Robocza art. 29, Opinia nr 5/2012 w sprawie przetwarzania danych chmurze obliczeniowej przyjęta 1 lipca 2012 r., WP 196.

Grupa Robocza art. 29, Wytyczne z 2 października 2013 r. w sprawie pozyskiwania zgody na zapisywanie plików cookies, WP 208.

Grupa Robocza art. 29, Opinia 05/2014 w sprawie technik anonimizacji przyjęta 10 kwietnia 2014 r., WP 216.

Grupa Robocza art. 29, Opinia dotycząca prawa do przenoszenia danych przyjęta 13 grudnia 2016 r., WP 242.

Grupa Robocza art. 29, Wytyczne z 13 grudnia 2016 r. dotyczące Inspektorów Ochrony Danych, WP 243.

Grupa Robocza art. 29, Opinia 1/2017 na temat proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej (2002/58/WE) przyjęta 4 kwietnia 2017 r., WP 247.

Grupa Robocza art. 29, Wytyczne z 4 kwietnia 2017 r. dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" dla celów rozporządzenia 2016/679 zmienione w dniu 4 października 2017 r., WP 248.

Grupa Robocza art. 29, Wytyczne z 3 października 2017 r. w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679, WP 250.

Grupa Robocza art. 29, Wytyczne z 3 października 2017 r. dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, ostatnio zmienione i przyjęte 6 lutego 2018 r., WP 251.

Grupa Robocza art. 29, Wytyczne z 28 listopada 2017 r. dotyczące zgody na mocy rozporządzenia 2016/679, WP 259.

Grupa Robocza art. 29, Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679, WP 260.

Prawo międzynarodowe

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 z 04.05.2016.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. UE L 281 z 23.11.1995.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej, Dz.Urz. UE L 194 z 19.07.2016.

Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz.U. z 1947 r. nr 23, poz. 90.

Międzynarodowy Pakt Praw Obywatelskich i Politycznych podpisany 19 grudnia 1966 r. w Nowym Jorku, Dz.U. z 1977 r. nr 38, poz. 167.

Karta Praw Podstawowych Unii Europejskiej z 30 marca 2010 r., C83/389.

Rezolucja Zgromadzenia Ogólnego ONZ z grudnia 1998 r., nr 53/70.

Rezolucja Zgromadzenia Ogólnego ONZ ze stycznia 2002 r., nr 56/121.

Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*, 22 stycznia 2015 r.

Komunikat Komisji Europa 2020, Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, Bruksela 3 marca 2010 r., KOM(2010).

Convention on Cybercrime, No185, www.ceo.int.

Prawo krajowe

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r. nr 78, poz. 483.

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, tekst jedn. Dz.U. z 2018 r., poz. 2096 ze zm.

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, tekst jedn. Dz.U. z 2018 r., poz. 1025 ze zm.

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, tekst jedn. Dz.U. z 2018 r., poz. 917 ze zm.

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, tekst jedn. Dz.U. z 2018 r., poz. 1191 ze zm.

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych, Dz.U. z 2001 r. nr 128, poz. 1402 ze zm.

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, tekst jedn. Dz.U. z 2018 r., poz. 1330 ze zm.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, tekst jedn. Dz.U. z 2017 r., poz. 1219 ze zm.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, tekst jedn. Dz.U. z 2017 r., poz. 570 ze zm.

Ustawa z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny, Dz.U. z 2011 r. nr 72, poz. 381.

Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz.U. z 2011 r. nr 222, poz. 1323.

Ustawa z dnia 25 września 2015 r. o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw, Dz.U. z 2015 r., poz. 1893.

Ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystaniu informacji sektora publicznego, tekst jedn. Dz.U. z 2018 r., poz. 1243 ze zm.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, tekst jedn. Dz.U. z 2018 r., poz. 452 ze zm.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. z 2018 r., poz. 1000 ze zm.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560.

Uzasadnienie do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, poz. 1560.

Uzasadnienie do ustawy o ochronie danych osobowych, Druk nr 2410, Sejm Rzeczypospolitej Polskiej VII Kadencja Prezesa Rady Ministrów RM10-49-18, www.orka.sejm.gov.pl.

Uzasadnienie do ustawy o działaniach antyterrorystycznych, www.sejm.gov.pl.

Uzasadnienie do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, poz. 1560, www.sejm.gov.pl.

Biuro Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

Orzecznictwo

Orzecznictwo TSUE

Wyrok TSUE z 13 maja 2014 r., Google Spain SL, Google Inc. przeciwko Agencia Española de Proteccion de Datos, Mario Costeja Gonzalez, C-131/12, ECLI:EU:C:2014:317.

Wyrok TSUE z 19 października 2016 r., Patric Breyer przeciwko Bundesrepublik Deutschland C-582/14, ECLI:EU:C:2016:779.

Orzecznictwo krajowe

Wyrok TK z 19 maja 1998 r., U 5/97.

SN

Wyrok SN z 19 listopada 2003 r., I PK 590/02.
Wyrok SN z 20 maja 2004 r., II CK 330/03.
Wyrok SN z 11 marca 2008 r., II CSK 539/07.
Wyrok SN z 30 września 2015 r., II K 115/15.

NSA

Wyrok NSA z 18 listopada 2009 r., I OSK 667/09.
Wyrok NSA z 1 grudnia 2009 r., I OSK 249/09.
Wyrok NSA z 13 stycznia 2011 r., I OSK 440/10.
Wyrok NSA z 19 maja 2011 r., I OSK 1079/10.

WSA

Wyrok WSA w Warszawie z 3 marca 2009 r., II SA/Wa 1495/08.
Wyrok WSA w Warszawie z 14 maja 2009 r., II SA/Wa 567/09.
Wyrok WSA w Warszawie z 3 lutego 2010 r., II SA/Wa 1598/09.
Wyrok WSA w Krakowie z 11 października 2013 r., II SA/Kr 682/13.
Wyrok WSA w Gdańsku z 28 września 2016 r., II Aka 111/16.

ISBN 978-83-64971-59-4

Społeczna Akademia Nauk
Łódź

www.san.edu.pl