URSZULA ADAMCZYK
ORCID: 0000-0002-4257-4745
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Prawo do prywatności i ochrony danych osobowych w Rzeczypospolitej Polskiej

Wprowadzenie

Każdy sposób posługiwania się informacją dotyczącą jednostki może być uznany za wkroczenie w sferę jej prywatności. Prawo do prywatności jest nierozerwalnie związane z godnością człowieka, będącą źródłem wszystkich praw i wolności[1], z czego wywodzi się ich charakter: uniwersalny (przysługują każdemu, niezależnie od miejsca zamieszkania, przynależności etnicznej, płci, religii itp.), przyrodzony (przysługują każdemu od chwili narodzin, nie wiążą się ze statusem społecznym), niezbywalny (jednostka nie może ich zbyć ani ograniczyć), nienaruszalny (brak prawnych możliwości pozbawienia praw jednostki).

Pojęcie prawa do prywatności ujawnia coraz to nowe aspekty w miarę rozwoju stosunków społecznych, politycznych oraz w wyniku rozwoju techniki. Z jednej strony istnieje naturalna chęć ograniczania prawa do prywatności przez władze publiczne, z różnych względów, zwykle motywowanych szeroko rozumianym dobrem obywateli, z drugiej – tendencja do jej chronienia po stronie osób fizycznych. Powszechna panika wywołana zamachami z 11 września 2001 r., i potęgowana ostatnio masowym napływem ludności zamieszkującej Syrię i niektóre obszary Północnej Afryki lub globalną pandemią związaną z COVID-19, stała się

[1] A. Gajda, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace" / OW SGH 2014, s. 59.

niejako usprawiedliwieniem władz publicznych dla ochrony bezpieczeństwa przed zagrożeniami i do coraz szerszej kontroli sfery prywatnej życia zwykłego obywatela. Takie stanowisko obywatele wielu państw gotowi są zaakceptować.

Prywatność w aspekcie psychologicznym i socjologicznym

Prywatność dopiero w drugiej połowie dwudziestego wieku stała się odrębnym przedmiotem badań nauk psychologicznych i socjologicznych. Wcześniej wiązano ją z innymi pojęciami takimi, jak afiliacja, terytorializm, samotność czy izolacja[2]. Można stwierdzić, że prywatność oznacza uniwersalną potrzebę każdego człowieka, niezależną od wpływu środowiska i kręgu kulturowego. Stanowi cechę osobowości objawiającą się potrzebą izolacji, wyraża potrzebę określonej jednostki, jednak granice prywatności nie są jednakowe dla wszystkich ludzi. Rozumienie prywatności jest zależne od kręgu kulturowego, wieku, osobistych preferencji w zakresie nawiązywania relacji społecznych, pozycji zawodowej czy społecznej. Ta sama osoba może w tym samym czasie, będąc w tym samym wieku, oceniać tę samą sytuację jako naruszającą jej poczucie prywatności lub nie – w zależności od kontekstu sytuacyjnego.

Jak podkreśla R. Dopierała, „rozwój i utrzymanie tożsamości jest zatem najwyżej umieszczoną w hierarchii, centralną funkcją prywatności, a jej dopełnieniem jest zarządzanie interakcjami społecznymi”[3]. Można stwierdzić, że prywatność jednostki to sposób kontrolowania przez nią budowanych relacji społecznych warunkujących prawidłową interakcję z otoczeniem. Istniejące normy społeczne i wynikające z nich wzorce zachowania nie pozostają bez wpływu na zakres oraz rozumienie prywatności. Socjolog M. Ossowska określiła prywatność w trzech perspektywach: jako uprawnienie do okresowej samotności, środek zabezpieczający przed kontrolą lub ingerencją ze strony osób trzecich oraz element godności człowieka[4]. Wskazane podejścia mogą się łączyć i przenikać, powodując, że faktyczne zrozumienie prywatności jest zmienne w czasie i zależne od

[2] K. Jędruszczak, *Prywatność jako potrzeba w ramach koncepcji siebie*, „Roczniki Psychologiczne” 2005, nr 2, s. 112.
[3] R. Dopierała, *Internetowe manifestacje prywatności*, „Media – Kultura – Społeczeństwo” 2008, nr 3, s. 108.
[4] M. Ossowska, *Normy moralne. Próba systematyzacji*, PWN, Warszawa 1985, s. 101-106.

uwarunkowań kulturowych[5]. Zasadnym jest więc oczekiwanie, że prywatność, tak jak wolność, godność i bezpieczeństwo, będzie chroniona nie tylko normami moralnymi, ale także prawnymi.

A. Kopff określił prywatność jako „prawo jednostki do życia swym własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[6]. Prawo do prywatności podzielił na dwie sfery: prawa do intymności życia osobistego oraz prawa do prywatności życia osobistego. Uważa on, że strefa życia intymnego zasługuje zawsze na ochronę prawną i nie ma żadnych okoliczności usprawiedliwiających jakiekolwiek wkroczenie w tę strefę"[7], w tym także związanych z prawem do informacji. Jednak granice strefy prywatności życia osobistego, powiązane ze światem zewnętrznym poprzez interakcje jednostki z otoczeniem i będące efektem tej relacji, mogą budzić „usprawiedliwione zainteresowanie". Teoria sfer Kopffa, w niemal niezmienionej formie, znalazła także miejsce w orzecznictwie Trybunału Konstytucyjnego: „o ile sfera życia intymnego (w znaczeniu szerszym niż potocznie przyjęte) objęta jest pełną prawną ochroną, o tyle ochrona sfery życia prywatnego podlega pewnym ograniczeniom, uzasadnionym usprawiedliwionym zainteresowaniem"[8].

Kopff określił naruszenie prawa do prywatności jako ingerencję w życie prywatne, rodzinne lub domowe, naruszenie integralności psychofizycznej jednostki, naruszenie wolności, przekonań lub obyczajów człowieka, naruszenie czci, honoru lub uzyskanej opinii, ukazanie innej osoby w niekorzystnym dla niej świetle, ujawnienie krępujących lub intymnych faktów odnoszących się do życia prywatnego, przywłaszczenie sobie cudzego nazwiska, pseudonimu lub osiągnięć, niepokojenie drugiej osoby przez jej śledzenie, narzucanie swojego towarzystwa lub w inny sposób, dopuszczenie się naruszenia korespondencji oraz rozpowszechniania cudzego wizerunku bez zezwolenia tej osoby, nadużywanie informacji uzyskanych prywatnie oraz ujawnienie informacji udzielonych w warunkach poufności[9].

[5] J. Kopka, *Prywatność w społecznej komunikacji. Odniesienia teoretyczne i dynamika przemian w społeczeństwie sieci*, [w:] *E-społeczeństwo w Europie Środkowej i Wschodniej. Teraźniejszość i perspektywy rozwoju*, red. S. Partycki, Wyd. KUL, Lublin 2015, s. 26.

[6] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilistyczne", t. XX, PWN, Warszawa 1972, s. 30.

[7] Tamże, s. 33.

[8] Wyrok TK z 21.10.1998, sygn. K 24/98, OTK 1998, nr 6, poz. 97.

[9] A. Kopff, *Koncepcja praw do intymności…*, dz. cyt., s. 30-33.

Rozwój społeczeństwa informacyjnego

Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych, jako komponentu sfery prywatności, który współcześnie podlega ochronie w większości systemów prawnych. Znacząco wzrosła skala zbierania i wymiany danych, a rozwój technologii umożliwił, na niespotykaną dotąd skalę, wykorzystywanie danych osobowych w działalności. Osoby fizyczne coraz częściej udostępniają informacje o sobie publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zapewniając wysoki stopień ich ochrony[10].

Współczesne korzystanie z sieci otrzymało nową jakość dzięki Internetowi, który służy jako środek komunikacji pozwalający na porozumiewanie się z wieloma osobami w jednym czasie, w skali globalnej. Coraz bardziej rosnąca dostępność, możliwość zastosowania i wykorzystywanie technik informatycznych i telekomunikacyjnych prowadzą do wzrostu złożoności systemów społecznych, gospodarczych i politycznych[11]. Według niektórych badaczy Internet nie jest zwykłą technologią, a rewolucją w sposobie porozumiewania się społeczeństwa i funkcjonowania całego świata. Dynamiczny rozwój Internetu jest najważniejszym czynnikiem i przyczyną pojawienia się społeczeństwa informacyjnego[12]. „Nie jest to już prognoza, lecz stwierdzenie tendencji rozwojowej. Nie spekuluje się, czy to społeczeństwo nadejdzie, lecz rozważa się, w jakim kierunku ewoluuje. To bowiem, że istnieje i określa ramy naszego życia indywidualnego i zbiorowego, stało się faktem. Jest to społeczeństwo najbardziej w historii nasycone techniką i od niej zależne”[13].

[10] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 6. Dziennik Urzędowy Unii Europejskiej.
[11] M. Goliński, *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru*, OW SGH, Warszawa 2011, s. 26.
[12] M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, PWN, Warszawa 2008, s. 83.
[13] K. Krzysztofek, M.S. Szczepański, *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wyd. UŚ, Katowice 2005, s. 169.

Społeczeństwo informacyjne charakteryzuje się ogólną otwartością, szybkością wymiany informacji, podniesieniem kwalifikacji i wiedzy. Informacja zaczęła odgrywać dominującą rolę oraz stanowić podstawowy zasób nowoczesnego społeczeństwa.

Możliwość gromadzenia i przetwarzania dużych zbiorów danych, pozyskanych z wielu rozproszonych baz danych i ich swobodne, globalne przetwarzanie, doprowadziły do powstania rynku brokerów danych (przedsiębiorców, posiadających bazy danych setek milionów osób, zawierających informacje na temat ich stanu zdrowia, indywidualnych preferencji, sytuacji finansowej czy przynależności do określonych mniejszości). Profilowanie, a więc budowanie w oparciu o informacje pozyskiwane z wielu elektronicznych baz danych opisujących jednostkę, stało się skuteczną techniką marketingu , ale także badania i przewidywania zachowań ludzi lub całych społeczności, stając się tym samym skutecznym narzędziem inwigilacji. Europejski Inspektor Ochrony Danych zauważył, że „nigdy wcześniej podstawowe prawa do prywatności i ochrony danych osobowych nie były tak istotne dla ochrony godności człowieka. (…) Dają one człowiekowi możliwość rozwijania własnej osobowości, prowadzenia niezależnego życia, wykazywania się innowacyjnością oraz korzystania z innych praw i wolności. (…) Technologia nie powinna narzucać wartości i praw, jednak relacji tej nie należy również sprowadzać do błędnej dychotomii. Z rewolucją cyfrową wiążą się obietnice korzyści w takich obszarach jak zdrowie, środowisko, międzynarodowy rozwój i efektywność ekonomiczna”[14].

Podkreśla się, że przepisy dotyczące ochrony danych osobowych mają być nie tylko instrumentem niezbędnym dla poszanowania podstawowych, uznanych powszechnie praw i wolności, zwłaszcza prawa do prywatności, ale też pełnić funkcję ochronną interesów użytkowników najnowszej technologii informatycznej i Internetu, w tym różnych instytucji publicznych, oraz zapewnić niezbędne do ich działania zaufanie i bezpieczeństwo[15].

[14] Europejski Inspektor Ochrony Danych, „*W kierunku nowej etyki cyfrowej: dane, godność i technologia*”, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_summary_pl.pdf [dostęp 9.04.2020].

[15] J. Barta, P. Fajgielski, R. Markiewicz, *Część pierwsza – Wstęp*, [w:] *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015.

M. Safjan wskazuje, że charakter prawny przepisów o ochronie danych osobowych jest ukierunkowany na zapobieganie naruszeniom, podczas gdy mechanizmy ochrony prywatności – na działanie „po fakcie" w postaci sankcji cywilnoprawnych i karnych[16]. O ile ochrona danych osobowych związana jest z kontrolowaniem zakresu wykorzystania informacji oraz nadzorowaniem administratorów danych poprzez nadanie specyficznych praw podmiotom danych (np. prawo do informacji, prawo do poprawienia i uzupełniania danych), to prawo do prywatności zorientowane jest na zachowanie poufności informacji. K. Motyka wskazuje, że „ekspansywność pojęcia prawa do prywatności przynajmniej w części jest rezultatem braku jego wyraźniej definicji, która miałaby jakieś szersze uznanie"[17], natomiast prawna definicja ochrony danych osobowych ma charakter bardziej szczegółowy.

Z uwagi na globalny charakter cyberprzestrzeni wiążą się z nią liczne zagrożenia i ryzyka dla ochrony praw podstawowych. Ważnym przykładem jest ochrona prywatności, rozumiana jako prawo do decydowania jednostek o zakresie przekazywanych innym informacji na swój temat, która jest szczególnie podatna na zagrożenia płynące z pozornie anonimowej cyberprzestrzeni. Oczekiwaniem jednostek, grup i instytucji jest decydowanie kiedy, gdzie i jakie informacje ich dotyczące zostaną udostępnione innym. Najpopularniejszymi zagrożeniami w cyberprzestrzeni są ataki z użyciem szkodliwego oprogramowania, kradzieże tożsamości, wyłudzenia mające na celu modyfikacje bądź niszczenie danych, blokowanie dostępu do usług, ataki socjotechniczne, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję[18].

Rozwój nowych sposobów przetwarzania danych związanych z nowoczesnymi technikami również niesie za sobą ryzyko kradzieży danych, ich bezprawnego niszczenia i publikowania, profilowania realizowanego bez poszanowania praw podmiotu danych, niezgodnie z jego interesem, często bez wiedzy danej osoby, cyberinwigilacji, utraty kontroli nad informacją w efekcie przetwarzania

[16] M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6, s. 7.
[17] K. Motyka, *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Seria Administracja i Zarządzanie" 2010, nr 85, s. 25.
[18] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 2, s. 131.

niezgodnego z pierwotnie ustalonym celem lub zakresem, ale również ujawnienia informacji wskutek błędu człowieka, awarii systemu, ale też normalnego działania e-usług[19].

Konstytucjonalizacja prawa do prywatności

Mechanizmy prowadzące do ochrony sfery prywatnej zostały określone już w Konstytucji marcowej z okresu II RP, gwarantującej ochronę nietykalności osobistej, ochronę miru domowego oraz zachowanie tajemnicy korespondencji[20]. Konstytucja kwietniowa z kolei gwarantowała (zgodnie z art. 5 ust. 2), że państwo zapewni obywatelom możność rozwoju ich wartości osobistych oraz wolności sumienia, słowa i zrzeszeń oraz – z art. 68 ust. 2 – „wolność osobistą, mieszkania i tajemnicę korespondencji", jednak granicą tych wolności było dobro powszechne. Norma art. 10 ust. 1, zgodnie z którą żadne działanie nie mogło stanąć w sprzeczności z celami państwa, wyrażonymi w jego prawach, w znaczny sposób ograniczała prawa i wolności osobiste w relacji z władzą publiczną[21]. W Konstytucji PRL utrzymano gwarancje związane z nietykalnością osobistą, jednak kwestię zakresu nienaruszalności mieszkania i tajemnicy korespondencji delegowano do regulacji zwykłej ustawy[22]. Z uwagi na brak poszanowania zasady rządów prawa w okresie PRL, faktyczne znaczenie tych regulacji było niewielkie.

Źródłem norm prawnych ochrony życia prywatnego były akty prawa międzynarodowego, ratyfikowane przez Polskę i przyjęte do bezpośredniego stosowania. Jednym z pierwszych, a zarazem podstawowych, aktów prawnych respektujących te wartości jest Konwencja o ochronie praw człowieka i podstawowych wolności (europejska konwencja praw człowieka) sporządzona w Rzymie dnia 4 listopada 1950 r.[23] Konwencja gwarantowała prawo do poszanowania życia prywatnego i rodzinnego, w tym mieszkania i korespondencji, oraz brak ingerencji

[19] P. Leja, *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, „Prawo Mediów Elektronicznych" 2017, nr 3, s. 10-17.

[20] Ustawa z dn. 17 marca 1921 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1921 r. Nr 44, poz. 267, art. 97, 100, 106).

[21] Ustawa Konstytucyjna z dn. 23 kwietnia 1935 r. (Dz.U. z 1935 r. Nr 30, poz. 227).

[22] Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dn. 22 lipca 1952 (Dz.U. z 1952 r. Nr 33, poz. 232 ze zm., art. 74).

[23] Konwencja o ochronie praw człowieka i podstawowych wolności (europejska konwencja praw człowieka) (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.).

władzy publicznej w korzystanie z tych praw, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom oraz ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Gwarancje związane z ochroną prywatności zostały wyrażone również w art. 17 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych[24], wprowadzając zakaz samowolnej lub bezprawnej ingerencji w życie prywatne, rodzinne, dom oraz korespondencję, w tym – prowadzące do naruszenia czci i dobrego imienia. Zgodnie z art. 17 ust. 2 Paktu każdy ma prawo do ochrony prawnej przed tego typu ingerencjami i zamachami.

Przemiany polityczne po 1989 r. wzmocniły znaczenie ochrony praw człowieka. W nadal obowiązującej Konstytucji PRL znowelizowano art. 1, w którym wybrzmiało, że „Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej”[25]. Sąd Najwyższy wyrokiem z dnia 8 kwietnia 1994 dokonał potwierdzenia istnienia oraz zakresu prawnej ochrony prywatności przed ingerencją władzy publicznej: „Wolności obywatelskie są (…) elementem wspólnego, demokratycznego i legalistycznego porządku, przeto mogą być również, z uwagi na wspólne dobro i interesy, w rozsądny i odpowiadający prawu sposób, ograniczone, przy uwzględnieniu służącego każdemu obywatelowi prawa do prywatności chroniącego indywidualną sferę jego osobistego życia”[26].

Po uchwaleniu Konstytucji Rzeczypospolitej Polskiej z 1997 r.[27], na mocy art. 47 („Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.”) oraz art. 49 („Zapewnia się wolność i ochronę tajemnicy komunikowania się.”) ochrona prywatności zyskała rangę gwarancji konstytucyjnej. Konstytucja nie wprowadziła zamkniętej definicji terminu prywatność ani zamkniętej listy dóbr chronionych,

[24]Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).
[25] Ustawa z dnia 29 grudnia 1989 o zmianie Konstytucji Polskiej Rzeczypospolitej Ludowej (Dz.U. z 1989 r. Nr 75, poz. 444).
[26] Wyrok SN z dnia 8 kwietnia1994 r., sygn. III ARN 18/94, OSNP 1994, nr 4, poz. 550.
[27] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 2009 r. Nr 114, poz. 946).

a jedynie wyliczała przykładowe wartości podlegające ochronie i tradycyjnie kojarzone z życiem prywatnym.

Przepis art. 47 został uzupełniony normą art. 51 ust. 1 odnoszącą się do kwestii ochrony danych osobowych: „Nikt nie może być obowiązany, inaczej niż na podstawie ustawy, do ujawniania informacji dotyczących jego osoby". Art. 51 określa również ograniczenia władz publicznych dotyczące pozyskiwania, gromadzenia i udostępniania informacji o obywatelach oraz nadaje prawo dostępu każdemu obywatelowi do dotyczących go urzędowych dokumentów i zbiorów danych oraz żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Konstytucyjne gwarancje związane z ochroną prywatności zawarto również w art. 41, zapewniającym nietykalność i wolność osobistą, art. 50, gwarantującym nienaruszalność mieszkania, oraz art. 53, zapewniającym wolność sumienia i wyznania. Ponadto z art. 76 Konstytucji wynika ochrona konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich prywatności.

Konstytucja RP art. 233 ust. 1 w czasie stanu wojennego i wyjątkowego przewiduje zakres ograniczeń wolności i praw człowieka i obywatela z wyłączeniem ograniczenia prawa do poszanowania prywatności (art. 47). Jak zauważa M. Safjan, konsekwencją zaliczenia prywatności do praw, które nie mogą podlegać ograniczeniom nawet w przypadku stanu wojennego lub wyjątkowego, jest uznanie, że ochrona prywatności należy do grona praw i gwarancji o najsilniejszej ochronie konstytucyjnej[28].

Ochrona danych osobowych

Prawo do poszanowania życia prywatnego i ochrona danych osobowych ściśle są ze sobą powiązane, ponieważ chronią to samo dobro – prywatność człowieka.

Zgodnie z konstytucyjną dyspozycją art. 51 ust. 5: „Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa". Pierwszym polskim aktem normatywnym dotyczącym danych osobowych była Ustawa z dnia 29 sierpnia

[28] M. Safjan, *Ochrona prywatności na tle Konstytucji z 1997 roku – ramy normatywne*, [w:] *Wyzwania dla państwa prawa*, Oficyna, Warszawa 2007, s. 86-92.

1997 r. o ochronie danych osobowych[29], nowelizowana przez wzgląd na dostosowanie jej do przepisów unijnych, w tym wdrożenia Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (UE) z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, wprowadzającej zniesienie przeszkód w przepływie danych osobowych poprzez jednakowy we wszystkich państwach członkowskich stopień ochrony praw i wolności jednostek w zakresie przetwarzania tych danych.

Różnice w stopniu ochrony praw i wolności osób fizycznych poszczególnych państw członkowskich w związku z przetwarzaniem danych osobowych powstałe w wyniku różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE skutkowały dalszymi pracami nad ujednoliceniem przepisów w tym zakresie na terenie całej Unii, czego efektem było Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[30]. Wszystkie kraje Unii z dniem 25 maja 2018 r. przyjęły rozporządzenie ogólne do bezpośredniego stosowania. Miało ono na celu wzmocnienie podstawowych praw obywateli w epoce cyfrowej oraz ułatwienie przedsiębiorcom i organizacjom działania na wspólnym rynku poprzez spójne i jednolite przepisy na terenie całej Unii. Równocześnie w Polsce weszła w życie nowa ustawa o ochronie danych osobowych[31]. Ustawa stanowi uzupełnienie rozporządzenia w zakresie, w jakim ustawodawca unijny dopuścił doprecyzowanie pewnych zagadnień w porządku prawnym na poziomie państw członkowskich UE.

Definicja danych osobowych w rozporządzeniu ogólnym

Funkcjonowanie w wirtualnym świecie ma wymiar transgraniczny i dotyczy całej międzynarodowej społeczności. Internet daje dostęp do nieograniczonej liczby informacji i wiąże się nie tylko z licznymi korzyściami, ale także z jeszcze

[29] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922).
[30] 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, tj. ogólne rozporządzenie o ochronie danych (Dz.Urz. UE L 119 z 04.05.2016).
[31] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

większą liczbą zagrożeń. Niemal każdy, bez większej weryfikacji, może umieszczać tam w zasadzie dowolną informację, nie zawsze prawdziwą, co może powodować negatywne skutki dla osoby, których dane dotyczą. Rosnąca liczba przypadków, w których osoby zostały niesłusznie ocenione lub szykanowane, zaowocowała decyzją o zabezpieczeniu praw osób w szerszym zakresie[32].

Dane osobowe to „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”[33].

„Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (…), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby ustalić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas, potrzebne do zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny”[34].

Katalog szczególnych kategorii danych, tzw. „wrażliwych”, zawiera dane biometryczne, wynikające ze specjalnego przetwarzania, dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, umożliwiające jednoznaczną identyfikację osoby: wizerunek twarzy czy dane daktyloskopijne oraz „dane dotyczące zdrowia” fizycznego i psychicznego osoby, w tym o korzystaniu z usług opieki zdrowotnej ujawniające informacje o stanie jej zdrowia. Art. 9 pkt 1 rozporządzenia ogólnego określa jako szczególne kategorie danych te,

[32] A. Stępień, *Ochrona danych osobowych w świetle rozporządzenia ogólnego – omówienie wybranych zagadnień*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Wyd. Nauk. UPH, Siedlce 2018, s. 132-133.

[33] Ogólne rozporządzenie o ochronie danych, art. 4 pkt 1.

[34] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 26.

ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne i biometryczne jednoznacznie identyfikujące osobę fizyczną lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Automatyczne przetwarzanie danych w celu podjęcia decyzji, w tym profilowanie, jest dziś bardzo powszechnym zjawiskiem. Branża reklamowa, marketing, bankowość, ubezpieczenia, ochrona zdrowia – to tylko niektóre sektory korzystające z narzędzi profilowania. Profilowanie, w myśl motywu 71 preambuły, polega na dowolnym zautomatyzowanym przetwarzaniu danych pozwalającym ocenić czynniki osobowe osoby fizycznej, analizować i prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowań, lokalizacji lub przemieszczania się osoby, której dane dotyczą.

Każda osoba, której dane dotyczą, ma prawo, by nie podlegać decyzjom, które opierają się na przetwarzaniu zautomatyzowanym, w tym profilowaniu, wywołującym dla tej osoby określone skutki prawne lub w istotny sposób na nią wpływające. Administrator danych obowiązany jest wdrożyć środki techniczne i organizacyjne, które zapewnią właściwe i bezpieczne przetwarzanie danych z wykorzystaniem profilowania[35]. Zwłaszcza jeśli do profilowania używa się szczególnych kategorii danych osobowych, tzw. danych wrażliwych lub danych osobowych dzieci[36].

Zgodnie z przewidzianym w rozporządzeniu ogólnym podejściem opartym na analizie ryzyka, zwłaszcza kiedy działania na danych odbywają się przy użyciu nowych technologii, obecnie to administrator przed rozpoczęciem przetwarzania zobowiązany jest dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, biorąc pod uwagę charakter, zakres i cele oraz prawdopodobieństwo spowodowania wysokiego ryzyka naruszenia praw i wolności osób fizycznych. Należy szacować je na podstawie obiektywnej oceny, w ramach której stwierdza się, czy operacje przetwarzania danych wiążą się z ryzykiem lub wysokim ryzykiem[37].

[35] Ogólne rozporządzenie o ochronie danych, art. 22.
[36] Gotowi na RODO. Opracowanie GIODO, https://uodo.gov.pl [dostęp 19.11.2018].
[37] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 76.

W przypadku gdy dane zbierane są bezpośrednio od osoby, której dotyczą, administrator, podczas ich pozyskiwania, zobowiązany jest do udzielenia wszelkich przewidzianych prawem informacji oraz do podania w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, zwłaszcza gdy informacja jest kierowana do dziecka[38]:

- danych organizacji, w tym danych kontaktowych i informacji o przedstawicielu, jeśli jest;
- danych kontaktowych inspektora ochrony danych, gdy ma to zastosowanie;
- celu przetwarzania danych i podstawy prawnej;
- odbiorców danych lub kategorii odbiorców, jeśli występują;
- informacji o zamiarze przekazania danych osobowych do państwa trzeciego, gdy ma to zastosowanie;
- informacji o okresie przechowywania danych, a gdy jest to możliwe, kryteriach ustalania tego okresu;
- informacji o prawie osoby do żądania dostępu do danych jej dotyczących, ich sprostowania, usunięcia, ograniczenia przetwarzania, prawie wniesienia sprzeciwu wobec przetwarzania, a także prawie do przenoszenia danych;
- informacji o prawie do cofnięcia zgody w dowolnym momencie i sposobie, w jaki można to zrobić;
- informacji o prawie do wniesienia skargi do organu nadzorczego;
- informacji, czy podanie danych osobowych jest wymogiem ustawowym, umownym czy warunkiem zawarcia umowy, oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą[39].

W przypadku pozyskania danych z innych źródeł (nie od osoby, której dane dotyczą), dodatkowo należy poinformować o źródle pozyskania danych. Informacje te administrator podaje w rozsądnym terminie, najpóźniej w ciągu miesiąca. Jeśli dane mają być stosowane do komunikacji z osobą, której dotyczą,

[38] Ogólne rozporządzenie o ochronie danych, art. 12, pkt. 1.
[39] Ogólne rozporządzenie o ochronie danych, art. 13.

takiej informacji udziela się najpóźniej przy pierwszej takiej komunikacji. Natomiast jeżeli planuje się ujawnić dane innemu odbiorcy – najpóźniej przy pierwszym ujawnieniu.

Bez względu na to, czy dane pozyskuje się od osoby, której one dotyczą, czy z innych źródeł, jeżeli administrator planuje przetwarzać dane osobowe w innym celu niż ten, w którym dane osobowe zostały zebrane, powinien o tym poinformować osobę, której dane dotyczą, oraz udzielić jej pozostałych stosownych informacji.

Przed wyrażeniem zgody osoba ujawniająca swoje dane osobowe powinna otrzymać informację, że ma prawo wycofania zgody w dowolnym momencie, a wycofanie zgody musi być równie łatwe jak jej wyrażenie. Oceniając, czy zgodę wyrażono dobrowolnie, uwzględnić należy między innymi, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, świadczenie usługi, jeśli przetwarzanie danych nie jest niezbędne do wykonania tej umowy. Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Jeżeli osoba, której dane dotyczą, wyrazi zgodę pisemnym oświadczeniem, które dotyczy więcej niż jednej kwestii, zapytanie o zgodę powinno wyraźnie odróżniać te kwestie w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem[40].

W przypadku oferowania usług społeczeństwa informacyjnego bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych dziecka, które ukończyło 16 lat. W innym przypadku zgodę na takie przetwarzanie musi wyrazić (lub zaakceptować ją) osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. Przetwarzanie jest zgodne z prawem wyłącznie w zakresie wyrażonej zgody[41].

Rozporządzenie ogólne wyposażyło obywateli w możliwość kontroli treści ich dotyczących poprzez prawo do żądania usunięcia danych: tzw. „prawo do bycia zapomnianym", które nakłada na administratora obowiązek niezwłocznego usunięcia tych danych, jeżeli zachodzi jedna z poniższych okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

[40] Ogólne rozporządzenie o ochronie danych, art. 7.
[41] Ogólne rozporządzenie o ochronie danych, art. 8.

- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
- dane osoby były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa, któremu podlega administrator[42].

Prawo do bycia zapomnianym nie ma charakteru absolutnego[43]. Ustawodawca wskazuje okoliczności ograniczające korzystanie z niego. Nie ma ono zastosowania, jeżeli prawdopodobnym jest, że uniemożliwi lub poważnie utrudni dochodzenie i obronę roszczeń, a także gdy narusza prawo do wolności wypowiedzi i informacji, utrudnia wykonanie zadań realizowanych w interesie publicznym w ramach sprawowania władzy publicznej powierzonej administratorowi, ze względu na interes publiczny w zakresie zdrowia publicznego, w przypadku badań naukowych oraz realizacji celów archiwalnych, historycznych i statystycznych[44].

Osoba, której dane dotyczą, ma również prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania jej danych, w tym profilowania. Administratorowi nie wolno przetwarzać tych danych, chyba że wykaże prawnie uzasadnione podstawy do przetwarzania nadrzędnych wobec interesów, praw i wolności tej osoby lub podstaw do ustalenia, dochodzenia lub obrony roszczeń[45].

Naruszenie ochrony danych osobowych

Obecnie w polskim prawie stosuje się procedurę powiadamiania o naruszeniu ochrony danych osobowych zarówno organu nadzorczego, jak i osoby,

[42] Ogólne rozporządzenie o ochronie danych, art. 17, pkt 1.
[43] J.J. Feliński, *Bezpieczeństwo danych osobowych w kontekście zmiany przepisów prawa polskiego i Unii Europejskiej dotyczącego gromadzenia, przechowywania, komercyjnego wykorzystywania – nowy zakres administratorów*, [w:] *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni: wymiar teoretyczny i praktyczny*, red. S. Topolewski, K. Karwacka, Wyd. Akademickie AMW, Gdynia 2015, s. 31.
[44] Ogólne rozporządzenie o ochronie danych, art. 17, pkt 3.
[45] Ogólne rozporządzenie o ochronie danych, art. 21, pkt 1.

której dane dotyczą. Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego, niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia oraz nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych[46]. Brak wiedzy o skali tego zjawiska uniemożliwiał dotąd wypracowanie skutecznych mechanizmów przeciwdziałających powstawaniu takich incydentów, a i osoba, której dane dotyczą, często nie wiedziała, że jej dane stały się przedmiotem naruszenia[47]. Upowszechnienie obowiązku zgłaszania przez administratorów danych naruszeń ma na celu, w głównej mierze, zminimalizowanie możliwych do wystąpienia szkód o charakterze majątkowym, jak i niemajątkowym, osób, których dane dotyczą[48].

Zgłoszenie naruszenia danych osobowych do organu nadzorczego musi nastąpić najpóźniej w ciągu 72 godzin od momentu stwierdzenia tego naruszenia, chyba że administrator jest w stanie, zgodnie z zasadą rozliczalności, uprawdopodobnić, że to naruszenie nie będzie powodować ryzyka naruszenia praw i wolności osób fizycznych. Jeżeli nie jest możliwe dokonanie zgłoszenia w obowiązującym terminie, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn tego opóźnienia, a informacje mogą być przekazywane sukcesywnie, bez zbędnej zwłoki[49].

Zgłoszenie naruszenia ochrony danych do organu nadzorczego musi zawierać co najmniej:

- opis charakteru 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;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;

[46] Ogólne rozporządzenie o ochronie danych, art. 4, pkt 12.
[47] A. Stępień, P. Biały, *Bezpieczeństwo danych osobowych zgodnie z RODO*, Wiedza i Praktyka, Warszawa 2017, s. 43.
[48] A. Stępień, *Ochrona danych osobowych…*, dz. cyt., s. 129.
[49] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 85.

- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków[50].

Na administratora został też nałożony obowiązek zawiadomienia o naruszeniu ochrony danych osoby, której dane dotyczą, w przypadku gdy może powodować ono wysokie ryzyko naruszenia jej praw i wolności. Informację, sformułowaną jasnym, prostym językiem, zawierającą opis charakteru naruszenia ochrony danych oraz zalecenia co do minimalizacji potencjalnych niekorzystnych skutków, należy przekazać najszybciej, jak to możliwe[51]. Ustawodawca na mocy art. 34 pkt 3 przewiduje zwolnienie administratora z obowiązku zawiadamiania osoby, której dane dotyczą, w przypadkach gdy:

- wdrożył odpowiednie środki techniczne i organizacyjne i zostały one zastosowane do danych osobowych, których dotyczy naruszenie;
- zastosował środki mające na celu wyeliminowanie prawdopodobieństwa wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą;
- zawiadomienie osoby, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku; w takiej sytuacji zostaje wydany publiczny komunikat informujący osoby, których dane dotyczą, o powstałym naruszeniu.

Przetwarzanie danych osobowych

Przetwarzanie dostosowane do wymogów nowoczesnej technologii oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany. Jest to każde zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[52].

Przetwarzanie danych podlega kilku zasadom. Są to:

[50] Ogólne rozporządzenie o ochronie danych, art. 33 pkt 3.
[51] Ogólne rozporządzenie o ochronie danych, preambuła, motyw 86.
[52] Ogólne rozporządzenie o ochronie danych, art. 4 pkt 2.

- zgodność z prawem, rzetelność i przejrzystość – przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- ograniczenie celu – zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- minimalizacja danych – dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- prawidłowość – prawidłowe i w razie potrzeby uaktualniane dane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- ograniczenie przechowywania – przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane;
- integralność i poufność – przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych[53].

Zasada rozliczalności nakłada na administratora obowiązek ewentualnego udowodnienia, że sposób przetwarzania i wprowadzone zabezpieczenia są wystarczające w stosunku do przetwarzanych przez niego kategorii danych, charakteru i celu przetwarzania bez ryzyka naruszenia praw lub wolności osób fizycznych. Przepisy prawa nie konkretyzują przykładów najlepszych rozwiązań i nie określają minimalnych standardów technicznych zabezpieczenia danych, wprowadzają jednak pojęcie pseudonimizacji, czyli przetwarzania danych w taki sposób, by nie można ich było przypisać konkretnej osobie bez użycia dodatkowych informacji, pod warunkiem że te dodatkowe informacje są przechowywane osobno i odpowiednio zabezpieczone. W praktyce oznacza to wdrożenie niezbędnych zabezpieczeń, adekwatnych dla każdego administratora, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, w celu skutecznej realizacji zasad ochrony danych[54].

[53] Ogólne rozporządzenie o ochronie danych, art. 5 pkt. 1 lit. a)-f).
[54] *Gotowi na RODO. Opracowanie GIODO*, https://uodo.gov.pl [dostęp 19.11.2018].

Przetwarzanie danych osobowych zgodnie z prawem odbywa się, jeżeli zostanie spełniony jeden z poniższych warunków:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym określonym celu lub w większej liczbie (również określonych) celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub przed zawarciem umowy – do podjęcia działań na żądanie osoby, której dane dotyczą;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem[55].

Wiele organizacji, instytucji, zarówno sektora publicznego, jak i prywatnego, wykorzystuje w swoich codziennych działaniach dane osobowe. Różnego rodzaju informacje, w tym także dane wrażliwe, są gromadzone i przetwarzane w celu sprawnego świadczenia usług. Współczesna rzeczywistość, w której informacja o osobie zyskała wymierną wartość materialną, znacznie utrudnia skuteczną ochronę prywatności i bezpieczeństwo danych osobowych, które mogą być w wielu przypadkach narażone na niewłaściwe wykorzystanie. Dynamika obszaru usług elektronicznych skutkuje coraz szerszym przetwarzaniem informacji, co może wiązać się ze wzrostem zagrożeń związanych z ich wykorzystaniem przez podmioty do tego nieuprawnione. Obecnie nie można lekceważyć nawet

[55] Ogólne rozporządzenie o ochronie danych, art. 6 pkt 1.

minimalnych cyberzagrożeń dla bezpieczeństwa danych osobowych, a co za tym idzie, szeroko rozumianego bezpieczeństwa prywatności jednostki.

Bibliografia

Akty prawne

Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 (Dz.U. z 1952 r. Nr 33, poz. 232 ze zm.).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 (Dz.U. z 2009 r. Nr 114, poz. 946).

Konwencja o ochronie praw człowieka i podstawowych wolności (europejska konwencja praw człowieka) (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016).

Ustawa z dnia 17 marca 1921 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1921 r. Nr 44, poz. 267).

Ustawa Konstytucyjna z dnia 23 kwietnia 1935 r. (Dz.U. z 1935 r. Nr 30, poz. 227).

Ustawa z dnia 19 grudnia 1989 o zmianie Konstytucji Polskiej Rzeczypospolitej Ludowej (Dz.U. z 1989 r. Nr 75, poz. 444).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

Wyrok SN z dnia 8 kwietnia 1994 r., sygn. III ARN 18/94, OSNP 1994, nr 4, poz. 550.

Wyrok TK z dnia 21 października 1998 r., sygn. K 24/98, OTK 1998, nr 6, poz. 97.

Opracowania

Barta J., Fajgielski P., Markiewicz R., *Część pierwsza – Wstęp*, [w:] *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2015.

Dopierała R., *Internetowe manifestacje prywatności*, „Media – Kultura – Społeczeństwo" 2008, nr 3.

Feliński J.J., *Bezpieczeństwo danych osobowych w kontekście zmiany przepisów prawa polskiego i Unii Europejskiej dotyczącego gromadzenia, przechowywania, komercyjnego wykorzystywania – nowy zakres administratorów*, [w:] *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczny*, red. S. Topolewski, K. Karwacka, Wyd. Akademickie AMW, Gdynia, 2015.

Gajda A., *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace" / OW SGH, 2014.

Goliński M., *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru*, OW SGH, Warszawa 2011.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, PWN, Warszawa 2008.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 2.

Jędruszczak K., *Prywatność jako potrzeba w ramach koncepcji siebie*, „Roczniki Psychologiczne" 2005, nr 2.

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

Kopka J., *Prywatność w społecznej komunikacji. Odniesienia teoretyczne i dynamika przemian w społeczeństwie sieci*, [w:] *E-społeczeństwo w Europie Środkowej i Wschodniej. Teraźniejszość i perspektywy rozwoju*, red. S. Partycki, Wyd. KUL, Lublin 2015.

Krzysztofek K., Szczepański M.S., *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wyd. UŚ, Katowice 2005.

Leja P., *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, „Prawo Mediów Elektronicznych" 2017, nr 3.

Motyka K., *Prawo do prywatności*, „Zeszyty Naukowe Akademii Podlaskiej w Siedlcach. Seria Administracja i Zarządzanie" 2010, nr 85.

Ossowska M., *Normy moralne. Próba systematyzacji*, PWN, Warszawa 1985.

Safjan M., *Ochrona prywatności na tle Konstytucji z 1997 roku – ramy normatywne*, [w:] *Wyzwania dla państwa prawa*, Oficyna, Warszawa 2007.

Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6.

Stępień A., Biały P., *Bezpieczeństwo danych osobowych zgodnie z RODO*, Wiedza i Praktyka, Warszawa 2017.

Stępień A., *Ochrona danych osobowych w świetle rozporządzenia ogólnego – omówienie wybranych zagadnień*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Wyd. Nauk. UPH, Siedlce 2018.

Źródła internetowe

Europejski Inspektor Ochrony Danych, „W kierunku nowej etyki cyfrowej: dane, godność i technologia", https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_summary_pl.pdf [dostęp 9.04.2020].

Gotowi na RODO. Opracowanie GIODO, https://uodo.gov.pl [dostęp 19.11.2018].

The right to privacy and personal data protection in the Republic of Poland

Summary: Allowing people to be innovative and to use other rights and freedoms, the right to privacy protects human dignity and opens up opportunities for independent life and personality development. Fast technical development and globalization have brought new challenges for the protection of personal data as part of privacy protection. Technology has transformed both economy and social life, and should further facilitate the free flow of personal data within the European Union and to third countries and international organizations, while ensuring a high level of personal data protection.
Keywords: *right to privacy, personal data protection*