Ustawa o ochronie danych osobowych w aspekcie bezpieczeństwa informacji

LESZEK KLICH

DR CEZARY SOCHALA

Bezpieczeństwo jest najwyższą wartością i potrzebą społeczną, ponieważ jego zagrożenie może w konsekwencji prowadzić m.in. do zahamowania rozwoju jednostki[1].

Słowa kluczowe: bezpieczeństwo, dane osobowe, ochrona danych osobowych, ustawa o ochronie danych osobowych.

Abstract: *As indicated by the research results – in Poland, the protection of personal data is not sufficient. The media are permanently alarming about the development in trading of personal data. According to the publications, many entities use new technology not only to collect personal data, but they also use behavioural analysis for user profiling. The consequence of these negative processes might be social segregation or exclusion, and – in the long run – discrimination. This paper is devoted to selected problems of data security originating from the Act on Personal Data Protection.*

Bezpieczeństwo informacji jest szczególną kategorią, która w dobie powszechnej technologii znacznie zyskuje na znaczeniu. Istotną rolę w ochronie tego obszaru pełni prawodawstwo, stanowiące podstawowy filar holistycznie ujmowanego bezpieczeństwa.

Tworzenie czytelnego prawa w tym obszarze służyć może zwiększaniu zaangażowania społeczeństwa w budowanie ochrony informacji oraz poczucia bezpieczeństwa prywatności przez obywateli, co w dużym stopniu zależy zarówno od sytuacji prawnej, ale także od skutecznych procedur profilaktycznych[1]. W dobie powszechnego osieciowienia, granice postrzegania bezpieczeństwa przez teoretyków stało się transsektorowe/transdziałowe[2]. W konsekwencji, stan bezpieczeństwa państwa jest ściśle związany ze stanem jego bezpieczeństwa teleinformatycznego, do którego zaliczyć można ochronę danych osobowych[3].

Obecnie, trudno jest sobie wyobrazić funkcjonowanie człowieka bez dobrodziejstw infrastruktury teleinformatycznej oraz technologii. Dostrzec jednak należy zwiększanie się liczby możliwych obszarów negatywnego oddziaływania, także w cyberprzestrzeni, zaś szczególnie w obszarze bezpieczeństwa informacji[4].

1. A. Polcyn-Radomska, Wartość, znaczenie i uwarunkowania bezpieczeństwa narodowego, Fides Et Ratio, 1(17)2014, s. 1.
2. M. Torczyńska, Społeczny wizerunek straży pożarnej jako filaru bezpieczeństwa państwowego, w: Bezpieczeństwo i technika pożarnicza, D. Wróblewski (red.), Józefów 2014, Vol. 36/4 2014, s. 51.
3. Zob. Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2013, s. 19 i 247.
4. A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kollegium Analiz Ekonomicznych nr 29/2013,

Kluczową kwestią w zwiększaniu bezpieczeństwa tego obszaru jest zrozumienie jego wpływu na całokształt funkcjonowania państwa oraz wprowadzanie takich zapisów prawnych, których efektem będzie czytelny podział zarówno praw, jak i obowiązków obywateli.

Tymczasem, jak wskazują wyniki badań, w Polsce powyższe dobra są chronione niedostatecznie. Media permanentnie alarmują o rozkwicie handlu danymi osobowymi. Liczne podmioty posługują się nowoczesną technologią nie tylko do zbierania danych osobowych. Często pozyskane informacje wykorzystują w analizie behawioralnej, profilując użytkowników[5] i budują wiedzę, która oprócz podstawowych informacji o osobach, pozwala dokonywać kategoryzacji czy segregacji. Konsekwencją tych negatywnych procesów może być segregacja społeczna czy wykluczenie, zaś w końcowym efekcie – dyskryminacja[6].

Zdaniem ekspertów, w Polsce proceder ten kwitnie jak nigdy wcześniej i w coraz większym stopniu wykorzystywany jest w celach marketingowych.

Jeszcze poważniejszym problemem jest budowanie spersonalizowanych baz osobowych i przekazywanie ich do innych baz marketingowych. Takie praktyki, niestety, bardzo trudno jest udowodnić. W polskim sektorze ochrony danych osobowych do bezprawnego wykorzystania danych, czy wręcz ich kradzieży, dochodzi bardzo często i niemal za każdym razem nikt nie ponosi za to odpowiedzialności[7].

Rynek danych osobowych

W marketingu bezpośrednim podstawą biznesu są bazy zawierające precyzyjnie sprofilowane dane osobowe, umożliwiające dotarcie z ofertą sprzedaży do potencjalnych klientów. Firmom coraz rzadziej zależy na jak największej liczbie odbiorców przekazu reklamowego, starają się dotrzeć do zainteresowanych konkretnym produktem czy usługą i dlatego czarny rynek baz stale rośnie, a ich cena zależy od precyzyjności wiedzy o osobach oraz ich preferencjach. Towarem są dane kontaktowe i zestaw informacji, dzięki którym można ściśle dopasować produkt do odbiorcy. Im więcej szczegółów dotyczących zachowań i zainteresowań profilowanej osoby konkretnym wachlarzem produktów lub usług, tym wyższa cena[8].

We współczesnych uwarunkowaniach regulacje prawne dotyczące ochrony danych osobowych spełniają kluczową rolę w zapewnieniu bezpieczeństwa człowieka. W dobie powszechnego wykorzystania technologii informacyjnych, muszą one zapewnić zachowanie określonych informacji w tajemnicy przed nieuprawnionymi podmiotami, chroniąc jednostkę przed nadmierną ingerencją ze strony innych.

Geneza i zasadnicze pojęcia

Pojęcie „prywatność" rozumiane jest zazwyczaj dwojako: jako jedno z podstawowych praw człowieka oraz jako termin prawny. Funkcjonuje relatywnie krótko, jako że poważna dyskusja dotycząca tej problematyki rozpoczęła się w roku 1890, po ukazaniu się artykułu Warrena i Brandeisa *The Right to Privacy*. Autorzy postulowali legalizację ochrony prywatności ze względu na postęp cywilizacyjny, który daje możliwość inwigilacji obywateli[9].

Prawo do prywatności zalicza się do pierwszej generacji praw człowieka. Ochrona sfery życia prywatnego jest fundamentem większości współczesnych systemów prawnych. W ujęciu normatywnym zakłada uprawnienie jednostki do kształtowania sfery prywatnej życia,

Wydział Humanistyczny Uniwersytet Pedagogiczny w Krakowie, http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z29_30.pdf, s. 452.

5. L. Klich, C. Sochala, Bezpieczeństwo w cyberprzestrzeni jako wyzwanie dla współczesnych państw. Zarys problemu, [w:] Bezpieczeństwo. Rodzina – naród – społeczeństwo, J. Zimny (red.), Wyższa Szkoła Ekonomiczna w Stalowej Woli, Katolicki Uniwersytet Lubelski, Stalowa Wola 2016, s. 277.
6. Profilowanie oznacza w tym przypadku analiza cech niezmiennych, jak np. wiek, płeć, pochodzenie etniczne, etc. Jak i zmiennych, jak preferencje, obyczaje, zainteresowania. Metoda służy dopasowaniu i korelacji określonych zachowań (np. wyborów konsumenckich) z cechami (np. wiek), tamże.
7. J. Niklas, Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji, Polskie Towarzystwo Prawa Antydyskryminacyjnego, http://ptpa.org.pl/public/files/Profilowanie%20w%20kontek%C5%9Bcie%20ochrony%20danych%20osobowych%20i%20zakazu%20dyskryminacji.pdf (stan na 30-05-2016).
8. http://natemat.pl/126475,zapomnij-o-anonimowosci-w-polsce-kwitnie-handel-danymi-osobowymi-prawnik-bedzie-coraz-gorzej (stan na 20.05.2016).
9. http://finanse.wp.pl/kat,1037883,title,Handel-danymi-osobowymi-Ile-kosztuje-twoje-nazwisko,wid,15895792,wiadomosc.html (stan na 20.05.2016).

dla zapewnienia wolności od ingerencji i niedostępności dla innych[10].

Ponieważ jednostki ingerujące w sprawy osobiste innych ludzi istnieją w każdej społeczności, współczesne państwa rozbudowują w znaczącym zakresie instrumenty prawa ochrony prywatności. Dynamiczny rozwój technik służących zbieraniu, gromadzeniu i wyszukiwaniu informacji dotyczących poszczególnych osób sprawia, że wzrasta konieczność prawnej ochrony ludzkiej prywatności. Implikuje to z kolei konieczność wyznaczenia sfery życia osobistego, w którą nieupoważniony podmiot nie będzie ingerował, gdyż każdy człowiek ma prawo dysponowania sobą oraz prawo do niezakłóconego rozwijania własnej fizycznej i psychicznej tożsamości, kształtowanej według własnej woli i bycia niezależnym w określonym zakresie od wpływów zewnętrznych[11].

Sformułowanie „prawo do prywatności" występuje zamiennie z innymi określeniami. Do najbardziej popularnych należą: „prywatność", „sfera osobista człowieka", „prawno-osobista sfera własna", „sfera osobowości", „ sfera intymności", „obszar tajności" oraz „sfera indywidualności",[12] zaś każde z wymienionych pojęć posiada określoną konotację.

Należy zatem zwracać uwagę na poszczególne znaczenia, odnoszące się do wyodrębnionej dziedziny nauki czy aktywności ludzkiej. Pojmowanie przedmiotowego znaczenia terminu uznać można za wspólne, gdyż każdorazowo chodzi o przekonanie o przeciwstawieniu sfery osobistej jednostki ze sferą najszerzej rozumianego interesu publicznego, realizowanego przez organy dysponujące aparatem państwowym, jako źródła prawa do prywatności.

W konsekwencji prawo do prywatności rozumieć należy jako zastrzeżoną przestrzeń osobistą, która wynika z godności jednostki – wolnej od ingerencji za strony innych jednostek czy podmiotów prawa[13].

Oprócz pojęcia „prawo do prywatności" funkcjonuje także pojęcie „dóbr osobistych", przysługujących wszystkim osobom fizycznym. Ze względu na swój charakter niemajątkowy są niezbywalne i nie można się ich zrzec. Wygasają wraz ze śmiercią podmiotu uprawnionego. Odniesienia do dóbr osobistych spotkać można w Kodeksie cywilnym, który co prawda nie zawiera definicji dobra osobistego, ale określa je jako związane ściśle z osobą ludzką: zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Warto podkreślić, że dobra te podlegają ochronie prawa cywilnego, niezależnie od ochrony przewidzianej w innych przepisach. Należy także zauważyć, że powyższy katalog dóbr osobistych jest otwarty. Obejmuje nie tylko wartości wymienione w kodeksie cywilnym, ale każde inne dobra, jak: sfery życia psychicznego, życie rodzinne, życie prywatne – w tym intymne, kult pamięci osoby zmarłej oraz poczucie przynależności do określonej płci[14].

Początkowo postrzeganie dóbr osobistych opierało się na kryterium subiektywnym, w którym nacisk kładziono na odczucia osoby żądającej[15]. Tego typu podejście reprezentował S. Grzybowski, który określił dobra osobiste jako indywidualne wartości świata uczuć czy stanu psychicznego człowieka[16]. Współcześnie, przy wyjaśnianiu istoty dóbr osobistych oraz ich naruszeń, dominuje pogląd, iż należy posługiwać się ujęciem obiektywnym, które odwołuje się do ocen przyjętych w społeczeństwie[17]. Tak zdefiniowane kryterium, literatura przedmiotu wskazuje jako dobra osobiste uznane przez system prawny za wartości obejmujące fizyczną i psychiczną integralność człowieka, jego indywidualność, godność oraz pozycję w społeczeństwie, stanowiące przesłankę do samorealizacji osoby ludzkiej[18].

W dobie nowoczesnych technologii kluczową rolę w zapewnieniu bezpieczeństwa człowieka pełnią regulacje prawne dotyczące ochrony danych osobowych. Powinny one zapewnić zachowanie określonych informacji w tajemnicy przed innymi, jednocześnie chroniąc jednostkę przed nadmierną ingerencją z zewnątrz.

10. A. Lewicka-Strzałecka, Prywatność: wartość czy towar, Kultura i ekonomia, 2003, nr 1, 309-321, Instytut Filozofii i Socjologii PAN.
11. M. Pryciak, Prawo do prywatności, s. 212.
12. Tamże.
13. J. Braciak, Prawo do prywatności, Warszawa 2004, s. 5.
14. http://www.infor.pl/prawo/prawa-konsumenta/prawa-konsumenta/308547,Dobra-osobiste-i-ich-ochrona.html (stan na 08-12-2015).
15. http://www.infor.pl/prawo/prawa-konsumenta/prawa-konsumenta/308547,Dobra-osobiste-i-ich-ochrona.html (stan na 08-12-2015).
16. K. Grzybczyk, Naruszenie dobra osobistego w reklamie, „Rejent" 1999, nr 9, s. 120.
17. S. Grzybowski, Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego, Warszawa 1957, s. 78.
18. M. Pazdan [w:] Kodeks cywilny. Komentarz do artykułów 1-449[1o], t. I, red. K. Pietrzykowski, Warszawa 2011, s. 119.

W polskim prawodawstwie odwołania do ochrony prywatności zawarto już w Konstytucji Rzeczypospolitej Polskiej. Przepis art. 47a, stanowi, że każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Jeszcze bardziej precyzyjne odniesienie do ochrony prywatności znaleźć można w art. 51, w którym zapisano między innymi, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby oraz że każdy ma prawo dostępu do własnych danych w zbiorach danych[19]. Konstytucja jednocześnie daje obywatelowi prawo dostępu do dotyczących go danych, ich poprawiania lub usuwania nieprawdziwych, niepełnych lub zebranych w sposób niezgodny z przepisami ustawy.

Problematyka ochrony danych osobowych w Polsce znajduje odzwierciedlenie w rozwiązaniach systemowych, dedykowanych zapewnieniu bezpieczeństwa państwa. Najwyższy system, nadrzędny w państwie, w stosunku do systemu dedykowanemu ochronie danych osobowych jest system bezpieczeństwa narodowego. W XXI w. jego zakres podmiotowy określono w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej zatwierdzonej przez Prezydenta Rzeczypospolitej Polskiej 13 listopada 2007 r.[20], jako drugiej już strategii bezpieczeństwa narodowego w Polsce. Dokument ten sprecyzował interesy narodowe i sformułował cele strategiczne, zgodnie z przepisami Konstytucji[21].

Zapisy Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej dotyczyły szeregu przedsięwzięć realizowanych na rzecz bezpieczeństwa i obronności państwa, wymagających określonych zdolności systemów wsparcia. W celu ich zapewnienia należało tworzyć i rozwijać długofalowe plany ochrony kluczowych systemów teleinformatycznych przed uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane, zakłócaniem normalnego ich funkcjonowania, kradzieżą tożsamości i sabotażem. Jako proces ciągły postulowano stałe ocenianie możliwości wtargnięcia do systemów teleinformatycznych. Właściwe podmioty zobligowane zostały do przygotowania możliwych form odpowiedzi na ataki oraz rozwijania metod ewaluacji poniesionych strat informacyjnych. Jako priorytet państwa ustanowiono wspieranie narodowych programów i technologii informacyjnych[22].

Szczegółowo ochronę danych osobowych reguluje przede wszystkim ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (dalej ustawa o ochronie danych osobowych)[23]. Regulacja ta obejmuje prawa i obowiązki przetwarzania[24] danych osobowych zarówno w zbiorach[25] tradycyjnych, jak i w systemach informatycznych[26], a także problematykę przetwarzania danych poza zbiorem danych.

19. Z. Radwański, Prawo cywilne – część ogólna, Warszawa 1997, s. 148.
20. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78 poz. 483).
21. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 r. kierowana była do wszystkich organów administracji publicznej oraz podmiotów realizujących zadania z zakresu bezpieczeństwa. W myśl zapisu strategii – dokument„[…], jako wyraz troski konstytucyjnych organów państwa o zapewnienie Polsce i Polakom bezpieczeństwa, określa formy narodowego wysiłku w tej dziedzinie". Urzeczywistnienie zawartych w nim kierunków działań stanowiło obowiązek władz Rzeczypospolitej Polskiej i całego społeczeństwa, który zapewnić miał Polsce bezpieczeństwo dzisiaj i w przyszłości oraz pozycje na arenie międzynarodowej na miarę jej aspiracji. Za wdrożenie jej ustaleń odpowiedzialnymi uczyniono ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych, wojewodów, organy samorządu terytorialnego oraz inne podmioty, którym ustawowo powierzono stosowne uprawnienia i obowiązki w obszarze przedmiotowym bezpieczeństwa narodowego. Po wejściu w życie Strategii Bezpieczeństwa Narodowego RP należało opracować lub skorygować strategie dla poszczególnych działów administracji rządowej, a także strategie działania poszczególnych instytucji, którym powierzono szczególne zadania w dziedzinie bezpieczeństwa narodowego. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007 r., s. 37.
22. Tamże.
23. Tamże, s. 20.
24. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135).
25. Za przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych (art. 7 pkt. 2 Ustawy o ochronie danych osobowych).
26. Jako zbiór, rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie (art. 7 pkt. 1 Ustawy o ochronie danych osobowych).

Ustawa o ochronie danych osobowych reguluje zasady postępowania przy przetwarzaniu danych osobowych, prawa osób fizycznych, wprowadza zasady zabezpieczania danych osobowych, procedurę rejestracji zbiorów danych osobowych, procedurę przekazywania danych osobowych do państw trzecich oraz ustala sankcje karne związane z naruszeniami prawa o ochronie danych osobowych. Przepisy w niej zawarte stosuje się zarówno w podmiotach państwowych jak i pozapaństwowych, które przetwarzają lub zamierzają przetwarzać informacje sklasyfikowane jako dane osobowe.

Wraz z ustawą opublikowanych zostało szereg aktów wykonawczych, które w sposób istotny dopełniają przestrzeganie obowiązków wynikających z ochrony danych osobowych[27].

Przedmiotem ochrony – wskazanym w ustawie o ochronie danych osobowych – są dane osobowe. Definicja klasyfikująca informacje jako dane osobowe zawarta została w art. 6, w myśl którego za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Należy także w tym miejscu przytoczyć podobną definicję, którą zawarto w konwencji nr 108, w myśl art. 2, gdzie do danych osobowych należy zaliczyć każdą informację dotyczącą osoby fizycznej o określonej tożsamości albo dającej się zidentyfikować[28].

Analizując powyższe przepisy i definicje, należy zauważyć, że oprócz podobieństwa, w obu wypadkach przesłanką jest informacja, która oznaczać może zarówno komunikat wyrażony w dowolnej formie (wiadomość, wypowiedź, prezentację), jak i znaki graficzne, symbole, fotografie, etc., niezależnie od sposobu, zakresu i swobody ich udostępniania, jak też niezależnie od sposobu, zakresu, swobody ich pozyskania. Istotną kwestią jest zwrócenie uwagi na fakt, że do danych osobowych zalicza się zarówno informacje już rozpowszechnione, jak i te jeszcze nieujawnione.[29]

W ustawie wprowadzono także pojęcie osoby możliwej do zidentyfikowania (pośrednio lub bezpośrednio), wymieniając kilka ogólnych determinantów, jak: numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne, których przetwarzanie podlega ustawie[30].

Ustawa wyróżnia dwa rodzaje danych osobowych – dane zwykłe oraz dane wrażliwe[31]. Dane zwykłe cechują się między innymi tym, że ich zdobycie nie wymaga nadzwyczajnych nakładów czasu, środków ani kosztów lub też są one zbyt ogólnikowe, przez co zidentyfikowanie na ich podstawie konkretnego człowieka może być trudne. Dodatkowo, dane te podawane są przez ich właścicieli stosunkowo często. Choć ustawa nie definiuje danych wrażliwych, w ustępie 1 art. 27 przedstawiona została zamknięta lista informacji, które mogą w znacznym stopniu naruszać intymność ich właściciela, co wynika z prawa każdego człowieka do prywatności[32]. Dane wrażliwe (sensytywne) mogą być przetwarzane wyłącznie w określonych przypadkach i po spełnieniu warunków zawartych w ust. 2 art. 27 ustawy o ochronie danych osobowych.

W wyniku badań szczegółowych, jednoznacznie wskazać należy brak ustawowego katalogu danych osobowych. Klauzula generalna została wprowadzona celowo, by uniknąć tworzenia zamkniętego katalogu informacji stanowiących dane osobowe, a użycie zwrotu „wszelkie informacje" ma na celu podkreślenie jego otwartości. Tak więc do zbioru zalicza się wszelkie aspekty osoby, w tym jej stosunków osobistych i rzeczowych, życia zawodowego, prywatnego, wykształcenia, wiedzy czy cech charakteru[33].

Wynika to między innymi z dynamiki i specyfiki współczesnej technologii, gdzie prawodawca nie nadąża za wprowadzaniem niezbędnych unormowań prawnych, ze względu na cechę legislacyjną, objawiającą się koniecznością dostatecznego zapoznania się z procesami informatyzacji (komputeryzacji, wirtualizacji, internetyzacji, cybernetyzacji), a co za tym idzie, niezbędnego czasu dla utrwalenia się procesu świadomości oraz

27. Ustawa precyzuje pojęcie systemu informatycznego w pkt. 2a art. 7, jako zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
28. Szerzej: http://www.giodo.gov.pl/233/ (stan na 13.05.2016).
29. Konwencja nr 108 RE o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dn. 28 stycznia 1981 r. (Ogłoszona D.n. 85-1203, 15 list. 1985. – JO 20 list. 1985. Weszła w życie 1.10.1985).
30. J. Barta, P. Fajgielski, R. Markiewicz, Komentarz do art.6 ustawy o ochronie danych osobowych, LEX, stan prawny na 01.07.2015.
31. Zob. Art. 6 Ustawy o ochronie danych osobowych.
32. Dane wrażliwe zwane także szczególnie chronionymi lub sensytywnymi.
33. Więcej: http://poradnik.wfirma.pl/-dane-osobowe-zwykle-i-wrazliwe (stan na 31.05.2016).

kształcenia w tym zakresie kadr prawników, administratywistów i menadżerów[34].

Przy analizie ustawy pewną wątpliwość budzi użycie frazy: zidentyfikowanej lub możliwej do zidentyfikowania, gdzie w przypadku drugim, prawdopodobnie chodzi o możliwość jednoznacznej identyfikacji, która na podstawie danych wejściowych potwierdza lub falsyfikuje wynik identyfikacji. Ujęcie jednoznacznej identyfikacji jest najbardziej pewne i nie budzi wątpliwości. Powiązać to należy bezpośrednio z etymologią słowa „identyfikować", które wywodzi się z łacińskiego zaimka *idem* (ten sam)[35], stąd w dokumencie rangi ustawy, dla czytelności, winno używać się właśnie takiego zwrotu[36].

Więcej informacji definiujących pojęcie jednoznacznej identyfikacji (prawdopodobnie w celu przekazu niebudzącego wątpliwości u odbiorcy), znaleźć można np. w ustawie z 11 marca 2004 r. o podatku od towarów i usług, gdzie w art. 106e w ust. 2 posłużono się określeniem jednoznacznej identyfikacji dokumentu (w tym wypadku fiskalnego)[37]. Biorąc pod uwagę powyższe rozważania, należy założyć, że ustawa określa pojęcie jednoznacznej identyfikacji, co ma istotne znaczenie dla dalszej części rozważań.

Te daleko idące uogólnienia, zwłaszcza w przypadku definicji prawnych, prowadzą do problemów interpretacyjnych. Ich konsekwencją są wątpliwości, które występują już na etapie rozstrzygania, czy informacja lub zbiór stanowi dane osobowe. Wynikiem takiej kwalifikacji jest chociażby fakt podlegania lub niepodlegania restrykcyjnym przepisom ustawy o ochronie danych osobowych. Dodatkowym wyzwaniem dla klasyfikującego jest sytuacja zaistniała w wyniku nieprecyzyjnego przepisu tej ustawy, wskazującego na konieczność przeprowadzenia zindywidualizowanej oceny, wymagającej uwzględnienia konkretnych okoliczności w określonej sytuacji do identyfikacji osoby[38].

Z ustawy wynika, że w zależności od typu, do danych osobowych zalicza się pojedynczą informację oraz zbiór informacji, stąd w zależności od treści, ochronie może podlegać zarówno informacja pojedyncza, jak i zbiór[39] informacji.

Podczas rozważań nad klasyfikacją zbioru informacji o osobach, uwzględniając przepis ustawy o ochronie danych osobowych o „ogólności informacji", przyjmuje się, że zbiór zawierający podstawowe informacje takie, jak imiona czy nazwiska, nawet w przypadku ich zestawienia, nie stanowi przedmiotu ochrony. Wynika to głównie z dużego prawdopodobieństwa występowania zbieżności imion oraz nazwisk. W przypadku przetwarzania zbiorów zawierających tak ogólne informacje, nie może być mowy o ich klasyfikacji jako zbiory danych osobowych. Na podstawie zgromadzonych informacji nie można przecież jednoznacznie zidentyfikować konkretnej osoby. Badania wykazują, że w Polsce występuje duża powtarzalność nazwisk, które w przypadku tych najpopularniejszych, sięga nawet kilkudziesięciu tysięcy[40]. Zatem nawet w przypadku przetwarzania zbiorów zawierających imiona i nazwiska, identyfikacja konkretnej osoby nie jest w rzeczywistości możliwa.

Wątpliwości budzi również kwalifikacja zbiorów zawierających imiona i nazwiska nietypowe[41], w których prawdopodobieństwo występowania tożsamych nazw może być niewielkie. Jednak w tym wypadku, pomimo zwiększonego prawdopodobieństwa identyfikacji, trzeba brać pod uwagę, że w celu jednoznacznej identyfikacji konkretnej osoby, należy posłużyć się bazą danych wszystkich mieszkańców kraju pod kątem występowania identyczności. Nawet w przypadku istnienia takiej bazy, można w tym miejscu powołać się na zapis art. 6 pkt. 3, wyłączający z ustawy o ochronie danych osobowych dane, których zdobycie wiąże się z nadmiernymi kosztami, działaniami oraz czasem[42].

34. Tamże.
35. J. Janowski, Elektroniczny obrót prawny, Wolters Kluwer, Warszawa 2008, s. 28.
36. Por. Słownik Języka Polskiego, http://sjp.pwn.pl/slowniki/identyfikacja.html (stan na 10.05.2016).
37. Pojęcie jednoznacznej (pewnej) identyfikacji można znaleźć także w teorii baz danych, gdzie tzw. klucz główny jest kolumną tabeli, która jednoznacznie identyfikuje pojedynczy wiesz.
38. Ustawa z dnia 11 marca.2004 r. o podatku od towarów i usług (Dz. U. z 2013 r. poz. 35).
39. Por: http://www.giodo.gov.pl/317/id_art/973/j/pl/ (stan na 11.05.2016).
40. Wg Słownika PWN, zbiorem nazywamy całość składającą się z jakichś elementów, ze względu na jakąś cechę, http://sjp.pwn.pl/sjp/zbior;2544923.html (stan na 13.05.2016).
41. Zob. Statystyki imion i nazwisk z bazy PESEL, https://mswia.gov.pl/pl/sprawy-obywatelskie/statystyki-imion-i-nazw (stan na 11.05.2016).
42. W tym wypadku chodzi o występowanie nazwisk lub zestawień imion i nazwisk nie mających cech typowych dla określonej serii, rzadko spotykanych, więcej: Encyklopedia PWN, http://sjp.pwn.pl/slowniki/nietypowy.html.

Identyfikacja osoby na podstawie pojedynczej informacji lub zbioru zawierającego jedynie imiona i nazwiska będzie z dużym prawdopodobieństwem negatywna, stąd w celu wykluczenia pomyłek podczas tego procesu, przetwarzane powszechnie zbiory danych (np. w urzędach), zawierają dodatkowe informacje zawężające, które pozwalają w sposób jednoznaczny zidentyfikować konkretną osobę.

Tego typu dodatkowe informacje, do których zaliczyć można np. datę urodzenia, imię ojca, matki, adres wraz z numerem domu, itp. same w sobie nie należą do danych osobowych, jednak w zestawieniu z imieniem i nazwiskiem, ich przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie[43].

Do zbiorów informacji danych osobowych należy więc zaliczyć pojedyncze informacje (jednoznaczne identyfikatory, jak np. numer dowodu, numer paszportu, PESEL[44], wizerunek[45], etc.).

Informacją identyfikującą osobę jest również jego adres e-mail, który podlega ochronie danych osobowych ze względu na jego unikalność[46]. Adresy poczty elektronicznej należy więc w świetle ustawy kwalifikować jako pojedyncze informacje jednoznacznie identyfikujące. Zatem zgromadzone dane adresów e-mail zalicza się do zbiorów danych osobowych.

W tym miejscu należy dostrzec problem umownego podziału adresów poczty e-mail, w których w pierwszym przypadku występuje ciąg zawierający imię i nazwisko, w drugim zaś może występować przypadkowy ciąg znaków. Jednakże ze względu na wymienioną wcześniej cechę unikalności, adres e-mail stanowi dane osobowe, skoro pozwala na identyfikację osoby[47].

W powyższym przypadku należy odwołać się do zapisów art. 6 ust. 3 o nadmiernych kosztach, czasie lub działaniach koniecznych do identyfikacji, na podstawie wyłącznie adresu e-mail, ze względu na powszechność funkcjonujących współcześnie portali społecznościowych, wyszukiwarek czy for. Stąd identyfikacja adresu, nawet w przypadku, gdy ciąg znaków nie zawiera całości lub części imienia i/lub nazwiska, współcześnie nie wymaga nadmiernych działań w procesie identyfikacji. Kolejnym spornym identyfikatorem, który musi budzić daleko idące wątpliwości jest adres IP komputera. Pewne wskazówki w tej sprawie można znaleźć na stronie Generalnego Inspektora Ochrony Danych Osobowych (GIODO)[48], gdzie podkreślono, że w pewnych okolicznościach adresy identyfikacyjne komputerów można uznać za dane osobowe. Przesłanką jest w tym przypadku typ przyznawania adresów, który w zależności od operatora, może mieć charakter statyczny[49] lub dynamiczny[50].

Dalsze informacje zidentyfikować można w oparciu o dodatkowe doprecyzowanie: „gdy adres IP jest na stałe lub na dłuższy czas przypisany do konkretnego urządzenia", co może oznaczać możliwość identyfikacji osoby, za wyjątkiem szczególnych przypadków[51]. W celu wyjaśnień dotyczących tej kwestii, powołano się na opinię Grupy Roboczej ds. Ochrony Danych powołanej przez Parlament Europejski i Radę Europejską (rozdz. III pkt. 3 przykład 15), która słusznie uznała adres IP za dane dotyczące osoby możliwej do zidentyfikowania przez dostawców Internetu.

Podkreślić należy występującą na stronie internetowej GIODO niejednoznaczność w kwalifikacji adresu IP w stosunku do katalogu danych osobowych, na co wskazuje doprecyzowanie, że adres IP nie zawsze stanowi informację

43. Warto także przytoczyć przykład z codzienności, gdzie w urzędach, przy załatwianiu formalności, oprócz podania imienia i nazwiska, w celu identyfikacji – a tym samym w celu uniknięcia pomyłek, oprócz imienia i nazwiska, podaje się inne dane zawężające zakres, jak np. PESEL, imię ojca, etc., co ostatecznie rozwiewa wątpliwości w tym zakresie.
44. Por. http://www.giodo.gov.pl/317/id_art/973/j/pl/ (stan na 13.05.2016).
45. Zgodnie z art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2015 r. poz. 388), PESEL jest 11-cyfrowym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną.
46. Fotografia stanowi niewątpliwie dane osobowe, zaliczane do danych biometrycznych, stąd oprócz ochrony wynikającej z ustawy o ochronie danych osobowych, podlegają także ochronie wynikającej z ustawy o prawie autorskim i prawach pokrewnych pozwala na ich prawna ochronę. Art. 81 tej ustawy w ust. 1.
47. Nazwa adresu pocztowego składa się z identyfikatora, znaku umownego @ oraz domeny, zaś ze względu na unikalność nazw domen, adres e-mail jest unikalny.
48. Więcej: http://www.giodo.gov.pl/330/id_art/3529/j/pl/ (stan na 11.05.2016).
49. Dalej: GIODO.
50. Tzn. stały, niezmienny przez okres użytkowania.
51. Tzn. Zmienny, zależnie od konfiguracji – zmieniający się w różnych interwałach czasu.