redakcja naukowa
Michał Jackowski

Ochrona danych medycznych

RODO w ochronie zdrowia

RODO 2018

3. wydanie

Wolters Kluwer

redakcja naukowa
Michał Jackowski

Ochrona danych medycznych

RODO w ochronie zdrowia

3. wydanie

Wolters Kluwer

Warszawa 2018

Stan prawny na 1 czerwca 2018 r.

Wydawca
Izabella Małecka

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Michał Dymiński

Łamanie
Fotoedytor

Poszczególne rozdziały napisali:

Marta Ciesielska – rozdz. 11
Katarzyna Iwańska – rozdz. 7 pkt 7.6
Michał Jackowski – rozdz. 1, 2
Łukasz Lewandowski – rozdz. 3–6
Konrad M. Mazur – rozdz. 7 pkt 7.4, 7.7 ppkt 7.7.4–7.7.8
Sylwia Nawrot – rozdz. 7 pkt 7.3, 7.5
Magdalena Przysławska – rozdz. 7 pkt 7.1, 7.2
Krzysztof Świtała – rozdz. 7 pkt 7.7 ppkt 7.7.1 –7.7.3
Aleksandra Urbanowicz – rozdz. 10
Katarzyna Węcłaś – rozdz. 8, rozdz. 9 pkt 9.1
Tomasz Wojech – rozdz. 9 pkt 9.2

ISBN 978-83-8124-607-1
3. wydanie

ISBN PDF-a: 978-83-8124-925-6

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa 95/46/WE – dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281, s. 31)

dyrektywa 2011/24/UE – dyrektywa 2011/24/UE Parlamentu Europejskiego i Rady z 9.03.2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.Urz. UE L 88, s. 45)

dyrektywa 2016/680 – dyrektywa 2016/680 Parlamentu Europejskiego i Rady z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)

EKPC – Europejska Konwencja Praw Człowieka (Konwencja o ochronie praw człowieka i podstawowych wolności), sporządzona w Rzymie 4.11.1950 r., zmieniona następnie protokołami nr 3, 5, 8 oraz uzupełniona protokołem nr 2, Dz.U. z 1993 r. poz. 284 ze zm.)

TFUE – Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)

KEL – Kodeks etyki lekarskiej

k.c. – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2018 r. poz. 1025 ze zm.)

k.k. – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2017 r. poz. 2204 ze zm.)

k.p.c. – ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2018 r. poz. 155 ze zm.)

k.p.k. – ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2017 r. poz. 1904 ze zm.)

k.p.s.w. – ustawa z 24.08.2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. z 2018 r. poz. 475 ze zm.)

k.r.o. – ustawa z 25.02.1964 r. – Kodeks rodzinny i opiekuńczy (Dz.U. z 2017 r. poz. 682 ze zm.)

k.w. – ustawa z 20.05.1971 r. – Kodeks wykroczeń (Dz.U. z 2018 r. poz. 618 ze zm.)

Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze zm.)

konwencja nr 108 – konwencja nr 108 Rady Europy z 28.01.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. poz. 25; uzup.: Dz.U. z 2006 r. poz. 15)

MPPOiP – Międzynarodowy Pakt Praw Obywatelskich i Politycznych, otwarty do podpisu w Nowym Jorku 19.12.1966 r. (Dz.U. z 1977 r. poz. 167, zał.)

p.p.m. – ustawa z 4.02.2011 r. – Prawo prywatne międzynarodowe (Dz.U. z 2015 r. poz. 1792)

p.u.m. – przepisy utrzymane w mocy na podstawie art. 77 ustawy konstytucyjnej z 17.10.1992 r. o wzajemnych stosunkach między władzą ustawodawczą i wykonawczą Rzeczypospolitej Polskiej oraz o samorządzie terytorialnym (Dz.U. poz. 426 ze zm.)

projekt u.o.d.o. z 2017 r. – projekt ustawy o ochronie danych osobowych z 12.09.2017 r.

projekt u.o.d.o. – projekt ustawy o ochronie danych osobowych z 8.02.2018 r. (https://www.gov.pl/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow)

rekomendacja R(97)5 – rekomendacja Komitetu Ministrów Rady Europy R(97)5 z 13.02.1997 r. do państw członkowskich dotycząca ochrony danych medycznych

RODO – rozporządzenie 2016/679 Parlamentu Europejskiego i Rady z 27.04.2016 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, s. 1)

u.o.d.o. z 1997 r. – ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)

u.o.d.o. – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000)

u.o.p. – ustawa z 6.04.1990 r. o Policji (Dz.U. z 2017 r. poz. 2067 ze zm.)

u.p.p. – ustawa z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2017 r. poz. 1318 ze zm.)

u.s.i.o.z. – ustawa z 28.04.2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2017 r. poz. 1845)

u.z.l. – ustawa z 5.12.1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 2018 r. poz. 125 ze zm.)

Publikatory i czasopisma

Dz.U. – Dziennik Ustaw

Dz.Urz. UE – Dziennik Urzędowy Unii Europejskiej

Dz.Urz. WE	– Dziennik Urzędowy Wspólnot Europejskich
GL	– Gazeta Lekarska
GSiA	– Gazeta Samorządu i Administracji
HLR	– Harvard Law Review
KPPryw.	– Kwartalnik Prawa Prywatnego
M. Praw.	– Monitor Prawniczy
M.P.	– Monitor Polski
MSiG	– Monitor Sądowy i Gospodarczy
NP	– Nowe Prawo
NSA	– Naczelny Sąd Administracyjny
ODOBABI	– Ochrona Danych Osobowych – Biuletyn Administratorów Bezpieczeństwa Informacji
ONSA	– Orzecznictwo Naczelnego Sądu Administracyjnego
OSA	– Orzecznictwo Sądów Apelacyjnych
OSN	– Orzecznictwo Sądu Najwyższego
OSNAP	– Orzecznictwo Sądu Najwyższego. Izba Administracyjna, Pracy i Ubezpieczeń Społecznych
OSNC	– Orzecznictwo Sądu Najwyższego. Izba Cywilna
OSNKW	– Orzecznictwo Sądu Najwyższego. Izba Karna i Izba Wojskowa
OSP	– Orzecznictwo Sądów Polskich
OSS	– Orzecznictwo w Sprawach Samorządowych
OTK	– Orzecznictwo Trybunału Konstytucyjnego
Pal.	– Palestra
PiM	– Prawo i Medycyna
PiZS	– Praca i Zabezpieczenie Społeczne
PiŻ	– Prawo i Życie
POSAG	– Przegląd Orzecznictwa Sądu Apelacyjnego w Gdańsku
PPH	– Przegląd Prawa Handlowego
PPiA	– Przegląd Prawa i Administracji
Pr. Gosp.	– Prawo Gospodarcze
Prok. i Pr.	– Prokuratura i Prawo
Prz. Sejm.	– Przegląd Sejmowy
PS	– Przegląd Sądowy
PUG	– Przegląd Ustawodawstwa Gospodarczego
PUSiG	– Przegląd Ubezpieczeń Społecznych i Gospodarczych
PWN	– Polskie Wydawnictwa Naukowe
R. Praw.	– Radca Prawny
Rej.	– Rejent
RPEiS	– Ruch Prawniczy, Ekonomiczny i Socjologiczny
Rzeczp.	– „Rzeczpospolita”
SIM	– System Informacji Medycznej
St. Cyw.	– Studia Cywilistyczne
St. Iur.	– Studia Iuridica
St. Praw.	– Studia Prawnicze

Instytucje, organizacje, sądy

EOG	– Europejski Obszar Gospodarczy
ETPC	– Europejski Trybunał Praw Człowieka
GIODO	– Generalny Inspektor Ochrony Danych Osobowych
Grupa Robocza Art. 29	– zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, niezależny podmiot o charakterze doradczym, powołany na mocy art. 29 dyrektywy 95/46/WE
Komisja	– Komisja Europejska
NIA	– Naczelna Izba Aptekarska
NSA	– Naczelny Sąd Administracyjny
OECD	– Organizacja Współpracy Gospodarczej i Rozwoju
ONZ	– Organizacja Narodów Zjednoczonych
RE	– Rada Europy
SA	– sąd apelacyjny
SN	– Sąd Najwyższy
SO	– sąd okręgowy
TK	– Trybunał Konstytucyjny
TSUE	– Trybunał Sprawiedliwości Unii Europejskiej
UE	– Unia Europejska
ZOZ	– zakład opieki zdrowotnej

WSTĘP DO III WYDANIA

Historia tej książki to historia ochrony danych osobowych w Polsce. Od problemów związanych z manualnym przetwarzaniem do zjawisk e-health i medical big data[1]. Od przepisów niszowych, których nie znał niemal nikt poza grupą bardzo wyspecjalizowanych prawników, aż po normatywne wydarzenie 2018 r.

Bezpośrednim impulsem do napisania trzeciego wydania książki jest oczywiście wejście w życie RODO. Rozporządzenie to od maja 2018 r. jest bezpośrednio stosowane i zastąpiło regulacje krajowe w całej Unii Europejskiej. Wbrew potocznym informacjom nie stanowi rewolucji normatywnej, ale poprzez zawarte w nim sankcje wymusza rewolucyjną w Polsce konieczność dostosowania się do niego i rzeczywistego przestrzegania w praktyce.

Prawo ochrony danych osobowych staje się coraz bardziej skomplikowane. Z tego względu trzecie wydanie tej publikacji zostało napisane nie przez jednego autora, ale przez grupę prawników zajmujących się zarówno w nauce, jak i praktyce ochroną danych osobowych, a szczególnie danych medycznych. Układ książki uległ więc zmianie. Każdy rozdział jest odrębnym opracowaniem na temat w nim poruszony. Jednak autorzy dokładali starań, by były one spójne. Nie uniknęliśmy jednak sytuacji, gdy ta sama instytucja prawna jest opisana więcej niż jeden raz. Zawsze jednak z innego punktu widzenia.

Autorzy przygotowywali poszczególne rozdziały w czerwcu 2018 r. Uwzględnili treść RODO i nowej ustawy o ochronie danych osobowych przyjętej w 2018 r. Jednak wiele aktów prawnych jest nadal w przygotowaniu. W chwili oddania tej książki do druku dopiero trafił do Sejmu projekt ustawy zmieniającej ustawy w związku z wejściem w życie RODO. Przepisy będą podlegały zatem zmianom.

---

[1] C.H. Lee, H.-J. Yoon, *Medical big data: promise and challenges*, Kidney Res. Clin. Pract. 2017/36(1), s. 3–11; J.S. Rumsfeld, K.E. Joynt, T.M. Maddox, *Big data analytics to improve cardiovascular care: promise and challenges*, Nat. Rev. Cardiol. 2016/13(6), s. 350–359.

Mamy jednak nadzieję, iż nie będą one znaczące, a publikacja będzie aktualna również po wejściu w życie nowych przepisów. Po zmianach z 2018 r. nadal czeka nas wiele zmian w sferze danych osobowych i danych medycznych. W dniu 25.05.2018 r. miało wejść w życie rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (tzw. rozporządzenie e-privacy). Już wiadomo, że wejdzie w życie w 2020 r. lub nawet później. Tymczasem ma to być akt ustanawiający standardy przetwarzania danych w internecie. Prowadzone są również dyskusje na temat unijnej regulacji odnoszącej się do danych anonimowych, możliwości ich wtórnej deanonimizacji i ich komercyjnego wykorzystania. W Polsce natomiast przesuwany jest termin wprowadzenia elektronicznej dokumentacji medycznej. Na dzień przygotowywania tej książki e-recepta ma być obowiązkowa od 1.01.2020 r., e-skierowanie od 1.01.2021 r., a obowiązek prowadzenia pozostałej dokumentacji w postaci elektronicznej ma być wprowadzony od 1.01.2019 r.[2] Te wszystkie zmiany spowodują, że również ta publikacja będzie wymagała dalszych zmian.

Poznań 2018 r.
dr hab. Michał Jackowski, prof. WSB

[2] Komunikat Ministerstwa Zdrowia, http://www.bip.mz.gov.pl/ogloszenia/reguly-tworzenia-elektronicznej-dokumentacji-medycznej/komunikat-dotyczacy-regulacji-prawnych-w-zakresie-elektronicznej--dokumentacji-medycznej-2/ (dostęp: 26.02.2018 r.).

WSTĘP DO II WYDANIA

Pierwsze wydanie tej książki było przygotowywane i pisane w latach 2000–2001, gdy polska ustawa o ochronie danych osobowych obowiązywała dopiero trzy lata, a autonomię informacyjną uważano powszechnie za jeden, wcale nie najważniejszy, element prawa do prywatności. Konwencja nr 108 Rady Europy z 28.01.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych i dyrektywa nr 95/46/WE Parlamentu Europejskiego i Rady Unii Europejskiej z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych nie były jeszcze aktami obowiązującymi w polskim porządku prawnym. Ta pierwsza – z uwagi na brak ratyfikacji, druga – z uwagi na toczące się dopiero negocjacje w sprawie przystąpienia Polski do Unii Europejskiej. Sądy polskie zaledwie zaczynały dostrzegać i chronić dane osobowe, a Generalny Inspektor Ochrony Danych Osobowych postrzegany był jako organ walczący o to, aby na klatkach schodowych domów wielorodzinnych nie wisiały spisy lokatorów. Nadal słychać było głosy, iż rozbudowany system ochrony danych osobowych jest zbędny.

System ochrony zdrowia również nie dostrzegał potrzeby ochrony autonomii informacyjnej pacjenta, a normy zwyczajowe (takie jak publicznie dostępne karty choroby, wywieszane spisy pacjentów itp.) wręcz kolidowały z ustawą o ochronie danych osobowych. Przepisy normujące ochronę danych medycznych uznawano za utrudnienie w systemie leczenia.

W chwili opracowywania drugiego wydania, jak się wydaje, sytuacja zmieniła się całkowicie. Rozwój sieci internet i urządzeń mobilnego dostępu do sieci spowodował, iż zjawiskiem normalnym jest bardzo szybka komunikacja i wymiana danych, i to w ujęciu globalnym. W konsekwencji bardzo łatwe jest obecnie tworzenie baz i zbiorów danych oraz udostępnianie danych on-line. Również system ochrony zdrowia nie oparł się elektronicznemu przetwarzaniu danych. Tworzenie baz danych medycznych czy systemów elektronicznych kart zdrowia ma bowiem wiele zalet:

1) koszty elektronicznego przetwarzania danych są znacznie niższe niż tradycyjnego (papierowego);
2) dostęp do elektronicznej bazy danych jest znacznie łatwiejszy dla samego pacjenta, umożliwiając mu pełniejszą realizację prawa do dostępu do własnych

danych, ale także dla innych osób uczestniczących w procesie leczenia pacjenta (np. innych lekarzy);
3) dostęp on-line do samego pacjenta (jego osoby) jest dużo łatwiejszy, a pacjent może swobodniej udzielić zgody na przetwarzanie jego danych on-line niż w sposób tradycyjny (off-line).

Z uwagi na techniczne możliwości oprogramowania dane przetwarzane w systemach informatycznych mogą być również wykorzystywane dla zarządzania usługami medycznymi, kontrolowania jakości tych usług, a w konsekwencji dla zwiększania ich dostępności, zwłaszcza w przypadku usług finansowanych ze środków publicznych.

Jednakże jest również druga strona tak powszechnego dostępu do danych. Dokumentacja medyczna jest jednym z najbardziej wrażliwych i poufnych rodzajów informacji dotyczących jednostek. Ujawnienie stanu zdrowia lub diagnozy może mieć negatywny wpływ na życie osobiste i zawodowe danej osoby. Nawet udostępnienie drobnych kłopotów zdrowotnych może spowodować problemy pacjenta. Przykłady dyskryminacji wskutek bezprawnego wyjawienia danych medycznych występują w tradycyjnych systemach przetwarzania danych. Odmawia się zatrudnienia, ubezpieczenia czy kredytowania w związku z ujawnieniem informacji medycznych osobom nieuprawnionym[1]. Przechowywanie dokumentacji medycznej w formie elektronicznej zwiększa w znacznym stopniu ryzyko, iż dostęp do nich uzyskają podmioty nieupoważnione. Korzystanie z internetu jest z natury niebezpieczne. Przechowywanie wrażliwych danych w niezabezpieczonych sieciach komputerowych albo bezprzewodowych opisane ryzyko jeszcze zwiększa.

Wszystkie te zmiany zaczął dostrzegać prawodawca (i europejski, i polski). Prawo zaczęło podążać za życiem społecznym. Stąd ciągły rozwój aktów chroniących dane osobowe, również w sektorze usług medycznych. Opisane czynniki ryzyka zaczęli również dostrzegać sami obywatele, zwracający coraz większą uwagę na ochronę własnej prywatności, także w internecie[2]. Zmiany te są na tyle znaczące, iż pierwsze wydanie książki musiało zostać zaktualizowane. Nie są to jednak zmiany rewolucyjne. Zatem pierwotny układ książki nie uległ zasadniczej zmianie, lecz został jedynie zaktualizowany.

Czytelnicy powinni mieć jednak świadomość, iż wiele kluczowych przemian systemu ochrony danych osobowych i medycznych jest jeszcze przed nami. Najważniejsze akty prawne regulujące przetwarzanie danych powstały bowiem w czasie, gdy internet dopiero zaczynał się upowszechniać, nie było portali społecznościowych i innych,

[1] Przykładem tego są autentyczne przypadki opisane na www.patientsprivacyrights.org czy też www.panoptykon.org/content/problemy-z-ochron-danych-medycznych (dostęp: 2.03.2018 r.).

[2] Por. debaty toczące się wokół zagadnienia polityki prywatności największych portali społecznościowych, takich jak Facebook czy NK.

powszechnych dziś technik komunikacyjnych. Jesteśmy zatem zapewne w trakcie procesu systemowych zmian prawa, które będą odpowiedzią na wyzwania związane z rozwojem technologii informatycznych oraz procesami globalizacji[3].

Poznań 2011 r.
dr Michał Jackowski

[3] Por. komunikat Komisji z 4.11.2010 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów – Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej, COM(2010)609. Dokument ten przedstawia strategię poprawy skuteczności unijnych przepisów dotyczących ochrony danych – tak komunikat prasowy z 4.11.2010 r., IP/10/462, dostępny na stronie internetowej europa.eu.

WSTĘP DO I WYDANIA

Prawo do ochrony danych medycznych jest prawem znajdującym oparcie w Konstytucji oraz podstawowych aktach międzynarodowego prawa człowieka. Potwierdza to w szczególności orzecznictwo Trybunału Konstytucyjnego i Europejskiego Trybunału Praw Człowieka.

Osiągnięcia współczesnej medycyny stawiają przed osobami zajmującymi się naukami medycznymi, zarówno od strony prawnej, naukowej, jak i praktycznej, coraz to nowe wyzwania. Dylematy dotyczące badań genetycznych, transplantologii, klonowania (także ludzi) czy transferu embrionalnego wymagają współpracy środowisk prawniczych, naukowych oraz lekarskich. Na tle tej swego rodzaju rewolucji naukowej ogromnie istotne wydaje się stworzenie zasad, które umożliwiłyby poszanowanie zagrożonej zdobyczami techniki autonomii jednostki. Jednocześnie konieczne jest stworzenie takiego prawa, które chroniąc sferę autonomii jednostki, umożliwi jednak swobodny (w określonych granicach) obieg informacji.

Na tle danych medycznych konieczność ta jest tym bardziej nagląca. Świat dążący do tego, by być lepszym, doskonalszym w realiach wolnego rynku, eliminuje słabszych lub gorszych. Dlatego też konieczne jest wprowadzenie niezbędnych zabezpieczeń zapobiegających dyskryminacji. Współczesne przykłady dyskryminacji ze względu na stan zdrowia wskazują, iż wszyscy, których działalność wiąże się z ryzykiem finansowym (pracodawcy, firmy ubezpieczeniowe), są skłonni wydać nawet sporą sumę pieniędzy na bazy danych medycznych, dążąc do zminimalizowania ponoszonego ryzyka związanego z ewentualnym zatrudnieniem czy ubezpieczeniem osoby chorej. Osiągnięcia medycyny w zakresie poznania genomu człowieka mogą spowodować, iż wkrótce już w fazie prenatalnej będzie można poznać przewidywany stan zdrowia jednostki i ewentualne choroby, nałogi czy choćby niekonwencjonalne zachowania. Osoba chora, której prawo do ochrony danych medycznych nie podlegałoby ochronie, mogłaby znaleźć się na marginesie współczesnego świata. Nikt nie chciałby jej zatrudnić, ubezpieczyć, a nawet nikt nie chciałby z nią utrzymywać kontaktu. Taka sytuacja mogłaby prowadzić do uprzedmiotowienia człowieka.

Jednocześnie ograniczony dostęp do takich informacji, np. lekarzy lub organów przyznających świadczenia osobom chorym, jest pożądany dla ochrony interesów samego podmiotu danych, a także dla ochrony interesów osób trzecich. Prawo do ochrony danych medycznych ma uchronić ludzi przed nieograniczonym wykorzystywaniem ich danych, również dla celów dla nich niekorzystnych, ale jednocześnie ma umożliwić ochronę innych praw podmiotu danych, jak i praw osób trzecich.

Pozostaje pytanie, dlaczego prawo to jest nadal niedoceniane w Polsce. Wpływ na to mają na pewno doświadczenia komunizmu, kiedy organy państwa i jednostki państwowe mogły gromadzić i gromadziły wszelkie dane o obywatelach, także i dane medyczne, nie potrzebując do tego żadnej podstawy prawnej. Okres pierwszych dwunastu lat III Rzeczypospolitej również nie został wykorzystany do zmiany podejścia organów państwa. Poważna dyskusja na temat wprowadzenia instytucji ochrony danych osobowych rozpoczęła się bowiem dopiero w 1996 r. Poziom świadomości prawnej w zakresie ochrony danych medycznych nie jest wysoki nawet wśród prawników, nie wspominając o przedstawicielach innych profesji, choć cały czas rośnie.

Ta książka jest pierwszym w Polsce opracowaniem skupiającym się na ochronie wyłącznie danych medycznych. Moim celem było pełne omówienie wszystkich instytucji chroniących prawo jednostki do ochrony danych medycznych. Oczywiście jest bardzo wiele przepisów administracyjnych normujących ochronę danych osobowych. Z uwagi na ograniczoną objętość tej książki część z nich mogła być jedynie przytoczona, a nie szczegółowo omówiona.

Część pierwsza (wstępna) poświęcona jest omówieniu podstawowych pojęć, które będą wykorzystywane w dalszej części opracowania. Szczególnie istotna jest część poświęcona definicji danych osobowych oraz danych medycznych. Ich sformułowanie ma kluczowe znaczenie dla zrozumienia całej książki.

Część druga dotyczy ochrony danych medycznych według przepisów prawa międzynarodowego. Położyłem w niej nacisk na przepisy powszechnie obowiązujących umów międzynarodowych, będących źródłem międzynarodowego prawa człowieka. W rozdziale tym omówione zostały również rozstrzygnięcia organów międzynarodowych uznające prawo do ochrony danych medycznych za podstawowe prawo człowieka. W tej części przedstawiłem także regulacje międzynarodowe poświęcone zagadnieniu ochrony danych osobowych, które były wzorem polskich uregulowań wewnętrznych. Dla pełnego obrazu instrumentów ochrony danych medycznych zaprezentowałem również akty miękkiego prawa międzynarodowego (tzw. *soft law*), stanowiącego zalecane standardy tej ochrony.

Część trzecia zawiera omówienie polskich narzędzi ochrony danych medycznych – od konstytucyjnych, przez administracyjnoprawne i cywilnoprawne, aż po środki

karne. W osobnym rozdziale została omówiona tajemnica lekarska jako specyficzny i unormowany całościowo, a także głęboko zakorzeniony w praktyce środek prawny.

Część czwarta książki została natomiast poświęcona najważniejszym pozaprawnym normom etycznym i obyczajowym, które wpływają na ochronę prawa do ochrony danych medycznych. Przedstawiłem w niej również najpoważniejsze zagrożenia prawa do ochrony danych medycznych.

Książka zawiera pełną bibliografię, uwzględniającą niemal wszystkie pozycje poruszające kwestię ochrony danych medycznych, a także wykaz podstawowych aktów prawnych normujących kwestię ochrony danych medycznych i najważniejsze orzecznictwo dotyczące tego zagadnienia.

Poznań 2002 r.
Michał Jackowski

Część I

ZAGADNIENIA WSTĘPNE

Rozdział 1

PODSTAWOWE POJĘCIA

1.1. Pojęcie danych osobowych

1.1.1. Informacje a dane

Dane medyczne stanowią szczególną kategorię danych o osobach[1]. Aby wyjaśnić, czym są dane medyczne, konieczne jest najpierw zdefiniowanie danych osobowych. To ostatnie pojęcie zaczęło się pojawiać w polskiej doktrynie prawniczej pod wpływem zachodniego piśmiennictwa już na początku lat 80.[2] Dopiero jednak w latach 90. ożywione dyskusje na łamach czasopism prawniczych oraz orzecznictwo pozostające pod wpływem standardów światowych i europejskich doprowadziły do tego, iż uchwalono regulacje mające na celu ochronę danych osobowych.

Pojęcie ochrony danych pojawiło się po raz pierwszy w ustawie o rachunkowości[3], a pierwsza definicja danych jednostkowych zawarta została w ustawie o statystyce publicznej[4]. Kolejną definicję danych osobowych wyrażał art. 6 ustawy z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.). W pierwotnym brzmieniu tego przepisu za dane osobowe uważało się każdą informację dotyczącą osoby fizycznej pozwalającą na określenie tożsamości tej osoby[5]. Na tle tej definicji pojawiły się kontrowersje w piśmiennictwie. Cała niemal doktryna prawnicza uznała, iż ściśle językowa wykładnia art. 6 prowadziła do absurdu,

[1] P. Zaborowski, referat z konferencji „Ochrona danych medycznych i ich przetwarzanie", która odbyła się w Warszawie w dniach 8–9.05.2000 r., materiały z konferencji, s. 5.

[2] Por. A. Mrózek, *Ustawowe prawo ochrony danych. Analiza prawno-porównawcza*, Toruń 1981.

[3] Ustawa z 29.09.1994 r. o rachunkowości (Dz.U. z 2018 r. poz. 395) – rozdział ósmy ustawy.

[4] Ustawa z 29.06.1995 r. o statystyce publicznej (Dz.U. z 2016 r. poz. 1068 ze zm.); według art. 2 pkt 9 ustawy danymi jednostkowymi są „dane osobowe dające się powiązać z konkretną osobą fizyczną".

[5] Art. 6 u.o.d.o. w pierwotnym brzmieniu: „W rozumieniu ustawy za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby".

a przepis ten sformułowany był wadliwie[6]. Interpretując go językowo, należałoby przyjąć, iż ochronie podlegają jedynie: 1) wszelkie informacje, 2) dotyczące osoby fizycznej, 3) które umożliwiają ustalenie tożsamości tej osoby. Zgodnie z takim rozumieniem przepisu większość informacji dotyczących osób fizycznych zostałaby wyłączona spod ochrony. Niewiele jest bowiem informacji, które dotyczą osoby fizycznej i które umożliwiają ustalenie tożsamości tej osoby: imię i nazwisko, PESEL, podawane łącznie z imionami rodziców lub miejscem czy datą urodzenia, wizerunek i kilka innych. Celem ustawy jest natomiast unormowanie kwestii zbierania informacji o osobach fizycznych, przechowywania takich informacji i ich udostępniania[7], a więc także informacji o osobach, które już znamy na podstawie innych danych[8]. Podejście takie nie harmonizowałoby także z innymi zawartymi w ustawie rozwiązaniami[9]. Piśmiennictwo prawnicze, odwołując się do unormowania zawartego w art. 51 Konstytucji RP[10] oraz do aktów prawnych wyznaczających europejski standard ochrony danych osobowych[11], zdefiniowało zatem dane osobowe jako: 1) informacje, 2) dotyczące osoby fizycznej, 3) zidentyfikowanej, lub 4) dającej się zidentyfikować. Należy jednak przyznać, że zarówno NSA[12], jak i część doktryny[13] stały na stanowisku literalnej wykładni art. 6 ustawy.

Wskutek zmiany art. 6 u.o.d.o. ustawą z 25.08.2001 r.[14] dane osobowe zdefiniowano jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Zgodnie z art. 6 ust. 2 i 3 u.o.d.o. „osobą możliwą do zidentyfikowania była osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważało się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań"[15].

---

[6] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2001, s. 277, oraz J. Barta, R. Markiewicz, *Pytania i wątpliwości*, Rzeczp. z 22.01.2001 r., s. 22; A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1998, s. 21; A.G. Harla, *Termin „dane osobowe" – uwagi de lege lata i de lege ferenda na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Pal. 2001/1–2, s. 36–38; A. Redelbach, *Ochrona tajemnicy zawodowej notariusza w świetle ustawy o ochronie danych osobowych*, Rej. 2001/5, s. 159.

[7] A.G. Harla, *Termin „dane osobowe"...*, s. 36.

[8] Taki cel wynika również z art. 1 u.o.d.o.: „Każdy ma prawo do ochrony dotyczących go danych osobowych".

[9] J. Barta, R. Markiewicz, *Pytania...*, s. 22.

[10] A. Mednis, *Ustawa o ochronie...*, s. 22.

[11] A.G. Harla, *Termin „dane osobowe"...*, s. 38.

[12] Orzeczenie NSA z 17.11.2000 r., II SA 1860/00, niepubl., cyt. za: J. Barta, R. Markiewicz, *Ochrona danych...*, s. 283: „Danymi osobowymi w rozumieniu ustawy są informacje pozwalające na określenie tożsamości osoby, czyli imię, nazwisko, adres, numery PESEL i NIP. Pozostałe dane, jak np. dane z rejestru urzędu pracy, zawierają natomiast informacje o osobie".

[13] M. Zielińska, *Nazwa spółki cywilnej jako dobro osobiste*, „Prawo Spółek" 1998/11, s. 7.

[14] Ustawa z 25.08.2001 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. poz. 1087).

[15] G. Sibiga, *Nowelizacja ustawy o ochronie danych osobowych*, M. Praw. 2001/23.

Od 25.05.2018 r., w myśl art. 4 pkt 1 RODO, dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). 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. Definicja nie uległa zatem znaczącej zmianie i odpowiada nadal sformułowaniom zawartym zarówno w Konstytucji, jak i w aktach międzynarodowego prawa ochrony danych osobowych.

Zgodnie z art. 51 ust. 1 Konstytucji RP „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby". Artykuł 2 konwencji nr 108 definiuje dane osobowe jako „każdą informację dotyczącą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować („osoba, której dane dotyczą")".

Definicja zawarta w RODO jest ze strony prawodawcy wyrazem woli przyjęcia szerokiej koncepcji danych osobowych, uwzględniającej wszelkie informacje mogące dotyczyć danej osoby. Przyjmując tę definicję, dążono do tego, aby była jak najogólniejsza, tak by uwzględnić wszystkie informacje dotyczące osoby możliwej do zidentyfikowania[16]. Pojęcie informacji oznacza wszelkie komunikaty, wiadomości, wypowiedzi i prezentacje, niezależnie od sposobu, zakresu i swobody udostępniania, sposobu ich pozyskania oraz sposobu wyrażania[17]. Obejmuje ono informacje **obiektywne** (takie jak obecność pewnych substancji w czyjejś krwi), a także informacje **subiektywne**, opinie lub oceny (np. oceny rzetelności dłużników, ryzyka ubezpieczeniowego czy opinie o pracownikach). Aby stanowić dane osobowe, informacja nie musi być prawdziwa ani sprawdzona[18]. Informacje stanowią dane osobowe niezależnie od nośnika, na którym zostały wyrażone. Mogą to być więc znaki graficzne, symbole w języku komputerowym, na fotografii, zapisie cyfrowym, informacje wyrażone dźwiękiem i obrazem[19].

[16] Opinia 4/2007 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 dyrektywy 95/46/WE przyjęta 20.06.2007 r. w sprawie pojęcia danych osobowych, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf (dostęp: 2.03.2018 r.).

[17] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2007, s. 345.

[18] Opinia 4/2007..., s. 6.

[19] Opinia 4/2007..., s. 8 i 9, oraz przytoczone tam przykłady danych osobowych w postaci nagrania głosowego, obrazów zarejestrowanych kamerą, rysunku dziecka sporządzonego w ramach badania psychologicznego czy danych biometrycznych, takich jak odciski palców, wzorzec siatkówki, struktura twarzy, głos, geometria dłoni, układ żył lub nawet pewne głęboko zakorzenione umiejętności lub inne cechy zachowania (takie jak własnoręczny podpis, uderzenie w klawisz, szczególny chód lub sposób mówienia). Por. także wyrok NSA z 18.11.2009 r., I OSK 667/09, LEX nr 588798, w którym sąd przyjął, iż wizerunek sprzed wielu lat stanowi również daną osobową podlegającą ochronie w oparciu o przepisy u.o.d.o.

W doktrynie i orzecznictwie powstały wątpliwości, czy na podstawie ustawy o ochronie danych osobowych ochronie podlegają informacje dotyczące osoby fizycznej w zakresie, w jakim osoba ta prowadzi działalność gospodarczą. Początkowo zarówno Generalny Inspektor Ochrony Danych Osobowych, NSA[20], jak i część doktryny[21] przyjęli, iż termin „dane osobowe" nie obejmuje danych indywidualnych dotyczących firmy i nie można żądać ochrony tych danych na podstawie ustawy o ochronie danych osobowych. Pogląd ten został poddany krytyce przez część piśmiennictwa[22]. Na tle RODO nie powinno ulegać wątpliwości, że spod zakresu obowiązywania wyłączono tylko informacje o osobach prawnych, a zatem obejmuje ono zastosowaniem osoby fizyczne prowadzące działalność gospodarczą[23].

1.1.2. Osobowy charakter informacji

Informacje, by mogły być chronione, muszą dotyczyć osoby. Często będzie oczywiste, iż dane dotyczą konkretnej osoby. W wielu przypadkach ustalenie takiego związku jest łatwe. W niektórych sytuacjach jednak dane przekazują przede wszystkim informacje o przedmiotach, a nie o osobach. Przedmioty te należą zazwyczaj do kogoś, podlegają wpływowi działania pewnych osób lub wywierają na nie pewien wpływ bądź też pozostają w pewnego rodzaju sąsiedztwie fizycznym lub geograficznym w stosunku do osób lub należących do nich przedmiotów. Można wtedy uznać, że informacje dotyczą tych osób lub przedmiotów jedynie pośrednio. Podnosi się, iż takie dane dotyczą osoby, jeżeli odnoszą się do tożsamości, cech lub zachowania danej osoby lub też jeśli informacje te determinują lub też wpływają na sposób traktowania lub ocenę danej osoby. Dane można uznać za dotyczące osoby, gdy:

1) ich **treść** wiąże się z osobą – tj. w przypadkach, gdy informacja jest na temat pewnej osoby, niezależnie od celu, którym kieruje się administrator danych lub osoba trzecia, lub od wpływu tej informacji na osobę, której dane dotyczą; lub
2) **cel** informacji wskazuje, iż są lub mogą być wykorzystywane, biorąc pod uwagę wszystkie okoliczności danej sprawy, w celu oceny osoby, jej traktowania w określony sposób lub też wpływania na jej status lub zachowanie; lub

[20] Wyrok NSA z 28.11.2002 r., II SA 3389/01, M. Praw. 2003/3, poz. 99.

[21] G. Szpor, *Publicznoprawna ochrona danych osobowych*, PUG 1999/12, s. 6, czy też A. Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne* [w:] *Ochrona danych osobowych*, red. W. Wyrzykowski, Warszawa 1999, s. 121; ten ostatni autor stoi na stanowisku, iż dane dotyczące stosunków majątkowych nie podlegają ochronie na podstawie przepisów u.o.d.o., lecz na podstawie innych przepisów szczególnych.

[22] A. Mednis, *Ustawa o ochronie...*, s. 25; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 348; D. Fleszer, *Zakres przetwarzania danych osobowych w działalności gospodarczej*, LEX 2008; M. Jackowski, *Glosa do wyroku NSA z 28.11.2002 r., II SA 3389/01*, PiP 2004/10, s. 126.

[23] P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017, s. 158; por. także motywy 14 i 18 RODO dookreślające wyłączenia spod zakresu rozporządzenia.

3) mimo iż ani treść, ani cel informacji nie wiążą się z określonymi osobami, występuje element **skutku** – użycie informacji będzie prawdopodobnie mieć wpływ na prawa i interesy określonej osoby, przy czym potencjalny skutek nie musi polegać na znacznym wpływie. Wystarczy, że pewna osoba może być traktowana odmiennie od innych osób na skutek przetwarzania takich danych.

Te trzy elementy (treść, cel, skutek) stanowią warunki występujące alternatywnie, a nie łącznie. Każdy z tych elementów może przy tym dotykać innej osoby[24].

Dane osobowe dotyczą wyłącznie osób fizycznych. Do wyjaśnienia pozostaje kwestia, od którego do którego momentu podlegają one ochronie, a także czy odnoszą się również do nienarodzonych i zmarłych. Duże znaczenie ma szczególnie zagadnienie ochrony danych medycznych dotyczących *nasciturusa.* Ogromny postęp medycyny spowodował wyodrębnienie nowej dziedziny wiedzy medycznej, zwanej medycyną matczyno-płodową, oraz jej sekcji zwanej perinatologią. Rozwój wiedzy medycznej powoduje, iż człowiek przed urodzeniem może być bardzo aktywnie obserwowany, diagnozowany i leczony. Część piśmiennictwa wręcz nazywa *nasciturusa* pacjentem[25].

Orzeczeniem z 28.05.1997 r. Trybunał Konstytucyjny potwierdził, iż na podstawie przepisów o randze konstytucyjnej dziecku nienarodzonemu przysługuje prawo do ochrony życia oraz zdrowia[26]. Uzasadniając to stanowisko, TK odwołał się w szczególności do Konwencji o prawach dziecka (Dz.U. z 1991 r. poz. 526 ze zm.). Preambuła konwencji deklaruje w akapicie 10, iż „dziecko, z uwagi na swą niedojrzałość fizyczną i umysłową, wymaga szczególnej opieki i troski, w tym właściwej ochrony prawnej, zarówno przed, jak i po urodzeniu". Zgodnie z art. 24 konwencji państwa-strony uznają prawo dziecka do korzystania z możliwie najlepszego stanu zdrowia i będą starały się zapewnić pełne urzeczywistnienie tego prawa, w szczególności podejmując właściwe środki w celu zapewnienia matkom właściwej opieki prenatalnej i postnatalnej. Prawo do ochrony zdrowia obejmuje zatem również dziecko poczęte.

Warto zwrócić również uwagę, iż Komitet Praw Dziecka ONZ w swoim komentarzu ogólnym nr 4 z 2003 r. na temat zdrowia małoletnich zaznacza, iż przepis art. 16 Konwencji o prawach dziecka, w myśl którego dziecko ma prawo do ochrony prawnej przeciwko m.in. arbitralnej ingerencji w sferę jego życia prywatnego, w kontekście zdrowia powinien być interpretowany jako zobowiązujący państwa-strony konwencji do przestrzegania ściśle prawa do prywatności i poufności dziecka w zakresie

[24] Opinia nr 4/2007..., s. 9–12.

[25] J. Haberko, *Cywilnoprawna ochrona dziecka poczętego a stosowanie procedur medycznych*, Warszawa 2010, s. 15–16; J. Haberko, R. Kocyłowski, *Medyczne i prawne aspekty leczenia płodu* [w:] *Deboli e indifesi nella società multiculturale europea. Atti della VI Conferenza Internazionale dei Diritti dell'Uomo. Lecce, 29-30 Maggio 2006*, red. G. Dammacco, B. Sitek, O. Cabaj, Olsztyn–Bari 2008, s. 515 i n.

[26] Orzeczenie TK z 28.05.1997 r., K 26/96, OTK 1997/2, poz. 19 – zostało wydane wprawdzie na podstawie art. 1 p.u.m., lecz wydaje się, iż pozostaje aktualne również na tle art. 30, 38 i 68 Konstytucji RP.

poradnictwa w sprawach zdrowotnych[27]. Dostarczyciele świadczeń zdrowotnych, uwzględniając podstawowe zasady konwencji, mają obowiązek zachowania w poufności informacji dotyczących małoletnich, które mogą być ujawnione tylko za ich zgodą, na analogicznych zasadach jak uchylenie tajemnicy zawodowej w przypadku dorosłych[28].

Na gruncie prawa cywilnego uznaje się również, iż *nasciturus* stanowi postać życia ludzkiego[29]. Zwolenników znajduje dość powszechnie pogląd, że dziecko poczęte ma warunkową zdolność prawną, którą wyraża zasada, iż dziecko nienarodzone należy traktować jak już narodzone, ilekroć chodzi o jego korzyść (*nasciturus pro iam nato habetur quotiens de commodis eius agitur*)[30]. Przejawem takiej warunkowej zdolności są m.in. przepisy przyznające poczętemu prawo do spadkobrania (art. 927 § 2 k.c.), umożliwiające uznanie dziecka poczętego (art. 75 § 1 k.r.o.), przyznające matce prawo do żądania pokrycia kosztów utrzymania matki przed urodzeniem oraz kosztów utrzymania dziecka po porodzie (art. 142 k.r.o.) czy też przewidujące instytucję kurateli dziecka poczętego (art. 182 k.r.o.). W tonie tym wielokrotnie wypowiadał się również Sąd Najwyższy, przyznając nienarodzonemu poszczególne uprawnienia[31], oraz doktryna prawa postulująca ochronę dóbr osobistych nienarodzonego na podstawie art. 23 i 446^1 k.c.[32]

Dziecko poczęte podlega również ochronie na gruncie prawa karnego (art. 152–154 i 157a k.k.) oraz innych norm prawa krajowego (np. art. 26 ust. 3 ustawy z 5.12.1996 r. o zawodach lekarza i lekarza dentysty, Dz.U. z 2017 r. poz. 125 ze zm.). Informacje o dziecku nienarodzonym podlegają ochronie także na podstawie przepisów o tajemnicy lekarskiej, jednakże nie jako informacje dotyczące części składowej – elementu stanu zdrowia ciężarnej, lecz jako informacje dotyczące autonomicznego podmiotu[33].

---

[27] Komentarz ogólny nr 4(2003) Komitetu Praw Dziecka z 1.07.2003 r. – Zdrowie i rozwój małoletnich w kontekście Konwencji o prawach dziecka, CRC/GC/2003/4, http://tb.ohchr.org/default.aspx?Symbol=CRC/GC/2003/4 (dostęp: 2.03.2018 r.).

[28] J. Kondratiewa-Bryzik, *Początek prawnej ochrony życia ludzkiego w świetle standardów międzynarodowych*, LEX 2009.

[29] T. Sokołowski, *Cywilnoprawna ochrona człowieka przed jego narodzeniem* [w:] *Ochrona człowieka w świetle prawa Rzeczypospolitej Polskiej. Materiały z II Międzynarodowej Konferencji Naukowej, Mierki 18–19 października 2001*, red. S. Pikulski, Olsztyn 2002, s. 106–116, oraz T. Smyczyński, *Pojęcie i status prawny dziecka poczętego*, St. Praw. 1989/4, s. 25.

[30] Z. Radwański, *Prawo cywilne – część ogólna*, Warszawa 2005, s. 143. Szerokie omówienie tej koncepcji przedstawia J. Haberko, *Cywilnoprawna ochrona*..., s. 74 i n.

[31] Por. orzeczenie SN z 7.10.1971 r., III CRN 255/71, OSN 1972/3, poz. 59, przyznające odszkodowanie od PZU dziecku nienarodzonemu po śmierci ojca; orzeczenie SN z 30.11.1987 r., III PZP 36/87, OSN 1988/2–3, poz. 23, uznające prawo dziecka do jednorazowego odszkodowania z tytułu wypadku przy pracy, który zdarzył się przed narodzeniem dziecka, i orzeczenie NSA z 28.11.1986 r., niepubl. – dopuszczające darowiznę na rzecz dziecka poczętego.

[32] J. Haberko, *Cywilnoprawna ochrona*..., s. 109–110.

[33] J. Haberko, *Cywilnoprawna ochrona*..., s. 294–299.

W konsekwencji powyższych ustaleń stoję na stanowisku, iż informacje dotyczące nienarodzonego, zebrane podczas życia płodowego, stanowią również dane osobowe[34]. Pogląd ten uwzględnia w szczególności treść rekomendacji Komitetu Ministrów Rady Europy R(97)5 z 13.02.1997 r. dotyczącej ochrony danych medycznych, która w art. 4.5 stanowi, iż dane medyczne dotyczące dzieci nienarodzonych powinny być uważane za dane osobowe[35].

Na tle ustawy o ochronie danych osobowych niejasne było, czy zmarły jest osobą w rozumieniu tego aktu. Większość doktryny prawa stanęła na stanowisku, iż ochrona dotyczy jedynie danych o osobach żyjących, wyłączając zmarłych[36]. Po wejściu w życie RODO kwestia ta została wyjaśniona w motywie 27, według którego rozporządzenie nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych. Przepisami takimi, które formułują ograniczenia rozpowszechniania informacji o zmarłych, są przepisy normujące dobro osobiste określane jako „kult pamięci osoby zmarłej"[37] oraz tajemnicę lekarską i tajemnicę pacjenta.

1.1.3. Identyfikowalność osoby

RODO wymaga, aby informacja stanowiąca daną osobową dotyczyła osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania. Osobę uważa się za zidentyfikowaną, jeśli w grupie osób można ją odróżnić od wszystkich pozostałych członków grupy. Jest też możliwa do zidentyfikowania, jeżeli – mimo że nie została jeszcze zidentyfikowana – taka identyfikacja jest możliwa. Identyfikacji dokonuje się zazwyczaj dzięki poszczególnym informacjom, które można nazwać czynnikami identyfikującymi i które wiążą się w sposób szczególny i bliski z daną osobą. Przykładem mogą być

[34] L. ten Haaf, *Unborn and Future Children as New Legal Subjects: An Evaluation of Two Subject--Oriented Approaches – The Subject of Rights and the Subject of Interests*, „German Law Journal" 2017, vol. 18, No. 5, s. 1103–1104: autorka prezentuje również interesujące rozważania na temat dzieci przyszłych (tj. dzieci w fazie przedkoncepcyjnej) i ich interesach. Tak J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 351; A. Szewc, *Z problematyki ochrony danych osobowych*, cz. 1, R. Praw. 1999/3, s. 23, oraz A. Krajewska, *Informacja genetyczna a zakres autonomii jednostki w europejskiej przestrzeni prawnej*, Wrocław 2008, s. 47; odmiennie A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2004, s. 45–46, który stwierdza, iż do momentu urodzenia dane osobowe nienarodzonego są chronione jako dane osobowe matki dziecka.

[35] Art. 4.5 rekomendacji Komitetu Ministrów Rady Europy R(97)5 z 13.02.1997 r. do państw członkowskich dotyczącej ochrony danych medycznych, cyt. za: www.coe.int: „Medical data concerning unborn children should be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor".

[36] M. Stryja, A. Stryja, *Teraz zacznie się na dobre*, Rzeczp. z 30.11.1999 r.

[37] Tak A. Mednis, *Ustawa o ochronie...*, s. 25; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 351; por. też wyroki SN: z 23.09.2009 r., I CSK 346/08, OSNC 2010/3, poz. 48, i z 6.02.2008 r., II CSK 474/07, LEX nr 452984.

cechy wyglądu zewnętrznego osoby, takie jak wzrost, kolor włosów, ubranie itp., lub pewne cechy tej osoby niedostrzegalne w pierwszej chwili, takie jak zawód, stanowisko, nazwisko itp. Tożsamość osoby fizycznej powinna być możliwa do zidentyfikowania **bezpośrednio** lub **pośrednio**. O tym, na ile poszczególne czynniki identyfikujące pozwalają na ostateczne ustalenie tożsamości, decydują szczególne okoliczności danej sytuacji[38].

Na tle dyrektywy 95/46/WE, a zwłaszcza zagadnienia odnoszącego się do kwalifikacji adresów IP jako danych osobowych, powstał spór, czy przesłankę identyfikowalności należy rozumieć obiektywnie czy subiektywnie. Obiektywne rozumienie oznacza, że osoba jest możliwa do zidentyfikowania, gdy administrator dysponuje informacjami na jej temat, które w powiązaniu z innymi danymi, dostarczonymi przez osobę trzecią, pozwolą na identyfikację. Rozumienie subiektywne natomiast wymaga weryfikacji, czy administrator mający potencjalnie dostęp do takich danych znajdujących się w dyspozycji osoby trzeciej ma rzeczywistą możliwość posłużenia się nimi w celu identyfikacji osoby. Podejście obiektywne jest zatem znacznie szersze i akceptując je, znacząco rozszerza się krąg informacji objętych pojęciem danych osobowych. Problem ten rozstrzygał TSUE w sprawie *Breyer* (C-582/14). Rzecznik Generalny wydający opinię w tej sprawie zaakceptował obiektywne podejście do identyfikowalności, uznając dynamiczny adres IP za daną osobową, albowiem istnieje osoba trzecia – dostawca dostępu do sieci – do której można się zwrócić w celu uzyskania dodatkowych danych umożliwiających, w połączeniu z tym adresem, identyfikację użytkownika. Pogląd ten podzielił Trybunał[39].

Na gruncie RODO opinia ta nie powinna jednak być bezkrytycznie akceptowana. W motywie 26 rozporządzenie wskazuje bowiem, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, 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 jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych oraz postęp technologiczny. Rozporządzenie odwołuje się zatem do kryterium „rozsądnego prawdopodobieństwa" sposobów identyfikacji oraz kryterium „uzasadnionego prawdopodobieństwa", iż zostaną one wykorzystane przez

[38] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 352–354.

[39] Wyrok TSUE z 19.10.2016 r., C-582/14, CURIA; por. także F. Zuiderveen Borgesius, *Case note. Breyer case of the Court of Justice of the European Union: IP addresses and the personal data definitione*, „European Data Protection Law Review" 2017, vol. 3, Issue 1, s. 130–137.

administratora. Należy zatem przyjąć, iż RODO odchodzi od kryterium obiektywnego na rzecz subiektywnego podejścia do identyfikowalności[40].

RODO nie chroni natomiast danych anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować (motyw 26). Należy odróżnić takie dane od danych poddanych pseudonimizacji, czyli takiemu przetworzeniu, by nie można ich było już 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[41]. O ile jednak anonimizacja ma skutek definitywny (albo co najmniej taki skutek wywiera przy wykorzystaniu rozsądnie dostępnych środków i sposobów), o tyle pseudonimizacja jest procesem ulegającym odwróceniu (motywy 75 i 85).

1.2. Pojęcie danych medycznych

W tej publikacji autorzy przedstawiają problem ochrony danych medycznych. We wcześniejszych wydaniach tej książki, w latach 2002 i 2011, podkreślano brak definicji legalnej tego pojęcia, a wyjaśniając je, odwoływano się do rekomendacji R(97)5 Komitetu Ministrów Rady Europy. Według art. 1 tej rekomendacji wyrażenie „dane medyczne" odnosi się zarówno do wszystkich danych wiążących się ze zdrowiem jednostki, jak i do danych w sposób oczywisty i bliski związanych ze zdrowiem oraz do danych genetycznych[42]. Zgodnie z memorandum wyjaśniającym do rekomendacji pojęcie danych medycznych obejmuje dane odnoszące się do przeszłego, obecnego i przyszłego stanu zdrowia podmiotu danych, zarówno zdrowia fizycznego, jak i psychicznego. Ponadto pojęcie to odnosi się do wszelkich informacji, które nie są informacjami upublicznionymi, a które pozwalają na ustalenie szeroko pojętego stanu zdrowia jednostki, takich jak styl życia osoby, życie seksualne czy nałogi[43].

[40] P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE...*, s. 186–187. Trochę mniej jednoznacznie D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017, s. 176–181.

[41] Na ten temat bardziej szczegółowo piszą S. Stalla-Bourdillon, A. Knight, *Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, „Wisconsin International Law Journal" 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945 (dostęp: 10.02.2018 r.).

[42] Art. 1 rekomendacji R(97)5 Komitetu Ministrów Rady Europy z 13.02.1997 r. do państw członkowskich dotyczącej ochrony danych medycznych, cyt. za: www.coe.int: „The expression «medical data» refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data".

[43] Explanatory Memorandum to Recommendation No. R(97)5 of the Committee of Ministers to Member States on the Protection of Medical Data, s. 5, cyt. za: www.coe.int.

Podnoszono również, że zawarty w art. 27 u.o.d.o. termin „dane o stanie zdrowia" jest zbyt wąski. Nawiązywano raczej do art. 2 pkt 7 ustawy o systemie informacji w ochronie zdrowia, zgodnie z którym jednostkowe dane medyczne to dane osobowe oraz inne dane osób fizycznych, dotyczące uprawnień do udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, stanu zdrowia, a także inne dane przetwarzane w związku z planowanymi, udzielanymi i udzielonymi świadczeniami opieki zdrowotnej oraz profilaktyką zdrowotną i realizacją programów zdrowotnych.

RODO nie odwołuje się również do pojęcia danych medycznych. Natomiast w art. 4 pkt 15 formułuje definicję „danych dotyczących stanu zdrowia". Są to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Według motywu 35 do tej kategorii należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia takich usług, w tym:

1) numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;
2) informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych;
3) wszelkie informacje o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Warto zwrócić uwagę, że sformułowanie zawarte w RODO „dane dotyczące stanu zdrowia" jest szersze od terminu „dane o stanie zdrowia" i nawiązuje do szerokiego rozumienia danych medycznych przyjętego w orzecznictwie TSUE[44]. W dalszej części tej książki autorzy nadal będą się posługiwać pojęciem danych medycznych, jako utrwalonym w literaturze prawniczej i orzecznictwie sądowym, ale rozumianym jako dane dotyczące stanu zdrowia.

Nie sposób jednak określić, czym są dane medyczne, bez odniesienia się do dwóch innych pojęć definiowanych w RODO – danych genetycznych i danych biometrycznych. Te pierwsze to dane osobowe dotyczące odziedziczonych lub nabytych cech ge-

[44] Wyrok ETS z 6.11.2003 r., C-101/01, *B. Lindqvist*, LEX nr 192425: „50. Zważywszy na przedmiot tej dyrektywy, należy dokonać wykładni rozszerzającej użytego w jej art. 8 ust. 1 wyrażenia «dane dotyczące zdrowia», tak aby obejmowało ono informacje dotyczące wszystkich aspektów, zarówno fizycznych, jak i psychicznych, zdrowia osoby. 51. Na pytanie czwarte należy zatem odpowiedzieć, że informacja, iż dana osoba doznała urazu stopy i przebywa na zwolnieniu lekarskim w niepełnym wymiarze, stanowi dane osobowe dotyczące zdrowia w rozumieniu art. 8 ust. 1 dyrektywy 95/46".

netycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej (art. 4 pkt 13 RODO), w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji (motyw 34). Natomiast dane biometryczne to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO). W motywie 51 preambuły RODO podkreśla się tę dodatkową przesłankę kwalifikowania informacji do tej szczególnej kategorii, jaką jest przetwarzanie specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Gdy informacje nie są przetwarzane w taki sposób, nie uznaje się danych o cechach osoby za dane biometryczne.

Z definicji danych genetycznych wynika, iż mogą ujawniać informacje o zdrowiu określonej osoby, będąc również danymi medycznymi, ale także odnosić się wyłącznie do fizjologii osoby, w żaden sposób nie dotycząc zdrowia (np. dane o kolorze włosów czy przeciętnym wzroście człowieka). Dane biometryczne także mogą ujawniać stan zdrowia określonej osoby (np. wizerunek twarzy może świadczyć o trwałym kalectwie osoby), ale często dane te mogą być irrelewantne z punktu widzenia stanu zdrowia. Pomiędzy pojęciem danych medycznych oraz danych genetycznych i biometrycznych zachodzi zatem stosunek krzyżowania zakresów znaczeń, przy czym z pewnością więcej danych genetycznych niż biometrycznych będzie danymi medycznymi.

1.3. Inne kluczowe definicje

Nie sposób przedstawić problematyki ochrony danych medycznych bez zdefiniowania szeregu pojęć. Są one ujęte w słowniczku zawartym w art. 4 RODO. Pierwszym typem są te odnoszące się do procesów zachodzących wobec danych. Kluczowa jest definicja pojęcia przetwarzania, które oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takimi jak: 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. Katalog operacji ma charakter przykładowy i otwarty[45]. Również inne procesy dotyczące danych będą ich przetwarzaniem. Nie ma znaczenia, czy przebiegać będą

[45] Poszczególne typy operacji na danych definiuje m.in. P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE...*, s. 200–204.

w sposób zautomatyzowany czy też niezautomatyzowany. Na tle dyrektywy 95/46/WE TSUE wyjaśnił, że prowadzona przez wyszukiwarki internetowe działalność, która polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w sieci przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie udostępnianiu ich internautom w sposób uporządkowany zgodnie z określonymi preferencjami, w sytuacji gdy informacje takie zawierają dane osobowe, należy uznać za „przetwarzanie danych osobowych". Operator wyszukiwarki internetowej, przeszukując internet w zautomatyzowany, stały i systematyczny sposób w poszukiwaniu opublikowanych w nim informacji, „gromadzi" takie dane, „odzyskiwane", „zapisywane" i „porządkowane" przezeń następnie za pomocą oprogramowania indeksującego, „przechowuje" je na swych serwerach oraz, w określonych sytuacjach „ujawnia" i „udostępnia" je swym użytkownikom w postaci listy wyników ich wyszukiwań. Ze względu na to, że operacje te zostały wyraźnie i bezwarunkowo wskazane w art. 2 lit. b dyrektywy 95/46/WE, należy uznać je za „przetwarzanie" w rozumieniu tego przepisu, i bez znaczenia jest przy tym podnoszony przez Google fakt, iż ten operator wyszukiwarki internetowej przeprowadza te same operacje również w odniesieniu do innego rodzaju informacji, niebędących danymi osobowymi, i nie wprowadza rozróżnienia między nimi a tymi danymi osobowymi[46].

RODO definiuje także pojęcie ograniczenia przetwarzania jako oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Jest ono doprecyzowane w art. 5 ust. 1 lit. e, który wyjaśnia, iż „ograniczenie przechowywania" to z kolei przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Szczególne znaczenie RODO nadaje operacji profilowania danych. O skutkach profilowania oraz szczególnych zasadach takiego przetwarzania danych medycznych będzie mowa w dalszych częściach tej książki. W tym miejscu należy jedynie wyjaśnić, że oznacza ono dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Jest to profilowanie zwykłe, które nie wiąże się z żadnymi szczególnymi obowiązkami administratorów danych, z wyjątkiem tych, które odpowiadają prawu sprzeciwu wynikającemu z art. 21 RODO i odnoszącemu się do wszelkich form profilowania. Natomiast art. 22 RODO przewiduje profilowanie kwalifikowane, które poza ogólnymi przesłankami z art. 4 wymaga również, aby wobec podmiotu danych została podjęta decyzja oparta na zautomatyzowanym przetwarzaniu, która

[46] Wyrok TSUE z 13.05.2014 r., C-131/12, *Google Spain SL i Google Inc v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, CURIA.

wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Profilowanie kwalifikowane podlega znacznie większym ograniczeniom, które zostaną omówione w dalszej części publikacji.

Zbiorem danych, zgodnie z RODO, jest uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie. Elementy składające się na tę definicję pozostają niezmienione w stosunku do dyrektywy 95/46/WE i ustawy o ochronie danych osobowych. Zatem zbiór danych to zespół danych o charakterze osobowym (nazywany zestawem danych), spełniający dwa warunki: jest uporządkowany i dostępny według określonego kryterium. Uporządkowany charakter wyraża się w tym, iż zbiór danych ma cechy pozwalające na odnalezienie poszukiwanych informacji bez potrzeby przeglądania całego zbioru[47]. Ponadto zbiorem danych jest zestaw danych, w którym dostęp do danych jest możliwy przez jakiekolwiek kryterium osobowe[48]. Według Generalnego Inspektora Ochrony Danych Osobowych wystarcza alfabetyczne ułożenie danych według nazwisk (lub nazwisk i imion), by zestaw danych mógł być uznany za zbiór danych osobowych[49]. Wydaje się, iż na gruncie RODO wystarczające jest jedno kryterium uporządkowania zestawu danych, by uznać go za zbiór danych. Definicja zbioru danych jest niezbędna, aby dookreślić zakres zastosowania RODO. Jego przepisy stosuje się bowiem do niezautomatyzowanego przetwarzania danych w zbiorach, o czym będzie mowa w dalszym rozdziale.

RODO zawiera również szereg definicji odnoszących się do podmiotów uczestniczących w przetwarzaniu danych. W myśl art. 4 pkt 7 rozporządzenia „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Dodatkowo przepis ten wskazuje, iż jeżeli cele i sposoby przetwarzania są określone w przepisach prawa UE lub prawa krajowego, przepisy te mogą określać, kto jest administratorem albo w jaki sposób ma on być wyznaczony. Przepis ten jest podobny do obowiązującego wcześniej art. 7 pkt 4 u.o.d.o., uznającego za administratora podmiot, który decydował o celach i środkach przetwarzania danych[50]. Ad-

[47] A. Mednis, *Ustawa o ochronie...*, s. 26.

[48] A. Mednis, *Ustawa o ochronie...*, s. 26.

[49] Za www.giodo.gov.pl. Por. jednak wyroki: NSA z 12.01.2007 r., I OSK 218/06, LEX nr 290699, oraz WSA w Warszawie z 4.06.2012 r., II SA/Wa 289/12, LEX nr 1260338, w których sąd stwierdził, iż skoro ustawodawca użył w art. 7 pkt 1 u.o.d.o. określenia „kryteria" w liczbie mnogiej, to zgodnie z założeniem racjonalnego ustawodawcy należy przyjąć, że dostępność zestawu danych o charakterze osobowym musi być możliwa w oparciu o co najmniej dwa kryteria.

[50] Na temat szczegółowego znaczenia pojęcia administratora danych osobowych oraz odróżnionego od niego pojęcia podmiotu przetwarzającego na tle wcześniejszych przepisów – por. Opinia 1/2010 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 dyrektywy 95/46/WE przyjęta 16.02.2010 r. w sprawie pojęć „administrator danych" i „przetwarzający", https://giodo.gov.pl/1520057/id_art/3595/j/pl (dostęp: 25.02.2018 r.).