

Justyna Kunysz

Skuteczność prawa do ochrony danych osobowych a prawo dostępu do informacji publicznej

Administracja : teoria, dydaktyka, praktyka nr 3(32), 114-133

2013

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

Skuteczność prawa do ochrony danych osobowych a prawo dostępu do informacji publicznej

I. XXI wiek to czas szybko rozwijającej się cywilizacji. Gwałtowny wzrost znaczenia informacji, a także wykorzystywania nowych technologii komunikacyjnych w życiu zawodowym oraz codziennym można określić jako pewnego rodzaju transformację ukierunkowaną na utworzenie społeczeństwa informacyjnego. Podkreślić przy tym należy, że skłonność do poszukiwania informacji i dostępu do niej jest wynikiem podstawowej potrzeby człowieka o charakterze egzystencjalnym – potrzeby poznania¹. Jeszcze kilkanaście lat temu nie zdawano sobie powszechnie sprawy z tego jaką rolę w życiu społeczeństw będzie odgrywać technologia informacyjna i komunikacyjna. Obecnie osiągnięto moment, w którym z jednej strony dostęp oraz przepływ informacji stał się łatwy i szybki, ale z drugiej strony pojawiają się obawy o możliwe zagrożenia dla sfery prywatności osób fizycznych.

Gwarancje ochrony życia prywatnego są określone wprost w art. 47 Konstytucji Rzeczypospolitej Polskiej²; zgodnie z nim każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Wskazać przy tym należy, iż ochrona ta może mieć wymiar cywilnoprawny i karnoprawny; dostarczają jej również

¹ T. Górzyńska, *Geneza i rozwój prawa do informacji*, [w:] *Miscellanea Iuridica*, t. IV: *Współczesne problemy samorządu terytorialnego – Dostęp do informacji publicznej*, A. Dragoń, A. Lityński, G. Sibiga, Tychy 2004, s. 126.

² Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. nr 78, poz. 483 z późn. zm. i sprost. – zwana dalej Konstytucją RP.

przepisy ustawy o ochronie danych osobowych³. Trybunał Konstytucyjny uznał, iż prawo do prywatności, określone w art. 47 Konstytucji RP, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51 Konstytucji RP. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności – *expressis verbis* w ust. 1, 3, 4 i 5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2 – stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych⁴.

Prawo do ochrony danych osobowych funkcjonuje obok równie ważnego z punktu widzenia jednostki prawa do informacji znajdujących się w posiadaniu organów i instytucji państwa. Stanowi ono jedną z kardynalnych zasad współczesnej demokracji i społeczeństwa obywatelskiego⁵, ponadto umożliwia efektywną kontrolę obywatelską działań podejmowanych przez organy władzy publicznej⁶. Połączenie tych dwóch praw wydaje się być trudne do zrealizowania – a niekiedy wręcz niemożliwe. Dokonując bowiem ich prostego zestawienia, intuicyjnie wyczuwalne są zachodzące między nimi wzajemne relacje o charakterze zarówno komplementarnym, jak i sprzecznym. Ochrona danych osobowych stanowi fragment prawa do prywatności, ale jednocześnie funkcjonuje bardzo blisko prawa do informacji publicznej. Skoro tak to bezsprzecznym jest fakt możliwych „tarć” na linii styku tych chronionych prawnie wartości. A na tym tle pytanie o skuteczność regulacji o ochronie danych osobowych w kontekście udostępniania informacji publicznej nabiera szczególnego znaczenia.

³ Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, t.j. Dz. U. z 2002 r., nr 101, poz. 926 z późn. zm. – zwana dalej u.o.d.o.

⁴ Wyrok Trybunału Konstytucyjnego z 19 maja 1998 r., U 5/97, LEX 33147.

⁵ T. R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej*, Warszawa 2002, s. 7.

⁶ W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 65.

II. Prawo ochrony danych osobowych i prawo dostępu do informacji publicznej mają swoje umocowanie w normach konstytucyjnych. Przyczyną takiej regulacji jest fakt, że Konstytucja jest aktem prawnym o znaczeniu zasadniczym dla funkcjonowania państwa. Reguluje ona bowiem podstawy ustroju politycznego i społeczno-gospodarczego, ale równocześnie musi w swej treści nawiązywać do statusu jednostki w państwie i społeczeństwie⁷. Szczególną rolę w tej materii należy przypisać rozdziałowi II Konstytucji RP: „Wolności, prawa i obowiązki człowieka i obywatela”, który w art. 51 i 61 wartości te gwarantuje⁸. W jego zakres wchodzi warunek ustawowej podstawy ujawnienia przez jednostkę informacji dotyczących jej osoby (ust. 1), zakaz pozyskiwania, gromadzenia i udostępniania o obywatelach innych informacji, niż niezbędne w demokratycznym państwie prawnym (ust. 2), prawo dostępu jednostki do odnośnych dokumentów i zbiorów danych oraz żądania sprostowania bądź usunięcia danych nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (ust. 3 i 4).

Artykuł 61 Konstytucji RP wskazuje, że obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to dotyczy również możliwości uzyskiwania informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa (ust. 1). Ponadto obejmuje dostęp do

⁷ Doniosłość tej tematyki widoczna jest już w Deklaracji Praw Człowieka i Obywatela z 1789 r., która w art. 16 stanowi, że nie ma w państwie Konstytucji, jeśli nie została przyjęta zasada podziału władz i nie zagwarantowano praw jednostki – W. Skrzydło, *op. cit.*, s. 35.

⁸ Dodać należy, że znaczenie rozdziału II wzmacnia dodatkowo fakt, że w przypadku zaistnienia chęci zmiany jego postanowień, obok konieczności ich przyjęcia w jednakowym brzmieniu przez Sejm i Senat, zgodnie z art. 235 ust. 6 Konstytucji RP 1/5 ustawowej liczby posłów, Senat lub Prezydent RP mogą wystąpić do Marszałka Sejmu z wnioskiem o przeprowadzenie referendum zatwierdzającego.

dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzącej z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu (ust. 2).

Ustawa zasadnicza nie określa zatem wprost relacji między ochroną danych osobowych, a dostępem do informacji publicznej. Tworzy ogólne ramy tych praw, które zgodnie z regulacją prawną zawartą w art. 51 ust. 5 i art. 61 ust. 4 Konstytucji RP zostaną uszczegółowione w ustawach. Wspomniane uszczegółowienie realizuje u.o.d.o. i ustawa o dostępie do informacji publicznej z 6 września 2001 r.⁹ Akty te w sposób bardziej precyzyjny wyznaczają możliwości ich wzajemnego funkcjonowania.

III. Zagadnienie skuteczności regulacji o ochronie danych osobowych wymaga w pierwszej kolejności wyjaśnienia czym owa skuteczność jest. W literaturze przedmiotu przyjmuje się, że prawo jest skuteczne (w znaczeniu ogólnym), jeżeli wywołuje skutki zgodne w dostatecznie wysokim stopniu z założonym celem¹⁰. W związku z tym pytanie o skuteczność regulacji u.o.d.o. sprowadza się do wyznaczenia celu (lub celów), które ten akt normatywny ma realizować. Wskazać jednakże należy, że już pobieżna analiza pokazuje, że nie ma wyraźnych odesłań, które mogłyby świadczyć o motywach jego wprowadzenia. Ponadto nie ma odwołania do praw i wolności, w tym prawa do prywatności. Zgodzić jednakże należy się z twierdzeniem, że nie jest oczywiste, czy ustawę należałoby w tym kierunku zmieniać¹¹. W związku z tym możliwa wydaje się próba wyprowadzenia celu (celów) ustawy z punktu widzenia całościowego spojrzenia na tę regulację prawną.

Ochrona danych osobowych jawi się jako konieczność zabezpieczenia interesów jednostki, której dane osobowe są przetwa-

⁹ Dz. U. nr 112, poz. 1198 z późn. zm. – zwana dalej u.d.i.p.

¹⁰ Z. Kmiecik, *Skuteczność regulacji administracyjnoprawnej*, Łódź 1994, s. 15 i 27–28.

¹¹ G. Szpor, *Uwarunkowania skuteczności regulacji ochrony danych osobowych*, [w:] *Ochrona danych osobowych. Skuteczność regulacji*, G. Szpor (red.), Warszawa 2009, s. 26.

rzane. Ustawa swym zakresem działania obejmuje wszelkie postacie przetwarzania danych zarówno manualne (w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych) jak i w systemach informatycznych (automatycznie). Zgodnie z art. 7 pkt 2 u.o.d.o. wspomniane przetwarzanie to wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. Tak szerokie ujęcie należy ocenić pozytywnie, gdyż na każdym etapie pracy na danych osobowych – od ich uzyskania po wyeliminowanie – stosuje się przepisy u.o.d.o. Co więcej, na administratora danych¹², który decyduje o celach i środkach przetwarzania, nałożony został obowiązek szczególnej staranności by ochronić interesy osób, których dane dotyczą. Urzeczywistnienie tego zobowiązania jest możliwe poprzez zastosowanie następujących zasad: legalności (przetwarzanie danych zgodnie z obowiązującym prawem), celowości (zbieranie danych dla oznaczonych, zgodnych z prawem celów¹³), merytorycznej poprawności danych, adekwatności (w stosunku do celów w jakich są przetwarzane), ograniczenia czasowego (przechowywanie w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne dla osiągnięcia celu przetwarzania). Podstawową zasadą ustawy nie jest zakaz przetwarzania danych osobowych, ale przestrzeganie trybu i zakresu tego procesu. Troska o zapobieżenie negatywnym skutkom wynikającym z niezgodnego z prawem dokonywania którejkolwiek z czynności mieszczących się w zakresie przedmiotowym przetwarzania odgrywa zatem priorytetowe znaczenie. W tym sensie u.o.d.o. spełnia rolę aktu prawnego o charakterze prewencyjnym. Pamiętaj

¹² Może być to organ, jednostka organizacyjna, podmiot lub osoba (art. 7 ust. 4 u.o.d.o.).

¹³ Ustawa przewiduje wyjątki od tej zasady uregulowane w art. 26 ust. 2 u.o.d.o.

bowiem należy, że dane osobowe raz ujawnione nie dadzą się na powrót utajnić¹⁴.

Nie bez znaczenia jest fakt gwałtownego rozwoju technologii informacyjnej oraz stale rozszerzającego się dostępu do niej. Okoliczność tę potęguje fakt, że coraz częściej dane osobowe są przetwarzane przy pomocy środków komunikacji elektronicznej, a procesy te mają wymiar nie tylko lokalny czy krajowy, ale również globalny.

W literaturze przedmiotu podaje się, że celem ochrony danych osobowych jest również zapewnienie możliwości swobodnego przepływu danych osobowych. Podkreśla się, że jeśli przetwarzanie odbywać się będzie zgodnie z regułami określonymi przez przepisy prawa i zapewniona będzie należyta ochrona osób, których dane dotyczą, przepływ danych nie powinien napotykać na istotne ograniczenia i bariery¹⁵.

Ochrona danych osobowych przed niezgodnym z prawem ich przetwarzaniem nabiera istotnego znaczenia na polu realizowania prawa dostępu do informacji publicznej. Nietrudno bowiem wyobrazić sobie sytuację w której udzielając informacji publicznej dochodzi do udostępnienia danych osobowych osobom nieupoważnionym. Jest to okoliczność niebezpieczna z uwagi na znaczenie informacji w dzisiejszym świecie w różnych sferach życia. W związku z tym w pierwszej kolejności należy przyrzeć się zakresowi podmiotowemu ustaw, jak również kluczowym pojęciom obu aktów normatywnych. Jest to kwestia zasadnicza skoro podkreśla się ich wzajemne relacje.

IV. Zakres podmiotowy ustawy wymaga wyznaczenia kręgu podmiotów, które będą uprawnione do korzystania z prawa oraz tych, które są zobowiązane do jego realizowania. W pierwszej grupie znajdzie się bezsprzecznie jednostka, która jest beneficjen-

¹⁴ B. Banaszak, K. Wygoda, *Regulacja prawna ochrony danych osobowych w Polsce w świetle ustawy z 29 sierpnia 1997 r. i standardów europejskich*, [w:] *Ochrona danych osobowych*, M. Wyrzykowski (red.), Warszawa 1999, s. 68.

¹⁵ P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne*, Lublin 2008, s. 35.

tem przyznanych jej praw. Należy jednakże w tym miejscu dokończyć pewnego doprecyzowania. Na mocy art. 1 ust. 1 u.o.d.o. każdy ma prawo do ochrony dotyczących go danych osobowych, co pozostaje zbieżne z postanowieniami Konstytucji RP (art. 51 ust. 1). Uwzględniając jednakże definicję danych osobowych, wynikającą z art. 6 u.o.d.o. (rozumianych jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej) należy wyprowadzić wniosek, że u.o.d.o. ma zastosowanie tylko i wyłącznie do osób fizycznych; nie dotyczy więc innych podmiotów prawa.

Nieco szerzej, choć przy pomocy tej samej techniki legislacyjnej, skonstruowane jest pojęcie strony uprawnionej w u.d.i.p. Obejmuje ono nie tylko osoby fizyczne, ale także osoby prawne i jednostki organizacyjne niemające osobowości prawnej np. organizacje społeczne¹⁶. Dodać przy tym należy, że ustawodawca poszerzył krąg podmiotów uprawnionych do dostępu do informacji publicznej w stosunku do tego co zostało zagwarantowane w ustawie zasadniczej. Jej art. 61 ust. 1 wskazuje, iż korzystać z niego mogą tylko osoby posiadające polskie obywatelstwo, natomiast w świetle postanowień u.d.i.p. kryterium to nie ma znaczenia. W tym przypadku należy uznać, iż Konstytucja RP określa jedynie pewne minimum dostępności i nic nie stoi na przeszkodzie by informację udzielić każdej zainteresowanej osobie niezależnie od jej obywatelstwa, czy też jego braku¹⁷.

Stronę zobowiązaną do przestrzegania zasad ochrony danych osobowych tworzą wszystkie podmioty, które dokonują przetwarzania danych osobowych. Co więcej, nie ma znaczenia fakt ich przynależności do sektora publicznego (organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne

¹⁶ Wyrok WSA w Warszawie z 11 lutego 2004 r., II SAB 391/03 – orzeczenie dostępne w Centralnej Bazie Orzeczeń Sądów Administracyjnych – zwanych dalej CBOSA, M. Jaśkowska, *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002, s. 41.

¹⁷ M. Chmaj [w:] *Ustawa o dostępie do informacji publicznej. Komentarz*, M. Bidziński, M. Chmaj, P. Szustakiewicz, Warszawa 2010, s. 35.

jednostki organizacyjne) czy prywatnego (podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne i prawne oraz jednostki organizacyjne nieposiadające osobowości prawnej, jeżeli przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej). W tym ostatnim przypadku ustawa zastrzega jedynie by podmiot miał siedzibę na terytorium Rzeczypospolitej Polskiej albo w państwie trzecim, o ile przetwarza dane osobowe przy pomocy środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej. Z kolei w u.d.i.p. ustawodawca stworzył niekompletne zestawienie podmiotów zobowiązanych do wykonywania obowiązku informacyjnego. Dokonał jedynie ich przykładowego wyliczenia oraz podziału na władze publiczne, podmioty wykonujące zadania publiczne, organizacje związkowe i pracodawców oraz partie polityczne.

Stwierdzić należy, że u.o.d.o. ma znacznie szerszy zakreślony zakres podmiotów zobowiązanych do jej realizowania, a w ich katalogu zawierają się te, których dotyczy u.d.i.p.

V. W tym miejscu dla ukazania istoty ochrony danych osobowych w kontekście dostępu do informacji publicznej konieczne wydaje się wyjaśnienie samego pojęcia dane osobowe i informacja publiczna. Wymagają one rozpatrzenia, z uwagi na to, że nie można rozumieć ich przypadkowo czy intuicyjnie.

Formuła „dane osobowe” ma swoją definicję legalną zawartą w art. 6 u.o.d.o. Zgodnie z nią są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (ust. 1). Nadmienić należy, iż wcześniejsze ujęcie danych osobowych było znacznie węższe i mocno krytykowane w literaturze przedmiotu¹⁸. Artykuł 6 u.o.d.o. w brzmieniu do zmiany ustawą z dnia 25 sierpnia 2001r. o zmianie ustawy o ochronie danych osobowych¹⁹ stanowił, iż za dane osobowe uważa się każdą in-

¹⁸ A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 21.

¹⁹ Dz. U. nr 100, poz. 1087.

formację dotyczącą osoby fizycznej, pozwalającą na określenie jej tożsamości. Na bazie tego przepisu NSA w wyroku z dnia 17 listopada 2000 r.²⁰ uznał za dane osobowe jedynie tzw. dane identyfikujące (np. imię, nazwisko, adres, numery PESEL i NIP), a tzw. dane osobopoznawcze – według sądu – nie korzystały z ochrony ustawowej.

Wyżej wymieniony podział nie ma znaczenia w kontekście obecnie obowiązującej regulacji art. 6 u.o.d.o. Posłużenie się bowiem przez ustawodawcę techniką legislacyjną polegającą na użyciu zwrotu „wszelkie informacje” nakazuje przyjąć szerokie znaczenie tego terminu co oznacza, że będzie się w nim mieścić każdy atrybut odnoszący się osoby fizycznej, począwszy od jej życia zawodowego i prywatnego po np. wiedzę czy cechy charakteru. Nie ma także znaczenia fakt w jakiej roli występuje w danym przypadku osoba fizyczna (np. członka rodziny, członka grupy zawodowej czy przedsiębiorcy)²¹. Takie twierdzenie umacnia regulacja prawna zawarta w art. 6 ust. 2 u.o.d.o. wskazując, że osoba jest możliwa do zidentyfikowania, gdy jej 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. Natomiast przesłanką uniemożliwiającą określenie tożsamości osoby fizycznej jest sytuacja, gdy jej oznaczenie wymaga nadmiernych kosztów, czasu lub działań (art. 6 ust. 3 u.o.d.o.). Ustawodawca „przerzucił” więc na administratora danych konieczność ustalenia czy owa nadmierność ma miejsce czy nie, a to w konsekwencji decyduje czy określone dane będą podlegać ochronie czy też zostaną jej pozbawione.

Pojęcie dane osobowe nie ma charakteru jednolitego. Można dokonać jego podziału na dane osobowe zwykłe (pospolite) i wrażliwe (sensytywne, delikatne). Tym drugim ustawodawca

²⁰ II SA 1860/00 – wyrok niepublikowany.

²¹ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 339.

zagwarantował bardziej intensywną ochronę oraz bardziej rygorystyczne zasady przetwarzania²². Artykuł 27 u.o.d.o. zalicza do nich pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dotyczące stanu zdrowia, kodzie genetycznym, nałogach, życiu seksualnym oraz odnoszące się do skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych wydanych w postępowaniu sądowym lub administracyjnym.

Z kolei informacja publiczna w świetle postanowień art. 1 ust. 1 u.d.i.p. to każda informacja o sprawach publicznych. Taka redakcja definicji legalnej jest bardzo szeroka, ale jednocześnie jest to ujęcie dosyć ogólnikowe; dodatkowo należy w nim dostrzec błąd logiczny przejawiający się w wyjaśnianiu pojęcia nieznanego przez inne również nieznanne (*ignotum per ignotum*)²³. Środkiem na te niedoskonałości – w jakimś stopniu – ma być art. 6 u.d.i.p. Przepis ten wylicza zakres danych mogących stanowić informację publiczną. Jest to jednak katalog przykładowy, ale daje pewien punkt odniesienia do zakresu przedmiotowego tego pojęcia. Przyjęta technika legislacyjna może być usprawiedliwiona choćby przez konieczność objęcia jak najszerszym zakresem dużej liczby informacji.

W literaturze przedmiotu wskazuje się, że termin ten nie może być rozpatrywany wyłącznie na tle art. 1 ust. 1 u.d.i.p.; należy uwzględnić jeszcze art. 61 Konstytucji RP. W przeciwnym wypadku zastosowana wykładnia językowa mogłaby wówczas prowadzić do zbyt wąskiego rozumienia tego pojęcia²⁴. Dlatego też informacją publiczną jest każda wiadomość wytworzona lub odnoszona do szeroko rozumianych władz publicznych oraz wytworzona lub odnoszona do innych podmiotów wykonujących funkcje publiczne w zakresie wykonywania przez nie zadań władzy pu-

²² Tamże, s. 548.

²³ I. Kamińska, M. Rozbicka-Ostrowska, *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2012, s. 12, M. Chmaj, *op. cit.*, s. 19–20, M. Jaśkowska, *op. cit.*, s. 26.

²⁴ Tamże, s. 26.

blicznej i gospodarowania mieniem komunalnym lub majątkiem Skarbu Państwa²⁵.

Wydaje się, że dość jednoznacznie można rozstrzygnąć jakie informacje uważane za publiczne mogą stanowić dane osobowe i na odwrót. Nadto zaznaczyć należy, że informacja publiczna jest kategorią szerszą, a dane osobowe są jedynie jej częścią²⁶.

VI. Zagadnienie skuteczności regulacji ochrony danych osobowych na tle udostępniania informacji publicznej można rozpatrzyć biorąc pod uwagę zakres przedmiotowy prawa do informacji publicznej. Artykuł 3 ust. 1 u.d.i.p. określa przysługujące jednostce następujące uprawnienia: uzyskanie informacji publicznej (w tym uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego); wglądu do dokumentów urzędowych oraz dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów²⁷. Realizacja każdego z nich wiąże się z koniecznością uwzględnienia regulacji u.o.d.o., dlatego że informacja publiczna nie może zawierać danych osobowych identyfikujących osobę fizyczną; dane te podlegają ochronie prawnej.

Większych problemów nie będzie w sytuacji gdy podmiot zobowiązany do udzielenia informacji publicznej uczyni to w formie

²⁵ Wyrok NSA z 23 maja 2003 r., II SA 4059/02, LEX 78063; wyrok WSA w Warszawie z 25 maja 2004 r., II SAB/Wa/83/04, LEX 158993; wyrok WSA w Rzeszowie z 17 stycznia 2013 r., II SAB/Rz/48/12, LEX 1285163.

²⁶ M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wrocław 2002, s. 238–242.

²⁷ Podstawą prawną ich realizacji jest art. 7 ust. 1 u.d.i.p., który precyzuje sposoby udostępniania informacji publicznych. Następuje to przez ogłoszenie informacji publicznych (w tym dokumentów urzędowych) w Biuletynie Informacji Publicznej; udostępnienie w drodze wyłożenia lub wywieszenia w miejscach ogólnie dostępnych lub przez zainstalowanie urządzenia umożliwiającego zapoznanie się z informacją; udostępnienie informacji na wniosek; wstępu na posiedzenia kolegialnych organów władzy pochodzących z powszechnych wyborów i udostępniania materiałów, tym audiowizualnych i teleinformatycznych, dokumentujących te posiedzenia; umieszczenia informacji w centralnym repozytorium informacji publicznych.

pisemnej. Ochrona danych osobowych jednostki odbywa się wówczas przez wykonanie czynności anonimizacji jej danych, czyli poprzez wykreślenie elementów mogących wpłynąć na jej rozpoznanie. W tym miejscu należy zwrócić uwagę na pewną gradację w intensywności ochrony. O ile daleko idącej ochronie podlegają dane osób będących adresatami np. orzeczeń sądowych czy decyzji administracyjnych, o tyle ochronie takiej nie podlegają dane osobowe osób pełniących funkcje publiczne, będących autorami konkretnych rozstrzygnięć. Dlatego też przygotowując dokument do udostępnienia nie należy anonimizować wszystkich danych osobowych, a jedynie te które dotyczą jej adresata. Imię i nazwisko osoby upoważnionej do ich wydania (a więc osoby wykonującej funkcje publiczne) powinno być dostępne z uwagi na fakt, że są to ważne elementy dokumentu urzędowego, pozwalające stwierdzić czy dokument i złożone w nim oświadczenie przyznające prawa bądź nakładające obowiązki pochodzą od podmiotu uprawnionego²⁸.

Nieco wyższy stopień zagrożenia jest w sytuacji realizowania prawa wglądu do dokumentów urzędowych. Uprawnienie to oznacza, że zainteresowany może zapoznać się z ich treścią, a także na podstawie art. 12 ust. 2 u.d.i.p. ma możliwość kopiowania informacji publicznej, sporządzenia jej wydruku, przesłania jej albo przeniesienia na odpowiedni powszechnie stosowany nośnik informacji. Podmiot zobowiązany do udostępnienia informacji publicznej powinien więc być szczególnie wyczulony na potencjalną możliwość ujawnienia danych osobowych, a to w praktyce może okazać się niezwykle trudne. W wielu przypadkach oczywista jest czasochłonność podejmowanych działań w tym zakresie, a także trudności o charakterze organizacyjno-technicznym. Podkreślić jednakże należy, że precyzyjność tego procesu staje się niejako gwarantem skuteczności ochrony danych osobowych.

Najwięcej niebezpieczeństw niesie ze sobą ostatecznie uprawnienie, a mianowicie dostęp do posiedzeń kolegialnych organów

²⁸ I. Kamińska, M. Rozbicka-Ostrowska, *op. cit.*, Warszawa 2012, s. 35–36.

władzy publicznej pochodzących z powszechnych wyborów²⁹, a także ustne udzielanie informacji publicznej. W czasie dyskusji – na żywo – w szczególności, gdy ma ona charakter bardzo żywiołowy, nietrudno o wyjawienie informacji, które bezpośrednio lub pośrednio zostaną związane z konkretną jednostką³⁰.

VII. Na analizowaną problematykę można jeszcze spojrzeć przez pryzmat uregulowań proceduralnych. W u.d.i.p. wprowadzono zasadę, że dostęp do informacji publicznej przysługuje każdemu; co więcej, ustawa ta stanowi, że nie można od nikogo żądać wykazania interesu prawnego lub faktycznego. Nie jest to jednak prawo o charakterze absolutnym w tym sensie, że nie podlega żadnym ograniczeniom. Artykuł 5 u.d.i.p., określa bowiem dopuszczalne zastrzeżenia stosowane przy realizowaniu tego uprawnienia. Zgodnie z nim prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, a także ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Wspomniana prywatność nie dotyczy osób pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, a także w odniesieniu do warunków powierzenia i wykonywania tych funkcji oraz w przypadku gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Wynika stąd, że informacje dotyczące powyższych elementów będą miały charakter powszechnie dostępne, choć niewątpliwie podkreślić trzeba, że mieszczą się one w pojęciu dane osobowe, definiowanym jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Dane osobowe osób pełniących funkcje publiczne z natury swej korzystają z ograniczonej ochrony, a prawo dostępu do nich

²⁹ Będą to Sejm, Senat, rada gminy, powiatu, sejmik województwa, zebranie wiejskie, rada dzielnicy oraz rada osiedla.

³⁰ Szerzej A. Błaszczczyńska, *Dostęp do informacji publicznej a ochrona danych osobowych*, „Przegląd Prawa Publicznego” 2011, nr 12, s. 24–28.

można wyprowadzić z art. 61 Konstytucji RP (obywatel ma prawo uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne)³¹. Ponadto warto zwrócić uwagę na wyrok Trybunału Konstytucyjnego³², który stwierdził, iż w odniesieniu do osób pełniących funkcje publiczne ochrona sfery ich życia prywatnego podlega pewnym ograniczeniom, uzasadnionym „usprawiedliwionym zainteresowaniem publicznym”. Muszą one zaakceptować szerszy zakres ingerencji w sferze ich prywatności niż w wypadku innych osób. Jest to usprawiedliwione ze względu na wartość, jaką jest jawność i dostępność informacji o funkcjonowaniu instytucji publicznych w państwie demokratycznym. Jednocześnie nie oznacza to, że wartość ta związana z transparentnością życia publicznego prowadzi do całkowitego przekreślenia i zanegowania ochrony związanej z życiem prywatnym osób wykonujących funkcje publiczne. Wkroczenie w sferę prywatności musi być zawsze uzasadnione istotnymi racjami interesu publicznego i pozostawać w związku z wykonywaną działalnością publiczną.

Sama u.o.d.o. nie zawiera bezpośredniego odwołania do prawa do prywatności. Z drugiej strony u.d.i.p. nie odnosi się w sposób jednoznaczny do ochrony danych osobowych³³. Ponadto w Konstytucji RP prawo do informacji publicznej i ochrony danych osobowych zostały uregulowane w odrębnych przepisach prawnych (47 i 51). Jednakże ich wzajemnych relacji można się dopatrzeć w zasygnalizowanym we wstępie wyroku Trybunału Konstytucyjnego w którym stwierdzono, że prawo do prywatności zagwarantowane jest między innymi w aspekcie ochrony danych osobowych, a także w literaturze przedmiotu gdzie wskazuje się, że ochrona danych osobowych jest wyspecjalizowaną formą ochrony

³¹ M. Podgłówek, *Dostęp do informacji publicznej [w:] Europeizacja polskiego prawa administracyjnego*, Z. Janku, Z. Leoński, M. Szewczyk, M. Waligórski, K. Wojtczak (red.), Wrocław 2005, s. 422–437.

³² Wyrok Trybunału Konstytucyjnego z 20 marca 2006 r., K 17/05, LEX 182494.

³³ Pojęcie to przewidywał już nieobowiązujący art. 22 u.d.i.p.

prawa do prywatności³⁴. Można jej przypisać charakter wtórny³⁵, jako zabezpieczającej przed niezgodnym z prawem wyjawianiem informacji o osobach fizycznych, które pośrednio lub bezpośrednio wpływają na jej identyfikację.

Ustawa o ochronie danych osobowych nie reguluje sytuacji udostępniania danych osobowych stanowiących informację publiczną. Zawiera ona jedynie przesłanki uzasadniające możliwość przetwarzania danych osobowych czyli dokonywania jakichkolwiek operacji na danych osobowych (w tym udostępniania). W odniesieniu do danych zwykłych ich zamknięty katalog zawiera art. 23 ust. 1 pkt 1–5. Zgodzić należy się przy tym z twierdzeniem, że wszelkie przetwarzanie danych, które nie jest dozwolone, jest zakazane³⁶. A zatem wystąpienie jednej z nich jest warunkiem wymaganym dla legalności procesu przetwarzania danych osobowych; mają więc one charakter samoistny. W zestawieniu tym najbardziej konfliktogenną w kontekście podejmowanego tematu może okazać się przesłanka uregulowana w art. 23 ust. 1 pkt 2³⁷. Daje ona możliwość przetwarzania (a więc i udostępniania) danych osobowych, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Dokonując analizy tej przesłanki legalizującej przetwarzanie nale-

³⁴ M. Safjan, *Ochrona danych osobowych – granice autonomii informacyjnej* [w:] *Ochrona danych osobowych*, M. Wyrzykowski (red.), Warszawa 1999, s. 10.

³⁵ M. Sakowska, *Relacje pomiędzy prawem do ochrony danych osobowych a prawem do informacji publicznej*, „*Studia Prawno-Ekonomiczne*” 2005, tom LXXII, s. 63.

³⁶ J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 449.

³⁷ Pozostałe przesłanki legalizujące przetwarzanie danych osobowych zwykłych to: zgoda osoby, której dane dotyczą na ich przetwarzanie; sytuacja, gdy jest to konieczne dla realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Wydaje się jednak, że nie będą one często stosowane w odniesieniu do analizowanego tematu.

ży zadać pytanie czy uprawnienie jednostki do uzyskania informacji publicznej i jednocześnie obowiązek podmiotu zobowiązanego do jej udzielenia wynikające z u.d.i.p. mieści się w jej treści. Odpowiedź twierdząca powoduje, że mamy do czynienia z paradoksalną sytuacją, która prowadzi do przekonania, że ochrona danych osobowych nie może być skuteczna bo jej w istocie nie ma – została wyłączona na skutek powołania się na prawo do udostępnienia informacji publicznej³⁸. Dodać należy, że w piśmiennictwie można spotkać się z poglądem, że ochrona na podstawie u.o.d.o. nie przysługuje jeśli przepis szczególny wyłącza ochronę. Jeśli więc przetwarzane są dane osobowe będące jednocześnie informacjami publicznymi w rozumieniu art. 1 u.d.i.p., ochrona na podstawie u.o.d.o. nie istnieje³⁹.

Z drugiej strony podaje się, że informacje o osobach publicznych, mające związek z pełnieniem tych funkcji, mogą być udostępnione na zasadach określonych w u.d.i.p. z powołaniem się właśnie na art. 23 ust. 2 pkt 2 u.o.d.o., który to przepis pełni rolę zezwalającego na przetwarzanie i udostępnianie danych osobowych⁴⁰. A zatem przepisy te ze sobą współgrają – mają charakter komplementarny. Ewentualne spory co do zgodności określonego w u.d.i.p. prawa do informacji z warunkami u.o.d.o. mogą dotyczyć danych wrażliwych⁴¹.

Przetwarzanie danych wrażliwych jest co do zasady niedozwolone. Zakaz może zostać jednakże zniesiony w sytuacji, gdy zaistnieje przesłanka wynikająca z art. 27 ust. 2 u.o.d.o. Zestawienie ustawowe jest dosyć pojemne – liczy dziesięć pozycji, ale w podejmowanej problematyce uzasadnione jest zwrócenie uwagi na

³⁸ A. Błaszczczyńska, *op. cit.*, s. 33.

³⁹ A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2008, s. 15

⁴⁰ G. Sibiga, *Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych*, „Samorząd Terytorialny” 2002, nr 11, s. 9.

⁴¹ G. Sibiga, *Komplementarność czy kolizja? Prawna ochrona danych osobowych a dostęp do informacji publicznych oraz informacji o środowisku i jego ochronie* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, P. Fajgielski (red.), s. 165.

dwie: gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych, bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony (pkt 2) oraz gdy przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą (pkt 8)⁴². W pierwszym przypadku przetwarzanie jest dozwolone gdy inna ustawa wyraźnie na to zezwala⁴³ (ustawa musi zapewnić pełne gwarancje ochrony). Warunków tych nie spełniają przepisy u.d.i.p.⁴⁴ Dane wrażliwe istotne z punktu widzenia osób pełniących funkcje publiczne, mających związek z pełnieniem funkcji publicznych dotyczą

⁴² Pozostałe sytuacje uzasadniające dopuszczalność przetwarzania danych wrażliwych mają miejsce jeżeli: osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych; przetwarzanie takich danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora; jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych; przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem; przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie; przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych; jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, publikowanie w wyniku badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone; przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

⁴³ E. Kulesza, *Istotne rozróżnienie*, „Rzeczpospolita” z dnia 14 lutego 2000 r.

⁴⁴ G. Sibiga, *Komplementarność...*, s. 165.

przede wszystkim skazań, orzeczeń o ukaraniu, mandatów karnych oraz innych orzeczeń wydanych w postępowaniu sądowym i administracyjnym. Drugi przypadek, w którym uchylony zostaje zakaz przetwarzania danych sensytywnych to sytuacja, gdy zostały one podane do publicznej wiadomości przez osobę, której dane dotyczą. Osoby pełniące funkcje publiczne oraz mające związek z pełnieniem funkcji publicznych często udostępniają te informacje za pośrednictwem środków masowego przekazu (prasa, radio, telewizja).

Należy zwrócić uwagę na kwestie ewentualnego pierwszeństwa jednej z tych ustaw przed drugą w sytuacji, gdy informacja publiczna zawiera dane osobowe, a te są istotą wniosku uprawnionego podmiotu. Poglądy w tej kwestii kształtują się dwutorowo. Z jednej strony wskazuje się, że jeżeli informacja publiczna zawiera w swej treści dane osobowe (dane wrażliwe) niezbędne jest także dokonanie analizy zgodności jej treści z wymogami określonymi w u.o.d.o.⁴⁵ Ujęcie to znajduje odzwierciedlenie w wyrokach WSA w Warszawie z 13 czerwca 2006 r. i 20 kwietnia 2006 r.⁴⁶, w których wskazuje się, że u.o.d.o. w sytuacji, gdy w treści informacji publicznej zawarte są dane osobowe jest *lex specialis* w stosunku do u.d.i.p. Jeśli zatem informacja publiczna zawiera dane osobowe, a nie wchodzi w grę art. 5 ust. 2 u.d.i.p., nie można uznać, że zaistniała przesłanka legalizująca ich udostępnienie, o której mowa w art. 23 ust. 1 pkt 1 u.o.d.o. (zgoda) w zw. z art. 1 ust. 2 u.d.i.p. Pierwszeństwo w ochronie mają dane osobowe, a tym samym wykonanie obowiązku informacyjnego nie stanowi przesłanki legalizującej ich udostępnienie. Podkreśla się, że odmienna wykładnia prowadziłaby do tego, że na podstawie u.d.i.p. można byłoby uzyskać legalnie dostęp do danych chronionych u.o.d.o.

⁴⁵ M. Bidziński [w:] *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2010, s. 70.

⁴⁶ II SA/Wa 2016/05, LEX 219349, II SA/Wa 2227/05, LEX 220927, wyrok SN z dnia 21 października 2008 r., II PK 71/08, LEX 1110973.

Z drugiej strony podaje się, że przepisy u.o.d.o. nie mają charakteru szczególnego w stosunku do u.d.i.p., a w konsekwencji nie przysługuje im pierwszeństwo zgodnie z zasadą *lex specialis derogat legi generali*. Obie ustawy stanowią równorzędne akty prawne i w każdej sprawie konieczne staje się wyważenie możliwości realizacji prawa do informacji publicznej w sytuacji, gdy w tej informacji zawarte są jednocześnie dane osobowe. Organ będzie musiał dokonać wstępnej oceny, czy udostępnienie informacji publicznej (w tym zawierającej dane osobowe) będzie dopuszczalne na gruncie u.d.i.p. w tym względzie, że nie będzie również naruszało u.o.d.o. (że będzie z nią zgodne), a w konsekwencji nie będzie naruszało sfery prywatności osoby, której dane dotyczą⁴⁷.

Na płaszczyźnie aksjologicznej trudno byłoby wskazać racje, które miałyby w konkretnym przypadku uzasadnić pierwszeństwo prawa do ochrony danych osobowych przed prawem dostępu do informacji publicznej. Ustawodawca kształtując obie wartości dąży bowiem do pełnej realizacji każdej z nich.

VIII. W konkluzji należy stwierdzić, że problematyka skuteczności regulacji dotyczącej ochrony danych osobowych jest istotna z punktu widzenia jednostki. Informacje zawierające dane osobowe przypisane są do sfery życia prywatnego, a przy tym niejednokrotnie są związane z pełnieniem funkcji publicznych. Może to wywoływać kontrowersje i problemy w praktyce stosowania prawa z uwagi na fakt, że powołując się na prawo dostępu do informacji publicznej wnioskodawca niejako „przy okazji” może otrzymać dane osobowe innego podmiotu. Ochrona danych osobowych wymaga więc uwzględnienia przeciwstawnych interesów – dostępu do informacji publicznej z jednej strony i nienadużywania prywatności jednostki z drugiej. Powinna ona mieć zaufanie do organów państwowych oraz innych podmiotów, które dysponują jej danymi osobowymi. Dlatego w celu zmniejszenia ewentu-

⁴⁷ Wyrok NSA z 5 marca 2013 r., I OSK 2872/12 – wyrok dostępny w CBOSA, I. Maciejuk, *Dostęp do informacji publicznej zawierającej dane osobowe*, „Zeszyty Naukowe Sądownictwa Administracyjnego” 2009, nr 9, s. 77.

alnego ryzyka związanego z naruszeniem ustawy o ochronie danych osobowych trzeba zwrócić uwagę także na element organizacyjny w postaci odpowiedniego doboru i przeszkolenia kadr, które będą nie tylko znać obowiązki ustawowe, ale i należycie je wypełniać w ramach wykonywanej przez siebie pracy.

ABSTRACT

Efficiency of a right to protect personal data versus a right of access to public information

The problems of efficiency of regulation concerning protection of personal data in a context of making available public information is essential from the point of view of an individual. Since it is not difficult to imagine a situation in which public information is given and then personal data are made available to an authorised person. It is an undesirable phenomenon looking at it even by a prism of meaning of information in a contemporary world. Thus, protection of personal data requires taking into account contrary interests of access to public information and non-misusing an individual's right to privacy, which in the practice of application of the law can provoke problems and controversies.