WPROWADZENIE

Problematyka ochrony danych osobowych wyodrębniła się stosunkowo niedawno. Dość powiedzieć, że jako samodzielne zagadnienie wymagające badań zaczęła być traktowana dopiero w latach sześćdziesiątych XX wieku, natomiast pierwsze regulacje ustawowe w tym zakresie pojawiły się niespełna trzydzieści lat temu. Nie oznacza to jednak, że tematyka ochrony danych osobowych nie była zauważana już wcześniej. Pojawiała się już od końca XIX wieku, tyle że była traktowana jako jeden z elementów ochrony prywatności i wraz z nią stopniowo torowała sobie drogę do uznania jako istotny element praw i wolności człowieka. Analiza orzecznictwa i doktryny przełomu XIX i XX wieku wykazuje, że jako naruszenie prywatności już wtedy traktowano takie czyny jak zbieranie informacji o jakiejś osobie bez jej zgody lub metodami uznanymi za niedopuszczalne, czy też czynienie użytku przez zbierającego dla własnych korzyści z materiałów o innej osobie. Gdy więc w połowie ubiegłego stulecia doszło do powszechnego uznania prywatności za dobro wymagające zabezpieczenia ze strony prawa, ochrona danych osobowych została niejako automatycznie potraktowana jako element tej konstrukcji. Stąd też twórcy ówczesnych aktów o ochronie praw człowieka nie znaleźli powodów dla osobnej regulacji omawianego przez nas zagadnienia.

Zmiana podejścia – jak już wspomniano – nastąpiła dopiero w latach sześćdziesiątych XX wieku. Była ona konsekwencją rozwoju technologicznego, zwłaszcza zaś pojawienia się pierwszych komputerów pozwalających na łatwe gromadzenie, opracowywanie i przesyłanie danych. Zaczęły one zastępować tradycyjne katalogi i kartoteki. W ten sposób dostęp do rozproszonych i trudno dotychczas dostępnych baz danych zawierających dokumenty o charakterze osobowym stawał się nieporównywalnie łatwiejszy. Możliwości zaś odszukania w ich treści, wyodrębnienia i wykorzystania danych dotyczących konkretnej osoby nieporównywalne. W sposób oczywisty niosło to ze sobą niebezpieczeństwo naruszenia interesów osób, których dane dotyczą. Dotychczas wypracowane instrumenty i mechanizmy zabezpieczające z zakresu ochrony prywatności okazały się niewystarczające. Koniecznością stało się stworzenie zupełnie nowych regulacji będących kompilacją rozwiązań o charakterze administracyjnym, technicznym, organizacyjnym i informatycznym. Pociągnęło to za sobą powstanie nowej dziedziny działalności nazywanej odtąd problematyką ochrony danych osobowych.

Prace nad stworzeniem odpowiednich regulacji, rozpoczęte w poszczególnych państwach w latach sześćdziesiątych, zaczęły przynosić wymierne efekty legislacyjne na początku następnego dziesięciolecia. Pierwsza ustawa o ochronie danych osobowych została uchwalona w Hesji (kraju związkowym RFN) w 1970 roku. Pierwszym państwem, które przyjęło odpowiednią regulację ogólnokrajową była Szwecja – zrobiła to w 1973 r. Później podążyły za nimi inne państwa. W 1977 r. ogólnopaństwowe legislacje uchwaliły: Republika Federalna Niemiec i Kanada, rok później Francja, Austria, Dania i Norwegia. Na początku lat osiemdziesiątych

praktycznie wszystkie wysokorozwinięte państwa demokratyczne dysponowały odpowiednimi regulacjami.

Równolegle z pracami na szczeblu państwowym problematyka ochrony danych osobowych stała się przedmiotem zabiegów na forum międzynarodowym. W 1968 roku Zgromadzenie Parlamentarne Rady Europy wystąpiło do Komitetu Ministrów (zalecenie nr 509), by ten sprawdził, czy europejska konwencja o ochronie praw człowieka i podstawowych wolności oraz prawo wewnętrzne państw-członków Rady Europy należycie chronią prywatność, wobec zagrożeń wynikających z ówczesnego stopnia rozwoju nauki i technologii. Powołana przez Komitet Ministrów grupa ekspertów uznała, że zagrożenie istnieje, a związane jest głównie z pojawieniem się i rozwojem „zautomatyzowanych banków danych" (czyli – w istocie – pierwszych komputerów). Na tej podstawie Komitet Ministrów przyjął dwie rezolucje – rezolucję 22 z 1973 roku o zasadach ochrony danych w sektorze prywatnym oraz rezolucję 29 z 1974 roku o zasadach ochrony danych w sektorze publicznym. Jednocześnie zalecono pracę nad aktem międzynarodowym o charakterze wiążącym dla państw-członków. Ich efektem była konwencja nr 108 Rady Europy z 28 stycznia 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Weszła ona w życie cztery lata później – 1 października 1985 roku.

Tak więc lata osiemdziesiąte zaowocowały powstaniem w poszczególnych państwach w miarę spójnego systemu ochrony danych osobowych. Niemniej rozwiązania przyjęte w poszczególnych krajach odbiegały od siebie dość znacznie, tak pod względem przedmiotu, jak i zakresu ochrony. Stanowiło to istotną niedogodność w związku z rozwijającą się wymianą międzynarodową (ustawodawstwo przyjęte w poszczególnych państwach wymuszało stosowanie własnych standardów także poza granicami kraju, co hamowało przepływ informacji konieczny dla sprawnego funkcjonowania działalności handlowej, usługowej itd.). Brak jednolitych rozwiązań stanowił wyzwanie zwłaszcza dla państw tworzących Unię Europejską, hamując proces integracji i utrudniając budowę Wspólnego Rynku. W końcu, Unia Europejska zdecydowała się zareagować, zwłaszcza, że z biegiem lat wypracowane w latach siedemdziesiątych i osiemdziesiątych mechanizmy zabezpieczające okazały się niewystarczające. 24 października 1995 roku Parlament Europejski i Rada Unii Europejskiej przyjęły dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Dyrektywa dała państwom-członkom Wspólnoty 3 lata na przeniesienie jej postanowień na grunt prawa krajowego. Termin ów upłynął 24 października 1998 roku.

W Polsce tematyka ochrony danych osobowych jako istotny problem wymagający przedsięwzięcia środków zaradczych pojawiła się stosunkowo późno. Prace nad przygotowaniem ustawy o ochronie danych osobowych rozpoczęły się w roku 1991. Odpowiedni projekt został przez Radę Ministrów przyjęty ostatecznie dopiero 13 sierpnia 1996 roku. Do Sejmu trafił w listopadzie 1996 – pierwsze czytanie odbyło się 20 listopada. Ustawa o ochronie danych osobowych została przez Sejm uchwalona 29 sierpnia 1997 roku (weszła w życie 6 miesięcy później 30 kwietnia

1998 r.). Równolegle trwały prace nad przygotowaniem tekstu nowej Konstytucji. Polski ustrojodawca uznał problematykę ochrony danych osobowych za na tyle istotną dla podmiotowości jednostki, by nadać jej rangę konstytucyjną (umieszczono ją w tytule drugim – wolności i prawa osobiste – rozdziału drugiego – wolności, prawa i obowiązki człowieka i obywatela). Jednocześnie, zgodnie z tendencjami światowymi, zdecydowano, by wyodrębnić zagadnienie ochrony danych osobowych z materii ochrony prywatności i uregulować ją w osobnym artykule. Interesujące nas przepisy brzmią następująco:

Art. 47. Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci, i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 51. 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Uchwalenie konstytucji oraz ustawy o ochronie danych osobowych pozwoliło Polsce – po blisko 20 latach – na podpisanie konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Nastąpiło to 21 kwietnia 1999 roku (ratyfikacja nastąpiła 23 maja 2002 r.). Nawet jednak ten niewątpliwie symboliczny akt nie zakończył budowy systemu ochrony danych osobowych w naszym kraju. Rychło bowiem okazało się, że przyjęte w Polsce rozwiązania są dalece nieprecyzyjne, często niedopracowane i w szczegółach odbiegają od standardów przyjętych w Unii Europejskiej. Wymusiło to istotną nowelizację ustawy o ochronie danych osobowych. Spośród kilku zmian najistotniejsza została dokonana 25 sierpnia 2001 roku – weszła w życie 3 października 2001 roku. Jakkolwiek życie wymusi zapewne z czasem pewne modyfikacje, to można chyba uznać, że zasadniczy zrąb systemu ochrony danych osobowych w naszym kraju został już zbudowany.

* * *

Dane osobowe – zgodnie z art. 2.a KONWENCJI – to każda informacja dotycząca osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować. Tak więc za cechę charakterystyczną danych osobowych należy uznać brak anonimowości osoby, której dotyczą – informacja będzie miała charakter osobowy, jeżeli na jej podstawie możemy ustalić tożsamość osoby, do której się odnosi (zidentyfikować ją) lub jeżeli dotyczy ona osoby już zidentyfikowanej. Tak określona definicja budzi pewne wątpliwości – nie odpowiada na pytanie, kiedy możemy powiedzieć, że ustaliliśmy tożsamość jakiejś osoby? Z problemem tym, tzw. problemem iden-

tyfikalności – mierzą się: rekomendacja nr 10 z 1991 roku na temat udostępniania danych osobowych posiadanych przez instytucje publiczne oraz raport wyjaśniający do KONWENCJI. Zgodnie z zawartą tam interpretacją, osoba nie jest „identyfikowalna", jeżeli ustalenie jej tożsamości wymaga nieproporcjonalnych środków (czasu, kosztów, działań). Możemy więc doprecyzować konwencyjną definicję – chodzi o informacje na temat osoby, której tożsamość znamy lub której tożsamość z łatwością możemy ustalić.

Kolejne wyjaśnienia zawiera DYREKTYWA. Zgodnie z art.2.(a) osobą możliwą do zidentyfikowania jest osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie poprzez powołanie się na numer identyfikacyjny lub jeden bądź kilka specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Wyliczenie to jest przykładowe, co oznacza, że istotą rzeczy jest sam fakt określenia tożsamości, nie zaś jego sposób. Analogiczne rozwiązania przyjęła także polska USTAWA (art. 6).

W tym miejscu warto zwrócić uwagę na dwie sprawy. Po pierwsze odnotujmy, że uznanie, iż informacje stanowią dane osobowe, zależy wyłącznie od przypisania im wyżej wymienionych cech. Inne natomiast cechy informacji są bez znaczenia – i to tak te odnoszące się do jej treści, np.: charakter, waga, stopień intymności, jak i do formy (sposób utrwalenia pisemny, elektroniczny, fotograficzny, itd.). Ważny jest tylko fakt, że informacja odnosi się do osoby zidentyfikowanej lub którą z łatwością możemy zidentyfikować. Ujmując rzecz najprościej – wiemy lub z łatwością możemy się dowiedzieć kogo dotyczą.

Po drugie należy zauważyć, że niemożliwe jest stworzenie katalogu danych osobowych. Charakter osobowy zależy od kontekstu, każda więc informacja potencjalnie może mieć charakter osobowy i jednocześnie żadna nie ma na stałe przypisanego wyznacznika osobowego.

KONWENCJA (art. 1) i DYREKTYWA (art.1.1) określając przedmiot ochrony mówią o prawach i wolnościach osób fizycznych. Nie ma więc wątpliwości, że dane osobowe to dane o osobach fizycznych. Niemniej KONWENCJA (art. 3.2.b) pozwala rozszerzyć stronę podmiotową ochrony uznając, że może być ona stosowana także do ochrony innych niż człowiek podmiotów (chodzi o ugrupowania, stowarzyszenia, fundacje, spółki, korporacje oraz o wszelkie inne organizacje gromadzące osoby fizyczne niezależnie od posiadania przez nie osobowości prawnej). W tym przypadku dane o powyższych podmiotach też będą podlegały ochronie. Kilka państw europejskich – m. in. Austria, Dania, Islandia, Norwegia, Szwajcaria – zdecydowało się na dokonanie takiego właśnie rozszerzenia. Polska nie poszła jednak tą drogą. Tak więc, w naszym kraju za dane osobowe uznaje się jedynie dane o osobach fizycznych. Z drugiej strony trzeba jeszcze raz podkreślić, że chodzi o wszystkie dane o osobach fizycznych – a więc także dane o przedsiębiorcach, wspólnikach, członkach stowarzyszeń itd.– nawet jeżeli dotyczą wyłącznie działalności w ramach powyższych struktur.

Ochrona danych osobowych nie ma charakteru absolutnego. Nie wszystkie dane i nie zawsze podlegają ochronie. Często zastosowanie instrumentów ochronnych uzależnione jest od spełnienia dodatkowych przesłanek, a stopień ochrony zależy od okoliczności lub rodzaju danych. Dla precyzyjnego określenia granic ochrony koniecznym jest uprzednie zapoznanie się z dwoma pojęciami – „przetwarzanie danych osobowych" oraz „zbiór danych osobowych".

Jako punkt wyjścia dla określenia pierwszego z tych pojęć niech posłuży nam KONWENCJA. Zawiera ona definicję „automatycznego przetwarzania". Zgodnie z art.2.c oznacza ono następujące operacje wykonywane w całości lub części przy pomocy metod zautomatyzowanych: rejestrowanie danych, ich modyfikowanie, usuwanie, odzyskiwanie lub rozpowszechnianie. Definicja powyższa – ograniczająca pojęcie przetwarzania do operacji „automatycznych" – nie wytrzymała próby czasu. Stąd też DYREKTYWA (art.2.(b)) wychodzi poza to określenie, za przetwarzanie uznając każdą operację lub zestaw operacji dokonywanych na danych przy pomocy środków zautomatyzowanych lub innych. Akt ten powiększa również znacznie katalog czynności uznanych za przykłady przetwarzania (najistotniejsze uzupełnienie to uznanie za przetwarzanie także gromadzenia danych, inne – w większości przypadków – można uznać za element konwencyjnej „modyfikacji"). Tą samą drogą podąża polska USTAWA stanowiąca – art.7(2) – iż przez przetwarzanie rozumie się jakiekolwiek operacje wykonywane na danych osobowych (katalog przykładów jak w dyrektywie). A zatem, praktycznie każda czynność dotycząca danych osobowych z punktu widzenia prawa stanowi ich przetwarzanie. Dwie „brzegowe" czynności przetwarzania to zbieranie (gromadzenie) na początku – czyli wejście w posiadanie danych osobowych w dowolny sposób – oraz usuwanie (niszczenie) na końcu – czyli fizyczne zniszczenie lub taka ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dotyczą.

Podobnie jak w przypadku przetwarzania danych osobowych, pewne rozbieżności istnieją także w rozumieniu pojęcia zbioru danych osobowych. I tym razem najwęższe ujęcie prezentuje KONWENCJA. Akt ten zawiera definicję zautomatyzowanego zbioru danych. Art.2.b rozumie pod tym określeniem każdy zestaw danych podlegających automatycznemu przetwarzaniu. To zaś – jak pamiętamy – oznacza operacje wykonywane „przy pomocy metod zautomatyzowanych". Inne zbiory danych mogą być poddane konwencji fakultatywnie, o czym państwo-strona powinna poinformować Sekretarza Generalnego Rady Europy w specjalnej deklaracji (art. 3.2.c). Co do zasady nie podlegają więc konwencji zbiory przetwarzane w sposób niezautomatyzowany (np. kartoteki manualne). Inaczej jest w przypadku DYREKTYWY. Posługuje się ona pojęciem zbioru danych osobowych („zbiór danych"). Zgodnie z art.2.(c) jest to każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów. Analogiczną definicję zawiera również polska USTAWA – za zbiór danych uznaje się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów (art.7(1)). Wynika z tego, że abyśmy mieli do czynienia ze zbiorem, dane muszą być tak uporządkowane, by móc dotrzeć do poszukiwanej informacji bez konieczności przeglądania całego zbioru. Musi on zatem posiadać cechę lub cechy

umożliwiające wyszukiwanie konkretnych danych (tzw. kryterium dostępu). Siłą rzeczy kryterium to musi mieć charakter osobowy.

Przejdźmy teraz do wyznaczenia zakresu ochrony danych osobowych ustalonego w poszczególnych aktach. W przypadku KONWENCJI określa go art.3.1. Akt ten znajdzie zastosowanie do zautomatyzowanych zbiorów danych osobowych i do automatycznego ich przetwarzania. Dane osobowe będą więc chronione jeżeli są przetwarzane automatycznie w zautomatyzowanych zbiorach danych. Co jednak w sytuacji, gdy dane znajdują się poza zbiorem? Przykładowo w pamięci komputera mogą być zapisane dane nie ujęte w żaden zbiór („dane pojedyncze"). Przyjęto interpretację, że w takiej sytuacji KONWENCJA również znajdzie zastosowanie byleby dane były przetwarzane automatycznie (ten ostatni warunek w przypadku przetwarzania komputerowego jest niewątpliwie spełniony). Tak więc dane osobowe będą podlegać obligatoryjnie ochronie konwencyjnej w dwóch przypadkach. Po pierwsze, jeżeli znajdują się w zautomatyzowanym zbiorze danych, po drugie, jeżeli będąc poza zbiorem, są przetwarzane automatycznie. Przypomnijmy jeszcze, że KONWENCJA pozwala każdemu państwu-stronie rozszerzyć zakres swojego zastosowania. Taka fakultatywna ochrona KONWENCJI będzie dotyczyć zbiorów danych osobowych nie objętych automatycznym przetwarzaniem (art.3.2.c), oraz danych podmiotów nie będących osobami fizycznymi, a jedynie gromadzącymi takie osoby niezależnie od posiadania przez nie osobowości prawnej – np. ugrupowania, stowarzyszenia, fundacje, spółki, korporacje (art.3.2.b).

Nieco inaczej został określony zakres zastosowania DYREKTYWY. Zgodnie z art.3.1 dotyczy ona przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych. A zatem dane osobowe – podobnie jak w przypadku KONWENCJI – będą podlegały ochronie przewidzianej w DYREKTYWIE zawsze, gdy są przetwarzane automatycznie (bez względu na to czy stanowią część zbioru czy też nie). Ponadto DYREKTYWA znajdzie też zastosowanie dla danych nie przetwarzanych w sposób zautomatyzowany – a więc przetwarzanych manualnie – pod warunkiem jednak, że stanowią one lub mają stanowić część zbioru.

Przejdźmy teraz do rozwiązań przyjętych w polskiej USTAWIE. Zakres jej zastosowania wyznacza art.2.2 stanowiąc, że stosuje się ją do przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych. Przy czym system informatyczny – zgodnie z art.7(2.a) – to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Definicja powyższa werbalnie odbiega nieco od ujęć przyjętych w zaprezentowanych powyżej aktach europejskich, przy odrobinie dobrej woli może – i powinna – być jednak interpretowana „proeuropejsko". Tak więc, dane osobowe będą podlegać ochronie zawsze, gdy są przetwarzane w zbiorze danych (katalog z art.2.2 trzeba traktować jako przykładowe wyliczenie takich zbiorów). Dane osobowe będą też objęte ochroną przewidzianą w USTA-

WIE – tym razem bez względu na to czy są przetwarzane w zbiorze, czy też poza nim – gdy będą przetwarzane w „systemach informatycznych" (to ostatnie określenie należy interpretować jako funkcjonalny odpowiednik używanego w aktach europejskich pojęcia „przetwarzanie zautomatyzowane"). W efekcie dane osobowe nie będą podlegać ustawowej ochronie jedynie w przypadku, gdy nie będąc elementem zbioru danych, będą przetwarzane poza systemem informatycznym (w sposób niezautomatyzowany) – chodzi przykładowo o dane osobowe zawarte w książkach i czasopismach, rozpowszechniane w radiu i telewizji, podawane w wystąpieniach czy na wykładach). Dla uzyskania większej precyzji przypomnijmy jeszcze raz, że zgodnie z definicją przetwarzania danych jego składowym elementem jest także zbieranie (gromadzenie) danych. Oznacza to, że dane podlegają ustawowej ochronie nawet jeszcze zanim znajdą się w zbiorze czy systemie informatycznym – już na etapie pozyskiwania.

Tak więc, podsumowując, możemy uznać, że ukształtowany został jednolity standard co do zakresu ochrony danych osobowych. Ochronie podlegają wszystkie dane osobowe, które przetwarzane są w sposób zautomatyzowany (w systemach informatycznych) – bez względu na to czy są częścią zbioru danych (są przetwarzane w zbiorze), czy też nie. Ochronie podlegają także dane będące częścią zbioru (przetwarzane w zbiorach) – bez względu na sposób przetwarzania. Poza ochroną pozostaną natomiast dane, które nie są przetwarzane w sposób zautomatyzowany (nie znajdują się w systemie informatycznym) i jednocześnie nie są elementami żadnego zbioru danych.

Wszystkie omawiane akty ustanawiają pewne wyjątki od tak zarysowanego schematu. Najmniej restrykcyjna pod tym względem jest KONWENCJA. Z jednej strony umożliwia ona każdemu państwu-stronie odstąpienie od stosowania jej postanowień w przypadku wybranych przez nie kategorii zautomatyzowanych zbiorów danych osobowych (art.3.2.a), z drugiej pozwala na określenie terytorium lub terytoriów, na których KONWENCJA nie będzie stosowana (art.24). Ponadto KONWENCJA daje możliwość odstąpienia od stosowania przewidzianych w niej zasad ochrony danych dotyczących ich jakości (art.5), tzw. danych wrażliwych (art.6) oraz pewnych innych praw osób, których dane są przetwarzane (art.8), jeżeli odstąpienie to stanowi konstytucyjny środek konieczny w demokratycznym społeczeństwie dla ochrony państwa, bezpieczeństwa publicznego, interesów walutowych państwa lub zwalczania przestępczości (art.9.2.a), albo też ochrony podmiotu danych oraz praw i wolności innych osób (art.9.2.b).

Podobne ograniczenie do powyższego zawiera także DYREKTYWA. Zgodnie z art. 3.2.1 nie będzie miała ona w ogóle zastosowania w przypadku przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz z działalnością państwa w dziedzinach prawa karnego. Analogiczne względy – wyliczenie w art.13.1 – mogą stanowić podstawę ograniczenia zakresu stosowania niektórych postanowień DYREKTYWY w zakresie jakości danych (art.6.1), praw osób których dotyczą (art.10, 11.1, 12) oraz

upublicznienia przetwarzania (art.21). Ważną okolicznością, którą należy uwzględnić, określając zakres stosowania dyrektywy, jest również konieczność pogodzenia prawa do prywatności z przepisami dotyczącymi wolności wypowiedzi. Art.9 nakazuje państwom członkowskim zastosowanie „wyłączeń lub zwolnień" z przyjętych w DYREKTYWIE zasad w przypadku przetwarzania danych wykonywanego wyłącznie w celach dziennikarskich lub dla celu artystycznej, lub literackicj wypowiedzi, jeżeli jest to konieczne dla zbalansowania powyższych wartości. W końcu, zaznaczmy jeszcze, że postanowienia dyrektywy w ogóle nie dotyczą sytuacji, gdy przetwarzanie danych osobowych wykonywane jest w ramach działalności wykraczającej poza zakres przewidziany prawem Wspólnoty, określonym w rozdziałach V i VI Traktatu o Unii Europejskiej (art.3.2.1) oraz gdy przetwarzanie danych osobowych wykonywane jest przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze (art.3.2.2.).

Określone w powyższy sposób zakres i granice zastosowania omawianych przez nas aktów międzynarodowych mają niezmiernie istotne znaczenie z punktu widzenia prawa wewnętrznego państw-stron. Wyznaczają one bowiem ramy, w granicach których może „poruszać się" ustawodawstwo. Ograniczenia wyeksponowane w aktach międzynarodowych w prawie wewnętrznym zostały przełożone na tekst konkretnych rozwiązań prawnych. Nic więc dziwnego, że w tego typu aktach generalnych wyjątków jest mniej niż w prawie międzynarodowym, natomiast szczegółowe rozwiązania są obudowane liczniejszymi wyjątkami. Polska USTAWA zawiera zasadniczo tylko jeden generalny wyjątek. Za DYREKTYWĄ postanawia – art.3.4 – że nie stosuje się jcj w ogóle do osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych. Rozwiązanie to uzupełnia norma art. 2.3, zgodnie z którym w przypadku zbiorów sporządzonych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, zastosowanie znajdą jedynie przepisy USTAWY dotyczące zabezpieczenia zbiorów danych osobowych. Dla porządku dodajmy na zakończenie, że wszystkie omawiane wyżej akty określają ponadto pewne wyjątki, co do standardów ochrony danych, jeżeli jedyną przesłankę ich przetwarzania stanowią cele statystyczne lub naukowe, a nie zachodzi ryzyko naruszenia prywatności osób, których dane dotyczą (KONWENCJA art.9.3., DYREKTYWA art.13.2, USTAWA art.25.2.3, art.26.2.1, art.27.2.9, art.43.1.10).

Jak już wspomniano wyżej, ochrona danych osobowych nie ma charakteru absolutnego. W gruncie rzeczy przedmiotem dziedziny, którą się tutaj zajmujemy jest nie tyle uniemożliwienie przetwarzania danych o innych osobach, ile raczej zapewnienie, że będzie się to odbywało w zgodzie z określonymi zasadami. W konsekwencji przyjęte regulacje koncentrują się na określeniu warunków, na jakich odbywać się będzie przetwarzanie danych osobowych, nakładają na podmioty dokonujące przetwarzania określone obowiązki, których celem jest zminimalizowanie niedogodności i niebezpieczeństw, jakie dla jednostki niesie przetwarzanie danych o niej oraz gwarantują osobom, których dane dotyczą uprawnienia pozwala-

jące na ochronę własnych interesów w związku z przetwarzaniem danych oraz kontrolę nad tym procesem.

Niestety, nie ma tutaj miejsca na szczegółową analizę przyjętych rozwiązań. Stanowi to zadanie wykraczające daleko poza charakter niniejszego opracowania. Nie od rzeczy będzie jednak w tym miejscu zwrócenie uwagi na pewne okoliczności natury ogólnej istotne dla interpretacji treści zamieszczonych w niniejszym zbiorze aktów. Przede wszystkim należy zauważyć, że każdy z omawianych aktów nieco inaczej określa zasady i warunki, na których winno się odbywać przetwarzanie danych osobowych. Inny jest też zakres i szczegółowość przyjętych w nich rozwiązań. Wynika to poniekąd z charakteru tych regulacji oraz związane jest z historycznym momentem ich przyjmowania. Niemniej, trzeba zaznaczyć, że wszystkie one wspólnie tworzą jednolity system, w ramach którego odbywa się przetwarzanie danych w konkretnym przypadku. Jeżeli nawet KONWENCJA i DYREKTYWA, jako akty, które nie mają charakteru samowykonalnego, nie znajdą bezpośredniego zastosowania, to jednak wyznaczają określone standardy i w ramach wewnętrznego porządku prawnego powinny być traktowane co najmniej jako reguły interpretacyjne.

Należy również pamiętać, że przyjmowane w poszczególnych państwach – w tym w Polsce – ustawy o ochronie danych osobowych nie mają charakteru kompletnego. Z jednej strony istotne regulacje znajdują się w innych aktach o randze ustawowej (w kontekście polskim wspomnijmy chociażby ustawę o Policji, o działalności ubezpieczeniowej, o statystyce publicznej, ordynację podatkową – nie uwzględnione w zbiorze), z drugiej nie do przeoczenia z punktu widzenia mechanizmu ochrony danych osobowych są rozwiązania przyjęte w aktach wykonawczych do tych ustaw (w Polsce będą to: rozporządzenie Prezydenta RP w sprawie nadania statutu biuru Generalnego Inspektora Ochrony Danych Osobowych oraz dwa rozporządzenia Ministra Spraw Wewnętrznych i Administracji, pierwsze w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, a drugie – w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych). Relacje ustawy o ochronie danych osobowych z tymi aktami kształtują się podług powszechnie przyjętych reguł kolizyjnych – co do zasady *lex specialis derogat legi generalis* w przypadku innych ustaw i *lex superior derogat priori* w odniesieniu do aktów podustawowych. Dopiero uwzględnienie tych okoliczności pozwala na właściwą interpretację zamieszczonych w zbiorze aktów.

Jak widać z powyższego, opracowanie niniejsze nie rości sobie pretensji do kompletności. Biorąc pod uwagę ilość unormowań, ich zróżnicowany charakter i fakt rozproszenia w rozmaitych częściach systemu prawnego wydaje się to zresztą być zadaniem niewykonalnym. Niniejszy zbiór został pomyślany jako pomoc dydaktyczna dla studentów kierunków administracyjnych, ekonomicznych i prawniczych. Jego zawartość została więc dostosowana do potrzeb wyznaczonych przez

programy nauczania. Zamieszczone w zbiorze podstawowe akty dotyczące ochrony danych osobowych dają wyobrażenie o obowiązujących w tym zakresie standardach, pozwalają zorientować się w przyjętych mechanizmach przetwarzania danych i umożliwiają zapoznanie się z zakresem prawa osób, których dane dotyczą, jak i obowiązków nałożonych na administratorów danych o innych osobach. Autor, wyrażając nadzieję, że zbiór ten okaże się czytelnikowi pomocny, jednocześnie zachęca do sięgnięcia po dalszą literaturę – szczególnie do opracowań fachowych – z których zresztą sam korzystał przygotowując niniejsze wprowadzenie. Lektura „czystego" tekstu prawnego, jakkolwiek w procesie nauczania niewątpliwie wskazana, nie może zastąpić teoretyczno-doktrynalnego wykładu, naukowej krytyki i fachowego komentarza.

I tak, czytelnika zainteresowanego filozoficzno-doktrynalnym aspektem zagadnienia ochrony danych osobowych odsyłam do artykułu M. Safjana, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym* („Państwo i Prawo" 2002, z. 6). O prawie do prywatności i ewolucji jego rozumienia pisze, m.in., B. Kordasiewicz (*Cywilnoprawna ochrona prawa do prywatności,* „Kwartalnik Prawa Prywatnego" 2000, nr 9). Z publikacji poświęconych standardom europejskim w zakresie ochrony danych polecam artykuł A. Mednisa, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej* („Państwo i Prawo" 1997, z. 6). Zainteresowanym dogłębniejszymi studiami nad omawianą problematyką polecam przede wszystkim opracowanie *Ochrona danych osobowych,* pod red. M. Wyrzykowskiego (Instytut Spraw Publicznych, Warszawa 1999 r.) Czytelnik znajdzie tam wiele artykułów, w których autorzy omawiają poszczególne aspekty zagadnienia ochrony danych osobowych. Z kolei teksty licznych nieuwzględnionych w niniejszym zbiorze aktów międzynarodowych i europejskich zebrał T. Jasudowicz (*Ochrona danych. Standardy Europejskie. Zbiór materiałów,* TNOiK, Toruń 1998). Warto też sięgnąć po komentarze do ustawy o ochronie danych osobowych. Najlepszym jest niewątpliwie komentarz J. Barty i R. Markiewicza, *Ochrona danych osobowych. Komentarz,* Zakamycze, Kraków 2001. Zachęcam też do sięgnięcia po komentarz A. Mednisa (*Ustawa o ochronie danych osobowych. Komentarz,* Wydawnictwo Prawnicze, Warszawa 1999). Jakkolwiek stracił on już częściowo swą aktualność, to nadal pozostaje bogatym źródłem wiedzy teoretycznej. Na zakończenie wspomnijmy jeszcze o stronach internetowych Generalnego Inspektora Ochrony Danych Osobowych (www.giodo.gov.pl), gdzie można znaleźć, m.in., teksty istotniejszych międzynarodowych i polskich aktów prawnych dotyczących ochrony danych osobowych, bibliografię tekstów na ten temat oraz liczne wyjaśnienia i porady o charakterze praktycznym.