

Ochrona danych osobowych w Polsce

Wstęp

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (DzU nr 133, poz. 883) obowiązuje w Polsce już ponad cztery lata. Na podstawie obserwacji przestrzegania ww. ustawy przez podmioty prywatne i podmioty administracji publicznej możemy dokonać próby jej oceny i pokusić się o sformułowanie wniosków *de lege ferenda*. Okres obowiązywania ustawy niewiele bowiem zmienił w świadomości naszych obywateli. W umysłach ludzi nadal nie zakodowała się informacja, że nasza prywatność jest chroniona przez konstytucję i wspomnianą ustawę. Jesteśmy zalewani ulotkami, reklamówkami, w których wizją obiecanej nagrody sami ujawniamy swoje dane, wypełniając dołączone do reklamówek ankiety. Ujawnione w ten sposób informacje firmy marketingowe mogą przetwarzać dla celów zarobkowych zgodnie z prawem. Często jednak są one wykorzystywane w sposób sprzeczny z podstawowymi zasadami prawa.

Zagrożenie ingerencją w nasze prywatne życie istnieje nie tylko jednak ze strony firm marketingowych przysyłających nam reklamówki. Większe niebezpieczeństwo wiąże się m.in. z działalnością firm ubezpieczeniowych, placówek ochrony zdrowia, administracji prowadzącej rozmaite ewidencje i rejestry.

Wizja świata orwellowskiego, gdzie każda sfera życia człowieka zewsząd jest obserwowana przez Wielkiego Brata, mogłaby się stać w dobie rewolucji informatyki rzeczywistością. Komputery, sieć internetowa, osiągnięcia telekomunikacji, telewizji i satelity mogą stanowić doskonały instrument obserwacji i ingerencji w prywatne życie obywateli oraz manipulacji ludźmi. Z tych przyczyn kwestia ochrony danych osobowych stała się istotnym problemem w XX i XXI wieku. Niewiele osób uświadamia sobie jak ważna jest ochrona jednego z najważniejszych praw podmiotowych człowieka – prawa do prywatności, ochrony informacji dotyczących jego prywatnego życia.

W związku z powyższym celem niniejszego artykułu jest przybliżenie rozwiązań stosowanych przez polskiego ustawodawcę w kwestii ochrony danych osobowych naszych obywateli.

Rys historyczny

Prawo do prywatności

Ochrona danych osobowych, czyli ochrona każdej informacji dotyczącej określonej osoby, jej prywatnego życia, jest stosunkowo nowym instrumentem ochrony życia prywatnego każdego obywatela.

Ochrona danych osobowych wywodzi się od najważniejszego prawa człowieka – prawa do prywatności („right to privacy”). Instytucja *prawa do prywatności* została sformułowana w pełnym zakresie przez amerykańskich profesorów S. Warrena i L. Brandeisa w 1890 r. w artykule pt. *The Right to Privacy* (Harvard Law Review, 1890).

W XIX wieku stworzono wiele definicji *prawa do prywatności*. Według jednych, prawo do prywatności to „prawo do określenia, jakimi informacjami o sobie chcemy się dzielić z innymi” (A. Westin, *Science, Privacy and Freedom, Issues and Proposals for 1970's.*, Columbia law Review, 1966). Inni traktowali prawo do prywatności jako prawo do pozostawania w spokoju „right to be alone” lub „prawo jednostki do decydowania o tym, w jakim stopniu będzie się dzielić z innymi swymi myślami, uczuciami i faktami ze swojego życia osobistego”.

Prawo do prywatności znalazło normatywne odzwierciedlenie w **art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r.** (DzU z 1993 r., nr 61, poz. 284 z późn. zm.), zgodnie z którym: *Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.*

Konwencja ta zakreśla również granice ingerencji organów państwowych i osób trzecich w sferę prywatną jednostki. Stanowi ona bowiem, że: *Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępczości, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.*

Tak więc ingerencja organów władzy państwowej dopuszczona została na zasadzie wyjątków. Natomiast ingerencja ze strony osób trzecich jest niedopuszczalna.

W polskiej doktrynie prawnej problem ochrony prawa do prywatności poruszył profesor A. Kopff. Jego zdaniem, prawo do prywatności „to prawo jednostki do życia własnym życiem, układanym według własnej woli, z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej” (A. Kopff, *Koncepcja prawa do intymności i prywatności życia osobistego*, Studia

Cywilistyczne t. XX, 1972 r.). W sprawie ochrony prawa do prywatności wypowiedział się również Sąd Najwyższy (SN) w orzeczeniu z 18 stycznia 1984 r. (I CR 400/83), w którym uznał prawo do prywatności za dobro osobiste chronione przepisami kodeksu cywilnego. SN w ww. orzeczeniu stwierdził, że: *Otwarty katalog dóbr osobistych (art.23 i 24 k.c.) obejmuje także dobro osobiste związane ze sferą życia prywatnego, rodzinnego, ze sferą intymności. Ochrona w tym zakresie może odnosić się do wypadków ujawnienia faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać (...).*

W związku z powyższym prawo ochrony danych osobowych oznacza prawo obywateli do prywatności, prawo do ochrony informacji z zakresu życia intymnego jednostki przed nielegalnym ich gromadzeniem, przetwarzaniem i wykorzystywaniem w celach niezgodnych z prawem.

Początki prawnej regulacji ochrony danych osobowych

W dobie rozwoju technologii informacji problem ochrony danych osobowych stał się nurtującym problemem. Informatyka, nowe osiągnięcia w dziedzinie internetu, telekomunikacji przyczyniły się do pełnej automatyzacji przetwarzania danych. W ten sposób podmioty przetwarzające dane uzyskały przytłaczającą przewagę nad jednostkami, których te dane dotyczą. Bardzo szybko okazało się, że dotychczasowe cywilnoprawne konstrukcje ochrony prywatności są niewystarczające. Pojawiła się potrzeba stworzenia nowych instrumentów prawnych, obejmujących swoim oddziaływaniem całkiem nowy obszar w obrocie gospodarczym, jakim jest przetwarzanie danych osobowych i obrót informacjami z zakresu prywatnej sfery życia jednostki. Nowy zbiór przepisów miał łączyć przepisy cywilne, karne i administracyjne, by w ten sposób stworzyć właściwy, a przede wszystkim skuteczny system ochrony danych osobowych.

Pierwsze dyskusje na temat potrzeby stworzenia rozwiązań prawnych porządkujących gromadzenie informacji o jednostce podjęli Amerykanie. Zauważyli oni bowiem zagrożenie, jakie niesie ze sobą komputeryzacja. Nowe techniki elektroniczne przetwarzania danych stwarzają okoliczności stosowania nielegalnych praktyk zdobywania danych z poufnych źródeł publicznych i ich wykorzystywania, również w sposób nielegalny. W grudniu 1974 r. Kongres USA uchwalił pierwszą kompleksową regulację postępowania z danymi osobowymi w ramach administracji federalnej – „Act of Privacy”.

Kraje europejskie także w latach 70. podjęły problem regulacji prawnej przetwarzania danych przez organy władzy publicznej i podmioty prywatne. W Hesji w 1970 r. uchwalono pierwszą w Europie ustawę krajową odnoszącą

się do zbiorów danych osobowych administracji krajowej. Natomiast pierwszą ustawą w świecie regulującą powyższą problematykę w skali całego kraju była ustawa szwedzka z 1973 r. Kolejną ustawą europejską jest francuska ustawa o informatyce, kartotekach i wolnościach pochodząca z 6 stycznia 1978 r., która wyraźnie stanowi, iż *informatyka, pozostająca do dyspozycji każdego obywatela, musi rozwijać się z uwzględnieniem współpracy międzynarodowej, nie może jednak przynosić szkody ani ludzkiej tożsamości, ani prawom człowieka, ani jego życiu prywatnemu, ani też wolnością indywidualnym lub publicznym*. Podobne regulacje zostały przyjęte w 1978 roku w Austrii, Danii, Norwegii i Księstwie Luksemburga.

Początkowo regulacje prawne dotyczące problematyki ochrony danych osobowych widziały zagrożenie tylko w przypadku przetwarzania danych zgromadzonych w zbiorach przez różne podmioty. Później jednak zrozumiano, że nawet pojedyncza informacja ze sfery życia prywatnego może być wykorzystywana w celach sprzecznych z prawem. Ustawodawca w związku z powyższym określił w ustawach zasady gromadzenia danych osobowych, ich przetwarzania przez różne podmioty oraz uprawnienia osób, których dane są przetwarzane.

Prawo do ochrony tożsamości i prywatności zostało podniesione do rangi praw chronionych na arenie międzynarodowej, m.in. **Konwencją nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych o charakterze osobowym**, podpisaną w Strasburgu (ogłoszona w D.n. 85-1203 15.11.1985; weszła w życie 1 listopada 1985 r.) oraz **Dyrektywą 95/46/EC Parlamentu Europejskiego oraz Rady Europy z 24 października 1995 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz swobodnym obiegu tychże danych**.

Konwencja nr 108 uchwalona przez Radę Europy ma na celu zagwarantowanie na terytorium każdej strony, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wolności, w szczególności jej prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych.

Natomiast zgodnie z **Dyrektywą 95/46/EC**, *systemy przetwarzania danych zostały opracowane, żeby służyć człowiekowi*. Oznacza to, że mają one przede wszystkim przestrzegać fundamentalnych praw i wolności każdej osoby fizycznej bez względu na narodowość i miejsce zamieszkania, a zwłaszcza powinny przestrzegać prawa do prywatności. W drugiej kolejności systemy przetwarzania danych powinny przyczyniać się do postępu gospodarczego i społecznego oraz rozwoju handlu.

Polska ustawa o ochronie danych osobowych z 1997 r.

Rzeczpospolita Polska dostosowała swoje ustawodawstwo do regulacji *Konwencji nr 108 z 1985 r. i Dyrektywy Parlamentu Europejskiego z 1995 r.* uchwalając 28 sierpnia 1997 roku *ustawę o ochronie danych osobowych* (DzU z 1997 r., nr 133, poz. 883).

Ustawa przyznaje każdemu obywatelowi prawo do ochrony dotyczących go danych osobowych. Przetwarzanie danych natomiast może odbywać się tylko w zakresie i trybie przewidzianym w tej ustawie i tylko ze względu na: dobro publiczne; dobro osoby, której dane dotyczą; dobro osób trzecich.

Prawo do ochrony danych osobowych stanowi istotny element ochrony naszej prywatności. Każdy z nas powinien mieć prawo do decydowania, jakie informacje o sobie chce ujawnić i komu. Prawo do anonimowości to prawo do decydowania o tym, czy udostępnimy innym podmiotom informacje o naszym życiu prywatnym i w jakim zakresie.

Prawo do prywatności zostało podniesione do rangi prawa chronionego przepisami konstytucji. *Konstytucja RP z 2 kwietnia 1997 r.* zawiera przepisy odnoszące się do ochrony prywatności oraz niektórych jej aspektów chronionych prawnie, m.in. prawo nienaruszalności mieszkania, prawo tajemnicy korespondencji.

Art. 51 *Konstytucji* stanowi, że *nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawa. Natomiast każdy obywatel ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych.*

Konstytucja wyraźnie odsyła w art. 51 do ustawy o ochronie danych osobowych, która ma określić tryb i zasady przetwarzania danych.

Prawo do prywatności, w tym wypadku prawo do ochrony danych o charakterze osobistym, może być ograniczone tylko ustawą ze względu na interes publiczny lub usprawiedliwiony interes innych osób. Nie jest więc ono prawem bezwzględnie chroniącym, tym bardziej iż ustawa o ochronie danych osobowych przewiduje odstępstwa od przestrzegania określonych w niej zasad przetwarzania ww. danych. Tak jak w przypadku ograniczania innych praw i wolności chronionych *Konstytucją*, zgodnie z orzecznictwem Trybunału Konstytucyjnego, również w przypadku ograniczenia ochrony danych osobowych organy administracyjne powinny określić w ustawie, jaki interes publiczny leży u podłoża ograniczenia ww. ochrony.

Zakres przedmiotowy

Ustawa z 1997 r. określa zasady przetwarzania danych osobowych, prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych. Określa także przypadki przetwarzania danych, do których należy stosować procedury w tej ustawie przewidziane.

Ustawa obejmuje przetwarzanie danych w systemach informatycznych, w kartotekach, skorowidzach, księgach, wykazach, zbiorach ewidencyjnych. Nie obejmuje ona natomiast zbiorów sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych. Do zbiorów doraźnych stosuje się tylko przepisy dotyczące ich zabezpieczenia uregulowane w rozdziale 5 *Ustawy*. Warunkiem wyłączenia wyraźnie sformułowanym w art. 3 ust. 4 jest to, aby zbiory ww. były tworzone doraźnie, a więc dla chwilowej potrzeby, a po ich wykorzystaniu dane osobowe zawarte w tych zbiorach zostaną usunięte lub poddane anonimizacji. „Anonimizacja” oznacza pozostawienie tylko takich danych, których wykorzystanie nie umożliwi identyfikację jednostki, której te dane dotyczą.

Zakres podmiotowy

Przepisy ustawy mają zastosowanie zarówno do organów państwowych, samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepaństwowych realizujących zadania publiczne, jak i do osób fizycznych, osób prawnych i jednostek organizacyjnych nie mających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.

Nie stosuje się przepisów *Ustawy o ochronie danych osobowych* do osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych. Ustawodawca nie sprecyzował jednak, co rozumie przez pojęcie „cele osobiste lub domowe”. W praktyce trudno jest rozgraniczyć cel osobisty od celu domowego. Z tego względu należy uznać, iż chodzi tu o cele niezarobkowe. Dla zilustrowania, o jakie cele osobiste lub domowe chodzi możemy wskazać następujące przykłady: notatki z adresami i telefonami, zbiory wizytówek, tworzenie drzewa genealogicznego rodziny.

Pojęcie „danych osobowych”

Podstawowym pojęciem dla omawianej *Ustawy* jest pojęcie **danych osobowych**. Zgodnie z art. 6 przez **dane osobowe** rozumiemy **każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.**

Z powyższej definicji wynika, że *Ustawa* chroni tylko informacje dotyczące osoby fizycznej. Nie chroni informacji odnoszących się do osób prawnych i jednostek organizacyjnych. Poza tym *Ustawa* chroni tylko takie informacje, które pozwolą na identyfikację konkretnej osoby. Takie ujęcie definicji danych osobowych jest węższe niż definicja przyjęta w ustawodawstwie europejskim zarówno w *Konwencji nr 108*, jak i *Dyrektywie 95/46/EC*. Polska ustawa wyłączyła bowiem z zakresu swojego zainteresowania większość dotyczących nas informacji. Chroni ona tylko te dane, które umożliwiają ustalenie tożsamości danej jednostki. Informacji umożliwiających identyfikację osoby fizycznej tak naprawdę jest niewiele i są to przede wszystkim nazwisko, adres i ewentualnie wizerunek.

Definicja danych osobowych w ustawodawstwie europejskim kładzie natomiast nacisk na to, iż informacje mają mieć charakter osobowy – powinny dotyczyć osoby fizycznej. Oznacza to, że każda informacja nam podana, którą jesteśmy w stanie skojarzyć z konkretną osobą, jest informacją podlegającą zgodnie z *ww. Dyrektywą* i *Konwencją* ochronie.

W związku z powyższym, wskazując zakres ochrony danych osobowych w Polsce, należy posługiwać się nie tylko wąską definicją z art. 6 *Ustawy o ochronie danych osobowych*, ale także należy mieć na uwadze art. 51 *Konstytucji z 1997 r.* Interpretując dwa *ww. artykuły* – art. 6 *Ustawy* i art. 51 *Konstytucji* – możemy powiedzieć, iż w Polsce ochroną są objęte wszystkie informacje dotyczące osoby fizycznej zgodnie z regulacją Unii Europejskiej.

Przetwarzanie danych

Ustawa o ochronie danych osobowych z 1997 r. wyraźnie określa procedury przetwarzania danych przez podmioty do tego uprawnione. Przez **przetwarzanie danych** należy rozumieć wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym. Zgodnie z art. 23 *Ustawy*, jest ono dopuszczalne tylko wtedy, gdy:

- 1) osoba, której dane dotyczą wyrazi na to zgodę, chyba że chodzi o usunięcie jej danych. Zgoda ta może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania (art. 23 ust. 2);
- 2) zezwalają na to przepisy prawa;
- 3) dane są niezbędne dla realizacji umowy, której osoba ta jest stroną lub – na jej życzenie – w celu podjęcia działań niezbędnych przed zawarciem umowy;
- 4) jest niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego;

- 5) jest niezbędne do wypełniania usprawiedliwionych celów osób fizycznych i prawnych oraz jednostek organizacyjnych nie mających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową lub statutową, a przetwarzanie danych nie narusza praw i wolności osoby, której dotyczą.

Art. 23 *Ustawy* wymienił przesłanki legalności przetwarzania danych osobowych. Administrator danych powinien wykazać się co najmniej jedną z ww. przesłanek, aby jego działania były uznane za zgodne z prawem.

Ustawa przewiduje dwa sposoby gromadzenia danych osobowych: 1) bezpośrednio od osoby, której dotyczą, lub 2) od osób trzecich, których te dane nie dotyczą. W przypadku pierwszym, czyli gromadzenia danych bezpośrednio od osób, których dane dotyczą, administrator danych jest zobowiązany poinformować tą osobę o (art. 24):

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu jej zamieszkania oraz imieniu i nazwisku,
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców,
- prawie wglądu do swoich danych oraz ich poprawiania,
- dobrowolności podawania danych albo – jeżeli istnieje obowiązek ich podania – o jego podstawie prawnej (np. podczas spisu powszechnego).

Z ww. obowiązku poinformowania osób, których dane dotyczą, zostali zwolnieni administratorzy, wobec których przepis szczególny zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania (np. Policja).

W przypadku wtórnego gromadzenia danych, tzn. zbierania danych od osób trzecich (art. 25), których zgromadzone informacje nie dotyczą, administrator danych jest zobowiązany bezpośrednio po ich utrwaleniu podać osobie, której one dotyczą, nie tylko o ww. informacje, ale także poinformować ją o źródle danych oraz o uprawnieniu do żądania zaprzestania ich przetwarzania oraz prawie sprzeciwu wynikających z art. 32 ust. 1 pkt 7 i 8. Przepisy nie określają, w jakiej formie udzielenie powyższej informacji ma nastąpić. Możemy się zgodzić z poglądami niektórych teoretyków prawa, iż informacja telefoniczna jest wystarczająca.

Art. 25 ust. 2 zawiera cztery wyjątki od obowiązku informowania osoby, której dane osobowe dotyczą. Są to następujące przypadki:

- przepisy innej ustawy przewidują lub dopuszczają zbieranie danych osobowych bez wiedzy osoby, której dotyczą (np. służby specjalne),
- dane są ogólnie dostępne,
- dane są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badań opinii publicznej, ich przetwarzanie nie narusza

praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań informacyjnych wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badań,

- administrator nie przetwarza dalej zbieranych danych po ich jednorazowym wykorzystaniu.

Ochrona danych osobowych nie ogranicza się wyłącznie do zachowania tajemnicy tych danych. Administrator danych, gromadząc je i przetwarzając, zobowiązany jest do dołożenia szczególnej staranności w celu ochrony interesów osoby, której dane dotyczą, przede wszystkim zaś musi zadbać o to, aby dane te były:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami lub przetwarzane w innym celu niż ten, dla którego zostały zgromadzone, jeżeli nie naruszają praw i wolności osoby, a ich przetwarzanie następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych,
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to konieczne do osiągnięcia celu przetwarzania.

W związku z powyższym praktyki firm, które przechowują dane osobowe po osiągnięciu zamierzonego celu są ewidentnym naruszeniem przepisów *Ustawy*. Pozostawienie danych w zbiorze na ewentualne potrzeby w przyszłości wymaga zgody osoby, której dane dotyczą.

Ustawa wyodrębnia kategorię danych o charakterze szczególnym, które dotyczą każdego człowieka, a zostały wyłączone z możliwości ich przetwarzania. Danych określonych w katalogu w art. 27 *Ustawy* nie można przetwarzać. Chodzi tu o informacje ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub polityczne, przynależność wyznaniową, przynależność partyjną lub związkową, stan zdrowia, kod genetyczny, nałogi lub życie seksualne.

Zakaz przetwarzania kategorii tych danych ma istotne znaczenie z punktu widzenia prawa do prywatności. Pewne dane z naszego życia intymnego, m.in. dotyczące stanu zdrowia, preferencji seksualnych, powinny pozostać sprawą prywatną każdego człowieka. Na pewno nie mogą one być wykorzystywane przeciwko osobie, której dotyczą. Przetwarzanie danych tej kategorii jest możliwe tylko i wyłącznie w przypadkach szczególnych, ściśle określonych przepisami ustawy. Podobna regulacja związana jest z danymi dotyczącymi skazań, orzeczeń o ukaraniu, mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, które można przetwarzać wyłącznie na podstawie ustaw szczególnych (art. 28).

Prawa osoby, której dane dotyczą

Ustawa w art. 32 reguluje prawa, jakie przysługują każdej osobie w związku z automatycznym przetwarzaniem danych osobowych, które jej dotyczą. Po pierwsze, każdej osobie, której dane osobowe zawarte w zbiorach ulegają przetwarzaniu, przysługuje prawo do kontroli przetwarzania tych danych. Po drugie, w związku z ww. kontrolą danych, każda osoba fizyczna ma prawo do:

- a) informacji o istnieniu zbioru i pełnych danych administratora, o fakcie przetwarzania przez administratora informacji jej dotyczących,
- b) informacji o treści danych zgromadzonych w zbiorze,
- c) informacji o celach, zakresie i sposobie przetwarzania danych w zbiorze,
- d) informacji, od kiedy przetwarzane są dane tej osoby dotyczące,
- e) informacji o źródle, z którego pochodzą dane jej dotyczące,
- f) informacji o sposobie udostępniania danych,
- g) prawo żądania uzupełnienia, uaktualnienia i sprostowania danych,
- h) prawo żądania czasowego lub stałego wstrzymania przetwarzania danych lub ich usunięcia, jeżeli zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane,
- i) prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację,
- j) prawo wniesienia sprzeciwu wobec przetwarzania jej danych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Na wniosek osoby zainteresowanej administrator obowiązany jest w terminie 30 dni poinformować ją o przysługujących jej prawach, a przede wszystkim wskazać w formie zrozumiałej, jakie dane zawiera zbiór i w jaki sposób dane zebrano, a także podać cel i zakres przetwarzania danych. Jeżeli administrator udostępnił dane osobom trzecim, zobowiązany jest poinformować osobę zainteresowaną, w jakim zakresie i komu je przekazał. Na wniosek osoby zainteresowanej informacje te powinny być udzielone w formie pisemnej.

Odpowiedzialność

Administrator danych, który posiada ich zbiór zobowiązany jest do prawidłowego zabezpieczenia zgromadzonych w nim informacji. Administrator w szczególności powinien stosować odpowiednie środki techniczne i organizacyjne, które zapewnią odpowiednią ochronę zgromadzonym danym, zabezpieczając je przed ich udostępnieniem osobom nieupoważnionym, uszkodzeniem, zniszczeniem lub zabránieniem przez osobę niepowołaną (art. 36). Poza tym administrator musi zapewnić dobór właściwej kadry obsługującej system infor-

matyczny przetwarzający dane osobowe. Administrator zobowiązany jest również prowadzić ewidencję osób zatrudnionych przy przetwarzaniu danych.

Podstawowym obowiązkiem każdego administratora danych jest zgłoszenie zbioru danych i jego zmian do Generalnego Inspektora Ochrony Danych Osobowych. Art. 43 *Ustawy* określa niektóre kategorie zbiorów danych zwolnionych od obowiązku rejestracji. Zwolnienia enumeratywnie wymienione w tym przepisie dotyczą administratorów danych:

- objętych tajemnicą państwową ze względu na bezpieczeństwo państwa, obronność, ochronę życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
- przetwarzanych przez właściwe organy na potrzeby postępowania sądowego,
- dotyczących członków kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej,
- dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się,
- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej lub radcy prawnego,
- tworzonych na podstawie ordynacji wyborczych do Sejmu, Senatu, rad gmin, ustawy o wyborze Prezydenta Rzeczypospolitej Polskiej oraz ustaw o referendum i ustaw o referendum gminnym,
- dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych,
- przetwarzanych w celu przygotowywania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Istnieje, więc kategoria danych, która nie podlega rejestracji. Nie oznacza to jednak swobody w ich wykorzystywaniu. Na każdym bowiem podmiocie wykorzystującym dane osobowe spoczywa obowiązek nienaruszania praw i wolności, jakie przysługują jednostce na podstawie ustaw szczególnych.

Ustawa za naruszanie podstawowych zasad przetwarzania danych osobowych, opisanych wyżej, przewiduje stosowanie sankcji karnych w postaci kary grzywny, kary ograniczenia wolności albo kary pozbawienia wolności od roku do lat trzech.

Podsumowanie

Rozwój gospodarki rynkowej spowodował wzrost konkurencji na rynku i walkę przy użyciu wszystkich dostępnych środków o klienta. Konkurencja na rynku wywołała popyt na informacje dotyczące potencjalnego konsumenta. Informacje te stały się towarem i podlegają obrotowi handlowemu. Zdobyte różnymi sposobami, często w sposób niezgodny z prawem, dane na temat klienta mają umożliwić dotarcie do niego poprzez złożenie mu oferty odpowiadającej jego wymaganiom i zapotrzebowaniom. Informacje pozyskiwane przez przedsiębiorców dotyczą różnych aspektów życia konsumenta, m.in. jego wykształcenia, stanu majątkowego, stanu rodziny, zainteresowań.

W dobie rozwoju informatyki uzyskanie takich informacji i ich przesyłanie oraz przetwarzanie nie stanowi większej przeszkody dla firm prowadzących działalność gospodarczą. Zgromadzone dane są przechowywane w zbiorach tworzonych przez producentów i handlowców w celach marketingowych oraz na inne potrzeby tych podmiotów. Zaznaczyć należy, że taka działalność nie zawsze jest zgodna z przepisami prawa. Technika komputerowa umożliwia również przesyłanie danych ponad granicami państw, i to na znaczne odległości. W związku z powyższym podjęto inicjatywę prawotwórczą, której rezultatem jest *Konwencja o ochronie jednostki w kontekście automatycznego przetwarzania danych o charakterze osobistym* z 28 stycznia 1981 r. oraz *Dyrektywa 95/46/EC* z 24 października 1995 r. Celem ww. regulacji jest zapewnienie każdej osobie, bez względu na jej narodowość lub miejsce zamieszkania, poszanowania jej praw, a zwłaszcza prawa do prywatności w związku z przetwarzaniem danych osobowych.

Polska dołączyła do grona państw, które w ustawodawstwie wewnętrznym uregulowały problematykę ochrony danych osobowych, wprowadzając zasady określone w *Konwencji* i *Dyrektywie*. Okres ponadczteroletniego obowiązywania w Polsce *Ustawy o ochronie danych osobowych* z 1997 r., niewiele zmienił jednak w świadomości obywateli naszego państwa.

Polscy obywatele nadal nie mają dostatecznej wiedzy na temat ochrony danych o charakterze osobowym. Nie wiedzą po prostu, jakie dane są chronione, jakie prawa w związku z tym im przysługują. Sami ujawniają informacje, często nie uświadamiając sobie, że dane, które ujawnili, firmy wykorzystują w swojej działalności marketingowej, handlują nimi itd. Nieświadomość obywateli w tym zakresie skwapliwie wykorzystywały firmy handlowe, marketingowe i sami producenci. Uchwalenie *ustawy o ochronie danych osobowych* z 1997 r. mocno ograniczyło nielegalne działania firm posiadających zbiory danych osobowych. W chwili obecnej wszystkie firmy, jak banki, instytucje ubezpieczeniowe, fundusze emerytalne itd., zobowiązane są zgłosić fakt posiadania takiego zbioru do Generalnego Inspektora Ochrony Danych Osobowych

i przestrzegać zasad przetwarzania tych danych określonych w ww. ustawie. Ustawa ta stanowi dobry instrument ochrony naszych danych osobowych, chroni nasze prawo do prywatności. W dużej jednak mierze to od nas samych zależy, jak postanowienia tej ustawy będą realizowane przez podmioty przetwarzające dane osobowe.

W związku z powyższym w dalszym ciągu należy prowadzić kampanię informacyjną dotyczącą ochrony danych osobowych, praw, jakie w tym zakresie przysługują każdemu człowiekowi, aby podnieść wiedzę na ten temat wśród naszych obywateli. Niniejszy artykuł miał m.in. na celu przybliżenie tej problematyki.

Literatura

- MEDNIS A., 1995: *Prawna ochrona danych osobowych*. Warszawa, Wydawnictwo Naukowe Scholar.
- MEDNIS A., 1999: *Ustawa o ochronie danych osobowych. Komentarz*. Warszawa, Wydawnictwo Prawnicze.
- ORZEWSKI W., 2000: *Elementy prawa w działalności wydawniczej. Poradnik*. Warszawa, Wydawnictwo Inicjał.
- DYREKTYWA 95/46/EC Parlamentu Europejskiego oraz Rady z 24 października 1995 roku o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym obiegu tychże danych – opracowanie P. Fajgielki.
- KONWENCJA z 28 stycznia 1981 r. dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych – opracowanie P. Fajgielki.
- KORECKI M.: Tajne – Jawne. Prawne aspekty tajności i jawności informacji, cz. 1, 2 i 3, tekst z internetu: <http://www.tajne-jawne...>
- MEDNIS A.: Akt prawny wielkiej wagi, tekst z internetu <http://www.rzeczpospolita.pl>
- GÓRZYŃSKA T.: Brak zaufania do Generalnego Inspektora, tekst z internetu: <http://www.rzeczpospolita.pl>

Personal Data Protection in Poland

Abstract

In Poland, a law on the protection of personal data of 29 August 1997 (DzU No. 155/883 of 1997) has been in force for above four years. Monitoring of the respect for this law by private operators and public administration allows for undertaking some attempts to assess the law and to withdraw some *de lege ferenda* conclusions.

The developments in the period of the law implementation suggest that individuals hardly changed their awareness with regard to their personal data

protection. They still do not recognise the fact that their privacy is protected both by the constitutional principle and the mentioned law and only low percentage of Polish citizens has some information about it. Generally, individual citizens neither perceived safeguards concerning data held on them nor their rights to privacy and regulatory framework to ensure these rights. Therefore, they disclose data of personal nature often unsuspecting that it is used by firms in their business activities (e.g. for marketing purposes or for data commercial exchange).

Hence, the paper addresses some questions concerning the protection of personal data in Poland. First, the Author presented short historical developments in the field of individuals' data protection, then the Polish legislation, i.e. the law on data protection adopted in 1997, was summarised. Moreover, the laid down rules on data processing, the specification of information protected under the law and the legal instruments of respect for data subjects' rights with regard to the processing of their personal data were presented.