Sebastian Ożóg

Standard ochrony danych osobowych w Polsce – omówienie wybranych elementów

Polski Rocznik Praw Człowieka i Prawa Humanitarnego 1, 149-164

2010

POLSKI ROCZNIK PRAW CZŁOWIEKA I PRAWA HUMANITARNEGO 1
UWM w Olsztynie 2010 ISSN 2082-1786

Sebastian Ożóg
Uniwersytet Warmińsko-Mazurski w Olsztynie, Katedra Praw Człowieka i Prawa Europejskiego

Standard ochrony danych osobowych w Polsce – omówienie wybranych elementów

Słowa kluczowe: prawa człowieka, prawo do prywatności, ochrona prawna prawa do prywatności, ochrona danych osobowych.

29 sierpnia 2009 r. minęło dwanaście lat od uchwalenia polskiej ustawy o ochronie danych osobowych[1] (dalej Ustawy). W tym czasie przebyła ona ciekawą drogę od prawnego *novum*, swoistej „efemerydy", której konieczności nie dostrzegała większość prawników, po akt o fundamentalnym znaczeniu dla ochrony danych osobowych w naszym kraju. Przemiana ta dotyczyła także postrzegania głównego organu kontrolnego, powołanego na podstawie Ustawy, czyli Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Organy kontrolne o charakterze zbliżonym do polskiego zostały w podobnym czasie powołane we wszystkich młodych demokracjach Europy Środkowej i Wschodniej. Z uwagi na podobną drogę i doświadczenia oraz występowanie nowych zjawisk, nieznanych wcześniej w krajach Europy Zachodniej, od początku organy te działały w bliskim kontakcie, dzieląc się nawzajem swymi krajowymi doświadczeniami. System ochrony danych osobowych w Polsce zawiera w związku z tym szereg podobieństw do rozwiązań innych państw naszego regionu, w szczególności z uwagi na podleganie przez nie tym samym standardom ochronnym w ramach regulacji międzynarodowych. W 2001 r. polski GIODO zainicjował cykl spotkań Rzeczników Ochrony Danych Osobowych Europy Środkowej i Wschodniej. W 2009 r. w miejscowości Sinaia w Rumunii odbyło się już jedenaste takie spotkanie.[2]

[1] Dz.U. z 1997 r. Nr 133, poz. 883 z późn. zm, tekst jedn. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.

[2] Jako narzędzie wspomagające prace grupy utworzono także stronę internetową (http://www.ceecprivacy.org), na której przedstawiane są aktualnie obowiązujące akty prawne z zakresu ochrony danych osobowych w poszczególnych krajach oraz tematy wspólnie dyskutowanych problemów.

Spotkania o podobnym charakterze odbywają się także w szerszym gronie na organizowanej od 1991 r. tzw. Wiosennej Konferencji Europejskich Organów Ochrony Danych. W jej ramach kolejne spotkania poświęcane są różnym aspektom ochrony danych osobowych w Europie, a ich uczestnicy podejmują działania, mające na celu nie tylko wdrażanie unijnych przepisów, ale również monitorowanie ich przestrzegania w poszczególnych krajach.[3] Od roku 2004 działa też Europejski Inspektor Ochrony Danych, który kontroluje przetwarzanie danych osobowych przez instytucje i organy Wspólnot Europejskich. Ponadto wszystkie porządki krajowe państw wspólnotowych pozostają pod silnym wpływem regulacji Rady Europy, która od lat promuje wysokie standardy w zakresie zbierania i przetwarzania danych osobowych oraz ich ochrony. Aktualnie regulacje tworzone na poziomie krajowym i międzynarodowym coraz bardziej się splatają, tworząc swoisty i niepowtarzalny system ochrony danych osobowych, w ramach którego kształtuje się także polski standard ochronny.

Problematyka ochrony danych osobowych stale przybiera na znaczeniu i z każdym rokiem pojawiają się nowe inicjatywy w zakresie jej poszerzania. Jest to konsekwencja narastania zagrożeń w tej dziedzinie i pojawiania się ciągle nowych problemów, wobec których dotychczasowe rozwiązania okazują się niewystarczające. Wymaga to stałego monitorowania występujących na tym polu zjawisk i możliwie szybkiego (jednak nie prowizorycznego) dostosowywania do nich istniejących rozwiązań prawnych – tak, by nadal stanowiły skuteczną ochronę przed możliwymi nadużyciami, nie prowadząc jednak przy tym do inflacji prawa.

Polską Ustawę nowelizowano od jej uchwalenia do chwili obecnej czternaście razy,[4] przy czym niektóre modyfikacje miały charakter drobny i porządkowy, niektóre zaś fundamentalnie zmieniały zakres i charakter tej regulacji.[5] Należy przy tym pamiętać, że Polska (podobnie jak reszta krajów Europy Środkowej i Wschodniej) nie miała wcześniej prawnych standardów ochronnych w tej dziedzinie. Tworzono je, odmiennie niż w państwach zachodnich, niemalże równolegle do szerszego standardu – ochrony prywatności. Z braku krajowych doświadczeń w tej materii Ustawa była

[3] Ostatnia konferencja odbyła się w dniach 17–18 kwietnia 2008 r. w Rzymie. W ramach Konferencji Wiosennej w szczególności poruszane są kwestie związane ze stosowaniem Dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, a także ochrona danych osobowych przetwarzanych na potrzeby współpracy policji, jak też współpracy sądów w sprawach karnych i cywilnych (czyli działań podejmowanych w zakresie tzw. trzeciego filaru UE).

[4] W Sejmie ważą się losy projektu kolejnej istotnej nowelizacji, wniesionej do laski marszałkowskiej przez Prezydenta RP. Projekt ten zaostrza m.in. szereg sankcji karnych przewidzianych w przypadkach naruszenia obowiązków przewidzianych w Ustawie.

[5] Np. nowelizacja z 30 sierpnia 2002 r. (Dz.U. z 2002 r. Nr 153, poz. 1271) zastępowała w jednym tylko przepisie wyrazy „Naczelnego Sądu Administracyjnego" zwrotem „sądu administracyjnego", podczas gdy nowelizacja z 22 stycznia 2004 r. (Dz.U. z 2004 r. Nr 33, poz. 285) zmieniała brzmienie aż 35 spośród wszystkich 62 artykułów.

mocno wzorowana na aktach prawnych innych państw[6] oraz na regulacjach międzynarodowych.[7]

Od momentu uchwalenia Ustawy postrzeganie jej przez prawników i specjalistów z zakresu ochrony danych znacznie się poprawiło (choć nadal ma ona pewne słabości). Ważniejsze jednak, że istotnie wzrosła (co można chyba uznać za sukces tej regulacji) świadomość prawna społeczeństwa polskiego w zakresie przedmiotu unormowania tego aktu. Obecnie, spośród wszystkich mieszkańców UE, Polacy są „najbardziej świadomi swoich praw do ochrony danych osobowych i prawa do prywatności", podczas gdy jeszcze trzy lata temu zajmowali w świetle badań odległe, osiemnaste miejsce.[8] Z ustawy znanej wyłącznie osobom zainteresowanym stała się aktem powszechnie kojarzonym i powoływanym. Podobnie GIODO z niemal anonimowego urzędnika stał się osobą często cytowaną i obecną nie tylko w literaturze specjalistycznej, ale także w mediach popularnych, coraz częściej zainteresowanych jego działalnością. Wyraźnym tego potwierdzeniem jest opublikowany 10 października 2008 r. raport TNS OBOP z badania dotyczącego postaw Polaków związanych z ochroną danych osobowych oraz standardów ochrony tych danych panujących w polskich firmach.[9] Według przeprowadzonego sondażu aż 88% Polaków ma świadomość, że ich zgoda jest niezbędna do wykorzystania ich danych osobowych, a 78% wie o obowiązkach informacyjnych instytucji zbierających takie dane.[10] Z uwagi m.in. na powszechność w obrocie gospodarczym tzw. „klauzul o przetwarzaniu danych osobowych", dołączanych do wielu wzorców umów, wiedza obywateli o istnieniu Ustawy i jej materii dalece przekracza znajomość innych aktów prawnych. Tej społecznej świadomości nie towarzyszy jednak proporcjonalny wzrost wiedzy wśród urzędniczej części społeczeństwa, czego dowodzą wpływające do GIODO skargi, dotyczące w znacznej mierze przetwarzania danych osobowych w strukturach administracji rządowej i samorządowej.

---

[6] Wzorce prawa krajowego zaczerpnięto przede wszystkim z państw Europy Zachodniej takich jak Francja, Niemcy i Szwajcaria.

[7] W szczególności na Konwencji nr 108 Rady Europy z dnia 28 stycznia 1981 r., dotyczącej ochrony osób w związku z automatycznym przetwarzaniem danych osobowych oraz Dyrektywie Unii Europejskiej nr 95/46/CE z dnia 24 października 1995 r., dotyczącej ochrony osób fizycznych ze względu na przetwarzanie danych o charakterze osobowym oraz swobodnego przepływu tych danych.

[8] Wywiad z polskim GIODO – Michałem Serzyckim w *Dzienniku Zachodnim*, dostępny w internecie pod adresem http://polskatimes.pl/stronaglowna/153159,internet-ma-pamiec-slonia,id,t.html (data dostępu: 20 grudnia 2009 r.).

[9] Raport TNS OBOP sporządzony 10 października 2008 r. na zlecenie firmy Fleishman-Hillard. Badanie telefoniczne złożone z 13 zamkniętych pytań (metodą CATI) przeprowadzono na terenie całego kraju w okresie od 25 września do 3 października 2008 r. Próbę podstawową stanowiła reprezentatywna grupa 300 osób w wieku 18 i więcej lat.

[10] Jednak statystyki te nie są już tak optymistyczne jeśli chodzi o przekonanie Polaków co do jakości przetwarzania danych w krajowych instytucjach – mniej niż połowa badanych (43%) ma pewność co do dobrego zabezpieczenia w nich danych osobowych. Co gorsza, nieliczne osoby (5–7%) samodzielnie chronią swoje dane osobowe poprzez niszczenie przed wyrzuceniem do kosza dokumentów zawierających dane adresowe, odręczne podpisy czy dane medyczne.

Z uwagi na swoistą popularność omawianej tematyki Ustawa doczekała się w ostatnich latach licznych komentarzy i opracowań – część z nich miała wpływ na kolejne zmiany brzmienia tego aktu. Materia Ustawy jest w związku z tym już dość szczegółowo poznana. Większość z zawartych w niej pojęć i instytucji, początkowo dość enigmatycznych, nie wzbudza już takich wątpliwości, a te nie w pełni jeszcze doprecyzowane są coraz trafniej i pewniej tłumaczone w ramach orzecznictwa sądowego. Polski system ochronny nie opiera się jednak wyłącznie na Ustawie, która jest skoncentrowana *stricte* na swym tytułowym zagadnieniu. Aby zrekonstruować pełny standard ochrony w tej dziedzinie trzeba uwzględnić także inne akty, dotyczące ochrony prywatności *sensu largo*. Regulacje te częściowo nakładają się na siebie, tworząc bardziej złożony system norm. Normy te przenikają się nawzajem, tworząc w ten sposób szczelniejszą, choć czasami przez to mniej przejrzystą barierę ochronną. Warto pamiętać, że Ustawa, z uwagi na swe miejsce w hierarchii źródeł prawa, musi być zgodna z wieloma innymi aktami, w których można poszukiwać dodatkowych środków ochronnych, nie zagwarantowanych w samej Ustawie. Niniejszy artykuł stanowi próbę ogólnego spojrzenia na te właśnie akty i wybrane zagadnienia, związane z ich stosowaniem.

Podstawę całego systemu prawnej ochrony prywatności w Polsce stanowi Konstytucja,[11] która z uwagi na swą normatywną pozycję wyznacza miejsce pozostałych aktów i determinuje w ten sposób ich wzajemne relacje. Prawa do prywatności dotyczą art. 47, 49, 50 i 51 ustawy zasadniczej, zaś kwestii ochrony samych danych osobowych w szczególności dotyczy art. 51. Część przepisów Ustawy stanowi swoiste rozwinięcie gwarancji zawartych w tym przepisie (użyty w art. 51 ust. 1. termin „informacji dotyczących osoby" zdaje się być bliskoznaczny pojęciu „danych osobowych" na gruncie Ustawy).

Zgodnie z wspomnianym przepisem „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby". Oznacza to wprowadzenie istotnego ograniczenia co do możliwości zobowiązywania obywateli do ujawniania wszelkich dotyczących ich danych. Przepis ten nie wyklucza wprawdzie możliwości regulowania w aktach niższego rzędu szczegółowych kwestii dotyczących statusu danych jednostki, jednak ustawowe upoważnienie do wydania takiego aktu musi spełniać wymagania określone w art. 92 Konstytucji, a samo rozporządzenie powinno być zgodne z innymi ustawami i mieścić się w granicach upoważnienia ustawowego.[12] W świetle tego przepisu niedopuszczalne zdaje się być wprowadzenie obowiązku ujawnienia takich danych w innych źródłach takich jak choćby regulaminy pracy czy układy zbiorowe.[13] Można na-

[11] Dz.U. z 1997 r. Nr 78, poz. 483 z późn. zm., sprost. Dz.U. z 2001 r. Nr 28, poz. 319.

[12] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 2 listopada 2005 r. (sygn. VI SA/Wa 1080/2005).

[13] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz (Wyd. 4)*, Kraków 2007, Wydawnictwo Wolters Kluwer Polska Sp. z o.o., s. 113–114.

tomiast w tego rodzaju aktach wprowadzić zapisy uzależniające przyznanie dodatkowych świadczeń (np. świadczenia socjalnego) od dobrowolnego złożenia przez uprawnionego zaświadczenia o wysokości zarobków uzyskiwanych u innego pracodawcy.[14]

W drugim ustępie wspomnianego artykułu[15] wprowadzono ogólne ograniczenie dopuszczalności przetwarzania danych przez władze publiczne naszego kraju do danych niezbędnych w demokratycznym państwie prawa. Ta generalna klauzula uniemożliwia gromadzenie przez ograny państwowe dowolnych danych „na wszelki wypadek". Każda kategoria zbieranych danych powinna być traktowana indywidualnie, a ich przetwarzanie dopuszczalne wyjątkowo – po spełnieniu warunku niezbędności w demokratycznym państwie prawa (którego elementem jest niewątpliwie skuteczna ochrona danych osobowych obywateli). Dodatkowo zasady i tryb gromadzenia i udostępniania informacji, zgodnie z art. 51 ust. 5, muszą być uregulowane w drodze ustawy.[16] W połączeniu z dyspozycją wspomnianego art. 51 ust. 2 oznacza to, że organy władzy publicznej w Polsce nie mogą zbierać i przetwarzać danych osobowych bez ustawowego upoważnienia. Upoważnienie takie powinno zaś precyzyjnie określać kategorie danych, które mogą być przetwarzane oraz zasady postępowania z takimi zbiorami informacji. Należy przy tym zwrócić uwagę, że ograniczenie to dotyczy wyłącznie organów władzy publicznej – podobnych gwarancji przepis nie daje w przypadku danych znajdujących się w posiadaniu osób prywatnych czy wszelkich innych jednostek nie posiadających atrybutu władzy publicznej. W przypadku przetwarzania danych przez te podmioty ochrony na gruncie Konstytucji należy więc poszukiwać w dyspozycji jej art. 47,[17] który chroni całość życia prywatnego, rodzinnego, cześć i dobre imię jednostek. Tego, że może być to ochrona skuteczna dowodzą państwa, które nie posiadają szczegółowej regulacji z zakresu ochrony danych osobowych – w nich prawo do ochrony takich danych wyprowadza się wprost z gwarancji prawa do prywatności, zawartych w ustawie zasadniczej, posiłkując się przy tym często bogatym w tej materii orzecznictwem Europejskiego Trybunału Praw Człowieka.

Wspomnianym powyżej ograniczeniom towarzyszą wyrażone w art. 51 ust. 3 i 4 swoiste uprawnienia kontrolne każdego obywatela w postaci „prawa dostępu do dotyczących go urzędowych dokumentów i zbiorów

[14] Tak w Wyroku Sądu Najwyższego – Izby Administracyjnej, Pracy i Ubezpieczeń Społecznych z dnia 8 maja 2002 r. (sygn. I PKN 267/2001).

[15] Art. 51 ust. 2 Konstytucji: „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym".

[16] Nieprzypadkowo przesłanki te brzmią podobnie do przesłanek standardu ochrony prywatności i życia rodzinnego z art. 8 Europejskiej Konwencji Praw Człowieka. Zapisy Konstytucji były bowiem w znacznym stopniu inspirowane Konwencją i orzecznictwem Europejskiego Trybunału Praw Człowieka.

[17] Art. 47 Konstytucji: „Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym".

danych", a także możliwości „żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą". Dokonując wykładni językowej art. 51 ust. 3 można dojść do wniosku, że jego dyspozycja obejmuje szerszą kategorię dokumentów i zbiorów danych niż tylko te zawierające dane osobowe, bowiem teoretycznie dokumenty „dotyczące go" nie zawsze muszą zawierać dane osobowe kogoś, kogo dotyczą, podczas gdy w świetle tego przepisu także takie zbiory powinny być dla obywatela dostępne.[18] Uprawnienie sformułowane we wskazanym przepisie może być, zgodnie z jego dalszą dyspozycją, ograniczone w drodze ustawy. Ponieważ norma mówi wyłącznie o „urzędowych dokumentach i zbiorach danych" nie można na podstawie tego artykułu żądać dostępu do materiałów (także tych urzędowych) znajdujących się w posiadaniu osób prywatnych.[19]

Istotne znaczenie dla polskiego systemu ochrony danych osobowych mają umowy międzynarodowe, które w przypadku „wolności, praw lub obowiązków obywatelskich określonych w Konstytucji" są ratyfikowane za uprzednią zgodą wyrażoną w ustawie.[20] To z kolei daje im uprzywilejowaną pozycję w polskim porządku prawnym, gdyż (zgodnie z art. 91 Konstytucji) mają one pierwszeństwo przed tymi ustawami, których treści nie da się pogodzić z treścią takiej umowy. Unormowania tych umów w dużej mierze ukształtowały obowiązujący w Polsce standard ochrony prywatności, a w jego ramach także przepisy z zakresu ochrony danych osobowych. W szczególności ważką rolę odgrywają tu dwa europejskie źródła takich regulacji – Rada Europy i Wspólnoty Europejskie, a także powszechnie obowiązujące standardy praw człowieka uchwalone w ramach ONZ.

Europejską organizacją o najstarszych tradycjach w zakresie ochrony praw człowieka jest niewątpliwie Rada Europy. To właśnie w ramach tej organizacji powstało najwięcej zaleceń w omawianej dziedzinie, a w 2006 r. na jej forum ustanowiono, obchodzony co roku 28 stycznia,[21] Dzień Ochrony Danych Osobowych. Uchwalone w ramach Rady Europy liczne konwencje i rezolucje oraz orzecznictwo Europejskiego Trybunału Praw Człowieka do Europejskiej Konwencji Praw Człowieka[22] (dalej EKPC) wywarły ogromny wpływ na rozwój praw człowieka na naszym kontynencie i poza nim.

Prawo do prywatności zostało uregulowane w art. 8 EKPC. Niepodobna oczywiście omówić tu nawet skrótowo całości orzecznictwa dotyczącego szeroko rozumianego prawa do prywatności, można jednak zwrócić uwagę na znaczenie wybranych tez z orzecznictwa dla zagadnienia ochrony danych

[18] Odmiennie, interpretując wskazaną dyspozycję zawężająco – tj. wyłącznie do zbiorów zawierających dane wprost dotyczące osoby – J. Barta i in., op. cit., s. 114.

[19] Ibidem, s. 114–115.

[20] Art. 89 ust. 1 p. 2) Konstytucji.

[21] Czyli w rocznicę otwarcia do podpisu Konwencji Rady Europy nr 108 z 28 stycznia 1981 r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych.

[22] Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61, poz. 284 z późn. zm.), ratyfikowana przez Polskę 19 stycznia 1993 r.

osobowych. Co ciekawe, pomimo znaczącej liczby skarg z Polski, wpływających do Trybunału każdego roku, właściwie nie wpływają z naszego kraju skargi dotyczące przetwarzania danych osobowych.[23] Można to chyba ostrożnie uznać za oznakę pewnej skuteczności krajowych środków odwoławczych w tej dziedzinie.

Aby przetwarzanie danych spełniało standardy EKPC, musi ono odbywać się na podstawie ustawy, realizować uprawniony cel i być przy tym konieczne w społeczeństwie demokratycznym.[24] Przepisy regulujące przetwarzanie danych powinny być dla obywatela dostępne i przewidywalne oraz na tyle precyzyjne, by każdy mógł dostrzec wynikające z nich konsekwencje i uniknąć ingerencji w sferę swojej prywatności.[25] W przypadku zaistnienia takiej ingerencji, gromadzone dane powinny być ograniczone wyłącznie do informacji niezbędnych dla potrzeb prowadzonego postępowania.[26] Przechowywanie i udostępnianie zebranych informacji powinno być szczegółowo unormowane, a osoby, których takie dane dotyczą, powinny mieć możliwość żądania zmiany tych informacji lub ich usunięcia w sytuacji, gdy byłyby one fałszywe, pomawiające lub gdy nie spełniałyby kryteriów wyznaczonych przepisami prawa.[27] Nie można też ograniczać prawa dostępu strony w postępowaniu sądowym do dotyczących jej dokumentów z uwagi na objęcie ich klauzulą tajności,[28] jak też zakładać nieprzemijającej aktualności takiej klauzuli w przypadku dokumentów archiwalnych, w szczególności wytworzonych jeszcze przez służby poprzedniego reżimu.[29]

Informacje chronione prawem do prywatności nie ograniczają się tylko do tzw. „wewnętrznego kręgu", w którym jednostka żyje własnym, osobistym życiem, wedle swego wyboru, wyłączając jednocześnie z tego pojęcia pozostający poza nim świat zewnętrzny. Poszanowanie życia prywatnego musi zawierać w sobie do pewnego stopnia prawo do nawiązywania i rozwijania relacji z innymi ludźmi.[30] Rozmowy telefoniczne prowadzone z miejsca pracy tak samo jak te z domu mogą być objęte zakresem „życia prywatnego" i „korespondencji" i podlegają ochronie.[31] Z drugiej

[23] Ostatnio jednak pojawiły się skargi na kanwie zgodności z EKPC tzw. postępowań lustracyjnych i dostępu do danych archiwalnych z czasów PRL, ciągle jeszcze zaopatrzonych w klauzulę tajności (sprawy Matyjek p. Polsce, Bobek p. Polsce, Luboch p. Polsce i Rasmussen p. Polsce). Więcej na temat tych spraw w niniejszym numerze *Rocznika* w artykule M. Lubiszewskiego, *Lustracja a prawa człowieka. W poszukiwaniu podstawowych standardów* w niniejszym nrze. „Polskiego rocznika...".

[24] Art. 8 ust. 2 EKPC.

[25] Orzeczenie w sprawie Kopp p. Szwajcarii z 1998 r.

[26] Orzeczenie w sprawie Amann p. Szwajcarii z 2000 r.

[27] Orzeczenie w sprawie Leander p. Szwecji z 1987 r. oraz orzeczenie w sprawie Rotaru p. Rumunii z 2000 r.

[28] Orzeczenie w sprawie Bobek p. Polsce z 2007 r.

[29] Orzeczenie w sprawie Turek p. Słowacji z 2006 r. oraz orzeczenie w sprawie Luboch p. Polsce z 2008 r.

[30] Orzeczenie w sprawie Niemietz p. Niemcom z 1992 r.

[31] Orzeczenia w sprawach: Klass i Inni p. Niemcom z 1978 r., Malone p. Wielkiej Brytanii z 1984 r., Huvig p. Francji z 1990 r. oraz Halford p. Wielkiej Brytanii z 1997 r.

strony nikt nie może oczekiwać pełnego poszanowania swojej prywatności w sytuacji, gdy świadomie angażuje się w czynności, które z uwagi na swą specyfikę (w szczególności sposób i miejsce ich dokonania) mogą podlegać automatycznemu rejestrowaniu i dalszemu przetwarzaniu za pomocą różnych środków technicznych.[32]

W łonie Rady Europy narodził się także akt o fundamentalnym znaczeniu dla międzynarodowej ochrony danych osobowych *sensu stricto*. Chodzi oczywiście o Konwencję Rady Europy nr 108 z 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Jest ona najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych.[33] Postanowienia konwencji uzupełnia Protokół Dodatkowy, który wszedł w życie 1 lipca 2004 r.[34] Konwencja wraz z protokołem wprowadza wśród państw-stron pewien jednolity standard ochronny w zakresie przetwarzania danych osobowych. Państwa, które ją ratyfikowały zobowiązują się standard ten chronić i rozwijać. Jest to, w duchu innych rozwiązań Rady Europy, standard minimalny i państwa są zachęcane do jego rozszerzania w ramach regulacji krajowych. Regulując ochronę danych osobowych w opisanym zakresie, konwencja nie wprowadza jednak gotowych i ustalonych wzorców. Respektuje ona w tej mierze już istniejące w niektórych państwach rozwiązania, innym państwom daje zaś możliwość autonomicznego i odmiennego kształtowania środków ochronnych (mających jednak zagwarantować przewidziany w konwencji poziom ochrony). Trzeba przy tym zauważyć, że (odmiennie niż EKPC) akt ten nie przyznaje żadnych uprawnień bezpośrednio obywatelom poszczególnych krajów – nakłada jedynie obowiązki w sferze publiczno-prawnej na same państwa-strony.

Celem konwencji jest „zapewnienie każdej osobie fizycznej [...] poszanowania jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych".[35] Do danych tych, w świetle definicji zawartej w art. 2 lit. a) aktu, zaliczymy każdą informację dotyczącą osoby fizycznej o określonej lub dającej się zidentyfikować tożsamości. W art. 5 konwencja nakłada na państwa obowiązki co do jakości przetwarzanych danych w zakresie ich gromadzenia i przetwarzania. Są to wymogi przetwarzania rzetelnego, zgodnego z prawem i wyłącznie dla usprawiedliwionych celów. Samo przechowywanie ma zaś być dokładne i umożliwiające aktualizację danych oraz nie może trwać dłużej niż jest to wymagane ze względu na cel, w którym dane zgromadzono. Dane powinny być przy tym

[32] Orzeczenie w sprawie P.G. i J.H. p. Wielkiej Brytanii z 2001 r.

[33] Konwencja RE nr 108 weszła w życie 1 października 1985 r., po ratyfikowaniu jej przez 5 państw (Francję, Niemcy, Norwegię, Hiszpanię i Szwecję). W stosunku do Polski konwencja weszła w życie 1 września 2002 r. (Dz.U. z 2003 r. Nr 3, poz. 25).

[34] Polska ratyfikowała go 12 lipca 2005 r. (Dz.U. z 2006 r. Nr 3 poz. 15). Protokół ten służy przede wszystkim złagodzeniu różnic pomiędzy konwencją a Dyrektywą 95/46/WE w materii dotyczącej organów nadzoru przetwarzania danych osobowych oraz transgranicznego przepływu tych danych.

[35] Art. 1 („Przedmiot i cel") Konwencji RE nr 108.

zabezpieczone przed zniszczeniem, zagubieniem, a także nieupoważnionym dostępem, zmienianiem ich lub rozpowszechnianiem.[36] Ponadto, zgodnie z art. 8, państwa muszą zapewnić każdej osobie dostęp do informacji o dotyczących jej zbiorach danych, możliwość ich poprawienia lub usunięcia w przypadku ich przetwarzania z naruszeniem standardów konwencji oraz odpowiednie środki prawne (w tym także system sankcji karnych i odszkodowawczych – art. 10) na wypadek naruszenia jej uprawnień. Konwencja wyróżnia też kategorię danych szczególnie wrażliwych, do których zalicza: pochodzenie rasowe, poglądy polityczne, przekonania religijne, a także dane dotyczące stanu zdrowia, życia seksualnego i karnego skazania. Dane takie nie mogą być przetwarzane automatycznie bez zapewnienia przez prawo wewnętrzne państwa dodatkowych gwarancji ochronnych.[37] Ograniczenia w stosowaniu opisanych gwarancji mogą mieć miejsce wyłącznie na podstawie przepisów prawa, w przypadku ich konieczności w społeczeństwie demokratycznym dla ochrony wskazanych w konwencji celów prawowitych, takich jak ochrona państwa, jego interesów finansowych, porządku i bezpieczeństwa publicznego, ochrony osób, których dane dotyczą albo praw lub wolności innych osób.[38]

W zakresie konwencji powołano też do życia komisję doradczą, złożoną z przedstawicieli wszystkich państw-stron. Organ ten proponuje zmiany mogące ułatwić stosowanie konwencji (w tym także zmiany treści samej konwencji), a na prośbę państw zajmuje stanowisko we wszelkich kwestiach związanych z wykonywaniem konwencji.

Zgodnie z art. 3, przystępując do konwencji państwa mogą, w drodze złożenia stosownych oświadczeń, zarówno rozszerzyć jak i ograniczyć zakres zbiorów danych objętych jej ochroną. (np. poprzez objęcie nią także zbiorów danych o instytucjach zrzeszających osoby fizyczne, czy dane nie przetwarzane automatycznie).

Wdrażanie odpowiednich środków ochronnych mogą państwom ułatwić rezolucje i rekomendacje Rady Europy uszczegóławiające standardy przetwarzania danych w poszczególnych dziedzinach. Nie mają one charakteru wiążącego, ale w praktyce stanowią swoiste kanony, do których państwa często się odwołują w ramach regulacji specyficznych aspektów przetwarzania danych osobowych. Dwie najważniejsze rezolucje dotyczą ochrony prywatności osób fizycznych w aspekcie wykorzystywania elektronicznych danych w sektorze prywatnym[39] i publicznym.[40] Zawarte w nich zasady doprecyzowują kategorie danych podlegających przetwarzaniu wraz ze sposobami ich przetwarzania i dostępu do nich, zalecają także określone środki zabezpieczające oraz ograniczenia czasowe przetwarzania. W drodze rekomendacji Rada Europy zaleca stosowanie określonych środków ochron-

[36] Art. 7 („Bezpieczeństwo danych") Konwencji RE nr 108.
[37] Art. 6 („Szczególne kategorie danych") Konwencji RE nr 108.
[38] Art. 9 („Wyjątki i ograniczenia") Konwencji RE nr 108.
[39] Rezolucja Komitetu Ministrów Rady Europy nr 22 (73).
[40] Rezolucja Komitetu Ministrów Rady Europy nr 29 (74).

nych w różnych dziedzinach, takich jak banki danych medycznych, prawniczych, statystycznych i naukowych, karnych, marketingowych, społecznych czy ubezpieczeniowych. Łącznie jest to kilkadziesiąt aktów, dotyczących różnych aspektów przetwarzania danych, których omówienie przekracza ramy niniejszego opracowania.[41]

W latach dziewięćdziesiątych XX w. ochrona danych osobowych znalazła się także w polu zainteresowania Unii Europejskiej. Początkowo rekomendowano państwom członkowskim podpisanie Konwencji nr 108 Rady Europy, z czasem jednak podjęto prace nad stworzeniem odpowiednich regulacji w ramach prawa wspólnotowego. Obecnie tematyki tej dotyczy kilka unijnych dyrektyw i rozporządzeń,[42] które były już także (z uwagi na rozbieżności interpretacyjne) przedmiotem orzeczeń Europejskiego Trybunału Sprawiedliwości w ramach zgłaszanych przez sądy krajowe państw członkowskich pytań prawnych.

Podstawowym aktem prawa wspólnotowego z zakresu danych osobowych jest Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu danych (dalej Dyrektywa).[43] Zobowiązała ona państwa członkowskie do implementacji jej założeń w ramach prawa krajowego (co nastąpiło nie bez opóźnień – Komisja Europejska musiała pozwać niektóre państwa w celu zainicjowania w nich odpowiednich procedur legislacyjnych). Należy przy tym pamiętać, że – w sytuacji braku implementacji postanowień Dyrektywy – osoby poszkodowane mogą powoływać się na nią przed sądami krajowymi bezpośrednio, w miejsce niewprowadzonych lub nieprawidłowo wprowadzonych przepisów prawa krajowego. Dyrektywa została oparta na podobnych zasadach co Konwencja Rady Europy, dostosowano ją jednak do nowych zagrożeń, które pojawiły się od czasu uchwalenia Konwencji. Regulacja Dyrektywy jest też bardziej szczegółowa, pozostawiając tym samym państwom członkowskim mniejszą swobodę w zakresie przyjętych w prawie krajowym rozwiązań. Podstawową różnicą jest wprowadzenie w Dyrektywie obowiązku powołania krajowych organów nadzorczych w celu stałego monitorowania stanu ochrony danych osobowych w danym kraju, a przede wszystkim uregulowanie kwestii transferu banków danych osobowych do państw trzecich.[44]

---

[41] Zestawienie rezolucji i rekomendacji Rady Europy wraz z krótkim omówieniem można znaleźć m.in. w komentarzu do Ustawy autorstwa J. Barty i in., op. cit., s. 75 – 83.

[42] Dyrektywy Parlamentu Europejskiego i Rady: 95/46/WE, 2000/31/WE, 2002/58/WE, 2006/24/WE, Rozporządzenie Rady (WE) nr 2725/2000, Rozporządzenie (WE) nr 45/2001 Parlamentu, Decyzja ramowa Rady 2008/977/WSiSW.

[43] Dz.U. L281 z 23 listopada 1995 – str. 31, z późn. zmianami wprowadzonymi Rozporządzeniem (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. (Dz.U. L284 z 21 października 2003 r. – str. 1). Termin implementacji Dyrektywy wyznaczono na 23 października 1998 r.

[44] Różnice te obecnie zmniejszono poprzez uchwalenie wspomnianego wcześniej Protokołu Dodatkowego do Konwencji.

Przekazanie danych może nastąpić, zgodnie z art. 25 Konwencji, tylko wówczas, gdy kraj, do którego są one przekazywane, zapewnia odpowiedni (*adequate*) poziom ochrony. Odpowiedniość ochrony należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zestawu takich operacji. Należy przy tym zwrócić szczególną uwagę na charakter przesyłanych danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, obowiązujące w kraju trzecim normy prawne (zarówno ogólne, jak i branżowe) oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym kraju.[45] Szczególne uprawnienia przysługują tu Komisji Europejskiej, która może zobowiązać państwa do zapobiegania przekazywaniu danych do wybranego państwa trzeciego (w przypadku stwierdzenia nieadekwatnych środków ochronnych), a także potwierdzić, że wybrane państwo spełnia wymogi Dyrektywy.[46] Niezależnym ciałem doradczym, wydającym opinie m.in. w powyższej kwestii, jest powołany na podstawie art. 29 Dyrektywy zespół roboczy, złożony z przedstawicieli krajowych organów ochrony danych oraz przedstawiciela Komisji. Wyjątkowo możliwe jest także przekazanie danych osobowych do państw nie zapewniających odpowiedniej ochrony, pod warunkiem spełnienia wymogów przewidzianych w art. 26 Dyrektywy. Poza możliwością potwierdzenia „adekwatności" ochrony przez Komisję Europejską możliwe jest także dokonanie jej w drodze decyzji krajowego organu ochrony danych (jednak w świetle polskiej Ustawy GIODO zasadniczo nie posiada tej kompetencji)[47], a także poprzez dokonanie jednostkowej oceny adekwatności poziomu ochrony przez administratora danych (przy czym podlega on jednak kontroli krajowego organu nadzoru).[48] Ponieważ właściwie nie jest możliwe kontrolowanie adekwatności ochrony każdego transferu danych do państwa trzeciego *ad casum*,[49] postuluje się utworzenie „białej listy" państw trzecich, „generalnie" zapewniających należytą ochronę. Lista ta nie miałaby wiążącego charakteru, jednak stanowiłaby wskazówkę co do tego, czy w konkretnej sytuacji niezbędna jest jednostkowa ocena dopuszczalności transferu danych.[50]

W kwestii oceny zagadnienia transferu danych (a ściślej tego, co należy, a czego nie należy uznać za transfer) duże znaczenie ma wyrok Europejskiego Trybunału Sprawiedliwości w sprawie Bodil Lindqvist (C-101/01).[51]

[45] Art. 25 ust. 2 („Zasady") Dyrektywy.

[46] Art. 25 ust. 3–6 Dyrektywy.

[47] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, Dom Wydawniczy ABC, s. 206.

[48] X. Konarski, G. Sibiga, *Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i Unii Europejskiej*, w: *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, red. X. Konarski, G. Sibiga, Kraków 2007, Wydawnictwo Wolters Kluwer Polska Sp. z o.o., s. 94.

[49] *First Orientation on Transfers of Personal Data to Third Countries Pissible Ways Forward in Assesing Adequacy*, WIPR 1997, vol. 11, 332.

[50] J. Barta i in., op. cit., s. 87–88.

[51] Dz.U. C007 z 10 stycznia 2004 r., s 3–4.

W orzeczeniu tym Trybunał stwierdził, że nie mamy do czynienia z transferem danych w rozumieniu art. 25 Dyrektywy, jeśli osoba w państwie członkowskim umieszcza dane osobowe na stronie internetowej serwera znajdującego się w tym lub innym państwie członkowskim, w sytuacji, gdy strona ta jest powszechnie dostępna, także dla osób z państw trzecich. W uzasadnieniu swego orzeczenia Trybunał podniósł m.in., że dla oceny, czy w danej sytuacji mamy do czynienia z „transferem danych", istotny jest sam sposób funkcjonowania internetu i procedura nawiązywania w nim połączeń oraz znaczenie w tym kontekście słowa „transfer". W świetle ustaleń Trybunału strona, na której pani Lindqvist umieściła dane innych osób, była dostępna dla wszystkich (także w państwach trzecich), jednak nie udowodniono, by dane z niej nie były wprost przekazywane (transferowane) do tych państw. Przyjmując, że w tej sytuacji nie doszło do „transferu" Trybunał dał pierwszeństwo wykładni językowej słowa „transfer" nad wykładnią celowościową (z której wynika, że umieszczenie danych na stronie internetowej może do takiego transferu danych prowadzić). Taka interpretacja może jednak powodować realne zagrożenie wykorzystania stron internetowych do niekontrolowanego przekazywania danych. Często trudno bowiem będzie udowodnić, czy dane umieszczone na stronie internetowej zostały w całości przesłane i zapisane na komputerze osoby z państwa trzeciego, czytającej treść takiej strony (w większości krajów dostawcy internetu nie mają obowiązku rejestrowania, jakie dane podlegały transferowi, a co najwyżej fakt połączenia z określoną stroną). W rezultacie niemożliwe może się okazać udowodnienie, czy i w jakim zakresie transfer danych miał miejsce (w szczególności, jeśli protokół takiej transmisji podlegał szyfrowaniu). W komentarzach do orzeczenia Trybunału zwraca się jednak także uwagę, że w tym przypadku musiano wyznaczyć granicę pomiędzy ochroną danych osobowych w postaci prewencyjnego całkowitego zakazu ich publikacji celem zapobieżenia ewentualnemu transferowi a wolnością wypowiedzi w internecie, która w konsekwencji takiego zakazu mogłaby zostać poważnie ograniczona.

Na gruncie prawa europejskiego tematyka ochrony danych osobowych aktualnie jest coraz bardziej obecna, a związane z danymi osobowymi kwestie są dodatkowo regulowane w rozlicznych aktach, dotyczących szczególnych dziedzin przetwarzania tych danych. Tematyka ta stała się także przedmiotem działań ONZ, która ogłosiła 14 grudnia 1990 r. rezolucję, zawierającą wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych.[52] Akt ten nie ma jednak charakteru wiążącego, dlatego ochrony przetwarzania danych osobowych na gruncie powszechnego prawa międzynarodowego należy na razie poszukiwać w źródłach wiążących o bardziej ogólnym charakterze, takich jak Międzynarodowy Pakt Praw Obywatelskich i Politycznych (dalej Pakt).[53]

[52] Rezolucja 45/95 Zgromadzenia Ogólnego ONZ z 26 czerwca 1985 r.

[53] Uchwalony 19 grudnia 1966 r., wszedł w życie 23 marca 1976 r., przez Polskę ratyfikowany 3 marca 1977 r., wszedł w życie wobec Polski 18 czerwca 1977 r. (Dz.U. z 1977 r. Nr 38,

System kontrolny Paktu (w przypadku ratyfikacji Protokołu Fakultatywnego obejmujący także prawo do skargi indywidualnej) nie jest systemem *stricte* sądowym – decyzje Komitetu Praw Człowieka nie wiążą wprost organów państw-stron. Nie zmienia to jednak faktu, że jako umowa międzynarodowa jest on źródłem prawa obowiązującego w Polsce i można się na niego powoływać w sytuacji, gdy akty niższej rangi (także ustawy) nie respektują przewidzianych w nim praw.

Szeroko pojęte prawo do prywatności jest uregulowane w art. 17 Paktu stanowiącym, że „nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię."

Zgodnie z samym Paktem, jak i w świetle Uwag Ogólnych Komitetu Praw Człowieka (dalej Uwagi i Komitet)[54] ochrona prywatności, a więc także danych osobowych nie ma charakteru bezwzględnego. Jednak wszelka ingerencja powinna być dokonywana wyłącznie wtedy, gdy jest niezbędna z punktu widzenia społeczeństwa, w ramach obowiązującego prawa i przez uprawnione do tego organy. Przepisy regulujące taką ingerencję powinny być maksymalnie szczegółowe, aby wyeliminować arbitralność decyzji osób działających w imieniu władzy państwowej. Państwo powinno w ramach składanych raportów okresowych informować Komitet o podmiotach uprawnionych do dokonywania takiej ingerencji oraz zasadach ich postępowania. Raporty powinny ponadto zawierać informację na temat skarg złożonych w sprawie arbitralnej lub bezprawnej ingerencji, liczbę potwierdzonych przypadków oraz zastosowane środki zaradcze.

W zakresie ochrony danych osobowych Komitet wymaga, by środki prawne, gwarantujące integralność i poufność korespondencji, były wyraźnie określone w prawie i rzeczywiście dostępne, podobnie jak środki przeciwko osobom odpowiedzialnym za naruszenia w tym zakresie. Wszelka korespondencja (także elektroniczna) powinna być doręczona do adresata bezpośrednio, bez jej otwierania czy odczytywania w inny sposób. Wszelkie elektroniczne i inne środki inwigilacji, przechwytywanie telefonicznych, telegraficznych i innych form komunikacji, podsłuchy oraz nagrywanie rozmów powinny być zabronione.

Zgodnie z Uwagami Komitetu „zbieranie i przechowywanie danych osobowych w komputerach, bankach danych i innych urządzeniach, zarówno przez władzę publiczną jak i prywatne osoby lub ich grupy, musi być uregulowane prawnie."[55] Pakt nie uzależnia w tym względzie faktu przysługiwania ochrony prawnej od rodzaju podmiotu dokonującego przetwarzania

poz. 167). Protokół Fakultatywny przewidujący prawo do skargi indywidualnej do Komitetu Praw Człowieka Polska ratyfikowała 14 października 1991 r., wszedł w życie wobec Polski 7 lutego 1992 r. (Dz.U. z 1994 r. Nr 23, poz. 80).

[54] *General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17)* : z 8 kwietnia 1988 r. (32. sesja Komitetu Praw Człowieka), tłum. wł.

[55] Ibidem.

danych. Państwo powinno zagwarantować, by informacje dotyczące życia prywatnego osób nie dostawały się w ręce osób nie uprawnionych oraz by nie mogły być wykorzystane w celu sprzecznym z Paktem.

W świetle Uwag Komitetu każdy „powinien mieć prawo ustalić w zrozumiały sposób czy, a jeśli tak to jakie dane osobowe i w jakim celu są przechowywane w plikach z danymi" oraz „móc ustalić jakie władze publiczne, osoby prywatne lub ich grupy mają kontrolę nad tymi plikami".[56] W przypadku, gdyby dane te były jakkolwiek nieprawidłowe czy zebrane niezgodnie z prawem, osoba, której dane dotyczą, ma prawo oczekiwać, wedle potrzeby, ich sprostowania lub usunięcia.

W konsekwencji, w drodze interpretacji, Komitet ustanowił w dziedzinie przetwarzania danych osobowych standard ochronny nie odbiegający mocno od, dużo bardziej szczegółowo uregulowanych, standardów wspólnotowych. Jest to dowód na to, że problemy pojawiające się przy wprowadzaniu nowych technologii często można z powodzeniem rozstrzygać w drodze mądrej i respektującej podstawowe wartości interpretacji, bez wprowadzania rozbudowanych, szczegółowych i pełnych technicznego żargonu regulacji.

Standard ochrony danych osobowych w Polsce jest systematycznie podnoszony. Jego zakres jest określony nie tylko w ramach Ustawy, ale także w szeregu innych aktów. Rozwój ten odbywa się nie tylko na płaszczyźnie krajowej, ale też w znacznym stopniu poza nią, w ramach prawa Wspólnot Europejskich i innych organizacji międzynarodowych. W niniejszym artykule w zasadzie nie poruszano kwestii szczegółowych regulacji krajowych i międzynarodowych z zakresu chociażby prawa telekomunikacyjnego, przetwarzania danych medycznych czy na potrzeby obronności i bezpieczeństwa państwa. W ich ramach istnieje szereg odmiennych uregulowań i odstępstw od zasad ogólnych. Wszystkie te akty tworzą coraz bardziej złożony system, w którym zakres ochrony określonych kategorii danych zależy od tego, pod który z tych szczegółowych aktów możemy konkretny zbiór danych zakwalifikować (Ustawę stosujemy w ograniczonym stopniu do zbiorów, których przetwarzanie uregulowane jest w innych ustawach). Tak narastającą regulację wymusza postęp technologiczny, stawiający przed legislatorami kolejne wyzwania. W tym swoistym normatywnym „pędzie" do objęcia przepisami wszelkich możliwych sytuacji przetwarzania danych nie można jednak zapominać, że im bardziej szczegółowa regulacja, tym mniejsze pole jej praktycznego zastosowania. Norm o dużym stopniu szczegółowości dotyczy też szybsza dezaktualizacja, powodująca konieczność nowelizacji zwiększającej i tak już dotkliwe zjawisko inflacji prawa. Ta swoista „nadregulacja" nie jest całkiem niekorzystna z perspektywy podmiotu chronionego, gdyż ten zawsze może poszukiwać ochrony w ramach innych przepisów. Opisane regulacje zachodzą bowiem na siebie, tworząc przez to system bardziej szczelny, choć przez to także mniej przejrzysty. Może to jednak stwarzać swoiste problemy interpretacyjne i wątpliwości co do za-

[56] Ibidem.

kresu obowiązywania poszczególnych aktów. Do takiego konfliktu prowadzić mogło stosowanie norm Konwencji i Dyrektywy w zakresie transferu danych do państw trzecich. Konwencja w art. 12 zobowiązywała państwa-strony do zapewnienia „swobodnego przepływu danych", podczas gdy Dyrektywa uzależniała go od zapewnienia przez państwo trzecie adekwatnego poziomu ochrony przekazywanych danych.[57] Dlatego w przyszłej regulacji trzeba będzie w coraz większym stopniu uwzględniać wzajemne przenikanie się norm różnych standardów ochronnych, co na pewnym etapie może wymagać bardziej kompleksowego rozwiązania problemu ich wzajemnego oddziaływania. W tym nawale coraz bardziej technicznych i szczegółowych norm, być może warto czasem przyjąć koncepcję odmienną, bazującą na ogólnych wartościach, już dawno uznanych w ramach praw człowieka i pozostawiać nieco szersze możliwości interpretacyjne organom stosującym prawo. Nie wyeliminuje to oczywiście konieczności nowelizowania prawa. To poniekąd zresztą naturalna tendencja do udoskonalania tego, co już zostało osiągnięte. Niezbędne jednak na pewnym etapie stanie się kompleksowe i jednolite uregulowanie kwestii, które obecnie są rozstrzygane wielotorowo, w ramach różnych, niepowiązanych rozwiązań. Stabilną podstawę do takiego rozwiązania mogą stanowić standardy międzynarodowe, od lat sprawdzone w ramach ochrony prawa do prywatności. Niejednokrotnie zdarzało się już bowiem, że zamiast tworzyć w prawie krajowym nowe, bardziej szczegółowe koncepcje prawne, wystarczyło oprzeć się na tych powszechnie uznanych, by w drodze ich interpretacji odnaleźć rozwiązanie.

PERSONAL DATA PROTECTION STANDARD IN POLAND – ELABORATION ON CHOSEN ELEMENTS

Key words: human rights, right to privacy, legal privacy protection, personal data protection.

Summary

Article is about Polish personal data protection system, nowadays consisting of many different legal acts from different legal sources. Article elaborates on some of these regulations.

Polish personal data protection act is almost twelve years old. Legal system has changed since introduction of this regulation. New international guarantees have been introduced by the European Union, the Council of Europe and other international organizations. Most important guarantees of the right to privacy these days are contained in Polish Constitution, Convention No 108 of Council of Europe, Directive 95/46/WE of European Union and International Pact of Civil and Political Rights of United Nations. This makes it more secure system, but also a more complicated one. Article concentrates on main differences between these acts.

Polish Constitution has essential role in Polish legal system. It determines the role of all other law sources and it also regulates the right to privacy itself, specifically personal

[57] Problem ten rozwiązano w drodze Protokołu do Konwencji, który wprowadza zakaz przekazywania danych, gdy państwo trzecie nie spełnia stosownych standardów ochronnych.

data protection (in art. 51). Its importance cannot be overestimated as Constitutional rules influence the interpretation of all other regulations.

Significant source of legal regulations concerning personal data protection is Council of Europe. Its Convention No 108 has defined legal limits in that matter for many years. Also the judicature of European Court of Human Rights has great importance in interpretation and understanding of the nature of the right to privacy.

On the foundations of these regulations bases the law of the European Union that nowadays affects legal systems of all the member states, as national regulations are to be fully harmonized with the directives of EU. Also General Comments of the Human Rights Committee to the International Pact of Civil and Political Rights have great importance for the interpretation of international obligations of Poland.

Unfortunately these international guarantees are not fully harmonized, which sometimes causes conflicting legislation. Some treaties obligate Poland to give free access to and transfer of information, while others prohibit such transfer when protective measures in the legal system of the country the data are being transferred to are not adequate to the national ones. It gives lawyers different ways to provide legal aid on the basis of different legal acts. On the other hand it causes uncertainty about the impact of some regulations. In consequence we have to choose which norms to abide. Article compares main legal regulations in the subject matter – their differences, similarities and scope. It also contains some thesis and suggestions of solutions for the conflicting rules of these regulations.