Bartosz Marcinkowski

Ochrona danych osobowych w Irlandii

Zeszyty Prawnicze 8/2, 245-261

2008

Zeszyty Prawnicze
UKSW 8.2 (2008)

Bartosz Marcinkowski

Uniwersytet Kardynała Stefana Wyszyńskiego

OCHRONA DANYCH OSOBOWYCH W IRLANDII

I. Uwagi wprowadzające

Poniższy artykuł ma na celu przybliżenie polskim czytelnikom irlandzkiej, a w pewnym zakresie także brytyjskiej[1], myśli prawniczej w dziedzinie ochrony danych osobowych. Nie jest wprawdzie możliwe w ramach artykułu dokonanie wyczerpującej prezentacji systemu ochrony danych osobowych w tych państwach, warto jednak zasygnalizować kierunki rozwoju omawianej materii w Irlandii oraz częściowo w Wielkiej Brytanii.

Impulsem dla powstania niniejszego tekstu stały się w szczególności tezy i wnioski formułowane przez Billy'ego Hawkesa oraz Roberta Clarka podczas konferencji *Data Protection Practical Compliance – 2nd Annual Conference*, która odbyła się w listopadzie 2007 r.

[1] Można zauważyć swoistą „intelektualną bliskość" irlandzkiej i brytyjskiej refleksji w omawianej dziedzinie; zdaje się, że irlandzcy prawnicy bacznie obserwują poczynania swoich brytyjskich kolegów (i *vice versa*) analizując i odwołując się w swoich pracach zarówno do brytyjskiego piśmiennictwa, jak i dorobku orzecznictwa sądowego Wielkiej Brytanii. Z tego powodu, za wzorem autorów irlandzkich, także w niniejszym artykule w szeregu przypadków przykłady pochodzące z literatury, praktyki i dorobku irlandzkiego oraz brytyjskiego stosowane są zamiennie i uzupełniająco. Niewątpliwie jednak nie można stawiać pełnego znaku równości pomiędzy wskazanymi systemami prawnymi, o czym też jest mowa poniżej.

w Dublinie. W konferencji licznie reprezentowani byli irlandzcy i brytyjscy prawnicy-akademicy, praktycy oraz administratorzy danych stosujący na co dzień przepisy o ochronie danych osobowych, a przewodniczył jej R. Clark, profesor Wydziału Prawa *University College* w Dublinie, konsultant w zakresie ochrony prywatności i problematyki danych osobowych. Jednym z kluczowych prelegentów był zaś wspomniany B. Hawkes, piastujący od lata 2005 roku stanowisko komisarza ochrony danych osobowych Irlandii (*Data Protection Commissionaire*, w dalszej części określanego jako DPC), będącego odpowiednikiem polskiego Generalnego Inspektora Ochrony Danych Osobowych (dalej określanego jako GIODO).

II. OCHRONA DANYCH OSOBOWYCH W IRLANDII – UWAGI OGÓLNE

Jak wskazuje DPC, w ostatnim czasie notowany jest szczególny wzrost zainteresowania tematyką ochrony prywatności i ochrony danych osobowych w Irlandii. Społeczeństwo irlandzkie zaczęło doceniać rangę problemu ochrony prywatności i wartość, jaką stanowi prywatność, a w tym zapewnienie bezpieczeństwa i ochrony danym osobowym. Ilustrują powyższe twierdzenie wyniki badań statystycznych przeprowadzonych przez biuro DPC w roku 2005. Aż 89% respondentów uznało, iż ochrona prywatności (obejmująca w szczególności ochronę danych osobowych) jest wartością „bardzo ważną". Prywatność ustąpiła pola jedynie szeroko rozumianej walce z przestępczością, którą za „bardzo ważną" uznało 91% badanych. Ochrona prywatności wśród wartości zasługujących na szczególną ochronę prawną wyprzedziła jednak między innymi dziedzinę ochrony praw konsumentów (85% respondentów uznało ją za „bardzo ważną"), równego traktowania w miejscu pracy (82% wskazań „sfera bardzo ważna") czy respektowania zasad etycznych przez organy publiczne (78% wskazań „sfera bardzo ważna")[2]. Jednocześnie badani wskazali, że w odniesieniu do ochrony prywatności największe znaczenie ma dla

[2] W powołanych badaniach ankietowani mogli wskazywać kilka odpowiedzi, zaliczając kilka wartości do sfer w ich ocenie „bardzo ważnych", „ważnych" itd.

nich kolejno bezpieczeństwo: (I) danych finansowych, (II) danych dotyczących stanu zdrowia, (III) numeru PPS (*Personal Public Service*, odpowiednika polskich numerów NIP i PESEL), (IV) danych dotyczących kart kredytowych i płatniczych oraz transakcji dokonywanych za ich pomocą, (V) danych obejmujących numery telefonów[3], (VI) danych zawierających adres domowy oraz (VII) daty urodzenia oraz stanu cywilnego.

W podobnym tonie wypowiada się GIODO, który między innymi w dorocznym Sprawozdaniu ze swej działalności w roku 2006 wskazał, iż „od chwili wejścia w życie ustawy o ochronie danych osobowych w kwietniu 1998 r. poziom świadomości prawnej społeczeństwa na temat ochrony danych osobowych [w Polsce – przyp. autora] z roku na rok ulega nieznacznemu, ale zauważalnemu zwiększeniu".[4]

III. OCHRONA DANYCH OSOBOWYCH W IRLANDII – UMIEJSCOWIENIE DZIEDZINY W IRLANDZKIM SYSTEMIE PRAWNYM

Prawo do prywatności nie znajduje swego bezpośredniego źródła w irlandzkiej konstytucji z roku 1937[5], zatem zgoła inaczej niż w przypadku Konstytucji Rzeczypospolitej Polskie z roku 1997[6], zgodnie z którą ochronie prawnej podlega nie tylko prywatność (art. 47 Konstytucji RP), ale także dane osobowe obywateli (art. 51 Konstytucji RP).

Konstytucja irlandzka mówi w tym zakresie jedynie o przysługującej obywatelom prawnej ochronie ich praw osobistych (*personal rights of the citizen* – art. 40.3 Konstytucji Irlandii).

---

[3] Powyższe może wynikać z rozpowszechniającego się w Irlandii zjawiska „marketingu smsowego", o którym mowa w dalszej części artykułu.

[4] Sprawozdanie z działalności GIODO w roku 2006, s. 8; Sprawozdanie jest dostępne na stronie internetowej http://www.giodo.gov.pl/156/.

[5] Tekst angielski dostępny na stronie internetowej: http://www.taoiseach.gov.ie/attached_files/html%20files/Constitution%20of%20Ireland%20(Eng)Nov2004.htm.

[6] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, Dz. U. Nr 78, poz. 483 ze zm.

Jednak mimo braku pisanej normy konstytucyjnej odnoszącej się wprost do ochrony prywatności nie ulega wątpliwości, iż prawo do prywatności stanowi jedno z podstawowych praw człowieka, głęboko zakorzenionych w irlandzkiej tradycji i kulturze[7]. Irlandzkie orzecznictwo sądowe było i jest w tej materii jednoznaczne: irlandzkie sądy wyraźnie stwierdziły, iż fakt istnienia prawa do prywatności jest w Irlandii bezdyskusyjny[8]. Także wśród irlandzkich, brytyjskich, a także amerykańskich autorów panuje pełna zgodność co do tego, że obywatel ma prawo „bycia pozostawionym samemu" (*right of the citizen to be left alone*)[9].

Poza tym ochrona prawa do prywatności, w tym ochrona danych osobowych, znalazła szczegółowe uregulowanie w szeregu obowiązujących w Irlandii aktów normatywnych niższego rzędu. Tytułem przykładu można wymienić ustawę o handlu elektronicznym (*Electronic Commerce Act 2000*) czy zasadnicze z punktu widzenia niniejszego artykułu irlandzkie ustawy o ochronie danych osobowych z lat 1988 i 2003 (*Data Protection Acts 1988 – 2003*, dalej zwane *Data Protection Acts*)[10].

---

[7] Można przytoczyć w tym miejscu anglosaskie porzekadło „mój dom jest moją twierdzą" (*my home is my castle*), którego praktycznym wyrazem jest częsty na Wyspach zwyczaj odstępowania od oznaczania domów numerami. Szerzej na temat sygnalizowanych tu socjologicznych spostrzeżeń piszą między innymi K. FOX, *Watching the English. The Hidden Rules of English Behaviour*, London 2004 oraz G. VIALLI i G. MARCOTTI, *The Italian Job. Journey to the Heart of the Great Footballing Culturies*, London 2006.

[8] D. KELLEHER, *Privacy and Data Protection Law in Ireland.*, Dublin 2006 s. 40, oraz przedstawiony tamże opis sprawy Bailey przeciwko Flood (s. 3 i n. oraz s. 26), w której irlandzki Sąd Najwyższy (*Supreme Court*) uznał w roku 2000, iż prawo do prywatności obywatela pozostaje „poza wszelką dyskusją".

[9] Por. D. KELLEHER, *op. cit*,, s. 3 i n. oraz G. SIBIGA, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 11 i 12 oraz powołane tam źródła, w tym zwłaszcza: S.D.WARREN i J.D. BARNADEIS, *The right to privice*, «Harvard Law Review» 4 (1890).

[10] Teksty angielskie dostępne na stronie internetowej: http://www.dataprotection.ie/ViewDoc.asp?DocId=-1&CatID=47&m=l. W tym kontekście trzeba odnotować, iż Europejski Trybunał Sprawiedliwości uznał irlandzką ustawę z roku 1988

Data Protection Acts stanowią podstawowe akty normatywne regulujące dziedzinę ochrony danych osobowych w Irlandii (podobnie jak w polskim systemie prawnym czyni to ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, dalej określana jako Ustawa)[11].

Godzi się przy tym zauważyć, iż jednym z celów zarówno *Data Protection Acts*, jak i Ustawy jest implementacja do krajowych systemów prawnych postanowień dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (dalej określanej mianem Dyrektywy)[12].

Data Protection Acts przewidują jednak kilka istotnych odmienności w stosunku do postanowień Dyrektywy. *Data Protection Acts* między innymi nie znajdują zastosowania do danych osobowych, które są publicznie dostępne na podstawie obowiązujących przepisów prawa. W przypadku prawa irlandzkiego powyższe wyłączenie dotyczy np. rejestru wyborców. Co ważne, ten konkretny wyjątek jest przedmiotem ostrej krytyki wyrażanej w irlandzkiej literaturze[13]. Także w praktyce działania DPC często pojawiają się skargi na wykorzystywanie publicznie dostępnych danych (w tym danych ze spisów wyborców) dla celów marketingowych[14].

Jednocześnie, zgodnie z tradycją *common law*, irlandzcy i brytyjscy prawnicy są zgodni: nawet zatrudnienie najsprawniejszych legis-

---

za niedostosowaną do wymogów dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Dopiero ustawa z roku 2003 wprowadziła powołaną dyrektywę do irlandzkiego systemu prawnego. Por. na ten temat szerzej D. HEISENBERG, *Negotiationg Privacy. The European Union, the United States, and Personal Data Protection*. London 2005, s. 115.

[11] Tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.

[12] Dz. Urz. WE L 281 z 21 listopada 1995 r.

[13] D. KELLEHER, *op. cit*., s.100.

[14] D. KELLEHER, *op. cit*., s. 101, odnotowuje podobne głosy podnoszone w Wielkiej Brytanii, gdzie przyjęto wyjątek analogiczny do opisywanego. W Irlandii próba zaradzenia problemowi została podjęta poprzez zawężenie zakresu danych ujawnionych w spisach wyborców.

latorów na etapie spisywania ustaw nie pozwoli rozwiązać wszystkich dylematów dotyczących omawianej dziedziny, a to w związku z niezwykłym tempem postępu technicznego oraz bezustannie rozwijającymi się możliwościami przetwarzania danych, rodzącymi coraz to nowe zagrożenia dla prywatności (idzie tu między innymi o takie techniczne nowinki, jak aparaty fotograficzne i kamery w telefonach komórkowych, kamery internetowe czy po prostu doskonalsze i coraz szybsze wyszukiwarki internetowe). Z tych powodów akty prawne uchwalane w omawianej dziedzinie winny określać raczej ogólne zasady postępowania bez zbędnej kazuistyki, które następnie będą mogły być elastycznie wykorzystane przez uczestników obrotu prawnego z uwzględnieniem realiów współczesności i zachodzącego postępu technicznego[15].

IV. OCHRONA DANYCH OSOBOWYCH W IRLANDII – UWAGI NA TEMAT AKTUALNIE IDENTYFIKOWANYCH SFER ZAGROŻEŃ DANYCH OSOBOWYCH

Dalsze rozważania zostaną poświęcone wybranym sferom zagrożeń danych osobowych aktualnie identyfikowanym przez DPC oraz irlandzkich prawników i administratorów danych.

B. Hawkes i R. Clark uznają, iż szczególnej uwagi i dbałości wymagają przede wszystkim następujące sfery:

− sfera faktycznego zapewnienia osobom, których dane dotyczą, prawa do uzyskania informacji odnoszących się do przetwarzania ich danych, w tym informacji, czy istnieje zbiór obejmujący kon-

[15] D. KELLEHER, *op. cit*., s. 13 i n. między innymi stwierdza, iż zbiory danych były scentralizowane (tak, jak wyobrażali to sobie twórcy Dyrektywy) w czasach, gdy komputery były scentralizowanymi, lokalnymi urządzeniami. Obecnie, w dobie Internetu, doszło do istotnej decentralizacji metod obróbki danych w systemach komputerowych. Na temat tempa rozwoju samego Internetu proszę por. np. F.H. CATE, *Privacy in the Information Age*, Waszyngton 1997, s. 6 i n. Można zauważyć, iż zbliżone, krytyczne stanowisko na temat braku koherencji między prawem stanowionym a rozwojem technologicznym zajął *de facto* Europejski Trybunał Sprawiedliwości w sprawie Bodil Lindqvist przeciwko Szwecji (orzeczenie C-101/01 dostępne na stronie internetowej http://www.ictlex.net?index.php/2003/11/06/eu-court-ot-justic-dec-c-101-01/).

kretne dane, w jakich celach, w jaki sposób i w jakim zakresie dane są przetwarzane, czy są one przekazywane jakimkolwiek odbiorcom (z ich wskazaniem lub co najmniej wskazaniem ich kategorii)[16].

Należy wszak odnotować, iż unijna – regulacja ochrony danych dąży do realizacji dwóch celów: (i) zapewnienia swobodnego przepływu danych osobowych w ramach wspólnego rynku oraz (ii) zagwarantowania odpowiedniego poziomu bezpieczeństwa danych czy szerzej: prywatności osób, których dane dotyczą.

Osiągnięciu drugiego ze wskazanych celów służy między innymi, obok gwarancji instytucjonalnych (zwłaszcza prawa skierowania skargi do niezależnego organu ochrony danych), zapewnienie dostępu do informacji na temat przetwarzania danych osobowych na swój temat,

− sfera coraz powszechniejszego stosowania, także w miejscach publicznych, systemów bezpieczeństwa, w tym zwłaszcza telewizji przemysłowej (tzw. CCTV – *Closed-circuit Television*)[17].

Zdaniem autora niniejszego tekstu wskazana tutaj sfera zasługuje na szczegółową i dogłębną analizę prawną (tak na gruncie prawa wspólnotowego, jak i systemów krajów członkowskich, w tym Polski[18]),

---

[16] Por. w tym kontekście art. 32 ust. 1 pkty 1-5 Ustawy.

[17] Szeroko na ten temat pisze D. KELLEHER, *op. cit*., s. 417 i n.

[18] Warto dodać, iż coraz więcej miast w Polsce szczyci się faktem bycia „miastem monitorowanym" – tablice tego rodzaju można było spotkać w grudniu 2007 r. między innymi wjeżdżając do Poznania. W Warszawie na koniec grudnia 2007 r. liczbę kamer telewizji przemysłowej szacowano na ok. 5 tys., z czego 353 to kamery miejskie, a niemal drugie tyle – kamery zainstalowane w warszawskim metrze; na rok 2008 władze Warszawy zaplanowały instalację ok. 50 kolejnych kamer, na zakup których zarezerwowano niemalże 4 mln złotych (por. M. KOZUBAL, *Kamery wypatrzą każdego*, «Rzeczpospolita» z 20 grudnia 2007 r.). Na szczególną uwagę zasługuje w tym kontekście wypowiedź Michała Serzyckiego piastującego aktualnie funkcję GIODO, który zabrał głos w sprawie systemów telewizji przemysłowej instalowanych w szkołach mówiąc, iż jest „zwolennikiem monitoringu w szkołach, ale ... nie powinno się nagrywać rozmów uczniów. ... Ograniczenie prawa do prywatności musi być usprawiedliwione, a środki adekwatne do celów. Monitoring jest dozwolony także w innych miejscach (np. urzędach, zakładach pracy, hotelach itp.), ale zainteresowani muszą być o nim poinformowani, np. poprzez wywieszenie tabliczki «obiekt monitorowany»". (por. «Rzeczpospolita» z 20 listopada 2007 r.). Refleksje na poziomie unijnym w przedmiocie problematyki

− sfera zapewnienia ochrony danym przetwarzanym w zbiorach prowadzonych przy wykorzystaniu metod tradycyjnych (nie informatycznych).

Z obserwacji irlandzkiej praktyki wynika, że tego typu zbiory nadal są stosunkowo szeroko stosowane (zwłaszcza w sektorze publicznym), bywając lekceważonymi z perspektywy zapewnienia bezpieczeństwa przetwarzanych w nich danym.

Zagadnieniem o znaczeniu uniwersalnym (dotyczącym w odpowiednim stopniu każdej z wyżej przytoczonych sfer) jest problem zaniedbywania przez administratorów danych oraz podmioty, którym powierzono przetwarzanie danych, niezbędnej refleksji poprzedzającej rozpoczęcie przetwarzania danych osobowych. Znaczenie prawne decyzji o przetwarzaniu danych bywa niedoceniane, a sama decyzja podejmowana pochopnie. DPC zwrócił uwagę na następujące kluczowe aspekty przygotowania do zbierania (i dalszego przetwarzania) danych osobowych:

− ustalenie i zapewnienie przez administratora danych istnienia prawnej podstawy lub podstaw przetwarzania danych,

− precyzyjne ustalenie przez administratora danych celu przetwarzania danych osobowych,

− zapewnienie przez administratora danych należytego i pełnego (zgodnego z przepisami) poinformowania osoby, której dane dotyczą, o celach przetwarzania danych osobowych,

− dopełnienie przez administratora danych wymogu adekwatności przetwarzanych danych (czyli zapewnienie, aby zbierane były jedynie dane potrzebne w związku z realizacją celu zakomunikowanego osobie, której dane dotyczą),

− zapewnienie właściwego przeszkolenia osób zatrudnionych przy przetwarzaniu danych oraz opracowanie i wdrożenie procedur bezpie-

---

CCTV można znaleźć między innymi w dokumentach Grupy Roboczej ds. Ochrony Danych Osobowych powołanej na mocy art. 29 Dyrektywy, dostępnych w języku angielskim na stronach internetowych: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf (dokument WP 67 z 25 listopada 2002 r.) oraz http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp129_pl.pdf (dokument WP 129 z 9 stycznia 2007 r.).

czeństwa, które powinny między innymi zawierać wytyczne w zakresie postępowania w razie stwierdzenia naruszenia zabezpieczeń danych.

Poprawne ukonstytuowanie przez administratora danych wskazanych wyżej elementarnych aspektów przetwarzania danych osobowych przesądza w znacznej mierze o poprawności całego procesu przetwarzania danych. Z tego też powodu DPC zachęca potencjalnych administratorów danych do konsultowania z jego biurem owej fazy koncepcyjnej (zgodnie z przyjętą przez DPC regułą *free and friendly consultancy* – na temat zasad działania organu ochrony danych w Irlandii napisano poniżej).

Na etapie dalszego przetwarzania danych DPC akcentuje w swych wytycznych między innymi konieczność: (I) zapewnienia przez administratora danych prawdziwości i aktualności danych, (II) zagwarantowania realnego dostępu do własnych danych osobie, której one dotyczą i udzieleniu tej osobie wszelkich wymaganych prawem informacji, (III) opracowania i stosowania przez administratora danych stosownej polityki postępowania, w tym polityki przechowywania i usuwania zbędnych danych (co służy między innymi zapewnieniu aktualności danych).

Naturalnie nie sposób nie dostrzec podobieństwa wymienionych powyżej zaleceń wynikających z *Data Protection Acts* z rekomendacjami GIODO czerpiącymi źródło w Ustawie[19].

Jednakże, jak się okazuje, sposób implementacji Dyrektywy i interpretacja przyjętych na jej podstawie aktów prawnych mogą się poważnie różnić. Dotyczy to niekiedy zagadnień fundamentalnych, na przykład definicji pojęcia „danych osobowych". DPC opowiada się za stosunkowo szerokim rozumieniem tego pojęcia (odnosząc je jednakże, co narzuca literalne brzmienie *Data Protection Acts*, jedynie do osób żyjących). Bardzo istotne wątpliwości pojawiają się przy tym na gruncie ustawodawstwa i judykatury brytyjskiej oraz ich ewentualnego wpływu na praktykę stosowania prawa w Irlandii. Brytyjska ustawa o ochronie danych osobowych (*Data Protection Act 1998*[20])

[19] Uwaga ta dotyczy zwłaszcza norm art. 24-26 Ustawy.

[20] Tekst *Data Protection Act 1998* dostępny jest na poniższej stronie internetowej:

stanowi jednoznacznie, podobnie jak czynią to *Data Protection Acts*, a inaczej niż Dyrektywa oraz Ustawa, iż dane osobowe to informacje dotyczące osób żyjących, przy czym zawierają one opinię [pokreślenie autora] na temat jednostki (osoby, której dane dotyczą) i wyrażają intencję [pokreślenie autora] kontrolera danych (lub innej osoby) w stosunku do tejże jednostki[21].

Na tym znaczeniowym zawężeniu omawianego pojęcia w stosunku do Dyrektywy oparł swoje orzeczenie angielski Sąd Apelacyjny (*Court of Appeal*) w sprawie Durant przeciwko Financial Services Authority. W irlandzkiej literaturze wyrażono stanowisko, iż brzmienie brytyjskiej ustawy i jej interpretacja dokonana przez Sąd Apelacyjny jest niezgodna z duchem Dyrektywy i orzecznictwem Europejskiego Trybunału Sprawiedliwości (idzie zwłaszcza o powoływane już w niniejszym tekście rozstrzygnięcie ETS w sprawie Bodil Lindqvist przeciwko Szwecji), wobec czego nie powinny wpływać na rozstrzygnięcia sądów irlandzkich. Wskazuje się jednocześnie, iż irlandzki DPC jednak w niektórych swych decyzjach sięga do powołanego kontrowersyjnego orzeczenia brytyjskiego Sądu Apelacyjnego[22].

V. DPC – WYBRANE ASPEKTY PRAKTYKI FUNKCJONOWANIA IRLANDZKIEGO ORGANU OCHRONY DANYCH OSOBOWYCH

W niniejszej części artykułu autor skupia uwagę na wybranych aspektach funkcjonowaniu irlandzkiego organu ochrony danych osobowych.

---

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

[21] Sekcja 1(1) brytyjskiej *Data Protection Act 1998* stanowi, iż: "personal data" means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

[22] Szerzej tę kwestię opisuje D. KELLEHER, *op. cit*., s. 137-139.

Na wstępie godzi się odnotować doniosłą rolę, jaką irlandzcy autorzy przypisują DPC (według D. Kellehera, DPC większy wpływ na życie społeczno-ekonomiczne Irlandii niż np. organ ochrony konkurencji[23]).

DPC, podobnie jak GIODO, pełni następujące zasadnicze funkcje[24]:

- funkcję doradczą i edukacyjną, sprowadzające się do propagowania wiedzy o zasadach ochrony danych osobowych, prawach osób, których dane dotyczą oraz rozpowszechniania dobrych praktyk w dziedzinie ochrony danych osobowych,
- funkcję reprezentowania i ochrony interesów osób, których dane są przetwarzane.

Wykonując tę funkcję DPC w szczególności rozstrzyga spory między administratorami danych i podmiotami, którym powierzono przetwarzanie danych z jednej strony a osobami, których dane dotyczą z drugiej. W zakresie powołanej tu kompetencji DPC mieści się w szczególności rozpoznawanie skarg i wniosków obywateli dotyczących przetwarzania ich danych osobowych,

- funkcję 'strażnika' przestrzegania norm ochrony danych przez administratorów danych i podmioty, którym powierzono przetwarzanie danych (*enforcer role*).

Tę funkcję DPC pełni między innymi wydając decyzje na przykład nakazujące wprowadzenie stosownych modyfikacji do stosowanych przez administratorów danych procedur przetwarzania danych czy decyzje zakazujące określonego sposobu przetwarzania danych przez poszczególnych administratorów,

- funkcję rejestrową, polegającą na prowadzeniu jawnego rejestru zbiorów danych osobowych w Irlandii.

Nie sposób nie zauważyć, iż funkcje i zadania stawiane przed DPC są praktycznie identyczne z funkcjami i zadaniami GIODO[25].

---

[23] D. KELLEHER, *op. cit*. s 351.

[24] Godzi się dodać, iż DPC jest w Irlandii powoływany przez rząd, podczas gdy w Polsce GIODO jest powoływany przez Sejm za zgodą Senatu, co zdaje się być rozwiązaniem gwarantującym większą niezależność i autonomię organu od bieżącej polityki.

[25] Por. zwłaszcza art. 12 Ustawy.

Warto przy tej okazji zwrócić uwagę na funkcje doradcze i edukacyjne, do których DPC przykłada szczególną wagę podkreślając konieczność pragmatycznego podejścia do problematyki ochrony danych osobowych oraz akcentując, iż z perspektywy DPC zdecydowanie łatwiej, taniej i efektywniej jest zapobiegać ewentualnym uchybieniom, które mogą pojawić się w procesie przetwarzania danych, niż władczo eliminować utrwalone już nieprawidłowości. Taka postawa stanowi realizację zasady darmowej i przyjaznej pomocy udzielanej przez DPC na rzecz podmiotów zainteresowanych (powołana już wyżej zasada *free and friendly consultancy*).

Z tego powodu DPC stanowczo zachęca administratorów danych oraz podmioty, którym powierza się przetwarzanie danych osobowych, do konsultowania z DPC rozwiązań służących ochronie danych już na etapie ich wdrażania (por. też uwagi powyżej na ten temat). DPC deklaruje gotowość do dialogu między innymi z przedsiębiorcami w celu ułatwienia im przyjmowania takich rozwiązań w dziedzinie ochrony danych osobowych, które zapewniając bezpieczeństwo danym będą zgodne z prawem i nie będą w przyszłości kwestionowane przez DPC.

Kierując się tymi przesłankami w biurze DPC działa komórka porad (*help desk*) konsultująca miedzy innymi sprawy zgłaszane anonimowo; pytania do *help desk* mogą być kierowane pisemnie, telefonicznie oraz drogą mailową. Wnioski wysnute przez DPC z sygnalizowanych problemów oraz wyjaśnienia DPC są publikowane na stronie internetowej tego organu[26]. Należy podkreślić, iż irlandzki ustawodawca w przepisach *Data Protection Acts* zobowiązał DPC do sprawowania swej funkcji w sposób promujący w społeczeństwie postawy i zachowania zgodne z *Data Protection Acts* [27].

[26] Podobną praktykę stosuje GIODO, którego strona internetowa może uchodzić w przekonaniu autora niniejszego tekstu za jedną z najlepszych witryn internetowych polskiej administracji. Na temat działalności doradczej i edukacyjnej GIODO więcej można przeczytać m.in. w powoływanych rocznych Sprawozdaniach GIODO z działalności, dostępnych na stronie http://www/giodo.gov.pl.

[27] Art. 13(1) (c) *Data Protection Acts*.

Dla lepszej ilustracji praktyk podejmowanych przez DPC warto dodać, iż w samym roku 2003 DPC i jego zespół przeprowadził około 70 prezentacji popularyzujących dziedzinę ochrony danych osobowych wśród podmiotów z sektora prywatnego i publicznego[28]. DPC nierzadko sięga do nietuzinkowych sposobów dotarcia do społeczeństwa w celu popularyzacji wiedzy o zasadach ochrony danych osobowych. Między innymi, według opisów B. Hawkesa, urzędnicy DPC występują w audycjach radiowych i telewizyjnych, uczestniczą w konferencjach[29], targach i pokazach organizowanych dla różnorodnych środowisk, w tym biznesowych, organizują konkursy (z nagrodami pieniężnymi!) dla studentów, w których tematy dotyczą zagadnień ochrony danych osobowych i ochrony prywatności.

Podsumowując ten wątek można stwierdzić, iż DPC zarówno inicjuje działania w zakresie ochrony danych wytyczając pożądane standardy w tej dziedzinie, jak i reaguje na sygnalizowane problemy, starając się je rozwiązywać i naświetlać pożądane kierunki działań angażując do współpracy środki masowego przekazu.

Rzecz jasna, jak napisano wyżej, działalność edukacyjna, doradcza i popularyzatorska nie wyczerpuje pól aktywności DPC. Obok tej sfery DPC zajmuje się w szczególności rozpatrywaniem bieżących skarg w zakresie przetwarzania danych osobowych oraz prowadzi postępowania kontrolne i wyjaśniające. Poniższe dane ilustrują aktywność DPC w tej dziedzinie. W roku 2006 DPC odnotował około 600 skarg obywateli (w porównaniu z około 300 skargami w roku 2005). Do końca zaś października 2007 do DPC wpłynęło blisko 900 skarg.

Interesująco kształtuje się tematyka skarg. W roku 2006 45% skarg dotyczyło sfery marketingu bezpośredniego (w tym głównie telemarketingu prowadzonego przez nowych operatorów telekomunikacyjnych), 28% skarg – prawa dostępu osób, których dane dotyczą, do swoich danych, 11% skarg – nieuprawnionego ujawnienia danych, 5% – braku adekwatności i aktualności przetwarzanych danych, pozostałe 11% skarg – innych kwestii.

[28] Dane za D. KELLEHEREM, *op. cit*., s. 333.

[29] Potwierdzeniem tego jest udział B. Hawkesa w dublińskiej konferencji.

Inaczej wyglądają dane statystyczne dotyczące skarg trafiających do DPC w roku 2007. Na czoło pod względem liczby wysuwają się skargi odnoszące się do realizacji prawa dostępu do treści swych danych. Dalsza duża część skarg trafiających do DPC w roku 2007 dotyka sfery marketingu smsowego, stanowiącego nową formę docierania przez przedsiębiorców do klientów lub potencjalnych klientów[30].

Dla porównania można dodać, iż w Polsce w roku 2006 do GIODO trafiło 712 skarg w przedmiocie naruszeń przepisów o ochronie danych osobowych, przy czym skargi dotyczące przetwarzania danych z wykorzystaniem Internetu znalazły się – wg kryterium liczby skarg – na miejscu 6, a skargi odnoszące się do przetwarzania danych w związku z działalnością marketingową – dopiero na miejscu 7[31].

Warto zwrócić w tym miejscu uwagę, iż DPC jest uprawniony do nakładania grzywny do 100 000 EURO. Należy przy tej okazji wspomnieć o rozważanej nowelizacji polskich przepisów w celu umożliwienia GIODO nakładania sankcji finansowych za naruszenia Ustawy[32]. W tym kontekście ciekawa jest opinia B. Hawkesa, który akcentował, iż to nie sankcje administracyjne, finansowe czy wreszcie karne są w praktyce najdotkliwsze dla naruszycieli przepisów o ochronie danych osobowych z sektora prywatnego. Najdotkliwszą jest utrata reputacji (w Irlandii i Wielkiej Brytanii na przestrzenie ostatnich lat doszło do kilku spektakularnych spraw o naruszenie bezpieczeństwa danych osobowych, nagłośnionych przez media; dotyczy to np. sprawy kradzieży danych posiadaczy kart kredytowych w sieci sklepów TK Maxx[33]).

---

[30] Wydaje się, że w Polsce problem marketingu smsowego zaczyna się dopiero pojawiać.

[31] Doroczne Sprawozdanie z działalności GIODO w roku 2006, *op. cit*., s. 21 i 22.

[32] Por. prezydencki projekt ustawy (z 21 grudnia 2007 r.) o zmianie ustawy o ochronie danych osobowych, dostępny wraz z uzasadnieniem na stronie internetowej http://orka.sejm.gov.pl/Druki6ka.nsf/0/1C375B9EBAEAA9EAC12574420044A07F/$file/488.pdf, oraz publikację w dzienniku «Rzeczpospolita» z 11 grudnia 2007 r.

[33] Por. na ten temat m.in. na stronie internetowej http://news.independent.co.uk/uk/legal/article2408006.ece.

Podsumowując czynione w tym miejscu wywody można sformułować wniosek, że DPC konsekwentnie dąży w szczególności do utrwalenia swego wizerunku jako organu przyjaznego obywatelom, gotowego do dialogu tak z osobami, których dane dotyczą, jak i administratorami danych oraz podmiotami, którym powierzono przetwarzanie danych osobowych[34].

Na zakończenie warto dodać, iż DPC jest uprawniony do inicjowania, opracowywania, opiniowania i zatwierdzenia kodeksów dobrych praktyk regulujących postępowanie w dziedzinie ochrony danych, tworzonych przez organizacje biznesowe i inne gremia zrzeszające administratorów danych czy podmioty, którym powierzono przetwarzanie danych (*codes of conduct, codes of practice*). Kodeksy tego rodzaju mają dodatkowo wesprzeć administratorów danych oraz podmioty, którym powierzono przetwarzanie danych, w zapewnieniu należytej ochrony danym osobowym. Oczywiście, kodeksy te nie mogą być sprzeczne z normami prawa powszechnie obowiązującego w Irlandii[35].

VI. UWAGI KOŃCOWE

Z powyższych spostrzeżeń wyłania się szkic systemu ochrony danych osobowych w Irlandii.

Nie można nie dostrzec istotnych podobieństw z regulacją i praktykami panującymi w tej dziedzinie w Polsce. Dają się jednocześnie zauważyć pewne odmienności i różne akcentowanie poszczególnych kwestii we wskazanych krajach – dotyczy to przede wszystkim różnic w przyjętych założeniach bieżącego funkcjonowania organów ochrony danych osobowych (podkreślane przez DPC znaczenia profilakty-

[34] Prowadzenie przez DPC przyjaznej polityki potwierdza fakt, iż na oficjalnej stronie internetowej DPC, wobec występowania w Irlandii dużej grupy przyjezdnych z Polski, Czech i Słowacji, podstawowe informacje dotyczące instytucji ochrony danych osobowych przedstawione są także w tych trzech językach (por. stronę internetową http://www.dataprotection.ie).

[35] D. KELLEHER, *op. cit.*, s. 330 i n. wskazuje jednak na znikome zainteresowanie tworzeniem takich kodeksów. Mimo to wydaje się, iż rzeczone kodeksy w przyszłości mogą odegrać istotną rolę w samoregulacji dziedziny ochrony danych osobowych.

ki i działań edukacyjno-zapobiegawczych wobec przejawianego przez GIODO w praktyce nacisku na następcze działania kontrolne). Silnie zarysowuje się kwestia problemów wymagających pogłębionej analizy – dotyczy to między innymi stosowania telewizji przemysłowej w aspekcie przepisów o ochronie prywatności (por. uwagi na temat *CCTV*) czy też – na gruncie prawa polskiego – problemu stosowania Ustawy w odniesieniu do danych osób zmarłych. Powraca także temat jakości i sposobu implementacji unijnych dyrektyw (por. uwagi na temat różnic w pojmowaniu pojęcia danych osobowych).

Wysnuć można wreszcie dalszy, zasadniczy wniosek: akademicki i orzeczniczy dorobek w dziedzinie ochrony danych osobowych w Polsce nie jest rażąco mniejszy czy uboższy od dorobku irlandzkiego, mimo iż przepisy o ochronie danych osobowych obowiązują w Irlandii dokładnie 10 lat dłużej niż w Polsce (naturalnie początkowo nie były te przepisy bazujące na Dyrektywie), a Irlandia ma na przykład wyjątkowo bogate doświadczenia praktyczne w zakresie przekazywania danych osobowych do państw trzecich, w tym do Stanów Zjednoczonych (co wynika z gospodarczej funkcji realizowanej na przestrzeni ostatnich lat przez Irlandię, występującą w charakterze swoistej forpoczty amerykańskiej gospodarki w Europie; dotyczy to między innymi usług świadczonych przez irlandzkich przedsiębiorców na rzecz amerykańskich partnerów w systemie BPO – *Business Processing Offshoring / Outsourcing*).

Jednocześnie, obserwując irlandzkie i brytyjskie doświadczenia warto zadać pytanie o to, w jakim kierunku zmierza praktyka ochrony danych osobowych w Polsce, w tym zwłaszcza wobec postępującej globalizacji przepływów danych osobowych oraz identyfikowanych kolejnych problemów praktycznych wynikających przede wszystkim z bezprecedensowego rozwoju technologii i związanych z tym zagadnień prawnych.

Personal Data Protection in Ireland

Summary

The article is a short review of the personal data protection system in the Republic of Ireland. The review is made in the light of the Polish Data Protection Act of 1997 and Directive 95/46/EC (sections I and II).

The introductory parts (sections I and II) include general remarks on the increasing importance and value of privacy and personal data. This increase results, among other things, from rapid development of the Internet and modern data processing and mining measures.

Subsequently, in section III, the author discusses the constitutional environment of privacy and personal data protection rules in Ireland, as well as the role of court precedents and Directive 95/46/EC in this respect.

Next part of the article (section IV) is dedicated to practical data protection issues identified and discussed by Irish authors, including specific exposures as well as differences between definitions in the Irish Data Protection Acts 1988-2003 and the UK Data Protection Act 1998, and influence of the latter (UK) Act on the Irish Data Protection Commissionaire's decision-making process.

Further comments (section V) focus on Data Protection Commissionaire's rights and obligations (including in particular comments on the Data Protection Commissionaire's *free and friendly consultancy policy*).

The conclusion (section VI) briefly and synthetically summarizes similarities and differences between Irish and Polish personal data protection rules and practices, stressing issues requiring the European-wide common approach (e.g. in the fields of basic definitions or CCTV legal issues).

Finally, the author observes that Polish authors' reflections on personal data protection and the Polish practice are not inferior to the Irish ones even though Irish regulations have been in place for 10 years longer than the Polish ones.