

**Ochrona danych osobowych
wczoraj, dziś, jutro**

**Personal Data Protection
Yesterday, Today, Tomorrow**

Warszawa 2006

Preparation:
Biuro Generalnego Inspektora
Ochrony Danych Osobowych

©Copyright 2005 by: **Biuro Generalnego Inspektora
Ochrony Danych Osobowych**

ISBN 83-913680-3-3

Editor's address:
Biuro Generalnego Inspektora Ochrony Danych Osobowych
00-193 Warszawa, ul. Stawki 2
www.giodo.gov.pl
kancelaria@giodo.gov.pl
tel.: (0-22) 860 70 81
fax: (0-22) 860 70 86

Printing production (composition, typesetting, print):
Printing house: Oficyna Wydawnicza Rem Script Sp. z o.o.
02-026 Warszawa, ul. Raszyńska 15 lok. 50
tel./fax: (0-22) 825 54 19

SPIS TREŚCI (TABLE OF CONTENTS)

WPROWADZENIE (INTRODUCTION)

Małgorzata Kałużyńska-Jasak 5

REFERATY (CONTRIBUTIONS)

Ewa Kulesza 7

Reijo Aarnio 16

Emilio Aced-Félez 40

Bogusław Banaszak, Krzysztof Wygoda 59

Alfred Büllsbach 77

Alexander Dix 93

Hansjürgen Garstka 99

Małgorzata Gersdorf 115

Billy Hawkes 122

Peter J. Hustinx 132

Małgorzata Jaśkowska 143

Monika Krasińska 168

Christopher Kuner 174

Peter Lieskovský 184

Vaida Linartaite 210

Czesław Martysz	229
Andrzej Mączyński	242
Peter Michael	257
Philippos Mitletton	269
Igor Němec	290
Karel Neuwirt	303
Michel Parisse	315
Attila Péterflavi	326
José Luis Piñar Mañas	337
Francesco Pizzetti	358
Marek Safjan, Katarzyna Berwid-Wilińska	371
Peter Schaar	398
Luís Lingnau da Silveira	404
Dorota Skolimowska	413
Richard Thomas	421
Alex Türk	436

Szanowni Państwo,

idea tej książki zrodziła się z potrzeby podsumowania ważnego, z punktu widzenia problematyki ochrony danych osobowych okresu, jakim jest zakończenie ośmioletniej działalności pierwszego w Polsce organu do spraw ochrony danych osobowych i stosowania uchwalonej po raz pierwszy, w polskim systemie prawnym, ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych.

Upływ drugiej i ostatniej, zgodnie z polskim prawem, kadencji Generalnego Inspektora Ochrony Danych Osobowych – dr Ewy Kuleszy, powołanej przez Sejm RP na to stanowisko w dniu 4 kwietnia 1998 r., dał asumpt do dokonania zawartych w publikacji podsumowań i refleksji.

Swoimi przemyśleniami i doświadczeniem dzielą się w książce najwybitniejsi znawcy przedmiotu, teoretycy i praktycy, autorytety z zakresu ochrony prywatności i danych osobowych, autorzy z różnych państw Europy. Najważniejsze pytanie, jakie stawiają, brzmi: czy obecny poziom ochrony jest wystarczający, czy nie idziemy na zbyt duże ustępstwa w imię respektowania innych demokratycznych praw – prawa do informacji, bezpieczeństwa publicznego czy wolności słowa. Czy w świecie gwałtownego rozwoju nowych technologii, w świecie Internetu, wszechobecnych kamer, systemów RFID i GPS, globalnego przepływu informacji, totalnego wścibstwa, a przede wszystkim – zagrożenia terroryzmem, w całej tej dynamicznie zmieniającej się rzeczywistości, jest jeszcze miejsce na, choć trochę intymności, tak potrzebnej każdemu człowiekowi?! Jak pogodzić korzystanie ze zdobyczy techniki ułatwiających codzienne życie – z prawem do ochrony danych? Czy zbyt łatwe i skomercjalizowane ujawnianie prywatności, nie zagraża prawu do godnego życia?

Książka jest zbiorem rozważań nad dzisiejszymi i przyszłymi problemami ochrony prywatności w ogóle. Jest jednocześnie wyrazem uznania dla dokonań polskiego Generalnego Inspektora Ochrony Danych Osobowych i świadectwem jego roli w wyznaczaniu ram i tworzeniu zasad stosowania ustawy nie tylko w Polsce. Generalny Inspektor inicjował wiele przedsięwzięć i był promotorem międzynarodowych ustaleń i deklaracji, które znacząco wpłynęły na poprawę standardów ochrony danych osobowych. Wniósł też nowe i świeże spojrzenie na wiele problemów, czym na trwałe wpisał doświadczenia Polski w historię międzynarodowej ochrony danych i prywatności.

Suma pierwszych dwóch kadencji Generalnego Inspektora Ochrony Danych Osobowych jest optymistyczna. Badania potwierdzają obserwację, że przepisy ustawy o ochronie danych osobowych zakorzeniły się w świadomości Polaków, coraz rozleglejsza jest wiedza o prawach związanych z ochroną danych. Wzrasta też poczucie bezpieczeństwa danych i można zaryzykować twierdzenie, że w tej materii w Polsce jest już tak, jak w krajach o znacznie dłuższych tradycjach demokratycznych.

Serdecznie dziękuję, jako redaktor tego wydawnictwa, wszystkim osobom, które pozytywnie odpowiedziały na prośbę zaprezentowania w tej formie swoich doświadczeń i opinii. Uczyniły one książkę, która bilansuje osiem lat pierwszego w Polsce Generalnego Inspektora Ochrony Danych Osobowych, dr Ewy Kuleszy – inspirującym kompendium w przedmiocie ważnym dla rozwoju demokracji.

Małgorzata Kałużyńska-Jasak

Rzecznik Prasowy Generalnego Inspektora
Ochrony Danych Osobowych, Polska

Ladies and Gentlemen,

The idea to publish this book was born from the need to sum up a very important period from the point of view of data protection. It is the eight year long period of the activity of the first Inspector General for the Protection of Personal Data in Poland and of the application of the first data protection law in the Polish system – the Personal Data Protection Act as of 29 August 1997.

The expiration of the second and the last, according to the Polish law, term of office of the Inspector General for the Protection of Personal Data – Ewa Kulesza Phd, appointed by the Parliament of the Republic of Poland on 4 April 1998, inspired summaries and reflections included in this publication.

The most eminent experts and theoreticians in the field of data protection and privacy as well as those who enforce data protection and privacy rules, authors from different European countries share their thoughts and experience. The most important question that they ask is the following: is the present level of protection sufficient, are we not making too many concessions for the sake of respecting other democratic rights – the right to information, public security or freedom of speech. Do the contemporary world with a rapid growth of modern technologies, with the Internet, omnipresent cameras, RFID and GPS systems, global flow of information, constant meddling and above all with the threat of terrorism, and this dynamically changing reality allow some privacy, that human beings need so much?! How can we reconcile the use of techniques that make our daily life so much more easy with the right to the protection of personal data? Isn't the right to life in dignity threatened by easy and commercialised disclosure of privacy?

This book is a collection of reflexions about contemporary and future problems related to the privacy protection in general. It also expresses recognition for the work of the Polish Inspector General for the Protection of Personal Data and the testimony to the Inspector's role in the definition of the framework and the creation of rules for the application of the Act not only in Poland. The Inspector General initiated many activities and promoted many international arrangements and declarations, which helped improve the personal data protection standards. The Inspector General also proposed a new and fresh attitude towards many problems and thus made Polish experience go down in the international history of personal data and privacy protection.

The summary of the first two terms of office of the Inspector General for the Protection of Personal Data is optimistic. The research confirms that the provisions of the Personal Data Protection Act have instilled in the conscience of the Poles. The knowledge about data protection rights is spreading. The feeling of data security is growing and we may even say that in this field, in Poland, the situation is similar to the situation in countries with longer democratic traditions.

As the editor of this publication I would like to thank all those who positively responded to the request of presenting their experience and views in this way. Thus, this book which sums up the eight years of work of the first Inspector General for the Protection of Personal Data in Poland, Ewa Kulesza Ph.D., is an inspiring compendium in the field and very important for the development of democracy.

Małgorzata Kałużyńska-Jasak

Spokesman for the Inspector General for
Personal Data Protection, Poland

Dr Ewa Kulesza

Generalny Inspektor Ochrony Danych Osobowych, Polska
Inspector General for Personal Data Protection, Poland

Kilka uwag o przetwarzaniu danych osobowych pracowników przez pracodawcę – regulacje obowiązujące i uwagi *de lege ferenda*

Wstęp

Jednym z zagadnień żywo dyskutowanych w polskiej literaturze prawniczej jest zakres danych osób zatrudnionych przetwarzanych przez pracodawcę. Nie są to dyskusje czysto dogmatyczne, ale podyktowane wątpliwościami zgłaszanymi przez pracodawców, zwłaszcza w kontekście sformułowanego w art. 22¹ kodeksu pracy (powoływanego dalej jako k.p.) wykazu danych, których pracodawca może żądać od pracownika. Rozwój techniki i możliwość wykorzystywania także innych danych osobowych pracowników sprawia, że coraz aktualniejszy staje się wniosek o jasne określenie w przepisach prawa zakresu, oraz sposobu pozyskiwania danych pracowników przez pracodawców.

1. Zgodnie z powoływanym przepisem k.p. pracodawca ma prawo żądać od pracownika podania imienia (imion) i nazwiska, imion rodziców, daty urodzenia, miejsca zamieszkania (adresu do korespondencji), informacji o wykształceniu oraz informacji o przebiegu dotychczasowego zatrudnienia. Ponadto także innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy oraz numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL). Przepis zezwala także na prawo żądania przez pracodawcę innych danych osobowych, jeżeli obowiązek ich podania wynika z odrębnych przepisów (art. 22 § 4 k.p.).

Przedstawienie wszystkich, różnej rangi przepisów, które dają podstawę do żądania danych pracownika wymagałoby szerszego opracowania. Warto jedynie podkreślić, iż z uwagi na wymogi stawiane przez ustawę o ochronie danych osobowych,¹ która w przypadku danych szczególnie chronionych zezwala ich przetwarzanie wyłącznie w oparciu o podstawę ustawową,² niezbędne jest istnienie takiej ustawowej regulacji, aby praco-

¹⁾ Ustawa z dnia 29 sierpnia 1997 r.; tj. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.

²⁾ W odniesieniu do danych przetwarzanych przez pracodawcę wymóg ten jest podwójnie podkreślony. Art. 27 ust.2 ustawy o ochronie danych osobowych, mimo ogólnej przesłanki zezwalającej na przetwarzanie danych szczególnie chronionych w postaci art. 27 ust. 2 pkt 2 ustawy, który mówi: „przepis szczególnie innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą (...)”, dopuszcza w ust. 2 pkt 6 tego samego przepisu przetwarzanie danych szczególnie chronionych, jeśli to „(...) jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzania danych jest określony w ustawie”.

dawca mógł żądać od pracowników danych zaliczanych do tej kategorii. Przykładem w tym zakresie mogą być choćby zasady uzyskiwania przez pracodawców danych o karalności pracownika (kandydata na pracownika). Ustawa o Krajowym Rejestrze Karnym³ w art. 6 wyraźnie wskazuje, iż dane z Rejestru udostępnia się pracodawcom, w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnień do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej.⁴

2. Wskazany przepis kodeksu pracy tworzy – wraz z przepisami innych aktów normatywnych – zamknięty katalog danych, które mogą być przetwarzane przez pracodawcę. Takie rozwiązanie, niewątpliwie chroni pracowników przed nadmierną ingerencją pracodawcy w sferę ich wolności i prywatności, poprzez niedopuszczenie do wymuszania danych innych, aniżeli te, o których zdecydował ustawodawca. I jakkolwiek istnienie owego zamkniętego katalogu danych rodzi określone problemy praktyczne, trudno byłoby obronić tezę, iż zakres danych osobowych pracowników można dowolnie rozszerzać wykorzystując np. zgodę pracownika, nawet potwierdzoną na piśmie. Pomijając fakt, iż decydująca w tym przypadku jest wola ustawodawcy,⁵ zawsze mogłyby powstać wątpliwości co do rzeczywistej dobrowolności zgody osoby zależnej od pracodawcy. Ponadto w przypadku dopuszczenia zgody jako przesłanki poszerzającej zakres danych, trudno wskazać granicę dopuszczalności przetwarzania danych. Zbieranie każdej kategorii danych pracodawca mógłby „przekonywująco” w – jego mniemaniu – uzasadnić, na co wskazują sprawy prowadzone przez Generalnego Inspektora.⁶ Nawet przetwarzanie danych genetycznych.

Z tego względu należy postulować nowelizację przepisów prawa pracy w celu jasnego określenia uprawnień i obowiązków pracodawców i pracowników wobec możliwości wykorzystania nowych rozwiązań technicznych w zakładach pracy. Zwłaszcza, że nowe rozwiązania techniczne są już wykorzystywane lub planowane przez niektórych pracodawców.

2. 1. Sprawą wymagającą klarownej regulacji prawnej jest nadzór nad pracownikami za pomocą kamer wideo. Wyraźnie należy zaznaczyć, iż kwestie te nie muszą, a nawet nie powinny być szczegółowo regulowane przepisami rangi ustawowej, jednak ustawa winna wskazywać generalne wskazówki, które powinny zostać uwzględnione w przepisach wykonawczych bądź w przepisach wewnątrzzakładowych określających organizację kontroli za pomocą kamer wideo,⁷ sposób wykorzystania danych, okresy ich prze-

twarzania, a przede wszystkim gwarancje zabezpieczenia praw pracowniczych, w tym prawa do godności i ochrony dóbr osobistych.

Przy tworzeniu owych ogólnych przepisów, jak też przy opracowywaniu szczegółowych, zakładowych rozwiązań celowe byłoby wykorzystanie roboczych dokumentów przygotowanych przez instytucje europejskie. Bowiem – ponieważ zagadnienie kontroli za pomocą kamer wideo stosunkowo dawno zostało zauważone i przeanalizowane przez instytucje europejskie – jakkolwiek nie powstał jeszcze żaden obowiązujący europejski akt normatywny, opracowane dokumenty robocze wyraźnie wskazują, jakie przesłanki powinny zostać uwzględnione przy tworzeniu zakładowej kontroli za pomocą kamer wideo. A problemów z kontrolą za pomocą kamer wideo jest sporo, na co wskazują skargi składane do Generalnego Inspektora często pokazujące, że prywatność pracowników i ich dobra osobiste nie są wartością szczególnie cenioną przez pracodawców, a czasem i przez związki zawodowe.

2.2. Niewątpliwie pilnego uregulowania wymaga wykorzystywanie danych biometrycznych pracowników. Także polscy pracodawcy w coraz szerszym zakresie i w celu kontroli pracowników, ale także np. w celu ochrony szczególnych stref w zakładzie pracy, sygnalizują potrzebę wykorzystywania danych biometrycznych pracowników, np. odcisków palców, zdjęć siatkówki oka, analizy głosu czy innych metod identyfikacji pracowników. O ile w przypadku kontroli punktualności, czy obecności w pracy pracowników można jeszcze wskazać inne, tradycyjne metody (wykonywanie kontroli przez osoby zajmujące się w zakładzie pracy sprawami pracowniczymi,⁸ to niewątpliwie zabezpieczenie szczególnych obszarów w zakładzie pracy musi odbywać się przy wykorzystaniu nowoczesnej techniki jako skuteczniejszej i bezpieczniejszej z punktu widzenia także ochrony danych osobowych.

Z formalnego punktu widzenia przetwarzanie takich danych pracowników jest niedopuszczalne. Dane biometryczne nie zostały bowiem wymienione w żadnych przepisach uprawniających pracodawcę do przetwarzania tego typu danych, nawet – jak wskazywano wcześniej – za zgodą pracownika. Z tego względu należałoby postulować wyraźne określenie w przepisach jakie dane biometryczne, pod jakimi warunkami i w jakich celach pracodawcy mogliby przetwarzać.

2.3. Wielce dyskusyjną sprawą jest poddawanie pracowników testom psychologicznym oraz badaniom poligraficznym. Sprawy te generalnie nie zostały uregulowane przepisami prawa pracy, jakkolwiek w niektórych przepisach szczególnych, np. określających status pracowniczy pracowników służb mundurowych, dopuszczona została możliwość przeprowadzenia badań poligraficznych pracowników.

Poddawanie takim badaniom pracowników, zwłaszcza zatrudnionych w sektorze prywatnym w coraz szerszym zakresie sprawia, że problem ten staje się problemem generalnym,⁹ mimo, iż są to metody kontroli pracowników głęboko wkraczające i ich

³⁾ Ustawa z 24 maja 2000 r. o Krajowym Rejestrze Karnym; Dz.U. z 2000 r., Nr 50 poz. 580.

⁴⁾ Należy zaznaczyć, iż ustawa o Krajowym Rejestrze Karnym powstała po wejściu w życie ustawy o ochronie danych osobowych i na skutek sygnalizacji kierowanych przez Generalnego Inspektora Ochrony Danych Osobowych do Parlamentu i Rządu o niespójności obowiązujących dotychczas przepisów w tym zakresie z ustawą o ochronie danych osobowych.

⁵⁾ Wyrok NSA z dnia 16 września 2004 r. sygn. akt OSK 340/04

⁶⁾ Np. w jednej ze spraw, zbieranie danych o przekonaniach religijnych pracowników pracodawca tłumaczył koniecznością „zapewnienia bezpieczeństwa” pracownikom wobec lokalizacji zakładu pracy w okolicy zamieszkałej przez wyznawców innej religii. W innej sprawie pracodawca żądając – obowiązkowo – informacji o przynależności związkowej pracowników, tłumaczył się koniecznością wykonywania w przyszłości obowiązków związanych z ochroną związkową w przypadku wypowiedzania umowy o pracę.

⁷⁾ Szczególnie cenna, do wykorzystania w polskich rozwiązaniach, jest sugestia eksperta Rady Europy i Komisji Europejskiej, autora wytycznych nt. kontroli za pomocą kamer wideo („Wytyczne w sprawie ochrony danych osobowych w związku z gromadzeniem i przetwarzaniem danych osobowych przy pomocy video nadzoru”) – G. Buttarelliego, który wskazał na celowość wspólnego opracowywania przez pracodawcę i przedstawicieli pracowników (związki zawodowe, samorząd pracowniczy) zasad wprowadzenia kontroli wideo w zakładzie pracy.

⁸⁾ Jakkolwiek wskazywanie pracodawcy, iż w XXI wieku powinien zdać się na metody XIX-wieczne przypomina zwalczanie postępu technicznego poprzez niszczenie maszyn parowych w XVIII wieku w Anglii.

⁹⁾ Jak wynika chociażby z publikacji w Gazecie Prawnej (z 13 marca b.r.), badaniom na wykrywaczu kłamstw poddaje się pracowników traktując to jako sposób weryfikacji kandydatów do pracy, a także jako sposób wykrywania przestępstw popełnianych w zakładzie pracy.

prywatność, a nawet intymność, co już stanowi naruszenie kodeksu pracy nakazującego pracodawcy ochronę dóbr osobistych pracowników. Zaniepokojenie budzi fakt, iż takie postępowania pracodawców nie znajdują stanowczego potępienia ze strony Państwowej Inspekcji Pracy oraz związków zawodowych, które to instytucje akceptują pozorną legalizację działań pracodawców poprzez uzyskiwanie zgody pracowników na poddanie się badaniom. Takie stanowisko, wskazujące na legalizację poddawania pracowników badaniom w drodze testów psychologicznych oraz na poligrafie prezentowane jest także przez niektórych przedstawicieli nauki, mimo, iż – jak wcześniej wspomniano – zawsze istnieją wątpliwości co do dobrowolności zgody pracownika.

Także z tego względu kwestia poddawania pracowników testom wymaga wyraźnego dopuszczenia, albo zakazu w przepisach prawa.

2.4. Kodeks pracy winien wyraźnie zakazywać przetwarzania przez pracodawcę danych genetycznych pracownika, jak też informacji pochodzących z badań genetycznych, chyba, że takie badania lub ich wyniki byłyby niezbędne dla dopuszczenia do wykonywania ściśle określonych, wyraźnie wskazanych przez ustawodawcę zawodów lub celów.

Należy pamiętać, że przetwarzanie danych genetycznych może służyć dla ochrony zdrowia pracowników ze względu na szczególny charakter i funkcje stanowiska pracy bądź też jeśli badania genetyczne stanowiłyby konieczny warunek dla ochrony zdrowia i bezpieczeństwa tych pracowników lub innych osób.

W projektach dokumentów europejskich, dotyczących ochrony danych osobowych pracowników przetwarzanych w kontekście zatrudnienia wyraźnie wskazuje się, że uprawnienie pracodawcy do przetwarzania informacji z badań genetycznych pracowników jest dopuszczalne pod określonymi warunkami. Dopuszcza się takie badania wówczas, gdy m.in. wcześniejsza kontrola, uwzględniająca wszystkie okoliczności, w tym jakość testów, istotę i wiarygodność wyników oraz konieczność osiągnięcia równowagi pomiędzy interesem publicznym a wolnością osób poddanych badaniom wskazuje, że istnieją poważne przesłanki, a zwłaszcza interes publiczny w postaci np. poważnego i pewnego ryzyka dla zdrowia i bezpieczeństwa osób trzecich, zwłaszcza jeśli bezpieczeństwo jest sprawą zasadniczą – przemawia to za przeprowadzaniem takich testów. Znaczącym warunkiem oceny jest także potwierdzenie, iż brak jest innego środka dla osiągnięcia oczekiwanego wyniku.

W sytuacji dopuszczenia badań genetycznych przepisami prawa, w wyjątkowych, określonych tymi przepisami przypadkach, konieczne byłoby zastrzeżenie, takie, jakie mamy już w polskich przepisach w odniesieniu do danych o stanie zdrowia, iż pracodawca byłby informowany jedynie o istnieniu bądź nie przeciwwskazań dla zatrudnienia osoby lub przystosowania miejsca pracy, natomiast nie miałby prawa wglądu w dokumentację medyczną.

Wnioski

W powyższym, krótkim z założenia tekście, wskazane zostały jedynie niektóre, najważniejsze zagadnienia dotyczące zakresu przetwarzanych przez pracodawcę danych pracowników, wykorzystywanych w związku z zatrudnieniem, wymagające klarownego określenia w przepisach prawa pracy.

Niezręczne sformułowanie art. 22¹ k.p., bardzo wąsko określające zakres danych, których przetwarzanie przez pracodawcę jest dopuszczalne, a zwłaszcza nieuwzględnienie konieczności wykorzystania nowych rozwiązań technicznych sprawia, że przepis ten traktowany jest „z dystansem”. Brak stosownych regulacji prawnych, wyraźnego dozwolenia na przetwarzanie danych albo zakazu, bądź określenia warunków, pod jakimi pracodawca – zważywszy także na interes publiczny – mógłby pewne dane przetwarzać, prowadzi do sytuacji, że ani pracownicy nie są chronieni przed nadmierną ingerencją pracodawcy, ani pracodawca nie jest pewien, jakie instrumenty prawne może wykorzystywać i czy nie narazi się na zarzuty naruszenia prawa. A przecież fundament państwa demokratycznego jest i powinno być pewne, klarowne, gwarantujące prawo do prywatności i prawo do godności, ale także uwzględniające interes publiczny, ustawodawstwo.

Several remarks on the processing of personal data about employees by employers – current legislation and *de lege ferenda* remarks

Introduction

The scope of data about employees being processed by an employer is one of the issues that are discussed animatedly in the Polish legal literature. Those discussions are not only of a dogmatic nature but also motivated by employers' doubts, in particular in the context of the list of data that may be required from employee, laid down in Article 22¹ of the Labour Code. The rapid technological development and possibility to use also many other personal data about employee makes that a call for the clear determination of the scope and method of the collection of personal data about employees by employers in the legal provisions becomes more and more open.

1. According to the above-mentioned provision of the Labour Code, the employer has the right to demand from an employee to give his/her personal data including: name(s) and surname, parents' names, date of birth, place of residence (mailing address), education, professional career. Moreover, the employer may also demand other personal data of the employee, names and surnames and birth dates of the employee's children, if giving such data is necessary in connection to the fact that the employee enjoys special rights provided for in the labour law, the employee's PESEL number granted by the Government Computer Centre of the General Electronic Population Census System (RCI PESEL). Additionally the employer can demand the employee to give other personal data, if such obligation results from separate provisions (Article 22 § 4).

¹⁾ Act of 29 August 1997 (uniformed text: Journal of Laws of 2002, No 101, item 926 with amendments).

The presentation of all provisions of different rank which could justify requesting disclosing the data by the employee would require a broader analysis. It is only worth to stress that considering the requirements imposed by the Personal Data Protection Act¹ that allows to process the sensitive data only when the statutory basis exists,² it is necessary for the employer who wants to process such category of data to plead such basis (e.g. the principles of collection of criminal records about employee or job applicants by the employers). The Article 6 of the Act on the National Register of Convicted Persons³ clearly states that data contained in the Register may be disclosed to the employers in the scope which is necessary to employ an employer who – under the statutory provisions – shall not be convicted, shall enjoy public rights, and also for the purpose of establishing qualifications to take up given position or perform given job or carry out economic activity of given type.⁴

2. The mentioned provision of the Labour Code – together with other legislation – makes the closed catalogue of data which may be processed by the employer. Undoubtedly, such solution protects the employees from the excessive interference in their sphere of freedom and privacy as it does not allow extorting other data than those provided for by the legislator. Despite the fact that the existence of that closed catalogue causes particular problems in practice it would be hard to defend the thesis that the scope of personal data about employees may be voluntarily expanded (i.e. by the employee's consent which even proved in writing). Except the fact that the will of legislator shall be crucial in this case⁵ there always might be a doubt as to whether the consent of person who is depended upon the employer was really freely-given. Moreover, in the case where the consent would be acceptable as the prerequisite which expands the scope of data it would be hard to indicate the limit of the admissibility of personal data processing. The cases which the Inspector General dealt with indicate that the employer would convincingly (in his/her opinion) justify the collection of each category of data, including the processing of genetic data.⁶

For that reason, one should propose the amendment of the provisions of labour law in order to determine clearly the rights and obligations of the employers and employees as regards the possibility to use new technology in the workplace, considering in particular that such solutions are being used at present or are intended to be used by some employers.

²⁾ With reference to data being processed by the employer that requirement is stress twice. Article 27 paragraph 2 of Personal Data Protection Act, except for the general prerequisite which allows for the processing of sensitive data, namely Article 27 paragraph 2 point 2 of the Act which states that 'the provisions of other specific statute provide for the processing of such data without the data subject's consent'. Whereas, according to paragraph 2 point 6 of the said provision the processing may take place where 'it is necessary for the purposes of carrying the obligations of the controller with regard to employment of his/her employees and other persons, and the scope of processing is provided by the law'.

³⁾ The Act of 24 May 2000 on the National Register of Convicted Persons (Journal of Laws of 2000, No. 50, item 580).

⁴⁾ It should be stressed that the Act on the National Register of Convicted Persons was created after the entry into force of the Personal Data Protection Act, as a result of the addresses of the Inspector General for Personal Data Protection to the Parliament and Government concerning the incoherence between the provisions concerned which had been in force then with the Personal Data Protection Act.

⁵⁾ Judgement of the Supreme Administrative Court of 16 September 2004 (file number: OSK 340/04)

⁶⁾ For example, in one case the employer justified the collection of data revealing religious beliefs saying that it is necessary to ensure the employers' safety because the workplace was located in neighbourhood inhabited by the believers of other religion. In other case, revealing of a trade union membership was required obligatorily by the employer who explained that it was necessary for the future obligations connected with a trade-union protection in case of notice of the termination of the employment contract.

2.1. Supervision of employees by means of video-surveillance at the workplace is a matter that requires clear legal regulation. It should be stressed that those issues would not necessarily be (or even should not be) regulated in detail in statutory provisions. However an act should indicate general guidelines which should be taken into account in the law enforcement provisions or internal regulations at the workplace which lay down the conditions of video surveillance,⁷ use of data, processing periods and foremost the guarantees of the protection of employees' rights, including the right to dignity and the protection of personal interests.

It would be advisable to use the working documents prepared by the European institution while creating those general provisions as well as drawing up detailed internal regulations. Although video-surveillance has been noticed and analysed by the European institutions relatively long time ago, there is still no European legislation in force. However, working documents which were prepared clearly indicate which prerequisites should be taken into account while establishing internal video surveillance at the workplace. Numerous complaints lodged to the Inspector General show that there is a certain amount of difficulties with video surveillance and privacy of employees and their personal interests are not very much respected by the employers and trade unions.

2.2. Undoubtedly, the use of employees' biometric data should be urgently regulated. The Polish employers indicate the need to use employees' biometric data such as finger prints, picture of retina, voice analysis or other method of identification of the employees for the purposes of control of employees in broader and broader scope but also security of particular areas at the workplace. While in the case of accuracy or attendance control of employees other traditional methods may be employed (e.g. control maintained by human resources personnel),⁸ security of particular areas at the workplace should without any doubt be ensured with the use of the latest technologies which are more efficient and safer also from the data protection point of view.

Formally, the processing of such data about employees is prohibited. Biometric data are not covered by any provisions which give the employer the right to process such data even – as it was mentioned before – with the consent of employee. Therefore, it would be advisable to propose that legislation should clearly determine what biometric data, on what conditions and for what purpose would be processed by the employers.

2.3. Psychological and lie detector tests that employees have to take is a very controversial issue which is not regulated by labour law, although some specified provisions (e.g. provisions that lay down an employee-status of military service employees) allow to put the employees to the lie detector test.

⁷⁾ The suggestion made by the expert of the Council of Europe and the European Commission, the author of the guidelines on video surveillance ("Guiding principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance") – Mr G. Buttarelli who stressed that the principles of video surveillance at the workplace should be prepared together by the employer and the representative of employees (trade unions, employees self-government) would be very useful for the Polish solutions concerned.

⁸⁾ However, the instruction given for the employer in the 21st century to rely on 19th century methods reminds the fighting against steam engines in the 18th century England.

In particular private sector employees are in much broader scope put to such test which makes that the issue described becomes a general problem despite of the fact that those methods of employees' supervision are very much privacy and intimacy invasive and constitute the breach of the Labour Code that imposes upon the employer the obligation to protect personal interests of the employees. It is alarming that the employers are not categorically condemned for such actions by the National Labour Inspectorate and trade unions which accept an apparent legalization of the employers' conduct by obtaining the employers' consent to put them to the tests. This standpoint indicating legalization of psychological and lie detector tests the employees are being put to is also presented by some representatives of theory despite the fact that – as it was mentioned before – there are always doubts as to whether the employee's consent has been really freely given.

Also for this reason the question of putting employees to the tests should be clearly allowed or forbidden by the law.

2.4. The Labour Code should clearly forbid to process an employee's genetic data by the employer as well as information deriving from genetic tests unless such tests of results would be necessary to permit execution of strictly specified jobs or for purposes laid down by the legislator.

One should remember that the processing of genetic data may serve the protection of employees' health with regard to the specific nature of the job or position, or when genetic tests would constitute the necessary condition for the protection of health and safety of the employees and other persons.

Drafts of the European documents on the protection of personal data about employees which are being processed in the employment context clearly indicate that the employer has the right to process information obtained from genetic tests under the specific conditions. Such tests are allowed when among other things the prior checking considering all the circumstances, including quality of the tests, essence and reliability of the results as well as the necessity to strike the balance between public interest and freedom of persons involved indicates that there are strong prerequisites and in particular public interest (e.g. serious and imminent threat to health or safety of third parties – especially when the safety is prevailing matter – to carry out such tests. A confirmation that there is no other means to obtain the intended result should be a significant condition of the assessment in question.

In the case where the provisions of law provide for genetic tests in exceptional situation laid down by those provisions, a reservation should be made (such reservation already exists in the Polish provisions concerning the processing of health data) that the employer would be informed only about the existence or non-existence of any contraindications for the employment of person or adjustment of the workplace, but would not have the right to look into health records.

Conclusions

In the above – originally short – paper only some the most significant issues concerning the processing of personal data about employee by the employer which are being used in the employment context that should be clearly laid down in the provisions of labour law have been indicated.

A clumsy wording of Article 22¹ of the Labour Code which narrowly determines the scope of data which may be processed by the employer, and in particular taking into account of the necessity to use new technological solutions cause that the said provision is treated with reserve. The lack of legislation in question that clearly allows or permits the processing of data or determines the conditions under which the employer – taking into consideration public interest – would have the right to process given data lead to the situation where the employees are not protected from the excessive interference of the employers and the latter are not sure which legal instruments they may use without being charged of breaching the law. Whereas, the clear and certain legislation that guarantees the right to privacy and dignity, but also taking into account public interest is and should be the foundation of a democratic country.

⁹⁾ According to the article in „Gazeta Prawna” (of 13 March, this year), employees are subject to lie detector tests used as a means of verification of candidates for a job as well as revealing offences committed in the workplace.

Data Protection in working life

1. Introduction

The Personal Data Act contains general provisions concerning the protection of privacy, which also apply as such to working life. The Act implements the general EC Data Protection Directive 95/46/EC into Finnish national legislation. In addition, protection of privacy in working life is governed by several mutually complementary provisions. They concern fundamental rights and legislation concerning labour, civil servants, occupational health and communications, and criminal law. Finland was the first Member State of the European Union to enact a special act on privacy in working life (Act on the Protection of Privacy in Working Life, 477/2001). It came into force on 1 October 2001. Under the implementation provisions of the Act, employers and employees should discuss the handling of personal data at workplaces in accordance with the provisions on codetermination talks by 1 March 2002. At the same time, the Parliament ordered the Government to prepare new provisions for drug testing and the use of e-mail. However, the working group preparing the bill decided to propose a comprehensive amendment of the Act instead. The act, which was partly prepared on a tripartite basis between the authorities and the labour market partners, came into force on 1 October 2004. In other words, Finland has a second-generation data protection act for working life in place. Data protection has become a concrete part of life at workplaces.

2. Overview of working life and data protection

Roughly half of the time working-age people spend awake is related to work in one way or another. Work and being out of work are very important to our physical and psychosocial wellbeing. Our livelihood, relationships and even our health are at least partly bound to our working life. On the other hand, issues of coping and marginalisation affect all working-age people, both old and young.

In Finland, protection of privacy in working life is considered part of mental occupational health protection. This is why occupational safety districts are also in charge of monitoring compliance with the Act on the Protection of Privacy in Working Life, in addition to the Data Protection Ombudsman. The districts are based on a national organisation and make almost 30,000 visits to workplaces each year. This provides additional resources to monitoring legality.

Employment and service relationships are based on a hierarchy between employees and employers that states the employers' managerial prerogative. By entering an employment

contract, an employee undertakes to work for remuneration under the management and control of an employer. In contrast, the purpose of the protection of privacy and especially the protection of personal data is to balance the relationship between the party that is subject to control and the party carrying out the control. It is obvious that the protection of privacy in working life creates tension between the parties to an employment relationship.

Managers like to repeat the human resources mantra that the most important resource of an organisation is its personnel. Good care must be taken of personnel and their development. Various projects to maintain working capacity and coping seem to have become a permanent part of working life. One probable reason is that the age structure of the European population has become distorted; in Finland, for instance, an estimated 25 per cent of working-age people will reach retirement age by 2010. The race to recruit skilled personnel is likely to become even tougher than it already is. This may, in turn, influence national immigration policies.

The greatest challenge in leadership is to motivate personnel to work to attain the objectives of the organisation. To this end, leadership consultants have used Abraham Maslow's tried and true hierarchy of needs, for example. According to Maslow, our highest goal is to be able to fulfil our dreams and gain respect and appreciation. When this happens, we will be motivated and efficient. Without knowing it, Maslow gave a rather good analogy of what data protection is about. The protection of privacy is critical to good human resources management and to good management in general. It is a part of a high-quality working life. In other words, a high standard of data protection promotes the operations of an organisation. It may even provide the competitive edge.

Today, societies and businesses are subject to rapid change. Information work and production are increasingly important industrial sectors. Organisations form networks and their interaction increases, thereby accentuating the role of information infrastructure. Competence and innovation management have become important to national competitiveness on the global market. On the other hand, processes have become increasingly vulnerable. The risks from information crime and disease have become more apparent. Work is done in the new forms and ways: distance work, teamwork and multi-professional collaboration are more and more common. Moreover, employers have an increasing need to gather personal information on their employees. The protection of privacy means, however, that job applicants, employees and civil servants have a maximal right to know and decide on how their personal data is handled and what the content of gathered data is, and to be assessed on the basis of correct and accurate personal data. This means that the various parties involved in working life must be aware of how conflicts concerning the handling of personal information can be solved at workplaces.

3. Data protection in working life: does it exist?

Some believe that the norms that govern the protection of privacy should not be applied to working life. However, the European Court of Human Rights has consistently taken the position in its rulings that the principles of the protection of privacy should also be applied to employees and that they do not only apply to private life.

The case *Niemitz vs. Germany* concerned the authorities' right to carry out an inspection in the offices of the appellant. The German authorities claimed that Article 8 of the

European Convention on Human Rights did not apply in the case because there is a clear difference between the private life and the home and running an enterprise, business and business premises. The court ruled against the authorities. In the court's opinion, safeguarding privacy also included the opportunity to form and improve relationships. It saw no reason to separate private life from professional and business activities. On the contrary, the court proposed that for the majority of people, working life offers a major, if not the most important opportunity to form contacts with others. The court justified its opinion in line with the opinion of the Commission by saying that it is not always possible to clearly distinguish between what belongs to working life and what does not.

In the case *Halford vs. the United Kingdom* (UK), the European Court of Human Rights ruled that intercepting employees' telephone calls violated Article 8 of the European Convention on Human Rights. Ms Halford had two telephones at her disposal, one of which was intended for private use. The use of the telephones had not been restricted in any way and she had not been provided with any instructions on their use. The plaintiff complained about the employers' actions to the Court of Human Rights. UK claimed that with regard to the plaintiff's communications, using the telephone at her workplace did not fall under Article 8 of the Convention because she should not have had a justified reason to even expect that her privacy would be honoured with regard to the calls in question. The Court ruled, however, that no matter whether calls are made from work or home, Article 8 of the Convention of Human Rights does apply.

The word „communication“ is not merely an exchange of correspondence on paper but also in the form of sent and received electronic messages.

I would like to remind you of item 2 in the Recitals of the Data Protection Directive:

„(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals“. This naturally applies to data protection in working life, too.

4. What is the protection of privacy?

Based on the above, it is obvious that the protection of privacy and safeguarding the confidentiality of communications also apply in working life. This alone does not explain what the protection of privacy means. However, we must also provide substance for the concept of protection of privacy.

Development

The first literary reference to an attempt to protect the privacy of individuals is the oath of Hippocrates, a physician and teacher from the island of Kos. By making this oath, physicians still today undertake to honour the privacy of their patients and to keep in confidence information concerning them. The Hippocratic oath is a 2400-year-old tradition. It reflects the need to form a confidential relationship between a patient and a doctor, which promotes care.

More recently, the French revolution and the Declaration of Independence of the United States emphasized the importance of individual freedoms. In the Anglo-American rights culture, the right to privacy is often defined as a freedom from interference.

The horrors of the Second World War lead to justified fears towards the systematic registration of citizens. On the other hand, the United Nations have expressed their concern that approximately 40–50 million children are born every year whose births go completely unregistered. When these children seek to exercise their rights as citizens, they find they do not exist or have the status of citizen.

The progress of data systems from centralised to distributed systems has increased the capacity of data processing almost limitlessly. This has altered the traditional „Big Brother“, so that data subjects cannot know who collects their personal data and for what purpose. Especially the Internet, the global information network, has caused concern. According to the studies, one of the primary obstacles to the spreading of electronic commerce is the fear consumers have for their personal data (and credit card details). However, one of the key objectives of the general data protection directive of the European Communities is to remove obstacles from the free flow of information between Member States. We must also take into consideration the trend in general European fundamental rights. Traditionally, the fundamental rights based on the European Convention of Human Rights have been viewed vertically, from the perspective of the relationship between a citizen and the state.¹ More recently, however, they have also been viewed horizontally, as a phenomenon between and mutual to natural and legal persons.

Definition

Since the days of Hippocrates, numerous attempts have been made to define privacy and private life as a phenomenon, but with little success. Dr Sami Mahkonen has, nonetheless, succeeded in his attempt. He bases his definition on the opposites: self-determination and communality, publicity and non-disclosure, isolation and „socialness“, and immunity and accessibility.² Privacy moves within these opposites. We can see that as a phenomenon privacy, or rather how we experience it, always depends on the place, time, situation and the persons involved. We all experience our personal privacy differently at different times and in different situations. To quote a Finnish author: „It is difficult to estimate the sensitivity of others.“³ This potentially causes great difficulties to legislators and it also might explain the emotional tensions that are often associated with data protection. Moreover, it can provide the authorities with a superior position in interpreting the law.

So what is privacy? The Government bill (96/1998) concerning the Personal Data Act that implemented the EC general Data Protection Directive (95/46/EC) in Finland, states: „A separate definition of privacy is not proposed for inclusion in the act.“ The phenomenon is easier to approach, however, if we keep in mind that the question here

¹⁾ The same trend has taken place in Finland with regard to debate on fundamental rights.

²⁾ Sami Mahkonen: *Oikeus yksityisyyteen* (Right to privacy). Porvoo 1997. Werner Söderström lakitieto Oy – WSLT, 159 pages. ISBN 951-670-015-2

³⁾ Veikko Huovinen: *Havukka-ahon ajattelija*.

is about the right to privacy. In other words, the stress is on the word „right“. Data protection, or rather the protection of privacy is a *right* that belongs to all natural persons. More precisely, it is a *cluster of rights*.

- The right to influence and determine the use of personal data⁴

„Informed consent“ is a basic requirement for processing personal data. It may be considered to mean that a decision-maker – in this case the data subject – receives sufficient information to make a decision and that he or she gives his or her consent freely.

- The right to receive information of the processing of one's personal data, including who collects, stores and uses data concerning the data subject and for what purpose

Here we must pay special attention to the right I mentioned above. It is widely agreed that one of the main problems in working life is poor internal communication within organisations. It is, in fact, surprising to see that a key justification of data protection is to increase the openness of the relationship between data subjects and controllers.

This principle of transparency means that employers must always be able to justify the processing of their employees' personal information. This principle can further be divided into the following constituents:

- a) employees must be informed of the processing of their personal information;⁵
- b) employees are entitled to acquaint themselves with information concerning them, including the results of the aptitude assessments and career plans; and
- c) data controllers must make the required notifications to data protection authorities controlling the processing of personal data.⁶

- The right to organise one's private life without unnecessary outside interference

Article 7 of the EC Data Protection Directive is especially important in this regard. Under Section f, Member States must pass legislation that provides that personal data may be processed only if it is „necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)“.

It is important to realise that because of its power, a legislative body plays a key role in safeguarding data protection. Unregulated compilation and use of data files is considered a risk because it may place the data controller in a position of power that is in

⁴) The special circumstances of working life, especially concerning the employee's subordinate status to the employer, have led to critical appraisals of the usefulness of consent as a basis for processing personal data in working life. See: WP 29 Opinion 8/2001.

⁵) Under Section 4 of the Finnish Act on the Protection of Privacy in Working Life (477/2001) collecting personal data in conjunction with hiring and in the course of an employment relationship also falls under the codetermination procedure referred to in the Act on Cooperation within Undertakings (725/1978), the Act on Cooperation within State Agencies and Bodies (651/1988).

⁶) Under Finnish law, the Data Protection Ombudsman need not be informed of personal data files kept by human resources management. However, a file description is required and it must be kept available.

conflict with the tradition of democracy and outside the control of society. Legislation on the protection of personal data stakes out an area of psychological immunity and domestic peace in which we can freely form our opinions and thus prepare to participate in the society and decision-making as we best see fit. In other words, protection of privacy is linked to access to information and freedom of speech. Data protection reinforces and safeguards fundamental rights. It is perhaps a little surprising that in this sense the protection of privacy and the principle of openness and transparency do not have to be opposing goals, because without one the other cannot meaningfully exist.

The question of employers' right to read their employees' e-mail messages or simply monitoring what websites they visit is very interesting. At the least, it has raised a lively debate. Employers have outlined the needs based on which they deem themselves entitled to such monitoring. This debate arose in Finland roughly at the same time when the Act on Protection of Privacy in Electronic Communications came into force on 1 July 1999.⁷ The purpose of the Act is to provide the same confidentiality to electronic communications as traditional correspondence has had.⁸ It is my personal opinion that e-mail messages are confidential. They are protected with personal passwords and login names. This places them within the scope of legislation on the protection of personal data. So can reading e-mail messages addressed to other people be justified and is it legal? Ultimately, the final decision on the confidentiality of communications must be made by the courts. If reading messages is prohibited in legislation on the confidentiality of communications, there can be no justification for processing personal data associated with communications.

- The right to be evaluated on the basis of correct and appropriate data

This right reflects the quality principle of data protection. In assessing the necessity and the legality of processing personal data, the only indicator should not be the data controller's own assessment. Instead, the assessment should be based on the objective need. Processing of personal data may be considered necessary when the data is *appropriate and essential and not excessively comprehensive* for the purpose for which it has been collected and for which it will be processed. We must also note that these principles should all be applied concurrently. One general problem I have encountered in practical application of the law is that often a particular issue involving data protection is seen in the light of the particular provision that governs it, apart from the entire realm of processing personal data.

Personal data must always be used solely for a purpose established before collecting of the information started (principle of appropriateness).

This requirement has, at times, raised heated debate, especially in the context of the varied circumstances of working life; when is drug testing needed and justified, may employers read e-mail messages and what information may be collected from job

⁷) The Act on Protection of Privacy in Electronic Communications (565/1999). The Act implemented the EC Telecoms Data Protection Directive (97/66/EC) into national law.

⁸) See the Finnish Constitution, Section 10.

applicants during recruitment? An often-asked question is the following: does consent displace the necessity requirement? On the surface it seems that this only involves consent and necessity. This is not the case, however. What must also be taken into consideration are the obligations of planning, informing and other good practices of processing personal data. The latter goal has been laid down in law. To attain it, data controllers must make sure that the entire data processing process and the "life-span of data" are lawful. In other words, the goal is to make sure that data controllers never come into a position where they would actually have to deal with this issue. Consent does not displace necessity!

There are two additional elements that concern the quality of data. They are the concept of error (requirement of correctness) and time of storage. Error means data that is faulty, unnecessary, incomplete or obsolete with regard to *the purpose for which the personal data is processed*. This, in turn, means that data controllers must actively update their data files and that the requirement of advance planning of processing of personal data provides that controllers must in advance determine how long data will be stored or by what mechanism it will be processed, so that its quality can be safeguarded. It has been observed in the context of working life that aptitude tests can pose serious problems to data protection. Tests are sometimes downloaded from the web, the questions they contain may be completely alien and unnecessary to the relevant duties,⁹ and there is no guarantee that the results produced by the test are correct.

Because data protection involves clusters of rights, even data systems should promote it. The quality of a data system can be considered to consist of three elements: time used, price paid and functions gained. The lawful operation of a system is a *feature of quality*, which the management of an organisation is ultimately responsible for. As a right, data protection is not bound to any techniques or technical solutions. Nevertheless, technology can and should promote data protection.

- The right to expect a sufficient level of information security

This obliges data controllers to take necessary and sufficient technical and organisational measures to make sure that the processing of personal data is protected from unauthorised use, alteration and destruction, and that outsiders have no access to it.¹⁰

It is important to note that this requirement of information security has led to several different of technical systems of monitoring, including ones with which employees can be monitored. For instance, protecting systems from viruses that may destroy personal data files may make it necessary to monitor e-mail systems. This problem has been solved in the Act on the Protection of Privacy in Electronic Communications, which protects data in electronic communications and implemented the EC Directive on privacy and electronic communications (2002/58/EC).

⁹⁾ The Office of the Data Protection Ombudsman has, for example, heard of aptitude tests used in Finland that ask the ethnicity of the applicant: „Are you a North American Indian?“

¹⁰⁾ Neglecting information security is penalised under the Finnish Personal Data Act. Similarly, violating the confidentiality of personal data can result in a penalty.

Evaluation

The processing of personal data and keeping of data files as described above are vital parts of the activities of both the private and the public sector. The purpose of data protection legislation and principles is to offer ways to resolve conflicts between the protection of privacy and the need of information of other members and actors of society, and how to attain an acceptable equilibrium between the various parties.

The functioning and general approval of systems that regulate personal data depend not only on how well the legislation strikes a balance between various values associated with information and its availability, but also how well data controllers and others involved in the processing of personal information understand the objectives of legislation and the fundamental human rights on which the regulation is based.

The system protecting privacy and private life can be considered to consist of two parts: a system of sanctions based on criminal law that comes into action *after the fact*, and one of data protection that concerns the automatic processing of personal data and keeping of data files that comes into action *before the fact*. As a result, we can say that the principles of data protection are an inalienable but, because of their steering effect, also a very modern part of the legal mechanism that protects data. These principles indicate to data controllers the limits of what is permissible and acceptable and also function as traffic signs that guide their actions. This is relevant to the obligations to plan and protect and to train personnel.¹¹

Do we then need the rights and principles that protect privacy? A study was published rather recently in Finland, which examined citizens' attitudes to data protection.¹² The study found that citizens' are rarely worried about the protection of their personal data. However, they do want to *know* if their data is processed and by whom. They also want to *participate* in making decisions that concern them. It is important to notice that probably mostly without knowing it, the respondents described the nature and principal content of data protection! We may also estimate that the Act on the Protection of Privacy in Working Life brings data protection closer to our daily life. Hence, the protection of privacy is an inalienable part of the good *quality* of life to which we all are entitled.

5. Concrete measures taken in Finland

As I stated earlier, the various provisions of the data protection legislation are to be applied concurrently; they are not mutually exclusive. Section 3 of the current Act on the Protection of Privacy in Working Life defines the necessity requirement as follows:

„The employer is only allowed to process personal data directly necessary for the employee's employment relationship which is connected with managing the rights and obligations

¹¹⁾ The Personal Data Act has, for example, been used in drafting request for tenders on data protection systems.

¹²⁾ Statistics Finland (Nurmela, Heinonen, Ollila, Virtanen). Matkapuhelin ja tietokone suomalaisen arjessa (Mobile phones and computers in daily Finnish life). Helsinki 2000. Reviews 2000/2.

of the parties to the relationship or with the benefits provided by the employer for the employee or which arise from the special nature of the work concerned. No exceptions can be made to the necessity requirement, not even with the employee's consent."

Sections of the legislation regarding drug tests, camera surveillance, and use of e-mail that I will discuss later are always compared with this necessity requirement and with the other principles used in the general data protection act.

Drug-free workplaces and drug testing

In preparing the Act, the point of departure was that drug use is an illness – an illness of addiction. Because public health legislation is applied to drug testing, the Act as such does not provide the right to force anyone to take a drug test. This means that examination of a patient requires the patient's consent and that the test can only be conducted by a health care professional. It does, however, explain the terms on which employers have the right to process a document showing test results. This right to process – when it is in general acceptable to process evidence – stems from the legislation and is related to the tasks entailed by the job. This ensures that other fundamental rights are secured.

The general conditions are the following: 1) employers have a duty to prepare an anti-drug programme together with personnel and 2) the jobs that entail the right to process evidence should be subject to codetermination procedure. The anti-drug programme together with labour law provisions instruct employees how to react to positive test results.

Employers must inform job applicants before making a contract and before altering the terms of employment that the task in question requires delivery of test results to the employer.

The employer always agrees to pay the costs of the test. The Ministry of Social Affairs and Health has issued a decree on testing that is binding on health care professionals. If an employer uses persons other than those mentioned for making the test, sanctions can be imposed.

Drug testing can also be made a part of occupational health services. In this case a physician assesses the need for a test, not the employer. The test result is not, in fact, given to the employer, who instead receives only general information about the suitability of the person in question for the job.

Moreover, the employer may process the result of the drug test if the employee has consented to care on the basis of a positive test, and processing is related to monitoring of the implementation of the care.

Technical control

To begin with, it must be noted that the elements of an employment relationship themselves entitle the employer to control the activity of an employee within the limits of employers' managerial prerogative. On the other hand, data security requirements may mean that the employer has a duty to perform technical control. The Act on the Protection of Privacy in Working Life does not entitle or require technical control of

employees. According to the Government's proposal, "Other legislation indirectly sets limits on the control rights of an employer, by for example imposing sanctions for certain acts that violate the protection of privacy."

The necessity of technical control and any changes to it must undergo the codetermination procedure. The employer must state the purpose for the control and the methods to be used in it. Then he must inform the employees of the content of the decision. They may bring the matter to the attention of law enforcement officials.

Camera surveillance

The law provides the right to implement camera surveillance in premises where employees work, although the purpose of the observation was not the surveillance of the employees. The employer may conduct camera surveillance, if the purpose is:

- to ensure the personal safety of the employees and other persons working in the premises,
- to protect property,
- to supervise the adequate operations of productional processes,
- to prevent or clarify situations endangering safety, property or productional processes.

As a rule, camera surveillance must not be used for observing a certain employee or certain employees at the working place.

There must not be any camera surveillance in toilets, locker rooms or social premises of the employees. It is also prohibited in working rooms which have been assigned for the personal use of the employees.

If camera surveillance is necessary, it can, however, be focused on a certain place of work, where there are employees working, if:

- its purpose is to prevent apparent threat of violence related to the work of the employee, or apparent disadvantage or danger to his safety or health, or
- observation is necessary for preventing and clarifying crimes against property, if an essential part of the employee's tasks consists of handling property that is significant as to its value or quality, such as money, bonds or valuables, or
- the interests and rights of the employee should be secured, if the camera surveillance is based on the request of the employee.

The camera surveillance should be as transparent as possible and necessary for reaching the purpose of measures. Recordings received through the surveillance may only be used for the purpose for which the observation has been conducted. Before introducing camera surveillance, clarifications should be made regarding the possibilities of using means less intervening with the privacy of the employees.

After the cooperation the employees must also be notified of the beginning of the camera surveillance, its implementation and of how and in what situations the recordings are used, as well as of the placement of the cameras, if they are focused on workplaces. Information of the camera surveillance must be also provided in a perceptible way so that it shows whether it is a question of recording camera surveillance or not.

There are also certain exceptions to the purpose of using the recordings received through camera surveillance:

- the recordings may be used for substantiating the ground for terminating an employment relationship,
- for clarifying or substantiating disturbance, harassment or inapt behaviour referred to in the Equality Act and Occupational Safety and Health Act, if the employer has a justified reason to suspect that the employee has been guilty of such behaviour,
- for clarifying industrial accidents.

As a rule, the recordings have to be destroyed as soon as they are not necessary for implementing the purpose of the surveillance, and within a year at the latest.

If the employer requires camera surveillance contrary to a provision or violates the provisions on the transparency of camera surveillance, he can be sentenced to a fine, unless the act, at the same time, fulfils the distinctive marks of illicit viewing condemned according to the most severe penal scale.

E-mails

According to the provisions, the message can be opened and read by another person with the employee's consent in compliance with the rules agreed on at the working place. This requires that the employee gives his user name and password, for example, to his fellow worker. The new provisions aim to give an answer to how to proceed, if the employee does not give his consent.

In order for the employer to be able to use his power, the precondition is that the employer prior to that has offered the employee different possibilities, which when being realized mean that there is usually no need to touch upon the e-mail communications of his employees. One possibility is that the e-mail system sends an automatic notification of the absence and substitute of the employee to the sender of the message. Another alternative is that the messages during the absence are directed to another person or to the e-mail address used by some other employee. The offering of such possibilities requires measures from the employee himself, because the employer has no right to make such directions in the e-mail of the employee.

Although the employer would ensure the above-mentioned measures, the employee is under no obligation to use the possibilities offered. Unless the employee uses the possibilities, the employer must find out whether any messages belonging to the employer have been sent to the employee in his absence or whether he has sent messages belonging to the employer immediately before his absence. These messages must, then, be of a kind which the employer necessarily has to be informed of in order to finish negotiations related to his activities, for serving customers or for otherwise securing his functions. Such situations include e.g. situation in connection with orders, invoicing and complaining as well as relevant business negotiations.

The assessment of whether a message belongs to the employer may in practice only happen on the basis of the information concerning the sender's identification data or the title space in the e-mail address. This information does not belong to the core

substance of a confidential message. Although in most cases, it is possible to conclude from this information whether the message is private or not, this is not always possible. For this reason, the precondition for retrieving e-mail messages are additional criteria which all must be fulfilled before the e-mail is brought out:

- 1) the employee attends to his tasks independently, which as a rule means that others do not attend to the matter at the same time,
- 2) because of the tasks or pending matters of the employee it is obvious that the messages have been sent to him,
- 3) the employee is absent from his work,
- 4) before beginning to open e-mail, the employer offers the employee an opportunity to give his consent to the opening,
- 5) clarifying the matter of the message does not endure delay.

The law also includes a special provision for situations where the employee has died, or he is permanently hindered in performing his work tasks, in which case he cannot give his consent to disclosing the messages.

A written clarification has to be made to the employee on the retrieving of message.

After disclosing the message, the message may be opened, if on the basis of above-mentioned clarification it is obvious that it clearly belongs to the employer and fulfils the criteria described above. A precondition is also that attempts have, without results, been made to contact the sender or recipient of the message in order to find out the content of the message or to send it to another e-mail address assigned by the employer.

A written notification of the opening the message has to be given to the employee.

6. Conclusion

To date, legislation on the protection of privacy in working life has not been enacted in other EU member countries. The special situations and categories of data in working life, such as data regarding health have, however, been made a part of special legislation. The third operational model is to use sector-specific codes of conduct.

Finnish experience of the Act on the Protection of Privacy in Working Life has on the whole been positive. Research shows that the right of employees to obtain information has improved, information systems are planned more effectively, and the drafting of codes of contact has begun.

Ochrona danych w życiu zawodowym

1. Wstęp

Ustawa o danych osobowych zawiera ogólne przepisy dotyczące ochrony prywatności odnoszące się również do życia zawodowego. Wprowadza do ustawodawstwa fińskiego ogólną Dyrektywę w sprawie ochrony danych 95/46/EC. Ponadto, ochronę pry-

watności w życiu zawodowym reguluje wiele przepisów wzajemnie się uzupełniających. Mówią one o podstawowych prawach i aktach prawnych dotyczących pracy, urzędników administracji państwowej, higieny pracy, wymiany informacji oraz prawa karnego. Finlandia była pierwszym Państwem Członkowskim Unii Europejskiej, które uchwaliło specjalną ustawę o prywatności w życiu zawodowym (ustawa o ochronie prywatności w życiu zawodowym, 477/2001). Weszła ona w życie 1 października 2001 r. W myśl zapisów tej ustawy pracodawcy i pracownicy powinni do 1 marca 2002 r. omówić sposób przetwarzania danych osobowych w miejscu pracy, zgodnie z przepisami dotyczącymi dokonywania uzgodnień. Jednocześnie parlament nakazał rządowi opracowanie nowych przepisów w sprawie przeprowadzania testów na obecność narkotyków oraz zasad korzystania z poczty elektronicznej. Jednak grupa robocza przygotowująca projekt ustawy zdecydowała się na zgłoszenie propozycji kompleksowej jej zmiany. Ustawa, przygotowana częściowo na podstawie trójstronnego porozumienia między rządem i przedstawicielami rynku pracy, weszła w życie 1 października 2004 r. Innymi słowy, Finlandia ma ustawę o ochronie danych w życiu zawodowym będącą ustawą drugiej generacji. Ochrona danych stała istotnym elementem funkcjonowania w miejscu pracy.

2. Życie zawodowe i ochrona danych w zarysie

Prawie połowę czasu, w którym ludzie będący w wieku produkcyjnym nie śpią, zajmuje w taki czy inny sposób praca. Praca lub jej brak są bardzo ważne dla naszego fizycznego i psychicznego samopoczucia. Środki na nasze utrzymanie, związki z innymi ludźmi, a nawet nasze zdrowie przynajmniej częściowo zależą od naszego życia zawodowego. Z drugiej jednak strony, konieczność radzenia sobie ze stresem i marginalizacją dotyczy wszystkich ludzi w wieku produkcyjnym – zarówno młodych, jak i starych.

W Finlandii ochrona prywatności w życiu zawodowym jest uważana za element ochrony zdrowia psychicznego pracowników. Dlatego też oprócz Rzecznika ds. Ochrony Danych władze odpowiedzialne za bezpieczeństwo pracy mają również obowiązek monitorowania czy ustawa o ochronie prywatności w życiu zawodowym jest przestrzegana. Kompetencje tych władz rozciągają się na przydzielone im rejony, podzielone na terytorium całego kraju, a ich przedstawiciele co roku przeprowadzają ponad 30 000 kontroli w miejscach pracy. Stanowią one dodatkowe źródło informacji dla potrzeb monitorowania legalności działań.

Zatrudnienie i stosunek pracy są oparte na hierarchii istniejącej między pracownikami i pracodawcami, która określa przywileje kierownicze pracodawcy. Zawierając umowę o pracę, pracownik podejmuje się, w zamian za wynagrodzenie, wykonywania pracy pod kierownictwem i kontrolą pracodawcy. Natomiast ochrona prywatności, a w szczególności ochrona danych osobowych ma na celu zrównoważenie stosunków między stroną podlegającą kontroli a stroną kontrolującą. Oczywiście jest bowiem, że ochrona prywatności w życiu zawodowym powoduje napięcia między stronami umowy o pracę.

Menadżerowie lubią powtarzać mantrę o zasobach ludzkich, według której najważniejszym zasobem organizacji jest jej personel. O personel i jego rozwój należy dbać. Wydaje się, że różnego rodzaju projekty mające na celu utrzymanie potencjału pracowniczego oraz ułatwienie radzenia sobie ze stresem, stały się nieodłącznym elementem życia zawodowego. Powodem jest zniekształcenie struktury wiekowej ludności w Europie; na przykład w Finlandii około 25 procent osób w wieku produkcyjnym osią-

gnie wiek emerytalny do roku 2010. Wyścig w ramach rekrutacji wykwalifikowanego personelu prawdopodobnie stanie się jeszcze bardziej zacięty niż obecnie. To z kolei może wpłynąć na politykę imigracyjną państwa.

Największe wyzwanie dla kierowników stanowi motywowanie personelu do pracy na rzecz osiągnięcia celów organizacji. Z tego względu ich konsultanci wykorzystują, na przykład, sprawdzoną piramidę potrzeb Abrahama Masłowa. Według Masłowa, naszym najważniejszym celem jest możliwość spełniania marzeń oraz zdobycie szacunku i uznania. Kiedy to nastąpi, będziemy mieć motywację do działania i będziemy wydajni. Nie wiedząc o tym, Masłow wskazał na bardzo trafną analogię pokazującą, czym jest ochrona danych. Ochrona prywatności jest krytycznym punktem w dobrym zarządzaniu zasobami ludzkimi oraz w dobrym zarządzaniu w ogóle. Jest częścią wysokiej jakości życia zawodowego. Innymi słowy, wysoki standard ochrony danych wspiera działalność organizacji. Może nawet zapewnić jej przewagę nad konkurencją.

Społeczeństwo i firmy podlegają obecnie szybkim zmianom. Działalność informacyjna oraz pozyskiwanie informacji stają się coraz ważniejszymi dziedzinami. Organizacje tworzą sieci, które w coraz większym stopniu oddziałują na siebie, a tym samym wskazują, jak ważna jest infrastruktura informacyjna. Zarządzanie kompetencjami i innowacjami stało się istotnym elementem w sferze konkurencyjności państwa na globalnym rynku. Z drugiej strony, procesy te są w coraz większym stopniu narażone na różne bodźce zewnętrzne. Ryzyko związane z przestępstwami i chorobami informacyjnymi jest bardziej widoczne. Pojawiły się nowe formy i sposoby pracy: praca na odległość, praca zespołowa i współpraca między różnymi profesjami, które stają się coraz powszechniejsze. Ponadto, pracodawcy odczuwają coraz większą potrzebę zbierania informacji na temat swoich pracowników. Ochrona prywatności oznacza jednak, że osoby ubiegające się o pracę, pracownicy i urzędnicy administracji państwowej mają pełne prawo wiedzieć i decydować, jak ich dane osobowe będą przetwarzane, jaka jest treść przechowywanych danych oraz wymagać, by podlegać ocenie na podstawie właściwych i dokładnych danych osobowych. Oznacza to, że różne strony biorące udział w życiu zawodowym muszą być świadome sposobu, w jaki można w miejscu pracy rozwiązać konflikty związane z przetwarzaniem danych osobowych.

3. Ochrona danych w życiu zawodowym – czy istnieje?

Niektórzy uważają, że normy regulujące sferę ochrony prywatności nie powinny dotyczyć życia zawodowego. Jednak Europejski Trybunał Praw Człowieka przyjął w swoich orzeczeniach konsekwentne stanowisko, zgodnie z którym zasady ochrony prywatności powinny być stosowane również w przypadku pracowników, a nie odnosić się wyłącznie do ich życia prywatnego.

Sprawa *Niemitz przeciwko Niemcom* dotyczyła prawa władz do przeprowadzania kontroli w biurach strony odwołującej się. Władze niemieckie twierdziły, że artykuł 8 „Europejskiej Konwencji Praw Człowieka” nie miał zastosowania w tej sprawie, ponieważ istnieje wyraźna różnica między życiem prywatnym i domem a prowadzeniem przedsiębiorstwa, firmy i siedzibą firmy. Trybunał wydał orzeczenie na niekorzyść władz. Zdaniem Trybunału, zapewnienie prywatności obejmowało również możliwość nawiązania i poprawy stosunków. Trybunał nie widział powodu oddzielania życia prywatnego od działalności zawodowej i biznesowej. Trybunał stwierdził natomiast, że dla większo-

ści ludzi życie zawodowe stanowi główną, jeżeli nie najważniejszą możliwość nawiązywania kontaktów z innymi. Trybunał uzasadnił swoją opinię zgodną z opinią Komisji, stwierdzając, że nie zawsze istnieje możliwość wyraźnego odróżnienia tego co należy a co nie należy do życia zawodowego.

W sprawie *Halford przeciwko Wielkiej Brytanii* Europejski Trybunał Praw Człowieka orzekł, że przechwytywanie rozmów telefonicznych pracowników naruszało artykuł 8 „Europejskiej Konwencji Praw Człowieka”. Pani Halford miała do dyspozycji dwa telefony, z których jeden był przeznaczony do użytku prywatnego. Korzystanie z telefonów nie było w żaden sposób ograniczone, a pani Halford nie otrzymała żadnych instrukcji co do korzystania z nich. Powódka złożyła skargę do Trybunału Praw Człowieka na działania pracodawcy. Wielka Brytania twierdziła, że w przypadku wymiany informacji przez powódkę za pomocą telefonu w miejscu pracy nie ma zastosowania artykuł 8 „Konwencji”, ponieważ nie powinna ona mieć uzasadnionego powodu, by nawet oczekiwać, że jej prywatność będzie honorowana w odniesieniu do spornych rozmów. Trybunał orzekł jednak, że nie jest istotne czy telefonowała z pracy czy z domu – artykuł 8 „Konwencji praw człowieka” ma tu zastosowanie.

Zwrot „wymiana informacji” nie oznacza wyłącznie wymiany korespondencji na papierze, ale również w formie wysyłanych i odbieranych wiadomości elektronicznych.

Chciałbym przypomnieć pozycję 2 w preambule Dyrektywy w sprawie ochrony danych:

„(2) Zważywszy, że systemy przetwarzania danych mają służyć człowiekowi, zważywszy, że muszą one, bez względu na narodowość czy miejsce zamieszkania osób fizycznych, przestrzegać ich podstawowych praw i wolności, w szczególności prawa do prywatności, i przyczyniać się do gospodarczego i społecznego postępu, rozwoju handlu i pomyślności jednostki”. Oczywiście, dotyczy to również ochrony danych w życiu zawodowym.

4. Co to jest ochrona prywatności?

Opierając się na tej preambule, oczywiste wydaje się, że ochrona prywatności oraz zabezpieczenie poufności wymiany informacji dotyczy również życia zawodowego. Nie wyjaśnia to jednak, co oznacza ochrona prywatności. Musimy zatem przedstawić podstawy koncepcji ochrony prywatności.

Rozwój

Pierwszą wzmianką w literaturze na temat próby ochrony prywatności jednostki jest przysięga Hipokratesa, lekarza i nauczyciela z wyspy Kos. Przez składanie tej przysięgi do dziś lekarze zobowiązują się do przestrzegania prywatności swoich pacjentów oraz do zachowania poufności informacji na ich temat. Przysięga Hipokratesa ma 2400-letnią tradycję. Odzwierciedla ona potrzebę tworzenia poufnego związku między pacjentem a lekarzem, co wzmaga troskę o tego pierwszego.

Następnie rewolucja francuska oraz Deklaracja Niepodległości Stanów Zjednoczonych pokazały, jak ważne są swobody jednostki. W kulturze angloamerykańskiej prawo do prywatności często jest definiowane jako wolność od ingerencji.

Okropności drugiej wojny światowej spowodowały uzasadnione obawy przed systemową rejestracją obywateli. Z drugiej strony, Organizacja Narodów Zjednoczonych wyraziła zaniepokojenie, że co roku na świat przychodzi około 40-50 milionów dzieci, których narodziny nie są nigdzie rejestrowane. Kiedy takie dzieci chcą skorzystać ze swoich praw jako obywatele, odkrywają, że w ogóle nie istnieją albo że nie mają statusu obywateli.

Przejsie od scentralizowanych systemów przechowywania danych do systemów rozproszonych zwiększyło możliwości przetwarzania danych niemalże bez ograniczeń. Spowodowało, że tradycyjny „Wielki Brat” uległ zmianie – podmioty, których dotyczą dane, nie wiedzą, kto przechowuje ich dane osobowe i w jakim celu. Zwłaszcza Internet, ogólnosiwiatowa sieć informacyjna, budzi zaniepokojenie. Według badań, jedną z głównych przeszkód w rozpowszechnieniu handlu metodą elektroniczną jest obawa konsumentów o swoje dane osobowe (oraz dane dotyczące kart kredytowych). Jednak jednym z zasadniczych celów ogólnej Dyrektywy w sprawie ochrony danych osobowych Unii Europejskiej jest usunięcie przeszkód w wolnym przepływie informacji między Państwami Członkowskimi. Musimy również wziąć pod uwagę tendencję odnoszącą się do podstawowych praw europejskich. Tradycyjnie prawa podstawowe oparte na „Europejskiej Konwencji Praw Człowieka” postrzegano „pionowo”, z perspektywy stosunków między obywatelem a państwem.¹ Ostatnio jednak zaczęto patrzeć na nie również „poziomo”, jak na zjawisko zachodzące wzajemnie pomiędzy osobami fizycznymi i prawnymi.

Definicja

Od czasów Hipokratesa podjęto wiele prób zdefiniowania prywatności i życia prywatnego jako zjawiska – z niewielkim skutkiem. Niemniej jednak dr Sami Mahkonen odniósł sukces. Opiera on swoją definicję na przeciwieństwach: samostanowienie i wspólnota, rozgłos i nieujawnianie, izolacja i „towarzyskość” oraz nietykalność i dostępność.² Prywatność mieści się między tymi przeciwieństwami. Widzimy zatem, że jako zjawisko prywatność czy raczej sposób, w jaki jej doświadczamy, zawsze zależy od miejsca, czasu, sytuacji i osób, których dotyczy. Każdy z nas doświadcza swojej osobistej prywatności w inny sposób, w różnych momentach i w różnych sytuacjach. Cytując fińskiego autora: „Trudno jest zmierzyć wrażliwość innych.”³ Potencjalnie jest to przyczyną ogromnych trudności dla ustawodawców i może również stanowić wyjaśnienie powodu napięć emocjonalnych, które często wiążą się z ochroną danych. Ponadto może to również wpływać na silniejszą pozycję władz w sferze interpretacji prawa.

Czym więc jest prywatność? Projekt zgłoszony przez rząd (96/1998), a dotyczący ustawy o ochronie danych osobowych, który wprowadzał w Finlandii ogólną Dyrektywę w sprawie ochrony danych (95/46/WE), stanowił: „Nie zgłasza się oddzielnej definicji prywatności, która miałaby zostać ujęta w ustawie.” Zjawisko łatwiej zrozumieć mając na uwadze, że pytanie dotyczy prawa do prywatności. Innymi słowy, nacisk jest położony na słowo „prawo”. Ochrona danych, czy raczej ochrona prywatności to prawo należne wszystkim osobom fizycznym. Ścisłej mówiąc, jest to *grupa praw*.

¹) Taki sam trend miał miejsce w Finlandii w przypadku debaty na temat podstawowych praw.

²) Sami Mahkonen: *Oikeus yksityisyyteen* (Prawo do prywatności). Porvoo 1997. Werner Söderström Iakitiety Oy – WSLT, s. 159. ISBN 951-670-015-2

³) Veikko Huovinen: *Havukka-ahon ajatteliija*.

- Prawo wpływu i decydowania o wykorzystaniu danych osobowych⁴

„Świadoma zgoda” to podstawowy wymóg w dziedzinie przetwarzania danych osobowych. Można uznać, że oznacza ona, iż podejmujący decyzję – w tym przypadku podmiot, którego dotyczą dane – otrzymał informacje wystarczające do podjęcia decyzji oraz że udzielił swojej zgody dobrowolnie.

- Prawo do uzyskania informacji o przetwarzaniu danych osobowych, w tym o tym, kto i w jakim celu zbiera, przechowuje i wykorzystuje dane dotyczące podmiotu

W tym miejscu musimy zwrócić szczególną uwagę na wymienione prawo. Powszechnie uważa się, że jednym z głównych problemów w życiu zawodowym jest słaba komunikacja wewnątrz organizacji. Faktycznie zadziwiające jest to, że głównym uzasadnieniem dla ochrony danych jest większa otwartość w stosunkach między podmiotami, których dotyczą dane, a administratorami.

Zasada przejrzystości oznacza, że pracownicy zawsze muszą być w stanie znaleźć uzasadnienie dotyczące przetwarzania ich danych osobowych. Ta zasada może zostać podzielona na następujące zagadnienia składowe:

- a) pracownicy muszą być informowani o przetwarzaniu ich danych osobowych;⁵
 - b) pracownicy mają prawo zapoznać się z informacjami, które ich dotyczą, włącznie z wynikami oceny ich przydatności i planami rozwoju zawodowego;
 - c) administratorzy danych muszą przysyłać wymagane zawiadomienia do władz odpowiedzialnych za ochronę danych i kontrolujących proces przetwarzania danych osobowych.⁶
- Prawo do organizowania życia prywatnego bez zbędnej ingerencji z zewnątrz

Artykuł 7 Dyrektywy w sprawie ochrony danych jest szczególnie istotny w tym względzie. W myśl paragrafu f Państwa Członkowskie muszą uchwalić ustawy, zgodnie z którymi dane osobowe mogą być przetwarzane wyłącznie wówczas, gdy jest to „konieczne ze względu na uzasadnione interesy administratora lub osoby trzeciej bądź osób, którym dane są ujawniane, z wyjątkiem sytuacji, w których podstawowe prawa i wolność podmiotów, których dotyczą dane, są nadrzędne w stosunku do takich interesów i wymagają ochrony, zgodnie z artykułem 1 (1)”.

Ważne jest przy tym, by organ ustawodawczy, ze względu na swoje uprawnienia, zdawał sobie sprawę, że odgrywa istotną rolę w zapewnieniu ochrony danych. Niekontrolowane zbieranie i wykorzystywanie danych uważa się za ryzykowne, ponieważ może dawać

administratorowi danych przewagę, która jest niezgodna z tradycją demokracji i znajduje się poza kontrolą społeczeństwa. Ustawy o ochronie danych osobowych wytyczają obszar psychologicznej nietykalności i spokoju, w którym możemy swobodnie formułować swoje opinie i w ten sposób przygotowywać się do udziału w życiu społecznym i w podejmowaniu decyzji w sposób, jaki uważamy za stosowne. Innymi słowy, ochrona prywatności jest związana z dostępem do informacji i wolnością słowa. Ochrona danych umacnia i zapewnia podstawowe prawa. Zapewne nieco zadziwiający jest fakt, że w tym sensie ochrona prywatności oraz zasada otwartości i przejrzystości nie mają przeciwnych celów, ponieważ jedna bez drugiej nie mogłaby istnieć w sposób sensowny.

Kwestia prawa pracodawców do czytania wiadomości e-mail pracowników lub zwykłego monitorowania odwiedzanych przez nich stron internetowych jest bardzo interesująca. Wzbudziła ona co najmniej ożywioną dyskusję. Pracodawcy w zarysie przedstawili potrzeby zgodnie z tym, co sami uznali za uprawniające ich do takiego monitorowania. Dyskusja rozpoczęła się w Finlandii mniej więcej w tym samym czasie, w którym weszła w życie ustawa o ochronie prywatności i wymianie informacji drogą elektroniczną – 1 lipca 1999 r.⁷ Ustawa ma na celu zapewnienie takiej samej poufności informacjom wymienianym drogą elektroniczną, jaką zapewniono tradycyjnej korespondencji.⁸ Moja opinia jest następująca: wiadomości e-mail są poufne. Są one chronione osobistymi hasłami i nazwami użytkowników. To powoduje, że są objęte ustawą o ochronie danych osobowych. Czy zatem czytanie wiadomości e-mail adresowanych do innych osób może być uzasadnione i jest zgodne z prawem? Ostateczna decyzja w sprawie poufności wymiany informacji należy do sądu. Jeżeli prawo dotyczące poufności wymiany informacji zabrania czytania wiadomości, nie ma uzasadnienia dla przetwarzania danych osobowych związanych z wymianą informacji.

- Prawo do podlegania ocenie na podstawie właściwych i dokładnych danych

Prawo to odzwierciedla zasadę jakości danych osobowych. Przy ocenie konieczności i legalności przetwarzania danych osobowych wskaźnikiem nie powinna być tylko ocena administratora danych. Ocena powinna opierać się na obiektywnej potrzebie. Przetwarzanie danych osobowych może zostać uznane za konieczne w przypadku, gdy dane są *właściwe i istotne, a nie zbyt obszerne* ze względu na cel, w jakim je zebrano i w jakim będą przetwarzane. Musimy również pamiętać, że zasady te powinny być stosowane jednocześnie. Jeden problem natury ogólnej, jaki napotkałem w stosowaniu tego prawa w praktyce, to fakt, że często konkretna sprawa obejmująca ochronę danych jest postrzegana w świetle konkretnego przepisu, który ją reguluje, przy pominięciu całej sfery przetwarzania danych osobowych.

Dane osobowe należy zawsze wykorzystywać wyłącznie do celu określonego przed rozpoczęciem zbierania informacji (zasada właściwości).

Wymóg ten powodował niekiedy gorące dyskusje, zwłaszcza w kontekście różnego rodzaju okoliczności występujących w życiu zawodowym: kiedy jest potrzebne i uzasadnione przeprowadzenie testu na obecność narkotyków, czy pracodawcy mogą czy-

⁴) Szczególne okoliczności pracy, zwłaszcza dotyczące statusu pracownika jako podwładnego pracodawcy, doprowadziły do krytycznej oceny użyteczności zgody jako podstawy przetwarzania danych osobowych w życiu zawodowym. Zob.: WP 29 opinia 8/2001.

⁵) Zgodnie z paragrafem 4 fińskiej ustawy o ochronie prywatności w życiu zawodowym (477/2001) zbieranie danych osobowych w związku z rekrutacją i w ramach stosunku pracy również jest objęte procedurą wspólnych uzgodnień, o której mowa w ustawie o współpracy w ramach przedsięwzięć (725/1978), w ustawie o współpracy w ramach agencji i organów władzy państwowej (651/1988).

⁶) Zgodnie z przepisami prawa fińskiego nie trzeba informować Rzecznika ds. Ochrony Danych o plikach z danymi osobowymi przechowywanymi przez dział personalny. Wymagany jest jednak opis plików i musi być on dostępny.

⁷) Ustawa o ochronie prywatności w wymianie informacji drogą elektroniczną (565/1999). Ustawa wprowadziła do krajowego prawa Dyrektywę w sprawie ochrony danych telekomunikacyjnych (97/66/EC).

⁸) (Zob.): Konstytucja Finlandii, paragraf 10.

tać wiadomości e-mail i jakie informacje można zbierać w procesie rekrutacji od osób ubiegających się o pracę. Często zadawane pytanie brzmi: czy zgoda znosi wymóg konieczności? Na pozór wydaje się, że istotna jest tylko zgoda i wystąpienie konieczności. Jednak tak nie jest. Musimy również uwzględnić obowiązek planowania, informowania oraz inne dobre zwyczaje związane z przetwarzaniem danych osobowych. Ostatni cel określa prawo. Aby go osiągnąć, administratorzy danych muszą mieć pewność, że cały proces przetwarzania danych oraz „żywołność danych” są zgodne z prawem. Innymi słowy, celem jest zapewnienie, że administratorzy danych nigdy nie znajdują się w sytuacji, w której rzeczywiście będą musieli zająć się tą sprawą. Zgoda nie usuwa zatem wymogu konieczności!

Są dwa dodatkowe elementy dotyczące jakości danych. Koncepcja błędu (wymóg ich właściwości) oraz czas przechowywania. Błąd oznacza dane, które są niewłaściwe, niepotrzebne, niekompletne lub nieaktualne pod względem *celu, dla którego dane osobowe są przetwarzane*. Oznacza to z kolei, że administratorzy danych muszą na bieżąco aktualizować pliki z danymi oraz że wymóg wcześniejszego planowania przetwarzania danych osobowych zobowiązuje administratorów do wcześniejszego ustalenia, jak długo dane będą przechowywane lub w jaki sposób będą one przetwarzane tak, by można było zapewnić odpowiednią ich jakość. W kontekście życia zawodowego zaobserwowano, że testy przydatności mogą stanowić poważny problem dla ochrony danych. Testy są niekiedy ściągane z Internetu, pytania znajdujące się w nich mogą być zupełnie niepotrzebne i niezwiązane z konkretnymi obowiązkami⁹ i nie ma gwarancji, że wyniki uzyskane dzięki takiemu testowi są prawidłowe.

Ponieważ ochrona danych obejmuje grupę praw, nawet systemy przechowywania danych powinny je wspierać. Można uznać, że na jakość systemu przechowywania danych składają się trzy elementy: czas użytkowania, jego cena i funkcje. Eksploatacja systemu zgodnie z prawem jest *cechą jakości*, za którą kierownictwo organizacji ponosi ostateczną odpowiedzialność. Jako prawo ochrona danych nie jest ograniczona przez żadną technikę czy rozwiązania techniczne. Mimo wszystko, technologia może i powinna wspierać ochronę danych.

- Prawo do oczekiwania wystarczającego poziomu bezpieczeństwa danych

Zobowiązuje ono administratorów danych do podjęcia koniecznych i wystarczających środków technicznych i organizacyjnych, aby mieć pewność, że dane osobowe są chronione przed wykorzystaniem ich przez osoby nieupoważnione, przed zmianami i zniszczeniem, a także przed dostępem osób nieuprawnionych.¹⁰

Warto zauważyć, że wymóg zapewnienia bezpieczeństwa danych doprowadził do powstania kilku różnych systemów monitorowania, łącznie ze służącymi do monitorowania pracowników. Na przykład systemy ochrony przez wirusami mogącami zniszczyć pliki z danymi osobowymi mogą wymagać monitoringu systemów poczty elektronicznej. Problem ten

rozwiązano w ustawie o ochronie prywatności wymiany informacji drogą elektroniczną, która chroni dane przesyłane w wiadomościach elektronicznych i wprowadza Dyrektywę WE w sprawie prywatności i wymiany informacji drogą elektroniczną (2002/58/WE).

Ocena

Przetwarzanie danych osobowych i przechowywanie plików z danymi w opisany sposób ma istotne znaczenie dla działalności zarówno sektora prywatnego, jak i państwowego. Akty prawne i zasady dotyczące ochrony danych mają na celu zaproponowanie sposobów rozwiązania konfliktu między ochroną prywatności a potrzebą posiadania informacji o innych członkach społeczeństwa, a także osiągnięcia zadowalającej równowagi między poszczególnymi stronami.

Funkcjonowanie i ogólna aprobata systemów regulujących przetwarzanie danych osobowych zależy nie tylko od tego, czy ustawodawcom udało się znaleźć kompromis między różnymi zagadnieniami związanymi z informacją i jej dostępnością, ale również od tego, jak administratorzy danych i inne osoby biorące udział w przetwarzaniu danych osobowych rozumieją cele ustaw oraz podstawowe prawa człowieka, na których przepisy te opierają się.

Można uznać, że system ochrony prywatności i życia prywatnego składa się z dwóch części: systemu sankcji opartych na przepisach prawa karnego, który zaczyna działać *po fakcie*, oraz systemu ochrony danych dotyczącego automatycznego przetwarzania danych osobowych i przechowywania plików z danymi osobowymi, który zaczyna działać *przed faktem*. Możemy zatem powiedzieć, że zasady ochrony danych są niezbywalne, ale ze względu na swoje działanie koordynacyjne są również niezwykle nowoczesnym elementem mechanizmu prawnego chroniącego dane. Zasady te wskazują administratorom danych granice, co jest dozwolone i dopuszczalne, a także funkcjonują jak znaki drogowe, kierując ich działaniami. Odnosi się to do obowiązku planowania i ochrony oraz szkolenia personelu.¹¹

Jakie więc są potrzebne prawa i zasady chroniące prywatność? Całkiem niedawno opublikowano w Finlandii wyniki badań, w których sprawdzono stosunek obywateli do ochrony danych.¹² Badania wskazały, że obywatele obawiają się raczej o ochronę swoich danych osobowych. Chcą przy tym *wiedzieć*, czy ich dane są przetwarzane i przez kogo. Chcą również *brać udział* w podejmowaniu decyzji ich dotyczących. Warto zauważyć, że prawdopodobnie w większości, nie wiedząc o tym, respondenci opisywali charakter i istotę ochrony danych! Możemy również stwierdzić, że ustawa o ochronie prywatności w życiu zawodowym przybliżyła problem ochrony danych do codziennego życia. Dlatego też ochrona prywatności stanowi niezbywalną część dobrej *jakości życia*, do której każdy z nas ma prawo.

5. Konkretnie działania podejmowane w Finlandii

Jak powiedziano już wcześniej, różne przepisy dotyczące ochrony danych mają być stosowane jednocześnie; nie wykluczają się bowiem wzajemnie. Paragraf 3 obecnej

⁹⁾ Urząd Rzecznika ds. Ochrony Danych wie, na przykład, o testach przydatności stosowanych w Finlandii, w których znajduje się pytanie o przynależność etniczną składającego podanie o pracę: „Czy jest Pan/Pani Indianinem z Ameryki Północnej?”

¹⁰⁾ Zaniedbanie w zakresie bezpieczeństwa informacji podlega karze zgodnie z fińską ustawą o danych osobowych. Podobnie naruszenie poufności danych osobowych może skutkować karą.

¹¹⁾ Ustawa o danych osobowych była wykorzystywana przy opracowywaniu zapytań ofertowych w sprawie systemów ochrony danych.

¹²⁾ Statystyki: Finlandia (Nurmela, Heinonen, Ollila, Virtanen). Matkapuhelin ja tietokone suomalaisen arjessa (Telefony komórkowe i komputery w codziennym życiu Finów). Helsinki 2000. Aktualizacja 2000/2.

ustawy o ochronie prywatności w życiu zawodowym określa wymóg konieczności w następujący sposób:

„Pracodawca może przetwarzać wyłącznie te dane osobowe, które są niezbędne bezpośrednio ze względu na stosunek pracy z pracownikiem, co łączy się z zarządzaniem prawami i obowiązkami stron lub korzyściami przekazywanymi pracownikowi przez pracodawcę lub wynikającymi ze szczególnego charakteru pracy. Nie ma żadnych wyjątków dla wymogu konieczności, nawet za zgodą pracownika.”

Paragrafy ustawy dotyczące testów na obecność narkotyków, obserwowania pracowników za pomocą kamery oraz korzystania z poczty elektronicznej, które omówię w dalszej części, są zawsze zestawiane z wymogiem konieczności oraz innymi zasadami opisanymi w ramowej ustawie o ochronie danych.

Miejsce pracy wolne od narkotyków i testy na obecność narkotyków

Przy opracowywaniu ustawy punktem wyjścia było stanowisko, że narkomania jest chorobą – uzależnieniem. Ponieważ akty prawne dotyczące zdrowia publicznego odnoszą się do przeprowadzania testów na obecność narkotyków, ustawa jako taka nie przewiduje prawa do zmuszenia kogokolwiek do poddania się testowi na obecność narkotyków. Oznacza to, że badanie pacjenta wymaga jego zgody, a test może przeprowadzić wyłącznie lekarz. Ustawa określa jednak warunki, na jakich pracodawcy mają prawo wykorzystania dokumentu zawierającego wyniki testu. Prawo do wykorzystania takiego dokumentu – o ile w ogóle jest do przyjęcia wykorzystanie takiego dowodu – wynika z ustawodawstwa i jest związane z zadaniami, które nakłada zajmowane stanowisko. Gwarantuje to zabezpieczenie pozostałych podstawowych praw.

Ogólne warunki są następujące: 1) pracodawcy mają obowiązek opracowania wraz z personelem programu antynarkotykowego, 2) stanowiska, które wiążą się z prawem do wykorzystania dowodu, powinny podlegać procedurze wspólnych uzgodnień. Program antynarkotykowy wraz z przepisami prawa pracy zawiera instrukcje dla pracowników, jak mają postępować w przypadku pozytywnych wyników testu.

Pracodawcy przed zawarciem umowy i przed zmianą warunków zatrudnienia muszą poinformować składających podania o pracę, że dane zadanie wymaga dostarczenia pracodawcy wyników testu.

Pracodawca wyraża zgodę na opłacenie kosztów testu. Ministerstwo Spraw Społecznych i Zdrowia wydało rozporządzenie w sprawie przeprowadzania testów, które jest wiążące dla lekarzy. Jeżeli pracodawca skorzysta z usług innych osób niż wymienione jako upoważnione do przeprowadzania testów, mogą zostać nałożone sankcje.

Testy na obecność narkotyków można również przeprowadzić w ramach usług lekarza medycyny pracy. W takim przypadku to lekarz – nie pracodawca – decyduje, czy test jest potrzebny. Wyniki testu nie są przekazywane pracodawcy, który zamiast nich otrzymuje ogólną informację, czy dana osoba nadaje się na dane stanowisko.

Ponadto pracodawca może wykorzystać wynik testu na obecność narkotyków, o ile pracownik wyraził zgodę na opiekę nad nim na podstawie pozytywnych wyników testu, a wykorzystanie wyników jest związane z monitoringiem sprawowanej opieki.

Kontrola techniczna

Na początku należy zaznaczyć, że niektóre elementy stosunku pracy same z siebie uprawniają pracodawcę do kontrolowania działań pracownika w ramach przywileju kierowniczego pracodawcy. Z drugiej jednak strony, wymagania dotyczące bezpieczeństwa mogą oznaczać, że pracodawca ma obowiązek przeprowadzania kontroli technicznej. Ustawa o ochronie prywatności w życiu zawodowym nie uprawnia do ani nie nakłada obowiązku kontroli technicznej pracowników. Zgodnie z rządową propozycją: „Inne akty prawne pośrednio nakładają ograniczenia na prawa pracodawcy do przeprowadzania kontroli, na przykład przez nakładanie sankcji za określone działania naruszające prywatność.”

Wymóg przeprowadzania kontroli technicznej oraz wszelkie zmiany w tym zakresie muszą przejść procedurę wspólnych uzgodnień. Pracodawca musi określić cel kontroli i metody jej przeprowadzenia. Następnie musi poinformować pracowników o swojej decyzji. Mogą oni oddać sprawę do rozpatrzenia osobom odpowiedzialnym za przestrzeganie porządku prawnego.

Obserwacja za pomocą kamery

Przepisy przewidują prawo użycia kamery do obserwowania pracowników w miejscu pracy, chociaż celem obserwacji nie jest kontrola pracowników. Pracodawca może wykorzystać kamerę do prowadzenia obserwacji, o ile ma to na celu:

- zapewnienie bezpieczeństwa pracownikom i innym osobom pracującym na danym terenie;
- ochronę mienia;
- nadzór nad prawidłowym przebiegiem operacji i procesów produkcyjnych;
- zapobieganie sytuacjom zagrażającym bezpieczeństwu, mieniu lub procesom produkcyjnym lub wyjaśnienie ich.

Zazwyczaj kamery nie wolno wykorzystywać do obserwowania określonego pracownika lub określonych pracowników w miejscu pracy.

Nie wolno prowadzić obserwacji za pomocą kamery w toaletach, w szatni ani w pomieszczeniach socjalnych dla pracowników. Jest to również zabronione w pomieszczeniach wyznaczonych do osobistego użytku pracowników.

Jeżeli obserwacja za pomocą kamery jest konieczna, może ona objąć określone miejsce pracy, w którym pracują pracownicy, o ile:

- jej celem jest zapobieganie rzekomemu zagrożeniu wystąpieniem zakłóceń związanych z pracą bądź rzekomej niedogodności lub zagrożeniu bezpieczeństwa lub zdrowia pracownika, lub
- obserwacja jest niezbędna dla zapobiegania wykroczeniom przeciwko mieniu i ich wyjaśniania, o ile podstawowa część zadań pracownika obejmuje obsługę mienia, którego wartość lub jakość jest znacząca, takiego jak pieniądze, obligacje czy kosztowności, lub
- interesy i prawa pracownika powinny być zabezpieczone przez prowadzenie obserwacji za pomocą kamery na prośbę pracownika.

Obserwacja przy użyciu kamery powinna być prowadzona na możliwie najbardziej przejrzystych zasadach i ma być niezbędna do osiągnięcia celu. Nagrania uzyskane w wyniku obserwacji można wykorzystać wyłącznie do celu, dla którego obserwacja była prowadzona. Przed

rozpoczęciem obserwacji za pomocą kamery należy sprawdzić, czy nie ma możliwości zastosowania innych środków, które w mniejszym stopniu ingerują w prywatność pracowników.

Należy poinformować pracowników o rozpoczęciu obserwacji za pomocą kamery, o jej prowadzeniu oraz o sposobie i sytuacjach, w jakich nagrania zostaną wykorzystane, a także o rozmieszczeniu kamer, jeżeli za ich pomocą obserwowane jest miejsce pracy. Informacja o obserwacji przy użyciu kamer musi zostać również przedstawiona w zauważalny sposób tak, by było wiadomo, czy dane miejsce podlega obserwacji.

Istnieją określone wyjątki dotyczące celu wykorzystania nagrań uzyskanych dzięki obserwacji za pomocą kamery:

- nagrania można wykorzystać jako uzasadnienie rozwiązania umowy o pracę,
- pozwolą na wyjaśnienie lub uzasadnienie zakłóceń porządku, molestowania lub nieodpowiedniego zachowania, o których mowa w ustawie o równouprawnieniu oraz w ustawie o higienie i bezpieczeństwie pracy, o ile pracodawca ma uzasadnione podstawy podejrzewać, że pracownik jest winny takiego zachowania,
- ułatwią wyjaśnienie wypadków przy pracy.

Zazwyczaj nagrania powinny zostać zniszczone w chwili, gdy przestają być potrzebne do osiągnięcia celu, dla którego prowadzono obserwację, a najpóźniej w ciągu roku.

Jeżeli pracodawca musi użyć kamery do obserwacji wbrew przepisom lub w sposób naruszający zasady przejrzystości prowadzenia obserwacji za pomocą kamery, może zostać ukarany grzywną, o ile czyn ten w tym samym czasie nie ma wyraźnych oznak nielegalnego podglądania podlegającego wyższej karze.

Poczta elektroniczna

W myśl przepisów inna osoba może otworzyć i przeczytać wiadomość za zgodą pracownika, według zasad ustalonych w danym miejscu pracy. Wymaga to podania przez pracownika nazwy użytkownika i hasła współpracownikowi. Nowe przepisy mają na celu udzielenie odpowiedzi, co zrobić w przypadku nieudzielenia przez pracownika takiej zgody.

Aby pracodawca mógł skorzystać ze swoich uprawnień, warunkiem koniecznym jest wcześniejsze zaproponowanie pracownikowi różnych możliwości, które – o ile pracownik z nich skorzysta – zazwyczaj oznaczają, że nie będzie potrzeby wykorzystania wiadomości e-mail pracowników. Jedną z możliwości jest automatyczne powiadomienie nadawcy wiadomości wysyłane przez system z informacją o nieobecności danego pracownika wraz z danymi jego zastępcy. Inną alternatywą jest przekierowywanie w czasie nieobecności pracownika wiadomości do innej osoby lub na inny adres używany przez innego pracownika. Zaproponowanie takich możliwości wymaga podjęcia działań przez samego pracownika, ponieważ pracodawca nie ma prawa do wprowadzania takich zmian w pocztę pracownika.

Mimo zapewnienia przez pracodawcę tych środków, pracownik nie ma obowiązku skorzystania z proponowanych możliwości. O ile pracownik nie skorzysta z tych możliwości, pracodawca musi dowiedzieć się, czy wiadomości należące do pracodawcy zostały przesłane do pracownika podczas jego nieobecności, czy wysłał on wiadomości należące do pra-

codawcy tuż przed swoją nieobecnością. Wiadomości te muszą mieć charakter informacji, które pracodawca powinien bezzwłocznie poznać w celu zakończenia negocjacji związanych z prowadzoną działalnością, w celu obsługi klientów lub z innych względów mających na celu umożliwienia wypełnienia jego funkcji. Takie sytuacje obejmują np. sprawy związane z zamówieniami, fakturowaniem i reklamacjami, jak również negocjacje handlowe.

Ocena, czy wiadomość należy do pracodawcy, może w praktyce nastąpić wyłącznie na podstawie informacji dotyczących danych identyfikacyjnych nadawcy lub tytułu w adresie. Informacje te nie należą do istoty treści wiadomości poufnej. Chociaż w większości przypadków z informacji tych można wywnioskować, czy wiadomość jest prywatna, nie zawsze jest to jednak możliwe. Z tego powodu warunkiem koniecznym odczytania wiadomości e-mail są dodatkowe kryteria, które muszą zostać spełnione przed ujawnieniem wiadomości e-mail:

- 1) pracownik wykonuje swoje zadania niezależnie, co zwykle oznacza, że nikt inny nie zajmuje się w tym samym czasie daną sprawą;
- 2) ze względu na zadania lub sprawy będące w toku załatwiania, a należące do pracownika, oczywiste jest, że wiadomość została przesłana do niego;
- 3) pracownik jest nieobecny w pracy;
- 4) przed otwarciem wiadomości pracodawca umożliwił pracownikowi wyrażenie zgody na otwarcie;
- 5) poznanie treści wiadomości to sprawa niecierpiąca zwłoki.

Prawo przewiduje również szczególny przepis w sytuacji, w której nastąpił zgon pracownika lub w której stał się on trwale niezdolny do wykonywania swoich zadań, kiedy to uzyskanie jego zgody na ujawnienie wiadomości jest niemożliwe.

Po odnalezieniu wiadomości pracownikowi należy przekazać pisemne wyjaśnienie (w odniesieniu do drugiego przypadku).

Po ujawnieniu wiadomości można ją otworzyć, o ile jest oczywiste, że należy ona do pracodawcy i spełnia opisane kryteria. Warunkiem koniecznym są również bezskuteczne próby skontaktowania się z nadawcą lub odbiorcą wiadomości w celu poznania treści wiadomości lub przesłania wiadomości na inny adres e-mail wskazany przez pracodawcę.

Pracownikowi należy przekazać pisemne zawiadomienie o otwarciu wiadomości.

6. Wniosek

Do dzisiaj inne Państwa Członkowskie Unii Europejskiej nie uchwaliły jeszcze ustawy o ochronie prywatności w życiu zawodowym. Jednak szczególne sytuacje i kategorie danych w miejscu pracy, takie jak dane dotyczące zdrowia, są objęte specjalnymi przepisami. Trzeci model postępowania ma wykorzystywać kody postępowania charakterystyczne dla danych sektorów.

Doświadczenia Finlandii w związku z ustawą o ochronie prywatności w życiu zawodowym generalnie są pozytywne. Z badań wynika, że prawo pracowników do otrzymania informacji uległo poprawie, systemy informacyjne są planowane w efektywniejszy sposób, a prace nad projektem kodów kontaktu już rozpoczęto.

Emilio Aced-Félez

President, Joint Supervisory Body of Europol
Przewodniczący, Wspólny Organ Nadzorczy nad Europol

The contribution of Joint Supervisory Body Europol in efficient implementation of data protection in the field of police cooperation in the European Union

Article 29 of the „Treaty on European Union” (TEU)¹ states that „(...)the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia. That objective shall be achieved by (...) closer cooperation between police forces, customs authorities and other competent authorities in the Member States, both directly and through the European Police Office (Europol) (...)”.

Also Article 30 of TEU, which lists the procedures for common actions of the European Union that should constitute the basis for police cooperation, in its part regarding the processing and exchange of information, states that: „(...) the collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions, in particular through Europol, subject to appropriate provisions on the protection of personal data” and further on, „(...) The Council shall promote cooperation through Europol (...)”.

This means that TEU assigns Europol a privileged status and a vital role in creating the necessary system of exchange of information between the police forces of the Member States as well as in increasing the technical possibilities and coordinating different forces and law enforcement agencies.

However, it is clear from the beginning that these actions that are vital for combating crime in the European Union, within the creation of a space of freedom, justice and security, have to take place in compliance with point b of Article 30(2) of TUE, in accordance with regulations on personal data protection.

This statement, as clear and simple as it is, contains in itself a reference to the complex system of applying various local and European (of the Council of Europe as well as those of the European Union) regulations in the field of police activity.

Indeed, the activities of Europol are contained in what has been named „The Third Pillar of the European Union”, which means police and judicial cooperation in criminal cases, in the area of cooperation not subject to community law, which is thus regulated by specific rules *ad hoc*.

So, the processing of personal data in this area shall be subject to state regulations, both in the field of data collection by Member States, and in the field of taking the decision regarding the possibility to transmit them to Europol. At the same time, from the moment when the decision to transmit data to Europol is taken, the specific regulations must be applied that are included in the Convention on the establishment of a European Police Office („Europol Convention”)² that limits data transmission to crimes that lie within the competences of Europol, and the categories of data that may be collected in its archives.

Finally, both Europol and the Member States must fulfil, on general basis, the recommendations contained in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – also known as the „Convention 108” and in the Recommendation No. (87) 15 on the use of personal data in the police sector³ (both documents are created by the Council of Europe), that establish basic principles for data processing by law enforcement agencies.

Thus, the Joint Supervisory Body of Europol (JSB), operates within a complex framework, and its structure, properties and competences are a reflection of that complexity, since in many decisions it has to take into consideration local legal regulations of each Member State, the above-mentioned legal framework of the Council of Europe, the provisions of the „Europol Convention” itself, and finally the general rules of the Treaty on European Union. Moreover, all these have to be applied with at the same time respecting the rights of individuals whose data are processed by Europol, and with the efficiency of the basic tasks that the body has to perform.

In order to analyse the contribution of JSB into data protection within the framework of police cooperation in the European Union, one needs, first, to define the role, the rights and competences that result from Europol Convention, and to emphasize, first of all, its basic characteristic feature, that results from its specific and principal character – the independence from any other institution or body, either national or European.

This distinctive trait of the Body is precisely defined in the first sentence of the article establishing Convention: „Article 24 Joint Supervisory Body 1. An independent joint supervisory body shall be set up (...). The joint supervisory body shall be composed of not more than two members or representatives (...) of each of the national supervisory bodies guaranteed to be independent and having the necessary abilities, and appointed for five years by each Member State. (...) In the performance of their duties, the members of the joint supervisory body shall not receive instructions from any other body”.

¹) Full text is available in OJ C325 of 24.12.2002, P.1.

Full legislation of the European Union is available online at <http://europa.eu.int/eur-lex/lex/en/index.htm>

²) OJ C316 of 27/11/1995 p. 0002-0032

³) All documents of the Council of Europe on data protection are available online at: http://www.coe.int/T/E/legal_affairs/Legal_co-operation/Data_protection

This article contains four basic principles that guarantee independence: a formal and principal declaration of the above-mentioned independence on the part of Convention as the greatest guarantee thereof, the necessity to present guarantees by each of its members, defining the impassable term of office of five years, during which the members are irremovable, and the obligation of members to reject any external intervention as well as the obligation of all other institutions or bodies, national or European, to abstain from any activities that might influence the decisions of JSB. The last point means that both any attempt to influence the decisions of any member by any body and any attempt of JSB to seek clue, advice or guidelines at any body shall be illegal.⁴

Within the general framework of the task which is to supervise the activities of Europol in order to guarantee that collecting, processing and utilization of data in possession of Europol does not violate rights of individuals, the Convention grants to Europol the following major tasks: analysing the resolutions on creating data files, analysing the principles for access to personal data files, and the general principles for transmitting personal data by Europol to third states and bodies; checking, on request of each individual whether the manner in which his personal data have been collected, stored, processed and utilized by Europol is lawful and accurate; drawing up activity reports at regular intervals, and investigating, through the Committee of Appeal created within the Body, any complaints placed by individuals who believe that Europol reacts inaccurately to their applications to execute the rights to access, check, correct and delete data.

In order to perform these functions, the Body, according to the provisions of Article 2 of Rules of Procedure „(...) shall be authorized to obtain information from Europol, to be given access to all documents and paper files as well as access to the data stored by Europol, and to be granted free access to all Europol premises at any time (...). This includes information on and access to hardware and software, whenever this is necessary for the performance of the tasks of the Joint Supervisory Body. Details may be stipulated in arrangements between the Joint Supervisory Body and the Management Board of Europol."

JSB has issued dozens of reports on research projects in various areas of organized crime that are subject to Europol, on which no closer information can be provided due to confidentiality regulations in Europol, as this information is classified.

However, it is necessary to remark on the initial works of JSB and Europol, that aimed at determining the pattern for creating data files – a manner that would enable to connect the need for appropriate supervision with the necessary flexibility of creating these files, so that they are useful for the purpose of achieving their set objectives and to facilitate police cooperation when it is needed.

In the opinions concerning the creation of specific files, JSB pointed out various aspects that need to be taken into account, which resulted in changing some of these files. Among these are the comments made by the Body in some cases, regarding the need

for proper justification for opening a file basing on clear guidelines that suggest that there is a possibility of committing a future crime that might lie in the competences of Europol; the need to treat data related to drug abuse as especially protected data and as a result, to subordinate to strict regulations on processing such data; the need to subordinate to guarantees contained in the national legal regulations on introducing biometric data, such as DNA, or the need to take specific precautions while processing data of witnesses or victims – in this case the JSB expresses the opinion that they should be processed anonymously, if possible.

In relation to the principles regulating keeping working files for analytical purposes, during the preparatory works prior to approving the Council Act of November 27, 2003 drawing up, on the basis of Article 43(1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention (2004/C/2/01)⁵, the JSB intervened firmly, proposing a solution of a crucial problem related to the procedures of data storage in specific analysis files. This proposal was approved and included by the Council in the amending protocol.

The regulations on data storage in specific analysis files, as defined in Article 21 (3), foresaw the deletion of personal data of individuals, which have not been updated or to which no additions have been made for a period of three years. Otherwise, a new three-year period was started, during which data could be legally stored.

However, such system, designed in order to protect individuals from infinite storage of their personal data without timelimit, without any reasons to justify such storage (it is difficult to justify the storage of personal data of an individual, for whom there has been no reason for data storage for the previous three years), proved absolutely unsuitable for combating specific forms of crime – especially terrorism – those where criminals remain hidden while they wait for orders to start action, or in case of criminals whose data are not updated, as they are currently imprisoned, but who may be suspected of remaining in the structure of terrorist organization, which hints they might return to criminal activity after their punishment.

After having analysed various alternative solutions, JSB suggested that a suitable solution that would satisfy both the need for police efficiency and the need to protect rights of individuals, would be to conduct an annual documented evaluation of the necessity to keep the data of individuals whose data are stored in AWF, together with a three-year evaluation on keeping each specific analysis file. Moreover, keeping personal data of an individual in a specific analysis file cannot exceed the period of existence of this file.

This system, in connection with the possibility to verify its proper application by JSB, especially thanks to the possibility to conduct inspections of Europol, allows to keep a balance between police needs and citizen's rights.

JSB has also expressed opinions on several Europol projects, in relation to management of the Index System that enables law enforcement agencies and liaison officers

4) All these points are further precisely defined in Article 4 of the Act 1/99 of Joint Supervisory Body of Europol of 22 April 1999, laying down its Rules of Procedure (1999/C 149/01), and defining the procedures for regulating any possible conflict of interest between members of the JSB.

5) OJ C 2 z 06.01.2004. P. 1

from Member States, who do not participate in a given investigation, to access specific information from AWF. JSB expressed its opinion on the case in 2001, and recently in 2005, by issuing two decisions.⁶

The main feature of these decisions, as well as others related to searching Europol systems (also known as *audit logs*) presented by Europol in relation to a temporary Index System or searching technological systems that constitute AWF carriers, is the activity of another working party of JSB – the IT Sub-group. The task of this Sub-group is to support Europol at the early stages of new projects, so that the position of the Body on their adaptation to data protection principles, on the need to introduce technological changes increasing the protection of personal data or allowing JSB higher efficiency of supervision, is taken into consideration already at the stage when decisions determining a further development of such projects are taken.

At the same time, the activities of the IT Sub-group enable an exchange of opinions with Europol, which facilitates the understanding of the goals of the projects and the problems related to their implementation, so that it is easier to find solutions that are acceptable both for Europol and for JSB.

The participation in agreements between Europol and third states and bodies is a vital issue that has required much time and effort on the part of JSB so far and probably will require as much in the future. Two aspects make this issue crucial.

Firstly, due to the fact that personal data transmitted by Europol to third states must be covered by appropriate guarantees, if not identical to those existing in the European Union, then at least suitable for the type and sensitivity of the data. Secondly, everybody can understand the international implications that may result from JSB taking, in the process of negotiating an agreement, a specific position that could obstruct taking a decision that would be considered strategic by the bodies governing Europol, and possibly by the agencies of the given third state.

So, JSB has again decided to establish a Sub-group that would be able to conduct detailed analysis of the projects that are received by the Body and to offer rational suggestions regarding their content.

Moreover, the JSB takes part in two stages of each project. First, it issues an opinion regarding the existence of irremovable obstacles for beginning negotiations with a given state or body, and then, on the last stage, when the project of agreement that results from the negotiating process is presented for approval. The participation of the International Sub-group is vital on both stages.

There are numerous opinions in this respect, that are available on the website of JSB. For illustrative purposes though, I shall present here two examples where the participation of the Body proved vital and decisive.

The first example refers to negotiating the agreement between Europol and the United States in the context of the difficult period that followed the terrorist attacks of 11 September 2001.

The process started with the decision of Director of Europol to transmit some data to American agencies – within the competences that he is given by point b, Article 2 (1) of Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third states and third bodies (1999/C 88/01)⁷ – referring to the existence of imminent danger.

When JSB was notified about this decision, it informed Europol that it would be considered unsuitable to continue transmitting data basing on the same prerequisite, and that it is necessary to use the general regulations for transmitting personal data to third states, in compliance with Article 2 (1), which means concluding an agreement between Europol and the United States.

As a result, a process was started, that might lead to ratification of this agreement. At the very beginning JSB issued an opinion that contained the whole series of comments, on what should be taken into consideration in the negotiating process. Cooperation with the Body was offered as well, in order to ensure including all provisions that were considered vital in the agreement without causing a detriment to the independence of the final opinion at the same time.

So, a delegation of JSB has followed the whole process closely, and even was present during several negotiating sessions. Finally, a project was developed that included all issues considered necessary by the Body.

Another essential agreement, where the comments of JSB even led to changes in the existing legal framework, were the negotiations of the agreement between Europol and Interpol. While negotiating this agreement, it proved that there was a problem with ensuring that the information transmitted from Europol to Interpol would really reach their true recipients which are the police agencies belonging to Interpol.

Article 5 (5) of the Council Act 1999/C 88/01 states it clearly that it is forbidden to further transmit to third parties the data that Europol transmits to third states or bodies. The interpretation issued by the JSB in this specific case showed that Interpol, as an independent and autonomous body, was the authorised recipient of data transmitted by Interpol, so it could not transmit them onward without violating the existing regulations.

The problem was the fact that the General Secretariat of Interpol acts mainly as a body enabling mediation and cooperation between its members, and the information it receives are of no value unless it can share it with other members of the body.

When the JSB pointed out the problem in its first decision after the start of the negotiations, the Council prepared an amendment to the Act 1999/C 88/01, that was presented to the JSB, and it found that the guarantees set to protect such onward transmission were appropriate, so it issued a positive opinion which led to the change in the

⁶) Both the decisions (02-10 and 05-12), as well as other documents not subject to regulations on classified documents are available on the JSB website <http://europoljsb.ue.int>

⁷) OJ C 88 z 30.03.00. P. 1.

Act 1999/C 88/01 which was changed by Council Act of 28 February 2002, amending the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies (2002/C 76/01).⁸

This legal instrument stated that onward transmission of data is possible in cases where the third state or body receiving the data has concluded an agreement with Europol on the transmission of personal data which covers data from onward transmission; or after authorisation by the Director of Europol if he considers onward transmission of the data by the third body to be absolutely necessary to safeguard the essential interests of the Member States or in the interests of preventing imminent danger associated with crime. In such case Europol was obliged to immediately notify the Management and the JSB on the Director's decision. Furthermore, no onward transmission of data would be allowed without the consent of the Member State that transmitted the data to Europol.

Another important element of the policy of supervising Europol by the JSB is the idea, that emerged at the very beginning of its activity, that it is necessary to periodically inspect Europol, which resulted in presenting an Inspection Plan that had been developed by the existing fixed interdisciplinary Inspection Sub-group, that performs an annual audit of Europol. After conducting the inspection, it prepares a report that is approved by the JSB at the General Meeting and then transmitted to Europol. The report, that contains facts and conclusions related to these, also features a series of attached recommendations, that Europol should implement in order to better adapt the processing of personal data to the provisions set by existing legal regulations. The degree of fulfilling these recommendations of an inspection is then checked during the following inspection, which is described in a separate report.

The inspections showed clearly that Europol pays due attention to the issue of protecting personal data, however during the inspections some elements were discovered, that, in the opinion of JSB, should be amended, safeguards that should be introduced and procedures that need improving. In several cases the inspections noticed certain activities of Europol related to Member States, that, in the opinion of JSB, which the management of Europol later agreed with, were not in full compliance with the provisions of the Convention and, as a result, were removed within several months.

Initially, the inspections were of general nature, which allowed to learn about Europol's technical infrastructure, general management of systems and implemented safeguards. Gradually, the inspections started to focus on more specific matters, and they became more content-oriented. This means that as the amount of information processed by Europol increased, the inspections started focusing on issues related to their quality, topicality and proportionality in relation to the goals set in decisions on creating specific files.

Another issue that the JSB focuses on are the activities aimed at increasing the transparency of its works and informing about ongoing activities and decisions taken, in order to increase citizens' awareness.

The IT Sub-group has done a job of great value, which included opening a website, which is constantly being updated and offers still more up-to-date information.

It has also actively cooperated with the secretariat of Europol in order to suggest necessary amendments in the Rules of Procedure to adapt the principles of access to JSB documents to the general principles of transparency for European institutions, at the same time maintaining the necessary confidentiality of some of its working documents and opinions.

Furthermore, these new norms formally confirm the principle that JSB activity reports are presented to the Parliament, which used to be a common practice, but only after the approved amendments to the Rules of Procedure are published in the Official Journal, they will become an additional element strengthening the relationship between both bodies, especially since the Parliament has always been particularly sensitive to the necessity for protection of personal data in the field of police cooperation.

One must also mention the works of this Sub-group related to the organization and planning of the conference organized by JSB in October 2006, in order to analyse the current and future situation of data protection in the field of European police cooperation, in particular the way in which it influences and in the future will influence Europol, and so the Body itself. Representatives of the European Parliament, the Council of European Union, Europol, national data protection authorities, representatives of the citizens' society, and of course the JSB itself, will take part in this Conference.

Further to the reports that the JSB has to present periodically, the Joint Supervisory Body developed two activity reports, which are both available on its website, the first for the period between 1998-2002, and the second one for the period between 2002-2004. Starting from the second report, the JSB decided to prepare reports for two-year periods, that are the same as the periods of presidency of the body, and so by the end of this year a new report should be prepared which should be published at the beginning of 2007.

These reports are treated by the JSB as a valuable means of communicating and spreading knowledge, so it attempts to present the ongoing works, existing problems and decisions taken in a given period in a clear and attractive manner, emphasizing the major issues, problems that it managed to solve and those that yet are to be solved, as well as plans and strategies for further activity.

Finally, it is necessary to mention the works of the JSB Appeals Committee, that was established basing on the provisions of Art. 24 (7) of "Europol Convention". The Committee is the only and last resort of appeal from decisions of Europol related to the execution of rights of individuals to access, change, correct or delete data.

The Convention grants these rights to all individuals whose data are processed. If they are not satisfied with the position of Europol, they may appeal to the Appeals Committee, whose decisions are binding for Europol, and there is no possibility to appeal from them to another resort, which gives them *quasi*-judicial validity and makes it a unique body within the European legal framework.

In the process of taking decisions the Committee takes into consideration mainly the norms defined in Article 19 of the Convention, which is very complex and introduces parallel application of state legal regulations and specific regulations of the Convention, which are often difficult to apply in real cases that the Committee encounters.

However, the Committee has always emphasized the necessity to analyse particular cases in detail by Europol, instead of taking standard decisions that do not take into account the specific circumstances of each case of appeal, and the necessity to promote the highest possible level of protection of citizens' rights. All the decisions of the Committee are open and available on the website of JSB.

Finally it is worth mentioning how the role of JSB members has been changing. Initially, the role of JSB was mainly reactive, which means that it mostly issued opinions and decisions related to documents or projects originating from Europol. This role, although it has never completely disappeared, and never will cease to exist, caused the emerging of the whole new series of more pro-active tasks, that certainly will become still more important.

The first sign of this new role were the inspections of Europol. They were not caused by any external factors but by the decision of JSB to improve their knowledge about the real practical activities of Europol in the field of processing personal data.

Later on, this role was developed by the IT Sub-group, which, thanks to direct contact and frank exchange of ideas, provided Europol with guidelines related to improving the adaptation of technological and operational requirements to the necessity to guarantee basic rights to protection of personal data on the initial stages of project development, with results that satisfied both parties. Thus, these activities will develop still more extensively and will constitute an integral part of Europol's project development strategy.

Gradually, this form of cooperation has moved to other areas under supervision of the JSB, such as negotiating agreements with third states, or formulating a new approach to data processing for the purpose of fighting crime, and even activities that aim at increasing the transparency and openness of the activity of JSB, mainly through the plan to organize a conference, for the first time in its history, or closer relationship with the European Parliament. The coordinating activities and works of the secretariat of JSB create the necessary support in all these fields.

Due to all the reasons mentioned above, I truly believe that the Joint Supervisory Body of Europol has made a vast contribution, within its competences, to the consolidation of a data protection system that respects principles and rights of individuals, from a pragmatic and well-balanced point of view, by means of developing guidelines, that instruct how to adapt police activities to the requirements of state and European legal regulations, by seeking solutions that do indeed practically improve the protection of individuals, at the same time avoiding the creation of obstacles that could hinder Europol from performing its tasks. When necessary, it objected firmly to these projects or interpretations of the Convention and acts that it considered unlawful.

Because of all that, any future changes in the legal framework within which Europol operates, will have to take the body into consideration, and also will be able to welcome valuable contribution from the state bodies, through their representatives in the Joint Supervisory Body of Europol.

Wkład Wspólnego Organu Nadzorczego Europol w skuteczne wdrażanie ochrony danych w dziedzinie współpracy policyjnej w Unii Europejskiej

Artykuł 29 „Traktatu o Unii Europejskiej” (TUE)¹ mówi, że „(...) celem Unii jest zapewnienie obywatelom wysokiego poziomu bezpieczeństwa wewnątrz przestrzeni wolności, bezpieczeństwa i sprawiedliwości poprzez opracowanie wspólnych działań między Państwami Członkowskimi w zakresie współpracy policyjnej i prawnej w sprawach karnych oraz poprzez zapobieganie i zwalczanie rasizmu i ksenofobii. Cel ten należy osiągnąć (...) za pomocą szerszej współpracy między siłami policyjnymi, służbami celnymi i innymi właściwymi organami Państw Członkowskich, bezpośrednio lub za pośrednictwem Europejskiego Urzędu Policji (Europol) (...)”.

Również artykuł 30 TUE, w którym wymienione są procedury wspólnych działań Unii Europejskiej, na których powinna opierać się współpraca policyjna, w ustępie mówiącym o przetwarzaniu i wymianie informacji, stanowi, że „(...) gromadzenie, przechowywanie, przetwarzanie, analizowanie i wymiana istotnych informacji, w szczególności za pośrednictwem Europolu, włącznie z informacjami dotyczącymi sprawozdań dotyczących podejrzanych operacji finansowych, znajdującymi się w posiadaniu organów ścigania, z poszanowaniem odpowiednich postanowień w zakresie ochrony danych osobowych” i dalej „(...) Rada będzie umacniać współpracę za pośrednictwem Europolu (...)”.

Oznacza to, że TUE przyznaje Europolowi uprzywilejowane miejsce i zasadniczą rolę w tworzeniu niezbędnego systemu wymiany informacji między służbami policyjnymi poszczególnych Państw Członkowskich i zwiększaniu możliwości technicznych oraz koordynacji między różnymi siłami i organami bezpieczeństwa.

Ale jednocześnie, od początku jest jasne, że te zasadnicze dla walki z przestępczością w Unii Europejskiej, w ramach tworzenia przestrzeni wolności, sprawiedliwości i bezpieczeństwa, działania muszą odbywać się, zgodnie z punktem b ustępu 2 artykułu 30 TUE, w ścisłej zgodzie z przepisami o ochronie danych osobowych.

To zdanie, krótkie i proste, zawiera w sobie odniesienie do złożonego systemu stosowania różnych norm krajowych i europejskich (zarówno Rady Europy, jak i Unii Europejskiej) w działalności policyjnej.

¹⁾ Tekst ujednolicony opublikowany jest w Dz.U. C325 z 24.12.2002, P.1. Pełne ustawodawstwo Unii Europejskiej jest dostępne pod adresem: <http://europa.eu.int/eur-lex/lex/es/index.htm>.

Rzeczywiście działania Europolu mieszczą się w ramach tego, co zostało nazwane „Trzecim Filarem Unii Europejskiej”, czyli współpracy policyjnej i prawnej w sprawach karnych, w dziedzinie współpracy niepodlegającej prawu wspólnotowemu, a więc uregulowanej szczególnymi przepisami *ad hoc*.

Dlatego przetwarzanie danych osobowych w tej dziedzinie będzie podlegało przepisom krajowym, zarówno w zakresie gromadzenia tych danych prowadzonego przez Państwa Członkowskie, jak i w zakresie decyzji o możliwości przekazywania ich do Europolu. Jednocześnie od momentu podjęcia decyzji o przekazaniu ich do Europolu, należy również stosować szczególne przepisy określone w „Konwencji o utworzeniu Europejskiego Urzędu Policji” („Konwencja o Europolu”)² zawierającej ograniczenie przekazywania danych do przestępstw mieszczących się w kompetencji Europolu i kategorii danych, jakie mogą być gromadzone w jego archiwach.

Na koniec, zarówno Europol, jak i Państwa Członkowskie muszą spełniać na ogólnych zasadach zalecenia, określone w „Konwencji o ochronie osób fizycznych w zakresie zautomatyzowanego przetwarzania danych osobowych” – czyli „Konwencji 108” oraz „Rekomendacji (87) 15 dotyczącej ochrony danych osobowych wykorzystywanych w sektorze policji”³ (oba dokumenty są dokumentami Rady Europy), ustalające podstawowe zasady przetwarzania danych osobowych przez siły policyjne.

Wspólny Organ Nadzorczy Europol (WON) działa więc w skomplikowanych ramach, a jego struktura, właściwości i uprawnienia stanowią odzwierciedlenie tej złożoności, ponieważ w wielu decyzjach musi uwzględniać jednocześnie przepisy prawa krajowego każdego Państwa Członkowskiego, wspomniane wcześniej ramy prawne Rady Europy, postanowienia samej „Konwencji Europolu” i ogólne zasady „Traktatu o Unii Europejskiej”, a ponadto połączyć to wszystko z odpowiednim poszanowaniem praw osób, których dane przetwarzane są przez Europol i ze skutecznością zasadniczych zadań, jakie ta organizacja ma spełniać.

Aby przeanalizować wkład WON w o ochronę danych w ramach współpracy policyjnej w Unii Europejskiej należy, po pierwsze, określić rolę, uprawnienia i kompetencje, jakie wynikają z „Konwencji Europolu” i podkreślić, przede wszystkim, jego podstawową cechę charakterystyczną, wynikającą ze szczególnego i zasadniczego charakteru – niezależność od jakiegokolwiek innej instytucji lub organu krajowego czy europejskiego.

Ta cecha wyróżniająca Organ określona jest wyraźnie w pierwszym zdaniu artykułu powołującego go „Konwencji”: „Artykuł 24. Wspólny organ nadzorczy. 1. Zostanie powołany niezależny organ nadzorczy (...). Wspólny organ nadzorczy będzie składał się z maksimum dwóch członków lub przedstawicieli (...), którzy będą dawać najwyższe gwarancje niezależności i posiadać wymagane zdolności, będą oni powoływani przez każde Państwo Członkowskie na okres pięciu lat. (...) W ramach pełnionych funkcji członkowie wspólnego organu nadzorczego nie będą otrzymywać poleceń od żadnego innego organu”.

W ustępie tym zawarte są cztery podstawowe zasady gwarantujące tę niezależność: formalna i zasadnicza deklaracja wspomnianej niezależności ze strony „Konwencji” jako największa jej gwarancja, konieczność przedstawienia gwarancji przez każdego z jej członków, określenie nieprzekraczalnej kadencji pięcioletniej, w czasie której członkowie są nieusuwalni oraz obowiązek członków do odrzucania jakiegokolwiek ingerencji z zewnątrz oraz obowiązek wszelkich innych instytucji lub organów, krajowych czy europejskich, powstrzymania się od jakichkolwiek działań mogących wpłynąć na decyzje WON. Ten ostatni punkt oznacza zarówno nielegalność jakiegokolwiek próby wpływu na decyzje któregoś z członków ze strony jakiegokolwiek organu, jak również zwracanie się przez WON lub któregoś z jej członków o wskazówki, porady lub wytyczne do jakiegokolwiek organu.⁴

W ramach ogólnych zadań czuwania nad działaniem Europolu w celu zagwarantowania, że gromadzenie, przetwarzanie i posługiwanie się danymi będącymi w posiadaniu Europolu nie narusza praw osób, „Konwencja” przyznaje WON następujące najważniejsze zadania: analizowanie postanowień o utworzeniu zbiorów, analizowanie zasad wglądu do zbiorów danych osobowych oraz ogólnych zasad w zakresie przekazywania przez Europol danych osobowych do państw i instytucji trzecich; sprawdzanie, na wniosek każdej osoby, czy pozyskiwanie, gromadzenie, przetwarzanie i używanie danych osobowych przez Europol prowadzone jest rzetelnie i zgodnie z prawem; opracowywanie okresowych sprawozdań z działalności i rozpatrywanie, za pośrednictwem Komitetu Odwoławczego utworzonego w ramach Organu, skarg składanych przez osoby, które uznają, że Europol nieprawidłowo reaguje na ich wniosek o wykonanie prawa dostępu, sprawdzenia, poprawienia i usunięcia danych.

Aby wypełniać te funkcje, Organ, zgodnie z postanowieniami artykułu 2 regulaminu wewnętrznego „(...) jest uprawniony do otrzymywania informacji od Europolu, ma prawo dostępu do wszelkich akt i dokumentów, jak również do danych zgromadzonych przez Europol, w dowolnym momencie zostaną mu udostępnione wszystkie pomieszczenia Europolu. Dotyczy to również informacji o urządzeniach i programach informatycznych oraz dostępu do nich, o ile jest to konieczne do wypełnienia zadań Wspólnego Organu Nadzorczego. Szczegóły będą określone w umowie między Wspólnym Organem Nadzorczym a Zarządem Europolu.”

WON wydał dziesiątki raportów w sprawie projektów badań w najróżniejszych dziedzinach przestępczości międzynarodowej podlegającej Europolowi, na temat których nie można udzielić bliższych informacji ze względu na zasady poufności obowiązujące Europol, ponieważ są to informacje zaklasyfikowane jako tajne.

Należy jednak wspomnieć o początkowych pracach WON i Europolu, aby określić wzór, według którego tworzone są zbiory – sposób pozwalający połączyć konieczność odpowiedniej kontroli z niezbędną elastycznością tworzenia tego rodzaju zbiorów po to, aby były przydatne dla celu, który im przyświeca i aby ułatwiał współpracę policyjną w odpowiednim momencie.

²⁾ Dz.U. C316 27/11/1995 str. 0002-0032.

³⁾ Wszelkie dokumenty Rady Europy dotyczące ochrony danych dostępne są na stronie: http://www.coe.int/T/E/egal_affairs/Legal_co-operation/Data_protection/.

⁴⁾ Wszystkie te punkty będą jeszcze bardziej szczegółowo określone w artykule 4 rozporządzenia 1/99 Wspólnego Organu Nadzorczego Europolu z 22 kwietnia 1999 r., wprowadzającego Wewnętrzny Regulamin (1999/C 149/01), określającego również zasady regulowania ewentualnych konfliktów interesów między członkami Wspólnego Organu Nadzorczego.

W opiniach o utworzeniu konkretnych zbiorów WON wskazał różne aspekty, jakie należy mieć na uwadze, co doprowadziło do zmiany niektórych zbiorów. Wśród nich możemy wskazać uwagi sformułowane przez Organ w niektórych przypadkach, w sprawie konieczności właściwego uzasadnienia otwarcia zbioru na podstawie wyraźnych wskázówek, pozwalających przypuszczać, że istnieje możliwość popełnienia w przyszłości przestępstwa podlegającego kompetencji Europolu; konieczność traktowania danych dotyczących zażywania narkotyków jako danych szczególnie chronionych, a więc podporządkowania się ścisłym zasadom dotyczącym przetwarzania takich danych; konieczność podporządkowania się gwarancjom zawartym w ustawodawstwie krajowym w zakresie wprowadzania danych biometrycznych, takich jak DNA, czy konieczność zachowania szczególnej ostrożności przy przetwarzaniu danych dotyczących świadków lub ofiar – w tym przypadku WON jest zdania, że powinny one być przetwarzane z zachowaniem anonimowości, jeśli tylko jest to możliwe.

W związku z zasadami dotyczącymi prowadzenia zbiorów roboczych dla celów analitycznych, w czasie prac przygotowawczych przed zatwierdzeniem rozporządzenia Rady z 27 listopada 2003 roku w sprawie wprowadzenia, na podstawie ustępu 1 artykułu 43 „Konwencji” powołującego Europejski Urząd Policji („Konwencja o Europolu”), protokołu zmieniającego tę „Konwencję” (2004/C/2/01),⁵ WON interweniował zdecydowanie, proponując rozwiązanie bardzo ważnego problemu związanego z zasadami przechowywania danych w zbiorach analitycznych. Propozycja ta została przyjęta i włączona przez Radę do protokołu zmieniającego.

Zasady dotyczące przechowywania danych w zbiorach analitycznych, o których mowa w ustępie 3 artykułu 21, przewidywały usunięcie danych osoby, do których w ciągu trzech lat nie wprowadzono żadnej aktualizacji ani nie dodano danych dotyczących tej osoby. W przeciwnym razie otwierano kolejny okres trzech lat, przez który dane mogły być zgodne z prawem przechowywane.

Jednakże system ten, pomyślany dla ochrony osób przed bezterminowym przechowywaniem dotyczących ich danych bez istnienia uzasadniających je powodów (trudno jest uzasadnić konieczność przechowywania danych osoby, co do której od trzech lat nie istnieje żaden powód, dla którego dane miałyby być przechowywane), okazał się absolutnie nieprzystosowany do ścigania niektórych form przestępczości – w szczególności terroryzmu – w których przestępcy pozostają przez długi czas utajeni w oczekiwaniu na rozkaz działania, lub też w przypadku przestępców, których dane nie są aktualizowane, ponieważ są w trakcie odbywania kary, lecz istnieją uzasadnione przesłanki, aby sądzić, że pozostają oni w strukturze organizacji terrorystycznej, co wskazuje na ich powrót do działalności przestępczej po odbyciu kary.

Po przeanalizowaniu różnych alternatywnych propozycji rozwiązań, WON zasugerował, że odpowiednim rozwiązaniem godzącym skuteczność policji z prawami osób byłoby przeprowadzanie udokumentowanej corocznej oceny konieczności pozostawiania danych osób figurujących w AWF, obok oceny trzyletniej dotyczącej przechowywania każdego zbioru analitycznego. Ponadto przechowywanie danych osoby w zbiorze analitycznym nie będzie mogło przekraczać okresu istnienia tego zbioru.

System ten, w połączeniu z posiadaną przez WON możliwością weryfikacji jego prawidłowego stosowania, szczególnie dzięki możliwości przeprowadzania kontroli w Europolu, pozwala zachować równowagę między potrzebami policji a prawami obywateli.

WON wyrażał również opinie dotyczące różnych projektów Europolu, w związku z zarządzaniem Systemem Wskaźników umożliwiającym dostęp do niektórych informacji z AWF jednostkom krajowym i oficerom łącznikowym Państw Członkowskich, którzy nie uczestniczą w danym badaniu. W tej sprawie WON wypowiedział się w 2001 roku i ostatnio w 2005 za pośrednictwem dwóch decyzji.⁶

Najważniejszą cechą tych decyzji, podobnie jak i innych związanych z przeszukiwaniem systemów Europolu (znanych jako *audit logs*) przedstawionych przez Europol w sprawie tymczasowego Systemu Informacji lub przeszukiwania systemów technologicznych stanowiących nośniki AWF, jest działanie innej grupy roboczej WON – podgrupy IT. Zadaniem tej podgrupy jest wspomaganie Europolu na wczesnych etapach nowych projektów po to, aby stanowisko Organu w sprawie ich dostosowania do zasad ochrony danych, w sprawie konieczności wprowadzenia zmian technicznych zwiększających ochronę danych osobowych lub dających większą skuteczność nadzoru WON, było brane pod uwagę już przy podejmowaniu decyzji warunkujących dalszy rozwój tych projektów.

Jednocześnie działania podgrupy IT umożliwiają wymianę poglądów z Europolem, co ułatwia zrozumienie celów tych projektów i problemów związanych z ich wprowadzeniem, dzięki czemu łatwiej jest znaleźć rozwiązania akceptowalne dla Europolu i dla WON.

Ważną sprawą, która zajęła wiele czasu i wymagała wielu wysiłków ze strony WON w przeszłości, i prawdopodobnie będzie tak również w przyszłości, jest udział w umowach między Europolem a państwami i organizacjami trzecimi. Jest to sprawa o wyjątkowym znaczeniu z dwóch powodów.

Po pierwsze, ze względu na to, że dane osobowe przekazywane przez Europol do państw trzecich muszą być objęte odpowiednimi gwarancjami, jeżeli nie takimi, jakie istnieją w Unii Europejskiej, to przynajmniej odpowiednimi dla ich rodzaju i wrażliwości. Po drugie, każdy rozumie implikacje międzynarodowe, jakie mogą wynikać z określonego stanowiska WON w procesie negocjacji umowy, które mogłoby utrudnić podjęcie decyzji uważanej za strategiczną przez organy zarządzające Europolem i być może przez organy danego państwa trzeciego.

Dlatego WON znowu postanowił powołać podgrupę, która mogłaby prowadzić szczegółowe analizy projektów, napływających do Organu i składać racjonalne propozycje odnośnie ich zawartości.

Ponadto WON bierze udział w dwóch etapach projektu. Po pierwsze wydaje opinię w sprawie istnienia nieusuwalnych przeszkód dla rozpoczęcia negocjacji z danym państwem lub organizacją oraz w końcowej fazie, kiedy projekt umowy uzyskany w wyni-

ku negocjacji przedstawiony jest mu do zaopiniowania. Na obu etapach udział Międzynarodowej Podgrupy jest kluczowy.

W tym zakresie istnieje wiele opinii, z którymi można się zapoznać na stronie internetowej WON, jednak dla ilustracji przedstawię dwa przykłady, w których udział Organu okazał się zasadniczy i decydujący.

Pierwszy dotyczy negocjacji umowy między Europolem i Stanami Zjednoczonymi w kontekście trudnego okresu, jaki nastąpił po atakach terrorystycznych 11 września 2001 r.

Proces rozpoczął się od decyzji Dyrektora Europolu o przekazaniu niektórych danych organom amerykańskim – w ramach uprawnień, jakie nadaje mu punkt b ustępu 1 artykułu 2 rozporządzenia Rady z 12 marca 1999 r. w sprawie ustalenia zasad przekazywania przez Europol danych osobowych do państw i organizacji trzecich (1999/C 88/01)⁷ – powołującej się na istnienie bezpośredniego zagrożenia.

Kiedy WON został poinformowany o tej decyzji, powiadomił Europol, że nie uważa za stosowne, aby dalsze przekazywanie danych opierało się na tych samych przesłankach, a więc konieczne jest zastosowanie ogólnych zasad przekazywania danych osobowych do państw trzecich, zgodnie z ustępem 1 artykułu 2, czyli zawarcie umowy między Europolem i organami amerykańskimi.

Dlatego właśnie rozpoczął się proces, który być może doprowadzi do zatwierdzenia tej umowy; już na początku WON wydał opinię, w której zawarto całą serię uwag, jakie powinny zostać uwzględnione w procesie negocjacyjnym oraz zaoferowano współpracę Organu, aby bez szkody dla niezależności przy wydawaniu końcowej opinii przyczynić się do zawarcia w umowie wszystkich warunków, jakie uznano za niezbędne.

Delegacja WON śledziła więc z bliska cały proces, a nawet była obecna przy niektórych sesjach negocjacyjnych. Na koniec został opracowany projekt zawierający wszystkie kwestie, które Organ uznał za niezbędne.

Inną bardzo ważną umową, w której uwagi WON doprowadziły nawet do zmiany istniejących ram prawnych, były negocjacje umowy między Europolem i Interpolem. W czasie negocjacji tej umowy okazało się, że istnieje problem z tym, aby informacje przekazywane przez Europol do Interpolu rzeczywiście docierały do prawdziwych odbiorców, jakimi są organy policyjne należące do Interpolu.

Ustęp 5 artykułu 5 rozporządzenia 1999/C 88/01 mówi o zakazie dalszego przekazywania osobom trzecim danych, które Europol przekazuje do organizacji lub państwa trzeciego. Interpretacja dokonana przez WON w tym konkretnym przypadku wskazywała, że Interpol, jako niezależna i autonomiczna organizacja, był uprawnionym odbiorcą danych przekazywanych przez Interpol, a więc nie mógł dalej przekazywać ich bez naruszenia istniejących przepisów.

Problem polegał na tym, że Sekretariat Generalny Interpolu działa przede wszystkim jako organ pośrednictwa i współpracy między swoimi członkami, a informacje, które otrzymuje nabierają prawdziwej wartości wtedy, gdy może się nimi podzielić z innymi członkami wchodzącymi w skład tej organizacji.

Po wskazaniu tego problemu przez WON w pierwszej decyzji po rozpoczęciu negocjacji, Rada przygotowała zmianę rozporządzenia 1999/C 88/01, którą przedstawiła Wspólnemu Organowi, a ten uznał, że gwarancje ustalone dla zabezpieczenia tego rodzaju dalszego przekazywania były odpowiednie, w związku z tym wydał pozytywną opinię, po której rozporządzenie 1999/C 88/01 zostało zmienione rozporządzeniem Rady z 28 lutego 2002 r., zmieniającym rozporządzenie Rady z 12 marca 1999 r. w sprawie zasad przekazywania przez Europol danych osobowych do państw i organizacji trzecich (2002/C 76/01).⁸

Ten instrument prawny mówi, że dalsze przekazywanie danych jest możliwe pod warunkiem istnienia obowiązującej umowy między Europolem i daną organizacją, wprowadzającej i określającej gwarancje dla danych dalej przekazywanych lub pod warunkiem stwierdzenia przez Dyrektora Europolu absolutnej konieczności przekazania danych dla ochrony podstawowych interesów Państw Członkowskich lub dla zapobieżenia bezpośredniemu zagrożeniu związanemu z przestępstwem. W tym przypadku Europol musiał bezzwłocznie poinformować o decyzji Dyrektora Zarząd oraz WON. Dalsze przekazywanie nie byłoby również możliwe bez zgody Państwa Członkowskiego, które przekazało dane Europolowi.

Innym ważnym elementem polityki nadzorowania Europolu przez WON jest przekonanie, już od początku jego działalności, o konieczności okresowego kontrolowania Europolu, a w konsekwencji, przedstawienie planu kontroli, który został opracowany dzięki istnieniu Podgrupy Inspekcji, stałej i interdyscyplinarnej, dokonującej przynajmniej raz w roku audytu Europolu. Po przeprowadzeniu kontroli przygotowuje ona sprawozdanie, zatwierdzone przez WON na sesji plenarnej i przekazywane Europolowi. Do sprawozdania zawierającego stwierdzone fakty i dotyczące ich wnioski, dołączana jest seria zaleceń, które Europol ma wprowadzić, aby lepiej dostosować przetwarzanie danych osobowych do warunków określonych obowiązującym ustawodawstwem. Stopień wykonania zaleceń sformułowanych w trakcie inspekcji weryfikowany jest w czasie kolejnej inspekcji, co odnotowane jest w nowym sprawozdaniu.

Inspekcje pozwoliły stwierdzić, że Europol traktuje poważnie kwestie ochrony danych osobowych, chociaż w trakcie inspekcji wykryto elementy, które według WON powinny zostać poprawione, zabezpieczenia, które powinny być wprowadzone i procedury wymagające poprawy, a w niektórych przypadkach zauważono pewne działania Europolu w stosunku do Państw Członkowskich, które – w opinii WON, z którą później zgodził się zarząd Europolu – nie były w pełni zgodne z postanowieniami „Konwencji” i wobec powyższego zostały usunięte w ciągu kilku miesięcy.

Początkowo inspekcje te miały charakter ogólny, co pozwoliło poznać infrastrukturę techniczną Europolu, ogólne zarządzanie systemami i wprowadzonymi środkami bez-

pieczeństwa. Stopniowo inspekcje zaczęły skupiać się na bardziej konkretnych kwestiach i bardziej skierowanych na treść, to znaczy, w miarę jak zwiększała się ilość informacji przetwarzanych przez Europol, coraz bardziej skupiano się na sprawach związanych z ich jakością, aktualnością i proporcjonalnością w stosunku do celów określonych w decyzjach o utworzeniu poszczególnych zbiorów.

Inną sprawą, na której skupia się uwaga WON, są działania skierowane na zwiększenie przejrzystości jego prac oraz informowanie o podejmowanych działaniach i decyzjach, co powinno zwiększyć uświadomienie obywateli.

W tej sprawie Podgrupa Informacyjna wykonała bardzo cenną pracę, w której mieściło się uruchomienie strony internetowej, stale ulepszanej i oferującej coraz więcej bardziej aktualnych informacji.

Współpracowała również aktywnie z Sekretariatem Europolu w celu zaproponowania koniecznych zmian w regulaminie wewnętrznym po to, aby dostosować zasady dostępu do dokumentów WON do ogólnych norm przejrzystości instytucji europejskich, zachowując jednocześnie konieczną poufność niektórych jego dokumentów roboczych i opinii.

Ponadto te nowe normy formalnie potwierdzają zasadę przedstawiania Parlamentowi Europejskiemu sprawozdań z działalności WON, co było przyjętą praktyką, ale dopiero po wejściu w życie zatwierdzonych zmian Regulaminu Wewnętrznego po publikacji w Dzienniku Urzędowym staną się dodatkowym elementem jeszcze bardziej wzmacniającym stosunki między obiema instytucjami, zwłaszcza, że Parlament zawsze był bardzo czuły na konieczność ochrony praw osób w dziedzinie współpracy policyjnej.

Należy również wspomnieć o pracach tej podgrupy w organizowaniu i planowaniu konferencji, jaką WON urządza w październiku 2006 roku, w celu przeanalizowania sytuacji bieżącej i przyszłej w zakresie ochrony danych w dziedzinie europejskiej współpracy policyjnej, a w szczególności w jaki sposób oddziałuje ona i będzie oddziaływać w przyszłości na Europol, a więc i na sam Organ. We wspomnianej konferencji wezmą udział przedstawiciele Parlamentu Europejskiego, Rady UE, Europolu, krajowych organów ochrony danych, przedstawiciele społeczeństwa obywatelskiego i oczywiście sam WON.

Wracając do sprawozdań, jakie WON musi okresowo przedstawiać, Wspólny Organ Nadzorczy opracował dwa sprawozdania z działalności – oba dostępne na stronie internetowej – pierwsze za okres 1998-2002 i drugie obejmujące okres 2002-2004. Po cząwszy od drugiego sprawozdania WON podjął decyzję o przygotowywaniu sprawozdań w okresach dwuletnich, odpowiadających okresom poszczególnych prezydentur organu, a więc na koniec bieżącego roku zostanie opracowane kolejne sprawozdanie, które powinno zostać opublikowane na początku 2007 roku.

WON traktuje te sprawozdania jako cenny sposób komunikowania się i szerzenia wiedzy, stara się w nich przedstawić prowadzone prace, istniejące problemy i podejmowane decyzje w danym okresie w sposób przystępny i atrakcyjny, kładąc szczególny nacisk na najważniejsze kwestie, na problemy, które udało się rozwiązać i te, które pozostały jeszcze do rozwiązania, oraz na plany i strategię dalszych działań.

Na koniec należy wspomnieć o pracach Komitetu Odwoławczego WON, powołanego na mocy ustępu 7 artykułu 24 „Konwencji o Europolu”. Komitet ten jest jedyną i najwyższą instancją odwoławczą od decyzji Europolu dotyczących wykonywania prawa osób do dostępu, sprawdzania, poprawiania i usuwania danych.

„Konwencja” przyznaje te prawa wszystkim osobom, których dane są przetwarzane i jeżeli stanowisko Europolu nie satysfakcjonuje tych osób, mogą one odwołać się do Komitetu Odwoławczego, którego decyzje są wiążące dla Europolu, nie ma możliwości odwołania się do innej instancji, co nadaje im wagę quasi jurysdykcyjną i powoduje, że stanowi on szczególną instytucję w ramach istniejącego europejskiego porządku prawnego.

W procesie podejmowania decyzji Komitet kieruje się przede wszystkim normami określonymi w artykule 19 „Konwencji”, którego treść jest nadzwyczajnie złożona, wprowadzająca równoległe stosowanie przepisów prawa krajowego i szczególnych przepisów „Konwencji”, często trudnych do zastosowania w rzeczywistych przypadkach, z jakimi spotyka się Komitet.

Jednakże Komitet zawsze podkreślał konieczność szczegółowego analizowania poszczególnych przypadków przez Europol, a nie podejmowania standardowych decyzji, nie uwzględniających szczególnych okoliczności każdego przypadku odwołania, oraz konieczność promowania jak największej ochrony praw obywateli. Wszystkie decyzje Komitetu są jawne, można zapoznać się z nimi na stronie internetowej WON.

Na koniec należy wspomnieć o tym, jak zmienia się rola członków WON. Początkowo WON pełnił rolę przede wszystkim reaktywną, to znaczy wydawał opinie i decyzje dotyczące dokumentów lub projektów pochodzących z Europolu. Ta rola, chociaż nie znikła i nigdy nie przestanie istnieć do końca, spowodowała pojawienie się całej serii nowych zadań, bardziej proaktywnych, które z pewnością będą stopniowo nabierały coraz większego znaczenia.

Pierwszym przejawem tej nowej roli były inspekcje w Europolu, nie były one spowodowane żadnym czynnikiem zewnętrznym, lecz tylko decyzją WON, aby lepiej poznać z pierwszej ręki rzeczywiste praktyczne działania Europolu w zakresie przetwarzania danych osobowych.

Później rola ta rozwinęła się za pośrednictwem Podgrupy IT, która, dzięki bezpośrednim kontaktom i szczerzej wymianie myśli, dostarczała Europolowi wskazówek dotyczących lepszego dostosowania wymogów technicznych i operacyjnych do konieczności zagwarantowania podstawowego prawa do ochrony danych osobowych w pierwszych etapach powstawania projektów, z satysfakcjonującymi wynikami dla obu stron. Wynika stąd, że działania te będą się rozwijać coraz intensywniej i będą stanowić integralną część strategii rozwoju projektów Europolu.

Stopniowo ta forma pracy przeniosła się na inne dziedziny podlegające WON, takie jak negocjowanie umów z państwami trzecimi, czy formułowanie nowego podejścia do przetwarzania danych dla celów ścigania przestępstw, a nawet działania zmierzające do większej przejrzystości i jawności działań Organu poprzez projekt zorganizowania konferencji, po raz pierwszy w jego historii, czy ściślejsze stosunki z Parlamentem

Europejskim – we wszystkich tych dziedzinach prace koordynacyjne i działania Sekretariatu WON stanowią nieodzowne wsparcie.

Ze wszystkich wyżej wymienionych powodów szczerze wierzę, że Wspólny Organ Nadzorczy Europolu miał ogromny wkład w konsolidację, w ramach swoich kompetencji, systemu ochrony danych szanującego zasady i prawa osób z pragmatycznego i wyważonego punktu widzenia, poprzez opracowywanie wytycznych, określających w jaki sposób dostosować prace policyjne do wymogów krajowych i europejskich ustawodawstw, szukając rozwiązań rzeczywiście ulepszających w praktyce ochronę osób, jednocześnie niepowodujących przeszkód w wykonywaniu zadań Europolu. A kiedy było to konieczne, wykazywał stanowczy sprzeciw wobec tych projektów lub interpretacji „Konwencji” i rozporządzeń wprowadzających, które uznawał za niezgodne z prawem.

Z tych wszystkich powodów, jakiegokolwiek przyszłe zmiany ram prawnych, w których działa Europol, będą musiały brać pod uwagę Organ i będą mogły liczyć na cenny wkład organów krajowych, za pośrednictwem ich przedstawicieli we Wspólnym Organie Nadzorczym Europolu.

Prof. dr hab. Bogusław Banaszak **Dr Krzysztof Wygoda**

Uniwersytet Wrocławski, Katedra Prawa Konstytucyjnego, Polska
University of Wrocław, Constitutional Law Faculty, Poland

Pojęcie funkcji publicznej jako przesłanka modyfikująca zakres ochrony danych osobowych

Już od 1997 roku zdanie „Każdy ma prawo do ochrony dotyczących go danych osobowych” możemy odnaleźć w pierwszym artykule ustawy o ochronie danych osobowych¹ (dalej u.o.d.o.). Powszechnie uważa się, iż ustawa, którą rozpoczęto tą deklaracją, stanowi rozwinięcie zasad wyrażonych w artykule 51 (ale również 47 czy nawet 49 i 53) Konstytucji RP. W tej samej ustawie zasadniczej zapisane zostały jednak i inne normy, których egzekucja prowadzi niejednokrotnie do wysnucia wniosków o swobodnym przepływie informacji – w tym tych dotyczących osób fizycznych. Jako egzemplifikację tego trendu wskazać wystarczy na art. 14, 54 czy 61 Konstytucji.

Sytuacja taka odzwierciedla dwie tendencje widoczne w każdym państwie demokratycznym. Z jednej strony prawodawca dąży do ochrony prywatności osób fizycznych, z drugiej zaś chce powołać do życia mechanizmy pozwalające na wgląd w życie i działania tych samych osób – jeśli tylko znajdują się one w szeroko ujętym kręgu władzy. Niezbawalnym prawem rządzonej jest bowiem możliwość kontroli poczynąń wszystkich osób, które władzę sprawują. Wśród przyczyn takiego stanu, modyfikującego zakres ochrony prywatności osób pełniących funkcje publiczne, na czoło wysuwa się przekonanie o tym, że transparentność ich działań jest jednym z podstawowych zabezpieczeń chroniących samą demokrację przed jej przemianą w system autorytarny czy totalitarny.

Od 1 stycznia 2002 roku obowiązuje w Polsce ustawa mająca, w założeniu, przyczynić się w znacznym stopniu do urzeczywistnienia tego prawa obywateli. Podobnie jak w przypadku u.o.d.o., również w początkowych postanowieniach ustawy o dostępie do informacji publicznej² (dalej u.d.i.p.) odnajdziemy doniosłe deklaracje. W tym przypadku, wskazujące na chęć uczynienia z tej ustawy podstawy tworzenia płaszczyzny swobodnego dostępu do informacji publicznej. Co więcej, u.d.i.p. wskazuje jako potencjalnego odbiorcę tych danych każdego i gwarantuje mu bardzo szeroki dostęp do informacji publicznej (pewne obostrzenia wynikają głównie z jej art. 5)³ bez konieczności wykazywania się przez ten podmiot jakimkolwiek interesem. Wspo-

¹⁾ Tj. Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.

²⁾ Dz.U. z 2001 r., Nr 112, poz. 1198 ze zm.

³⁾ Szerzej na temat wszystkich możliwych ograniczeń prawa dostępu do informacji publicznej zob. np.: M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji publicznej. Komentarz*, Wrocław 2002, czy M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej. Informatyzacja administracji*, Wrocław 2005.

mniana regulacja wprowadza ograniczenia prawa do informacji publicznej w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych (art. 5.1. u.d.i.p.). Wśród dóbr, z uwagi na które nie upowszechniamy informacji publicznych, ustawodawca na poczesnym miejscu wymienia prywatność. Jednak zgodnie z ust. 2 powołanego wyżej art. „Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa”.

Z uwagi na temat opracowania nie jest, naszym zdaniem, konieczne dokonywanie jakiegś głębszej analizy ostatniej części cytowanego przepisu. Dzieje się tak dlatego, że dotyczy ona dobrowolnej rezygnacji z prawa do ochrony informacji o charakterze osobowym, podkreślić przy tym należy, iż mieści się to w podstawowym założeniu u.o.d.o., wskazującym zgodę osoby, której dane dotyczą, jako jedną z dopuszczalnych i chyba najbardziej preferowanych (z uwagi na możliwość samodzielnego kształtowania swego wizerunku informacyjnego) płaszczyzn legalizujących przetwarzanie danych osobowych.

Bez wątpienia kluczowym zagadnieniem, choćby przez wgląd na tytuł, będzie natomiast próba dokonania wykładni początkowego fragmentu art. 5 ust. 2 u.d.i.p. i odpowiedź na pytanie, jakie rodzi on konsekwencje dla zasad związanych z przetwarzaniem danych osobowych.

Nie zagłębiając się w szczegóły u.d.i.p. i pamiętając, że zgodnie z art. 61 Konstytucji obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osobach pełniących funkcje publiczne musimy stwierdzić, że ustawodawca stworzył normę, której ranga jest równorzędna u.o.d.o. Jako że pochodzi z okresu późniejszego i odnosząc się jedynie do pewnej części danych osobowych, można się w jej przypadku odwołać do uznanych zasad *lex posterior derogat legi priori* oraz *lex specialis derogat legi generali*. Jest to istotne, gdyż teoretycznie można by jej zarzucić sprzeczność z regułą zapisaną w art. 5 u.o.d.o., wskazującym na sytuację, w której przepisy odrębnych ustaw, odnoszące się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z u.o.d.o., stosuje się przepisy tych ustaw. W tym konkretnym przypadku, wyłączającym prawie wszystkie możliwe ograniczenia w sferze udostępniania pewnej grupy danych osobowych, z dalej idącą ochroną z pewnością do czynienia mieć nie będziemy.⁴

W sprawie zarzutu ewentualnej niezgodności art. 5 u.d.i.p. z art. 51 Konstytucji należy przyjąć, iż stanowiąc konkretyzację art. 61 Konstytucji nie może być z góry odrzucony, są to bowiem normy o tej samej mocy prawnej. Jeśli więc nie wykracza on poza dopuszczalną swobodę ustawodawcy w rozwijaniu postanowień Konstytucji to jest z nią zgodny. Ostatnio wypowiadał się w tej właśnie sprawie Trybunał Konstytucyjny orzekając, że „Art. 5 ust. 2 zdanie 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112, poz. 1198, z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 240, poz. 2407 oraz z 2005 r. Nr 64, poz. 565 i Nr 132, poz. 1110)

jest zgodny z art. 31 ust. 3, art. 47 i art. 61 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz nie jest niezgodny z art. 61 ust. 4 Konstytucji.”⁵ Mając pewność, że w chwili obecnej art. 5 u.d.i.p. nie jest oceniany jako wykraczający poza dopuszczalne, konstytucyjne ramy ograniczeń prawa do prywatności, przejdziemy do próby stwierdzenia, jakiej grupy osób dotyczy ta regulacja.

Już na samym początku musimy stwierdzić, że prawodawca odwołując się w u.d.i.p. do pojęcia osób pełniących funkcje publiczne nie podał jednocześnie jego definicji oraz nie odesłał wprost do żadnej z istniejących już w owym czasie ustaw zawierającej takie sformułowania. Mamy na myśli choćby dwa akty prawne:

- ustawę z dnia 11 kwietnia 1997 r. o ujawnieniu pracy lub służby w organach bezpieczeństwa państwa lub współpracy z nimi w latach 1944-1990 osób pełniących funkcje publiczne;
- ustawę z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne.⁶

Można więc przyjąć, iż założeniem ustawodawcy było pozostawienie pewnej swobody interpretacyjnej tego pojęcia na gruncie u.d.i.p. Zapewne wiąże się z bardzo szerokim kręgiem podmiotów zobligowanych do ujawniania informacji publicznej (art. 4 u.d.i.p.) znajdujących się w ich posiadaniu. Przyjęcie dość wąskich definicji występujących w obu powołanych ustawach⁷, oczywiście w kontekście bardzo szerokiego potraktowania informacji publicznych jako takich, prowadziłyby do nadmiernego zawężenia kręgu osób, o których społeczeństwo miałoby prawo domagać się informacji, jeśli pozostają one w związku z pełnionymi przez te osoby funkcjami.

⁵ Wyrok z dnia 20 marca 2006 r., sygn. akt K 17/05. W chwili ostatecznego opracowywania tekstu TK nie podał jeszcze niestety pisemnego uzasadnienia do tego wyroku. Było by ono zapewne bardzo pomocne w szczegółowym przedstawieniu motywów, które TK przypisał ustawodawcy tworzącemu ten wyjątek od zasady możliwie wąskiego ujawniania informacji o charakterze osobowym. Pewne informacje na ten temat można jednak odnaleźć w komunikacie prasowym, który ukazał się po rozprawie. Stwierdzono w nim, że „... regulacja zawarta w kwestionowanym przepisie ustawy o dostępie do informacji tylko wtedy byłaby niezgodna z Konstytucją, gdyby jej stosowanie naruszało poniższe zasady. Tak, więc informacje nie mogą wykraczać poza konieczność określoną potrzebą transparentności życia publicznego ocenianą zgodnie ze standardami przyjętymi w demokratycznym państwie prawnym. Informacje nie powinny też przekreślać istoty ochrony prawa do życia prywatnego. Muszą zawsze mieć znaczenie dla oceny funkcjonowania instytucji oraz osób pełniących funkcje publiczne. Zdaniem Trybunału prywatność może w pewnych sytuacjach być przedmiotem ingerencji dla dobra wspólnego. Jednak wkraczanie w tę sferę musi być dokonywane w sposób ostrożny i wyważony, z należytą oceną racji, które przemawiają za taką ingerencją. Mamy, bowiem do czynienia z dobrami równorzędnymi. Ograniczenia dotyczące pewnych praw chronionych konstytucyjnie mogą być wprowadzane z uwagi na dobro wspólne. Do praw takich, zdaniem Trybunału Konstytucyjnego, należy prawo do prywatności.”

⁶ Odpowiednio: tj. Dz.U. z 1999, Nr 42, poz. 428 ze zm., oraz Dz.U. z 1997, Nr 106, poz. 679 ze zm.

⁷ W ustawie „lustracyjnej” chodzi o „...Art. 3. 1. Osobami pełniącymi funkcje publiczne w rozumieniu ustawy są: Prezydent Rzeczypospolitej Polskiej, poseł, senator oraz osoba powołana, wybrana lub mianowana na określone w innych ustawach kierownicze stanowisko państwowe, przez Prezydenta Rzeczypospolitej Polskiej, Sejm, Prezydium Sejmu, Senat, Sejm i Senat, Marszałka Sejmu, Marszałka Senatu lub Prezesa Rady Ministrów, Szef Służby Cywilnej, dyrektor generalny w ministerstwie, urzędzie centralnym lub urzędzie wojewódzkim oraz sędzia, prokurator i adwokat, a także rektor, prorektor, kierownik podstawowej jednostki organizacyjnej w publicznej i niepublicznej szkole wyższej, członek Rady Głównej Szkolnictwa Wyższego i członek Państwowej Komisji Akredytacyjnej, członek Centralnej Komisji do Spraw Stopni i Tytułów. 2. Osobami pełniącymi funkcje publiczne w rozumieniu ustawy są również: członkowie rad nadzorczych, członkowie zarządów, dyrektorzy programów oraz dyrektorzy ośrodków regionalnych i agencji „Telewizji Polskiej – Spółka Akcyjna” i „Polskiego Radia – Spółka Akcyjna”, dyrektor generalny Polskiej Agencji Prasowej, dyrektorzy biurowi, redaktorzy naczelni oraz kierownicy oddziałów regionalnych Polskiej Agencji Prasowej, prezes Polskiej Agencji Informacyjnej, wiceprezesi, członkowie zarządu oraz dyrektorzy – redaktorzy naczelni Polskiej Agencji Informacyjnej”.

W ustawie ograniczającej swobodę prowadzenia działalności gospodarczej chodzi o dwa artykuły określające zakres podmiotowy jej obowiązywania. Co ciekawe, założenie, że objęte nim osoby pełnią właśnie funkcje publiczne wynika przede wszystkim z samego tytułu tego aktu: „Art. 1. Ustawa określa ograniczenia

⁴ Szerzej na temat interpretacji art. 5 u.o.d.o. piszą, np., J. Barta. P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 363-368.

Proste porównanie przytoczonych (w przypisie 7) regulacji pozwala na wskazanie różnic w podejściu do postrzegania kręgu osób pełniących funkcje publiczne. Brak pełnej spójności definicyjnej jest zapewne wynikiem odmiennych przesłanek przyświecających uchwaleniu tych dwu aktów oraz innego zakresu danych osobowych ujawnianych z uwagi na nałożenie takiego obowiązku w obu aktach – różny też jest dostęp do tak ujawnionych informacji⁸. Wobec istniejących rozbieżności przyjęcie założenia, że któraś z tych dwu definicji jest właściwa również dla u.d.i.p. budzi wątpliwości.

Rzeczywisty zakres pojęcia pełnienia funkcji publicznej na gruncie u.d.i.p. był więc w początkowym okresie obowiązywania ustawy niepewny. Sądzymy jednak, że stan ten uległ poprawie w 2003 roku, kiedy to wprowadzono do k.k. zmiany obejmujące m. in.

w prowadzeniu działalności gospodarczej przez osoby zajmujące kierownicze stanowiska państwowe, w rozumieniu przepisów o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe oraz przez sędziów Trybunału Konstytucyjnego.

Art. 2. Ustawa określa także ograniczenia w prowadzeniu działalności gospodarczej przez:

- 1) pracowników urzędów państwowych, w tym członków korpusu służby cywilnej, zajmujących stanowiska kierownicze:
 - a) dyrektora generalnego, dyrektora departamentu (jednostki równorzędnej) i jego zastępcy oraz naczelnika wydziału (jednostki równorzędnej) - w urzędach naczelnym i centralnym organów państwowych,
 - b) dyrektora generalnego urzędu wojewódzkiego, dyrektora wydziału (jednostki równorzędnej) i jego zastępcy oraz głównego księgowego, kierownika urzędu rejonowego i jego zastępcy oraz głównego księgowego - w urzędach terenowych organów rządowej administracji ogólnej,
 - c) kierownika urzędu i jego zastępcy - w urzędach terenowych organów rządowej administracji specjalnej,
 - 2) pracowników urzędów państwowych, w tym członków korpusu służby cywilnej, zajmujących stanowiska równorzędne pod względem płacowym ze stanowiskami wymienionymi w pkt 1,
 - 2a) innych niż wymienieni w pkt 1 i 2 członków korpusu służby cywilnej zatrudnionych w urzędzie obsługującym ministra właściwego do spraw finansów publicznych,
 - 3) dyrektora generalnego Najwyższej Izby Kontroli oraz pracowników Najwyższej Izby Kontroli nadzorujących lub wykonujących czynności kontrolne,
 - 3a) Prezesa i wiceprezesów oraz starszych radców i radców Prokuratury Generalnej Skarbu Państwa,
 - 4) pracowników regionalnych izb obrachunkowych zajmujących stanowiska: prezesa, członka kolegium, naczelnika wydziału oraz inspektora do spraw kontroli,
 - 5) pracowników samorządowych kolegiów odwoławczych zajmujących stanowiska: przewodniczącego, jego zastępcy oraz etatowego członka kolegium,
 - 6) wójtów (burmistrzów, prezydentów miast), zastępców wójtów (burmistrzów, prezydentów miast), skarbników gmin, sekretarzy gmin, kierowników jednostek organizacyjnych gminy, osoby zarządzające i członków organów zarządzających gminnymi osobami prawnymi oraz inne osoby wydające decyzje administracyjne w imieniu wójta (burmistrza, prezydenta miasta),
 - 6a) członków zarządów powiatów, skarbników powiatów, sekretarzy powiatów, kierowników jednostek organizacyjnych powiatu, osoby zarządzające i członków organów zarządzających powiatowymi osobami prawnymi oraz inne osoby wydające decyzje administracyjne w imieniu starosty,
 - 6b) członków zarządów województw, skarbników województw, kierowników wojewódzkich samorządowych jednostek organizacyjnych, osoby zarządzające i członków organów zarządzających wojewódzkimi osobami prawnymi oraz inne osoby wydające decyzje administracyjne w imieniu marszałka województwa,
 - 7) pracowników banków państwowych zajmujących stanowiska: prezesa, wiceprezesa, członka zarządu oraz skarbnika,
 - 8) pracowników przedsiębiorstw państwowych zajmujących stanowiska: dyrektora przedsiębiorstwa, jego zastępcy oraz głównego księgowego,
 - 9) pracowników jednoosobowych spółek Skarbu Państwa oraz spółek, w których udział Skarbu Państwa przekracza 50% kapitału zakładowego lub 50% liczby akcji, zajmujących stanowiska: prezesa, wiceprezesa i członka zarządu.
 - 10) pracowników agencji państwowych zajmujących stanowiska: prezesa, wiceprezesa, dyrektora zespołu, dyrektora oddziału terenowego i jego zastępcy - lub stanowiska równorzędne,
 - 11) inne osoby pełniące funkcje publiczne, jeżeli ustawa szczególna tak stanowi.
- ⁸⁾ W przypadku oświadczeń lustracyjnych część z nich podaje się do wiadomości publicznej w formie obwieszczenia wyborczego – są więc w pełni jawne, inna część może być badana przez sąd, jeśli osoba je składająca zajmie określone stanowisko – zatem co najmniej sentencja wyroku będzie jawna. W odniesieniu do oświadczenia o prowadzonej przez małżonka działalności gospodarczej uwzględniamy tajemnicę służbową. Podobnie rzecz wygląda w przypadku oświadczeń o stanie majątku (choć ujawnienie tych informacji może nastąpić np. z uwagi na pisemną zgodę składającego oświadczenie), z kolei informacje wpisywane do Rejestru Korzyści są w pełni jawne.

dodanie art. 115 § 19 k.k.⁹ Z uwagi na charakter samego k.k., w szczególności jego powszechne obowiązywanie, oraz istnienie w samej u.d.i.p. części prawno-karnej zmuszeni jesteśmy do oceny przesłanek czynu poddanego w niej sankcjom właśnie przez pryzmat części ogólnej k.k. Penalizacja nieudostępnienia informacji publicznej (art. 23 u.d.i.p.) zmusza do zbadania czy w konkretnym przypadku doszło do naruszenia ustawy z uwagi na nieudostępnienie informacji publicznej na temat osoby pełniącej funkcję publiczną, czy też z czynem tym nie mamy do czynienia z uwagi na brak możliwości zakwalifikowania osoby, o którą pytano, do kategorii pełniących ową funkcję. Jeśli więc sama u.d.i.p. nie zawiera definicji tego pojęcia to powinno być ono rekonstruowane, szczególnie dla potrzeb postępowania karnego, właśnie w oparciu o art. 115 § 19 k.k. Jeśli taka reguła jest stosowana w sytuacji najbardziej dotkliwej dla udostępniającego informację publiczną to nie widzimy przeszkód, by stosować ją w czasie zwykłej, codziennej, realizacji postanowień u.d.i.p. Po przyjęciu tego wstępnego założenia możemy stwierdzić, że (w myśl art. 115 § 19 k.k.) dla potrzeb interpretacji u.d.i.p. osobą pełniącą funkcję publiczną jest:

- funkcjonariusz publiczny,
- członek organu samorządowego,
- osoba zatrudniona w jednostce organizacyjnej dysponującej środkami publicznymi, chyba że wykonuje wyłącznie czynności usługowe,
- a także inna osoba, której uprawnienia i obowiązki w zakresie działalności publicznej są określone lub uznane przez ustawę lub wiążącą Rzeczpospolitą Polską umowę międzynarodową.

Nie budzi więc wątpliwości, że zakres tego pojęcia jest zdecydowanie szerszy od pojęcia funkcjonariusza publicznego, do którego w początkowym okresie obowiązywania u.d.i.p. sięgano najczęściej, starając się ograniczyć pole działania ustawy tylko do przypadków niebudzących wątpliwości. Było to zrozumiałe choćby dlatego, że art. 51 u.o.d.o. stanowi: „1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku”. Zakwalifikowanie części danych osobowych jako informacji publicznej i udostępnienie ich w sytuacji, gdy osoba, której one dotyczyły, nie pełniła jednak funkcji publicznej mogło narazić na taką odpowiedzialność.

Starając się przybliżyć czytelnikowi samo pojęcie osoby pełniącej funkcję publiczną nie sposób jednak uciec od bliższego przyjrzenia się choćby niektórym jego częściom składowym. Zacząć należy od tak ważnej, jaką jest pojęcie funkcjonariusza publicznego. Zgodnie z treścią art. 115 § 13 k.k. jest nim:

- Prezydent Rzeczypospolitej Polskiej,
- poseł, senator, radny,
- poseł do Parlamentu Europejskiego,
- sędzia, ławnik, prokurator, notariusz, komornik, kurator sądowy, osoba orzekająca w sprawach o wykroczenia lub w organach dyscyplinarnych działających na podstawie ustawy,

⁹⁾ Art. 115 § 19 dodany przez art. 1 pkt 3 lit. b) ustawy z dnia 13 czerwca 2003 (Dz.U. z 2003, Nr 111, poz.1061) zmieniającej k.k. z dniem 1 lipca 2003 r.

- osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych,
- osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe,
- osoba zajmująca kierownicze stanowisko w innej instytucji państwowej,
- funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej,
- osoba pełniąca czynną służbę wojskową.

W literaturze trafnie zauważa się, iż w powołanym przepisie uzależniono przymiot funkcjonariusza publicznego od pozostawania w stosunku pracy w organie administracji rządowej lub innym organie państwowym lub samorządu terytorialnego. Formalną przesłanką zakwalifikowania konkretnej osoby do kategorii funkcjonariusza publicznego jest więc nawiązanie stosunku pracy.

Wyłączenie konkretnej osoby z kategorii funkcjonariusza publicznego związane jest z ustaleniem zakresu ciążących na nim obowiązków i przysługujących uprawnień. Chodzi tu więc o wykazanie czy konkretna osoba z racji zatrudnienia w administracji odpowiada za przekroczenie swoich uprawnień lub niedopełnienie obowiązków ze szkodą dla interesu publicznego lub prywatnego. Pracownicy, w stosunku do których odpowiedzialności takiej nie będzie można egzekwować właśnie ze względu na specyficzny ograniczony zakres obowiązków lub zadań, będą traktowani jako osoby wykonujące czynności usługowe. Pozostałe natomiast jako te, które podlegają wykładni art. 115 §13 kodeksu karnego.

Możliwa jest również interpretacja jeszcze bardziej zawężająca, zgodnie z którą za funkcjonariusza należy uznać tylko takiego pracownika, który bezpośrednio uczestniczy w wydaniu decyzji administracyjnej.¹⁰ Pojęcie bezpośredniego uczestnictwa nie jest jednak ściśle określone. Wydaje się, że chodzi tu o to samo, o czym wspomnieliśmy wcześniej, tzn. o ustalenie charakteru i zakresu wkładu konkretnej osoby w podjęcie określonego rozstrzygnięcia lub realizacji przysługującego konkretnemu podmiotowi władztwa.

Ten, kto nie jest funkcjonariuszem, może pełnić funkcję publiczną jako członek zarządu (np. powiatu, województwa), a także jako pracownik, który nie ma statusu pracownika administracji rządowej lub samorządowej, jest np. pracownikiem szpitala, spółdzielni mieszkaniowej, czy nawet pracownikiem upoważnionym do reprezentowania podmiotu prowadzącego działalność gospodarczą w zakresie wykonywania zadań użyteczności publicznej (np. pracownicy przedsiębiorstwa energetycznego).

Jeszcze przed wprowadzeniem tego przepisu SN za osobę pełniącą funkcję publiczną uznał ordynatora szpitala i to zarówno w związku z administrowaniem, jak i udziela-

¹⁰⁾ Na co wskazywał Sąd Najwyższy za funkcjonariusza publicznego można uznać konkretną osobę „jedynie wówczas, gdyby na mocy przepisów prawa lub upoważnienia właściwego organu był uprawniony do wydawania decyzji administracyjnych i tylko w zakresie tego uprawnienia”, Uchwała SN z 17 maja 2000, I KZP 10/00, OSNKW 2000/5-6/40.

niem świadczeń zdrowotnych,¹¹ dyrektora przedsiębiorstwa państwowego,¹² prezesa spółdzielni mieszkaniowej,¹³ a także upoważnionych przedstawicieli przedsiębiorstwa energetycznego dokonujących kontroli legalności poboru energii elektrycznej.¹⁴

Dokonując podsumowania dotychczasowej praktyki SN w kolejnym orzeczeniu, dotyczącym statusu pracownika naukowo-dydaktycznego uczelni wyższej stwierdził, iż można wyodrębnić dwa podstawowe kryteria pozwalające „na rozpoznanie znamion funkcji publicznej na gruncie konkretnego stanu faktycznego. Pozycja i zachowanie określonej osoby nabierają cech pełnienia funkcji publicznej, gdy jednocześnie spełnione są przesłanki umocowania normatywnego oraz działania w oparciu o środki publiczne. Wprawdzie pierwsze z tych kryteriów interpretowane jest dość szeroko, poczynając od takiego umocowania w przepisach rangi ustawowej, które sprawia, że podejmowane czynności należy traktować jako przejaw władczej działalności instytucji państwowych oraz samorządu terytorialnego, aż do przyjęcia, że wystarczające jest określenie w ustawie jedynie samego istnienia, zadań i kompetencji danego podmiotu (...)”.¹⁵

Na tym tle istotne znaczenie ma wykazanie czy działalność (praca) konkretnej osoby związana jest z:

- realizacją konstytucyjnie i ustawowo określonego zadania z zakresu administracji publicznej;
- zakresem praw, a z drugiej strony obowiązków nałożonych na pracownika;
- charakterem prawnego miejsca pracy przy jednoczesnym uwzględnieniu (...) „że w sytuacji, gdy państwo wycofało się z wielu dziedzin aktywności, przekazując je inicjatywie indywidualnej lub społecznej, to w tych sferach, które z mocy szczególnych regulacji pozostają w gestii specjalnie wykreowanych podmiotów państwowych jako zadania ogólnonarodowe, nadal mamy do czynienia z pełnieniem funkcji publicznej”.¹⁶

SN zauważył również, iż „...podobnie jak to ma miejsce w przypadku funkcjonariusza publicznego, również pełnienie funkcji publicznej musi być odnoszone nie do społeczeństwa jako nieoznaczonej zbiorowości, ale do tego kręgu podmiotów, które wchodzi w relację z konkretnym funkcjonariuszem lub osobą pełniącą funkcję publiczną i których dotyczą podejmowane decyzje tych osób, umocowane w ich kompetencjach. Nie ma też żadnych podstaw do tego, aby wiązać kryterium funkcji publicznej wyłącznie z realizowaniem działania o zasięgu ogólnospołecznym. Nawet wśród funkcjonariuszy publicznych taki zakres działania dotyczy jedynie bardzo wąskiej grupy”.¹⁷ Stanowisko takie jest równoznaczne z koniecznością odrębnego badania każdej ze spraw pod kątem stwierdzenia, czy da się wykazać istnienie wskazanych wyżej przesłanek oraz ich oceny pod kątem charakteru stosunku prawnego bądź wykorzystywania środków publicznych. Przypadek osoby zatrudnionej w jednostce organiza-

¹¹⁾ Uchwała składu 7 sędziów SN z dnia 20 czerwca 2001 r., I KZP 5/01, OSNKW 2001, z. 9-10, poz. 71.

¹²⁾ Uchwała składu 7 sędziów SN z dnia 18 października 2001 r., I KZP 9/01, OSNKW 2001, z. 11-12, poz. 87.

¹³⁾ Uchwała składu 7 sędziów SN z dnia 28 marca 2002 r., I KZP 35/01, OSNKW 2002, z. 5-6, poz. 29, w której Sąd uznał, że pełnienie funkcji publicznej w rozumieniu art. 228 § 1 k.k. obejmuje tylko takie czynności wykonywane przez prezesa zarządu spółdzielni mieszkaniowej na podstawie art. 55 § 1 ustawy z dnia 16 września 1982 r. – Prawo spółdzielcze, które wiążą się z dysponowaniem środkami publicznymi wskazując jednocześnie ich zakres.

¹⁴⁾ Postanowienie SN z dnia 15 listopada 2002 r., IV KKN 570/99, OSNKW 2003, z. 1-2, poz. 10.

¹⁵⁾ Postanowienie SN z dnia 15 listopada 2002 r., IV KKN 570/99, OSNKW 2003, z. 1-2, poz. 10.

¹⁶⁾ Tamże.

¹⁷⁾ Postanowienie SN z 25 czerwca 2004 r. V KK 74/04 OSNKW 2004 nr 7-8.

cyjnej dysponującej środkami publicznym wymaga z pewnością odrębnego zbadania. Niejasności tkwią choćby w samym określeniu granicy pomiędzy dysponowaniem środkami publicznymi a takim ich wykorzystaniem, które jednak nie mieści się w tym pojęciu. Z uwagi na ograniczenia formalne kwestii tej nie możemy jednak omówić szerzej.¹⁸

Podsumowując dotychczasowe rozważania stwierdzić należy, że pojęcie pełnienia funkcji publicznej jest rozumiane przez ustawodawcę i orzecznictwo niejednolicie. Podejście takie znajduje swój odrębny wymiar w kontekście przetwarzania danych osobowych. Możemy bowiem wskazać przynajmniej cztery sytuacje, w których przyjąć należy istnienie pewnych odrębności w zakresie przetwarzania danych osobowych osób należących pozornie do jednej kategorii określanej jako osoby pełniące funkcje publiczne.

Pierwsza z nich charakteryzuje się tym, że choć podmiot danych jest osobą pełniącą taką funkcję, to informacje go dotyczące nie stanowią informacji publicznej ani innej wskazanej w regulacji szczególnej i nakazującej ich inne traktowanie. W stosunku do tych danych u.o.d.o. będzie stosowana w pełni na każdym etapie ich przetwarzania.

Druga dotyczy osób pełniących funkcje publiczne szczególnego rodzaju, z którymi ustawodawca związał dodatkowe obowiązki informacyjne (np. oświadczenia lustracyjne czy majątkowe) – otwartą kwestią pozostaje zagadnienie czy w każdym przypadku informacje te stanowią informację publiczną – można mieć, co do tego wątpliwości (szczególnie, gdy dotyczą współmałżonków osób pełniących funkcje publiczne). Dane osobowe objęte tymi obowiązkami będą podlegały przetwarzaniu w oparciu o u.o.d.o. jedynie w niewielkim stopniu, bądź wcale. Dzieje się tak z uwagi na objęcie ich odrębnymi procedurami pozyskiwania, przechowywania i ujawniania.

Trzecia odnosi się do osób pełniących funkcje publiczne, których dane osobowe w pewnym zakresie zostaną zakwalifikowane jako informacja publiczna. Od tego momentu można mówić o wyłączeniu w stosunku do tych danych rygorów u.o.d.o., utrudniających udostępnianie danych. Dzieje się tak z uwagi na fakt, iż zgodnie z u.d.i.p. każdy staje się potencjalnym (uprawnionym) odbiorcą informacji publicznej. Ich ujawnienie odbywa się ponadto w innym trybie niż przewidziany w u.o.d.o. – a wynikającym z postępowania związanego z udostępnieniem informacji publicznej. Forma tego udostępnienia jest uzależniona od woli wnioskodawcy, i/lub działań oraz możliwości posiadacza tych informacji (część z nich ujawniana jest np. w BIP). Pozostałe zasady u.o.d.o. są w stosunku do tego rodzaju danych w pełni skuteczne, w szczególności osoba, której dane dotyczą, może się powoływać na swoje prawa związane z rektyfikacją informacji.

Ostatnia sytuacja to przypadek, w którym mamy do czynienia z osobą pełniącą funkcję publiczną i uznajemy, że część informacji o niej stanowi informację publiczną. Są to jednak informacje szczególne (z uwagi na rodzaj informacji lub osobę, której dotyczą), objęte różnego rodzaju obostrzeniami w sferze ich przetwarzania,

związanymi najczęściej z ochroną informacji niejawnych czy innych tajemnic ustawowo chronionych. Pomimo potencjalnej możliwości działania w ramach u.d.i.p. w praktyce żadna z nich nie może zostać udostępniona nikomu spoza wąskiego kręgu uprawnionych na mocy przepisów odrębnych dotyczących tajemnicy, która występuje w konkretnym przypadku.¹⁹ W stosunku do tego rodzaju danych osobowych u.o.d.o. praktycznie nie znajduje zastosowania lub jedynie w niewielkim stopniu. Interesujący jest jednak fakt, że objęcie jakiejś informacji publicznej tajemnicą daje, na mocy u.d.i.p., możliwość weryfikacji sądowej zasadności takiego postępowania.

Kończąc, nie sposób oprzeć się wrażeniu, że na tych kilku stronach dokonaliśmy jedynie ogólnego, wstępnego przybliżenia niektórych aspektów problematyki związanej z ujawnianiem danych osobowych osób pełniących funkcje publiczne – wśród wątków pominiętych znalazło się choćby wskazanie konkretnych kategorii informacji osobowych stanowiących jednocześnie informację publiczną. Jest to jednak zagadnienie jeszcze bardziej złożone i zindywidualizowane niż poruszana przez nas problematyka, ponadto w tej kwestii najwięcej do powiedzenia mają i mieć będą sądy, których orzecznictwo pozwala na powolne tworzenie katalogów informacji publicznej o charakterze osobowym. W tym kontekście, ciekawe okazać się może porównanie zakresu ujawnianych informacji publicznych w powiązaniu z *ratio legis* u.d.i.p. czyli stworzenia podstawy dla społecznej kontroli władzy. Czas pokaże, czy rezygnacja z pewnych elementów gwarantujących ochronę danych osobowych i prawo do prywatności rzeczywiście znajdzie odzwierciedlenie w poprawie funkcjonowania państwa. Transparentność życia publicznego musi bowiem osiągnąć pewien – zapewne dość głęboki – poziom, aby efekty stały się zauważalne nie tylko przez osoby, których dane podlegają udostępnieniu, ale i przez pozostałą część społeczeństwa.

Public function as the premise for modification of the scope of data protection

Since 1997, the sentence "Any person has the right to have his/her personal data protected" may be found in the first Article of the Act on the Protection of Personal Data¹ (hereinafter APPD). In the common opinion the Act commencing with this declaration constitutes the development of provisions set out in Article 51 (but also in Article 47, or even Articles 49 and 53) of the Constitution of the Republic of Poland. The same Constitution provides also for other norms, which interpretation quite often leads to conclusions concerning the free flow of information – including information on natural persons. Articles 14, 54 or 61 of the Constitution may serve as the exemplification of this tendency.

¹⁸⁾ Na ten temat zob. szerzej np. M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej. Informatyzacja administracji*, Wrocław 2005, s. 143-153.

¹⁹⁾ Jako prosty przykład tego typu informacji można podać dane o zatrudnieniu osób w służbach specjalnych na stanowiskach, z którymi wiąże się konieczność utajnienia personaliów pracowników.

This situation reflects two tendencies noted in each democratic country. On the one hand, the lawmakers aim at protection of natural persons; on the other hand, they want to create mechanisms allowing for insight into life and activities of the very same persons – as soon as they become part of the generally understood circle of power. For the inalienable right of those being governed is the ability to control activities of those who are in power. Of the grounds for that belief, which leads to limiting the scope of protection of privacy of those performing public functions, the first and foremost is the opinion that transparency of such activities is one of the basic mechanisms protecting the democracy from turning into authoritarian or totalitarian system.

Since January 1, 2002, the Act, which was to realize to a large extent the exercise of this very citizen right, has been in force in Poland. As in the case of APPD, in the first paragraphs of the Act on Access to Public Information² (hereinafter AAPI) one can find the momentous declarations. In this case they indicate the will to make this Act the foundation for providing free access to public information. Moreover, the AAPI indicates that anyone can be a potential recipient of such data and it guarantees very broad access to public information (some limitations result mainly from Article 5 of this Act)³ without substantiating any interest of that entity in the information. The above-mentioned regulation sets out limitations of the right to public information within the scope and on terms and conditions specified in the regulations on protection of confidential information and on protection of other secrets protected by law (Article 5.1 of the AAPI). Among the interests which limit the disclosure of public information, the privacy is regarded by the lawmaker to be crucial. However, according to paragraph 2 of the above-mentioned article "The limitation does not relate to the information on persons performing public functions which relates to performing these functions, including the conditions of entrusting and performing these functions, and cases where a natural person or entrepreneur resigns from their pertaining rights."

Considering the subject matter of this study it is not necessary, in our opinion, to make any further analysis of the last part of the above-quoted provision. It concerns voluntary resignation from the right to protect information of personal nature, but it should be emphasized that it falls within the fundamental assumption of the APPD indicating the approval of a person the data pertain to, as one of the possible, and probably the preferable (due to the ability of an individual to shape one's public image) way of legalisation of personal data processing.

Undoubtedly the key issue, just considering the title of this study, would be to the attempt to interpret the introductory part of Article 5 paragraph 2 of the AAPI, and to answer the question of consequences it bears for the rules of personal data processing.

¹⁾ Namely Dz.U. (Journal of Laws) of 2002, no. 101, item 926, as amended.

²⁾ Dz.U. of 2001 No. 112, item 1198, as amended.

³⁾ For details on any possible limitations of right to access the public information, see: M. Jabłoński, K. Wygoda *Ustawa o dostępie do informacji publicznej. Komentarz* (The act on access to the public information – Commentary), Wrocław 2002, or M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej. Informatyzacja administracji* (Public Information Bulletin. Computerisation of Administration), Wrocław 2005.

Without going deeper into the provisions of the AAPI and bearing in mind that according to Article 61 of the Constitution, a citizen has the right to obtain information on activities of public authority bodies and persons performing public functions, we must state that the lawmaker created the norm that is equal to the APPD. As the act was enacted later and concerning only a portion of personal data, then in case of this act we can cite the recognized rules of *lex posterior derogat legi priori* and *lex specialis derogat legi generali*. This is essential, as, in theory, one can claim that it is in contradiction with the Article 5 of the APPD indicating the situation when if the provisions of different regulations on data processing provide for wider protection of the data than the provisions of the APPD, then the provisions of those acts shall apply. In this particular case, which excludes almost all possible limitations with regard to providing certain part of personal data, we will definitely not deal with wider protection.⁴

In an event of the claim of possible inconsistency between Article 5 of the AAPI and Article 51 of the Constitution, that being the specification of Article 61 of the Constitution it cannot be dismissed immediately, as those two norms have equivalent legal force. If, therefore, it does not exceed the freedom of the lawmaker in developing the provisions of the Constitution, then it is in agreement with it. Lately the Constitutional Tribunal addressed this issue and it adjudicated that "Article 5 paragraph 2 sentence 2 of the Act of September 6, 2001 on access to public information (Dz.U. No. 112, item 1198, of 2002 No. 153, item 1271, of 2004 No. 240, item 2407 and of 2005 No. 64, item 565 and No. 132, item 1110) is in agreement with Article 31 paragraph 3, Article 47 and Article 61 paragraph 3 of the Constitution of the Republic of Poland, and it is not in contradiction with Article 61 paragraph 4 of the Constitution."⁵ With the confidence that at this time Article 5 of the AAPI is not considered to be exceeding the allowed, constitutional boundaries of the legal limitations of privacy we can try to determine which group this regulation applies to.

First of all, we have to state that the lawmaker, citing in the AAPI the term of "persons performing public functions" did neither provide definition of such term nor made reference to any acts including such definition and already existing at that time. We are thinking of at least two legal acts:

⁴⁾ More on the interpretation of Article 5 of the APPD in: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych, Komentarz*, (Protection of personal data – Commentary), Kraków 2004, pages 363 – 368.

⁵⁾ The ruling of March 20, 2006, file no. K 17/05. At the moment this study was developed, the Constitution Tribunal has not issued the written substantiation for that ruling yet. It would probably be very helpful for detailed presentation of the motives, the Constitution Tribunal attached to the lawmaker while creating this exemption from the rule of a limited disclosure of information of personal nature. Some information on that issue may be found in the press release issued after the hearing. It was stated that "... regulation in the questioned provision of the Act on Access to Public Information would only be in contradiction to the Constitution when application of such provision would infringe the below-mentioned rules. Therefore, information cannot go beyond the necessity formed by the need for transparency of public life, examined in accordance with norms adopted in the democratic state of law. Also, the information should not write off the idea of protection of the right to privacy. It always must have some importance for evaluation of operations of an institution and those performing public functions. In the opinion of the Tribunal, the privacy may, in certain situations, be the subject of intervention for the common welfare. But, entering this area must be made with prudence, with due evaluation of arguments that call for such intervention. For we are dealing with equal interests. Limitations with regard to some rights protected by the Constitution may be introduced due to the common interest. Such rights, in the opinion of the Constitution Tribunal, include the right for privacy".

- The Act of April 11, 1997 on disclosing employment or service of persons performing public functions in the state security institutions or cooperation with such institutions in years 1944-1900;
- The Act of August 21, 1997 on limitations of business activities performed by public officials.⁶

Therefore, it can be assumed that the lawmaker's assumption was to have some interpretation freedom for this term under the AAPI. Presumably, it is connected with the very wide range of entities obliged to disclose public information (Article 4 of the AAPI) and holding such information. Adopting rather narrow definitions appearing in both above-mentioned acts⁷, naturally in the context of wide recognition of public information as such, would lead to extensive exclusion of numbers of people about whom the community would have the right to require information, if it was related to their public positions.

⁶) Respectively: Dz.U. of 1999, no 42, item 428 as amended, and Dz.U. of 1997, no. 106, item 679 as amended.

⁷) The "vetting" act sets out that "... **Article 3.** 1 The persons performing public functions, in the meaning of this act, are: President of the Republic of Poland, member of the Parliament, senator and a person nominated, elected or appointed to the specific managerial posts within state administration by the President of the Republic of Poland, the Sejm (the Lower Chamber of the Parliament), the Presidium of the Sejm, the Senate, the Parliament, the Speaker of the Sejm, the Speaker of the Senate or the Chairman of the Council of Ministers, the Head of the Civil Service, general director within the ministry, central agency or the office of the voivode, and the judge, the prosecutor and the solicitor, as well as the president of the university, the vice-president, manager of the basic organization unit at the public and non-public higher education institution, member of the Central Board for the Higher Education, member of the National Accreditation Commission, member of the Central Commission for Degrees and Titles. 2. Persons performing public functions, as set out by the act, are also: members of the supervisory boards and management boards, the programme directors and directors of regional centres and agencies of "Telewizja Polska – Spółka Akcyjna" (Polish Television) and "Polskie Radio – Spółka Akcyjna" (Polish Radio), general director of the Polska Agencja Prasowa (Polish Press Agency), directors of offices, chief editors and managers of regional departments of the Polish Press Agency, president of the Polska Agencja Informacyjna (Polish Information Agency), vice-presidents, members of the management board and directors – chief editors of the Polish Information Agency."

The act restricting the freedom of business activity includes two articles specifying the group of persons the act applies to. What is interesting, the assumption that those groups of people indeed perform any public functions results primarily from the very title of this act: "**Article 1.** The act sets out restrictions for carrying out business activity by persons holding managerial posts within state administration, as provided for by regulations on remuneration of persons holding managerial posts within state administration, and by the judges of the Constitution Tribunal.

Article 2. The act also sets out the limitations for carrying out business activity by:

- employees of state offices, including members of the civil service corps, holding managerial positions of:
 - general director, director of department (equivalent unit) and his/her deputy, and head of division (equivalent unit) – in the national offices and central state bodies.
 - general director of the office of the voivode, director of department (equivalent unit) and his/her deputy and chief accountant, manager of regional office and his/her deputy and chief accountant – in local offices of the bodies of general state administration.
 - manager of the office and his/her deputy – in the local offices of the special state administration.
- employees of state offices, including members of the civil service corps, holding posts equal to those mentioned in point 1 with regard to remuneration,
- other than those mentioned in point 1 and 2 members of the civil service corps employed in the office supporting the minister relevant for the public finances,
- general director of the Supreme Chamber of Control and employees of the Supreme Chamber of Control supervising or performing inspection tasks,
- President and vice-presidents, and senior counsellors and counsellors of the Prokuratoria Generalna Skarbu Państwa (the General Office of the Legal Representation of the State Treasury).
- employees of regional clearing chambers holding positions of: president, member of the board, head of department and inspection officer,
- employees of self-government appeal courts holding positions of: chairman, deputy chairman, and full time member of the board,
- head of commune (mayor, president of a city), deputy head of commune (mayor, president of a city), the commune's treasurer, secretary, manager of the commune's organization unit, administrator and member of managing bodies of the communal legal entities and other persons issuing administrative decisions on behalf of the commune head (mayor, president of the city),

Simple comparison of above-mentioned regulations (in footnote 7) allows indicating different approaches to perception of persons performing public functions. Lack of full consistency of definitions is presumably the result of different premises of enacting those two acts and different scope of personal data disclosed due to the obligation arising from both acts – the access to information so disclosed is different too.⁸ In the light of existing discrepancies, adopting an assumption that one of those two definitions is correct also for the AAPI would be doubtful.

The actual scope of the term "performing public function" under the AAPI was unclear in the initial period of the operation of the Act. We are of the opinion that this situation improved in 2003 when the Penal Code was amended with changes including, among others, adding Article 115 § 19 of the Penal Code.⁹ Due to the nature of the Penal Code itself, in particular its general application, and the penal part within the AAPI, we are forced to examine premises of the actions sanctioned by the Act thereby from the perspective of general provisions of the Penal Code. The penalisation of withholding public information (Article 23 of the AAPI) forces us to determine whether in a specific case, the act is breached due to withholding of public information concerning a person performing a public function, or whether this is not the case due to inability to qualify a person about which the inquiry was made to those performing public functions. Therefore, if the AAPI does not provide the definition of this term, then it should be reconstructed, particularly for the purpose of penal proceedings, specifically with Article 115 § 19 of the Penal Code. If such a rule is applied in the most severe case for the entity providing public information, then we see no problem to apply the same in the regular, day-to-day execution of the AAPI regulations. Upon adopting this initial assumption, we can state that (according to Article 115 § 19 of the Penal Code) for the purposes of interpretation of the AAPI, a person performing public function is:

- public official,
- member of a self-government body,

6a) members of the management of a poviát, the poviát's treasurer, secretary, manager of the poviát's organization unit, administrator and member of managing bodies of the poviát's legal entities and other persons issuing administrative decisions on behalf of the starost,

6b) members of the management of voivodship, the voivodship's treasurer, manager of the voivodship's self-government organization unit, administrator and member of managing bodies of the voivodship's legal entities and other persons issuing administrative decisions on behalf of the marshal of the voivodship,

7) employees of state banks holding positions of: president, vice-president, management board member and treasurer,

8) employees of state enterprises holding positions of: director of the enterprise, his/her deputy and chief accountant,

9) employees of a company wholly owned by the State Treasury, and companies, where the State Treasury owns more than 50% of the share capital or 50% of number of shares, holding positions of: president, vice-president, and management board member,

10) employees of state agencies holding positions of: president, vice-president, director of the group, director of regional unit and his/her deputy – or equivalent positions,

11) other persons performing public functions, if the specific acts so provide for.

⁸) In case of vetting statement, some of them are presented to the public in form of election announcement – therefore they are open in full, another part may be examined by the court if a person submitting such statement takes a specific post – then at least the legal conclusion of the judgment will be open. With regard to the statements on business activity carried out by the spouse, a professional secret is taken into account. Similarly in the case of property statements (although such information may be disclosed upon written approval of a person submitting such statement), and then, information entered into the Register of Benefits are fully open.

⁹) Article 115 § 19 added by Article 1 point 3 b) of the Act of June 13, 2003 (Dz.U. of 2003, No 111, item 1061) amending the Penal Code as of July 1, 2003.

- person employed in an organisation unit utilizing public funds, unless that person performs support functions only,
- any other person if their rights and duties with regard to public activity are set out or recognized by the law or by an international agreement binding for the Republic of Poland.

Therefore, there is no doubt that the scope of this term is definitely wider than the term of “public official” which was used most often in the initial period of the AAPI operation, in order to limit the Act’s scope of operation only to clear-cut cases. It was understandable, if only for the fact that the Article 51 of the APPD provides that: “1. A person managing a data filing system or being obliged to protect personal data, who discloses them or provides the access to unauthorised persons, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to two years.

2. In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.” Qualifying part of personal data to public information and providing them in case when the person such information pertains to does not perform public function could result in such liability.

While explaining the concept of a person performing public function, it is impossible to avoid having a closer look at some of its elements. We should start from the essential issue of the definition of “public officer”. According to Article 115 § 13 of the Penal Code, a public officer is:

- President of the Republic of Poland,
- Member of the Sejm, Senator, councillor,
- Member of the European Parliament,
- judge, juror, prosecutor, notary public, bailiff, court appointed administrator, person adjudicating in cases for minor offences or within the disciplinary bodies operating in accordance with the act,
- person employed in the state administration, other state body or local self-government, unless such person performs support functions only, and any other person within the scope she/he is authorised to issue administrative decisions,
- person employed by the state control body or local self-government control body, unless that person is performing support functions only,
- person holding a managerial position within other public institution,
- official of the body established for protection of public security or an officer of the Prison Service,
- person in active military service.

The literature is right noting that the above-mentioned regulation makes the concept of the public officer dependant on employment at a governmental administration body, or any other public body, or local self-government. The formal premise for qualifying a person as a public officer is the commencement of employment.

Exclusion of a person from the category of public officers is related to determination of that person’s duties and authority. Therefore, the issue is to prove that a specific person, due to employment within the administration, is responsible for exceeding their authority or failure to perform their duties which is harmful to the public or

private interest. Employees who fail to be covered by such responsibility, specifically due to the specific and limited scope of their duties or tasks, will be treated as persons performing support function. The others will be treated as those being subject to interpretation of Article 115 §13 of the Penal Code.

A more narrow interpretation is also possible, according to which a public officer should only be such an employee who directly participates in issuing an administrative decision.¹⁰ However, the concept of direct participation is not precisely determined. It seems that the case is similar to what we have already mentioned, namely it is about establishing the nature and scope of a specific person’s contribution in undertaking a specific decision or execution of the authority vested in a specific body.

The person who is not a public officer may perform a public function as a member of the management board (i.e. of the poviát, or voivodship), and as an employee who is not an employee of the state or local administration, for example an employee of hospital, a housing cooperative, or even an employee authorised to represent an entity carrying out business activity with regard to execution of the public benefit corporation tasks (e.g. employees of the power company).

Even before this provision was introduced, the Supreme Court recognized the head of the hospital to be a person performing public function, both with regard to managing the institution and providing health care services;¹¹ director of the state-owned enterprise,¹² president of a housing cooperative,¹³ and authorised representatives of the power company to carry out inspections of electricity uptake legitimacy.¹⁴

The Supreme Court, summarising its practice to date in the following ruling on the position of research and teaching employee of a university, stated that two basic criteria can be specified in order to “determine the traits of a public function according to the specific actual situation. The position and conduct of a specific person bear the traits of performing a public function when the premises of authorization by law and activities utilizing public funds are fulfilled simultaneously. Admittedly, the first criterion is interpreted very widely, starting from the authorization of the provisions having the power of the act which causes that the undertaken functions should be treated as manifestation of the imperious activities of the state institution and the local self-government, ending with the assumption that it is enough to specify in the law the entity’s existence, tasks and competences as such (...)”.¹⁵

In the light of the above, it is of a significant importance to indicate whether activity (work) of a specific person is connected with execution of:

- a task within the scope of public administration, as set out by the constitution and the law,

¹⁰⁾ As it was indicated by the Supreme Court, the public officer may only be a specific person “only if, under provisions of the law or the authorisation of a relevant body, such person is authorised to issue administrative decisions, and only within the scope of such authorisation”, Resolution of the SC of 17 May, 2000, file no.: I KZP 10/00, OSNKW 2000/5-6/40.

¹¹⁾ Resolution of 7 judges of the SC of 20 June 2001, file no.: I KZP 5/01, OSNKW 2001, volume 9-10, item. 71.

¹²⁾ Resolution of 7 judges of the SC of October 18, 2001, file no.: I KZP 9/01, OSNKW 2001, volume 11-12, item. 87.

- scope of rights, and on the other hand scope of duties vested in an employee,
- legal nature of the place of employment with consideration (...) “that in a situation the state has withdrawn from a number of areas of activity, transferring them to the domain of individual or social initiatives, then in those areas which, under the specific regulations, are still managed by specifically established state entities as nationwide tasks, we are still dealing with performance of public function”.¹⁶

The Supreme Court also noted that “... similarly to the case of a public official, also performing a public function must be related not to the public as an indeterminate population, but to this group of entities that become a party to the relationship with a specific officer or a person performing public function and which are governed by decisions made by such persons, as authorised within the scope of their competence. There are no grounds to connect the public function criterion exclusively with execution of a community-wide activity. Even among the public officers such a scope of activity relates only to a small group”.¹⁷ This opinion is equal to the necessity of separate examination of each specific case in order to state whether existence of the above-mentioned premises may be proved and to evaluate them with regard to determination of the nature of legal relation or utilization of public funds. Certainly, the case of a person employed in an organisation unit utilizing public funds requires specific research. At least, there are ambiguities related to the separation of having public funds at disposal and their utilization that does not fall within such definition. Due to the formal limitation, this issue cannot be discussed further.¹⁸

To summarise the considerations made so far, it should be stated that the concept of performance of a public function is not understood by the lawmaker and the judicial decisions uniformly. Such approach has its own impact in the context of personal data processing. We can indicate at least four cases where differences should be assumed with regard to processing of personal data pertaining to persons that seemingly belong to one category described as persons performing public functions.

The first case is that even though a data subject is a person performing such function, the information pertaining to that person is not public information or any other information indicated in the specific regulation and providing for a different treatment of such. In case of such data the APPD will be applied in full, at each stage of their processing.

¹³⁾ Resolution of 7 judges of the SC of March 28, 2002, file no.: I KZP 35/01, OSNKW 2002, volume 5-6, item. 29, in which the Court decided that performing a public function under Article 228 §1 of the penal code covers only activities carried out by the president of management board of the housing cooperative under Article 55§1 of the act of September 16, 1982 – the Act on cooperatives, which relate to utilisation of public funds and indicating the scope of such at the same time.

¹⁴⁾ Resolution of the SC of November 15, 2002, file no.: IV KKN 570/99, OSNKW 2003, volume 1-2, item. 10.

¹⁵⁾ Resolution of the SC of November 15, 2002, file no.: IV KKN 570/99, OSNKW 2003, volume 1-2, item. 10.

¹⁶⁾ Ibid.

¹⁷⁾ Decision of the SC of June 25, 2004, file no.: V KK 74/04 OSNKW 2004 no. 7-8.

¹⁸⁾ For more information on the subject, see: M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej. Informatyzacja administracji* (Public Information Bulletin. Computerisation of Administration), Wrocław 2005, pages 143-153.

The second case relates to persons performing public functions of particular type, and for which the lawmaker specified additional informational obligations (e.g. “vetting” statements, or property statements) – it is still an open issue whether in each case such information constitutes public information – it is doubtful (particularly if it concerns spouses of persons performing public functions). Personal data subject to this obligation will be processed based on the APPD only to a small extent or not at all. This is due to the fact that such information is regulated by separate procedures for obtaining, storing and disclosing.

The third case relates to persons performing public functions and their personal data will be qualified, to some extent, as public information. From that point we can say such data are excluded from the provisions of the APPD making their disclosure more difficult. This is due to the fact that according to the AAPI, anyone is a potential (authorized) recipient of public information. Disclosure of such information is made by other means than those provided for in the APPD, and results from the proceedings connected with provision of public information. The form of such provision depends on the will of the applicant, and/or activities and possibilities of the entity holding such information (some information is provided in, e.g. the Public Information Bulletin). The other provisions of the APPD are fully enforceable towards such type of data, in particular a person the data pertain to may execute the rights connected with rectification of information.

In the last case a person is performing a public function and some information about such person is recognized as public information. Nevertheless, this is specific information (due to the type of information or a person it pertains to), covered by a number of various limitations with regard to their processing, and most of all connected with protection of confidential information or other secrets protected by law. Despite a potential possibility to act under the AAPI, in practice no information can be provided to anybody beyond a very narrow group of persons authorised under the separate regulations on secret material, which occurs in a specific case.¹⁹ With regard to such personal data, the APPD cannot be applied in practice, or can be applied to a very limited extent. It is interesting though, that justification of deeming some public information a secret may be, according to the AAPI, determined in court.

Concluding, it is hard to avoid impression that this paper may be only a general, introductory description of some aspects of issues relating to disclosure of personal data of persons performing public functions – among issues not discussed is, for example, determination of specific categories of personal information which is at the same time public information. However, this is an issue even more complex and specific than the problems we mention herein; moreover, the courts may and will have more to say about this, as their decisions allow for slow creation of catalogues of public information of personal nature. In this context, it might be interesting to compare the scope of disclosure of public information in connection with *ratio legis* of the AAPI, namely creating basis for social control of those in power. The time will

¹⁹⁾ A simple example would be data on employment in secret services on positions which require personal data of such employees to be classified.

show whether resignation from some elements guaranteeing protection of personal data and the right to privacy will actually be reflected in the improved functioning of the state. The public life transparency must reach a certain, presumably rather deep level in order for the results to be visible not only by those whose data are published, but by the public itself.

Prof. Dr Alfred Bülesbach

Chief Officer Corporate Data Protection, DaimlerChrysler AG
Główny Urzędnik Ochrony Danych, DaimlerChrysler AG

Binding Corporate Rules

- I. Introduction
- II. Legal background for international data transfers
- III. Evaluation of self-regulatory instruments
- IV. Development and enforcement of Binding Corporate Rules
- V. Recommendations for the content of Binding Corporate Rules
- VI. Procedure for an approval of Binding Corporate Rules in Europe
- VII. Conclusion

I. Introduction

The philosopher Seneca once said: „*Most powerful is he who has himself in his own power*”. This quotation summarizes in a few words the significance of self-determination for the development of one's own personality. It also shows that since early times self-determination has been a value that human beings strove for. It is generally agreed that it is much more rewarding, much more fulfilling, to be able to control one's own conduct instead of living in heteronomy, or, in other words, being directed by external factors. In fact, it might be said that on a personal level the ability to set one's own benchmarks and to live up to them is one of the highest forms of human development.

Nowadays this trend of behavioral philosophy is of increasing importance as it is closely linked to the protection of personal rights. The notion of self-determination might well be seen as the very basis of all personal rights. In today's world which is marked by international cash flows and the transnational exchange of goods and services the respect for personal rights, and hence for the idea of self-determination, is more and more of importance. The “human face” of the globalized commercial and economic society manifests itself in the lasting respect for personal rights, data protection and data security.

Today it is crucial for multinational companies to develop and integrate data security and data protection concepts in their products and services. The reason for this are the technical convergence and the worldwide economic interconnection which increase the possibilities of matching and processing personal data and which therefore raise the potential risk of personal data being used in a fraudulent way. At the same time the consumers' sensitivity regarding the handling of their personal data is much higher than it was only a few years ago. This is particularly evident when customers take advantage of e-commerce possibilities. In this context the integration of data security and data protection concepts is also a competitive factor between companies, and the economic

value of information is still rising. The more efficient customer data is protected, the higher is the probability that the concerned customer will adhere to the company in the future. This requires not only the protection aiming to prevent fraud for the customer, but also the protection of the company itself against economic loss resulting from lack or loss of the factor of production which is formed by high-quality information.

Such a high level of protection is required by customers, partners and employees even if their data is transferred to other countries for any legitimate purpose. Respect for human rights requires that the entity which exports data to a company seated abroad guarantees their protection any time.

II. Legal background for international data transfers

The transborder data flow, however, finds itself in a very diverse legal environment. While data flows do not stop at state borders, the validity of national laws does. Due to the lack of a globally competent legislator there exist many different legal approaches worldwide to cope with the challenge of guaranteeing effective data protection. Although efforts are made to harmonize the worldwide data protection standards, the current situation is characterized by divergence and difficult questions of legal delimitation. The awareness for questions of data protection is differing as much throughout the world as the regulatory approaches are. Some countries follow a comprehensive regulatory approach meaning that general data protection laws have been enacted which set requirements for the collection, processing and use of personal data by public and private entities. This approach is, for example, followed by Australia, New Zealand, Chile or the EU. Some other countries follow a sector-specific approach meaning that regulations have been enacted governing data protection issues for particular applications, such as the financial sector or the telecommunications sector. An example for this approach is the USA, where no abstract and general data protection laws for businesses exist. However, there sector-specific laws, such as the HIPAA, the Financial Modernization Act, the Telecommunication Act or the Security Information Breach Act in California contain data protection requirements for their specific sector of application.

To simplify business for multinational companies and to ensure unified protection of the human rights of all persons whose data is collected or processed in one of the Member States, the European Union has harmonized data protection requirements on its territory. What remains are difficulties and open questions resulting from the diverse legal requirements for data transfers to countries beyond the borders of the EU and EEC. The EU Directive on data protection,¹ which has been transformed into the national laws of the EU Member States, contains specific regulations concerning data transfers to third countries in Articles 25 and 26. The Article 29 Working Party issued in 1998 working paper no. 12,² which contains explanatory regulations for the application of these Articles, especially on how „adequacy“ has to be defined and how it can be created by self-regulatory instruments.

¹) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281/31, 23.11.1995; the full text is available in 16 languages at the data protection website of the EU Commission at: http://www.europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

²) Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP 12 of 24 July 1998; several other Working Papers concerning Articles 25 and 26 followed, see fn. 10, 17, 18 and 19.

According to Article 25 (1) of the EU Directive personal data generated in the EU may only be transferred to third countries which provide an adequate level of data protection. The criteria which have to be considered to define adequacy are laid down in Article 25 (2) and explained in WP 12 of the Article 29 Working Party. Article 25 (6) provides that the Commission may find the level of protection in a country adequate in the procedure referred to in Article 31 (2). So far, the adequacy of national data protection standards has only been recognized by the EU Commission for Switzerland,³ Canada,⁴ Argentina,⁵ Guernsey,⁶ Isle of Man,⁷ the US Department of Commerce's Safe Harbor Privacy Principles,⁸ and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection.⁹ Concerning the latter, an action by the European Parliament and the European Data Protection Supervisor against the Commission is currently pending at the Court of Justice of the European Communities.¹⁰

But also negative findings of the Commission in relation to the adequacy of data protection regulations in the procedure according to Article 31 (2) have to be enforced by the Member States. Article 25 (4) of the EU Directive requires that they take the necessary measures to prevent any transfer of data of the same type to the third country in question. The transfer of EU-generated data to countries that do not provide an adequate level of data protection is only permitted if an individual exception according to Article 26 (1) of the EU Directive applies (for example the explicit consent by the data subject); or if there exist other adequate safeguards adduced by the data controller and an authorization is given by the respective Member State according to Article 26 (2). The Article 29 Working Party has issued working paper no. 114 to clarify the requirements of Article 26 (1) of the Directive, which contains specific interpretation guidelines for the application of each of the derogations in Article 26 (1).¹¹ A restricted use of the derogations is required by the Working Party to ensure compatibility with the data subject's fundamental rights. Other adequate safeguards can consist in appropriate contractual clauses or binding corporate rules, such as Codes of Conduct. One more option is to use the standard contractual clauses decided by the Commission according to Art. 26 Sec. 4, which also have to be recognized by the member states as adequate safeguards.

This legal background is principally the same in a number of other countries, such as Argentina,¹² Australia¹³ and Hong Kong,¹⁴ because these countries have similar „adequacy“ regulations.

³) Commission Decision 2000/518/EC of 26.7.2000, O. J. L 215/1 of 25.8.2000.

⁴) Commission Decision 2002/2/EC of 20.12.2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, O.J. L 2/13 of 4.1.2002.

⁵) Commission Decision C(2003) 1731 of 30/06/2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, O.J. L 168 of 5.7.2003.

⁶) Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, O.J. L 308, 25.11.2003.

⁷) Commission Decision 2004/411/EC of 28.4.2004 on the adequate protection of personal data in the Isle of Man, 2004/411/EC, O.J. L 151/48 of 30.4.2004.

⁸) Commission Decision 2000/520/EC of 26.7.2000, O. J. L 215/7 of 25.8.2000.

⁹) Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914), 2004/535/EC, O.J. L 235/11 of 06.07.2004.

¹⁰) Cases C-317/04 and C-318/04; documents are available in the register of cases at the official website of the Court at <http://www.curia.eu.int/de/content/juris/index.htm>.

¹¹) Working Paper 114, available at the official Article 29 Working Party's website at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

¹²) Sec. 12 of the Data Protection Act of Argentina.

¹³) Data Protection Principle 9 of the Privacy Act of 1988.

¹⁴) Sec. 33 of the Privacy Ordinance of Hong Kong.

III. Evaluation of self-regulatory instruments

All these considerations reveal that, as long as there is no adequate level of data protection in the third country, it is the task of the data controller to ensure that the company which receives data from him provides an adequate level of data protection. Therefore, multinational companies have to face the question if there is a global solution for a global company to comply with the different legal requirements that exist in the field of data flow to third countries. In fact, there are several options to cope with the diverse legal environment. All of these options are part of the „self-regulatory approach". However, some of the instruments of self-regulation are more advantageous than others. This reveals the question, which of the self-regulatory options would be the most suitable solution for a company which is acting globally.

One option consists in obtaining the consent by the data subject for the transfer of his personal data to countries that do not provide an adequate level of data protection, according to Article 26 (1) (a) of the EU Directive. This possibility, however, would require high efforts of administration and could not cover data about all customers due to the voluntary character of the consent. Hence, it is not a very effective safeguard as the consent could be withheld or revoked.

A second option for multinational companies to cope with the legal requirements would be to incorporate appropriate contractual clauses. However, any contractual clause that is to be used for the creation of an adequate level of data protection must be approved by the respective authority according to Article 26 (2), what causes high administrative effort.

The administrative time and effort would also be high when using the EU model clauses,¹⁵ especially when they are part of complex systems of contracts, although in principle this would not require authorization. According to the provisions in Art. 26 Sec. 4, the Member States have to take appropriate measures to comply with this decision.

Another option is that companies commit to the Safe Harbor Principles,¹⁶ which provide an adequate protection level according to the Commission's decision referring to Article 25 (6). That way the respect for the existing legal requirements can be ensured in a fairly straightforward manner. However, the Safe Harbor Principles are only created to provide adequate safeguards for the transfer of personal data from the EU to the USA. They are standards of conduct which are guaranteed only on a bilateral level. Hence, the scope of this option is very limited and it does not provide a comprehensive solution to the global dimension of the problem.

Finally, multinational companies have the possibility to implement binding corporate rules (BCRs) in accordance with Article 26 (2). These internal company regulations set corporate standards of conduct in the field of data protection and data security. The main advantage of this option is that BCRs contain generally recognized data protection principles. Therefore, they provide a comprehensive answer to the challenges arising from globalization. In this respect BCRs are also suitable to satisfy the require-

ments of Electronic Commerce today and in the future. Furthermore, they can create competitive advantages for the company because data protection and data security are characteristics of „Premium Services". At the same time such rules enable the establishment of homogeneous corporate standards despite the heterogeneity of worldwide data protection regulations. And last but not least, BCRs foster the building of intercultural bridges since they manage to respect the diversity of national privacy regulations.

An evaluation of all the different means of self-regulation shows that one mean of a self-regulatory approach provides specific advantages which place this option at the top of all the other instruments. Therefore, BCRs are the most suitable means of self-regulation to facilitate a company-wide transfer of personal data in compliance with legal data protection requirements.

IV. Development and enforcement of Binding Corporate Rules

When developing such rules for a company or group, the applicable national law of all involved countries has to be taken into consideration as well as the provisions and requirements of the two EU Directives on Data Protection.¹⁷ Article 29 Working Party has set forth the above-mentioned working paper no. 12 which explains the necessary content of self-regulatory rules aiming to provide an adequate data protection level. Working paper no. 74¹⁸ provides detailed requirements on the binding nature and necessary substantial contents of BCRs. The EU model clauses may serve as an additional hint to know which content is required by the EU Commission to provide an adequate level of protection.

To set corporate rules in force internally, legal enforcement measures have to be taken depending on the applicable company and labour law. National law may also influence the content of BCRs either restricting or requiring certain provisions in such internal legal frameworks. Due to cultural and legal differences between several companies of a global group, the discussion of the content of the regulations in a BCR can take a major part of the time and effort in the procedure of their development. To overcome such cultural differences, BCRs also need a comprehensive data protection strategy and policy to become effective and to be enforced throughout a multinational company. A corporate data protection infrastructure and organizational environment is needed for internal law enforcement. Therefore, it is highly recommended to establish a Chief Privacy Officer whose task it is, among others, to ensure group-wide law enforcement.

The external binding force of the regulatory framework of a company or group finally arises from the respective national law and might require additional measures, such as the publication of the rules. Law enforcement is also monitored externally by the competent data protection supervisory authority.

V. Recommendations for the content of Binding Corporate Rules

Depending on the aim and scope of BCR, the content of its regulations can be differing. Most companies differentiate rules for the processing of human resource data and such for

¹⁵) Available at the EU Commission's website at; http://www.europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

¹⁶) Available from the US Department of Commerce at; <http://www.export.gov/safeharbor>.

¹⁷) Directives 95/46/EC and 2002/58/EC.

¹⁸) Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74 of 3 June 2003.

customer and supplier data and do not regulate both types of data in one framework. Due to the different nature of the respective personal data, a BCR for Human Resource data needs additional considerations which are not needed in BCR for Customers/Suppliers. Nevertheless, both regulations in principle can be developed with similar content.

First of all, each corporate regulatory framework has to define its aim and scope. To avoid conflicts of laws, it is essential that the internal rule clarifies its relation to national or local law and contains a subordination regulation. It should be confirmed that the processing of personal data is subject to the national or local law of the state where the data has originally been collected and processed. An exception can be made in the case of data transfers within the EU or to countries which provide an adequate level of data protection pursuant to Art. 25 of the EU Directive.

The regulations have to state essential principles for the processing of personal data as well as principles of data security that are to be observed within the companies to which the BCR shall apply. They should take into consideration mainly the principles of Articles 6 and 7 of the Data Protection Directive, containing especially fair and lawful processing, keeping data accurate and up to date, as well as the restriction to a certain purpose of processing. Additionally, it should be clearly determined on which basis processing or collection of data can be legitimated under the BCR.

Moreover, the rules should regulate the treatment of sensitive data and draw up the elementary criteria for data transfers to be legitimized. It should be clearly defined which data is specially protected. This definition should take into consideration Article 8 of the Data Protection Directive, but also the special requirements within the companies where the rules shall be applicable. The processing of such data has to be restricted according to the requirements of the Data Protection Directive.

For cases of complaints by the data subject the rules have to outline the rights which may be exercised by the data subject and the possibilities for the data subject to enforce his or her rights. The data subject has to be granted the right to obtain information about the data stored about him or her, have access to his or her data, and demand rectification or deletion of data which is incorrect or kept without legal legitimacy. The data subject must also have the right to object to illegitimate processing in general.

Confidentiality of processing is also an issue in this context. It should be determined in the BCR that only authorized persons should be given access to personal data of customers, prospects, partners or employees. This "need-to-know" principle is also applicable among colleagues of the same department if they deal with different sections of a database. All employees who handle personal data in their daily work should be obliged to maintain confidentiality by signing a pursuant declaration at the moment of employment.

Furthermore, special regulations for particular situations of data processing have to be included in the BCR, taking into consideration the situations which occur in the respective group or company. Such special rules can concern either data processing on behalf, or involvement of third parties, as well as special treatment of marketing data, or customer contact via telecommunication. A BCR for Human Resources can contain additional regulations about how telecommunication, Internet and Intranet may be used by the employees.

Finally, each BCR needs to regulate the consequences of breaches of its regulations. Sanctions and remedies for such behavior have to comply in particular with the provisions of national labour law, and claims often underlie compulsory national requirements. In many countries, the company might not be allowed to widen its instruments against employees or define its own provisions for remedies towards the data subjects. Hence, a BCR which shall be applicable in many companies in different countries will have to abstain from regulations which go beyond a reference to national provisions in this context.

It is recommended to add one more section to each BCR, which establishes a Chief Privacy Officer in the company or group. He should be entitled to supervise the implementation of the BCR and serve as an independent internal institution which all persons concerned with data processing can apply to for consultation, as well as data subjects can address their complaints and questions. The BCR should define his responsibilities and his position within the company.

VI. Procedure for an approval of Binding Corporate Rules in Europe

With regard to the procedure of getting data transmissions approved on a community-wide level, it was claimed that the approval was to be applied for at each Member State's Data Protection Authority. Whether the BCR provides adequate safeguards or not would have been answered by each authority separately. This procedure, however, was considered to be far from being a practical solution for multinational companies. Hence, the Article 29 Working Party developed a coordination procedure in its working paper no. 107 to simplify the approval by more than one national data protection authority.¹⁹ Subsequently, working paper no. 108 defines the requirements for the multinational approval of BCRs in a model checklist.²⁰

The procedure proposed by the Article 29 Working Party allows the applicant corporate group to choose one of the concerned authorities as the lead authority for the procedure, to which it communicates all required documents, especially all explanations and background information as required in WP 108. The choice of the applicant group for the lead authority can be decided to be changed by the involved authorities if they have the opinion that the chosen authority is not the most appropriate to have the leadership in this procedure. The lead authority then, according to WP 107, should start the discussion with the applicant about the content of the drafted BCR and afterwards present a consolidated draft to the other authorities for comments. They shall be implemented in a final version which can be adopted by all involved authorities.

VII. Conclusion

The first coordinated EU-wide approval procedures have been started in 2004 and were aimed to be finished in 2005.²¹ This goal, unfortunately, was failed to achieve. The procedures are still pending. The applicants had to provide a background paper

¹⁹⁾ Working Document Setting Forth a Cooperation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", WP 107 of 14.4.2005.

²⁰⁾ Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, WP 108 of 14.4.2005.

²¹⁾ National approvals have already been granted by national data protection authorities in several cases.

containing all information required by WP 108 to the involved data protection authorities serving as a basis for the discussions between all authorities involved. They, finally, shall result in a common view on the adequacy of the provisions of the BCR in question and enable all participants to proceed quickly to the aimed formal approval of the respective data transfers.

One aspect is of special significance for the issue of self-regulation: Any self-regulation through BCRs will only be accepted by customers, employees, and the public if it is accompanied by a serious self-engagement of the company regarding the obligations arising from BCRs. The question how self-engagement can be realized in accordance with statutory provisions has to be answered on the basis of the worldwide existing national laws. It is a challenge for multinational companies to invent such solutions and it forces the international data protection discussion to develop procedures and possibilities which enable companies to effectively set in force their self-regulatory solutions.

Wiążące reguły korporacyjne

- I. Wprowadzenie
- II. Podstawy prawne międzynarodowych transferów danych
- III. Ocena instrumentów służących do samoregulacji
- IV. Tworzenie i wprowadzanie w życie wiążących reguł korporacyjnych
- V. Zalecenia dotyczące treści wiążących regulaminów korporacyjnych
- VI. Europejska procedura zatwierdzania wiążących reguł korporacyjnych
- VII. Wnioski

I. Wprowadzenie

Starożytny filozof Seneka powiedział kiedyś: „*Ten, kto zwycięstwa sam nad sobą odnosi, jest człowiekiem potężnym*”. Powyższy cytat podsumowuje w kilku słowach znaczenie samostanowienia w kształtowaniu osobowości człowieka. Pokazuje także, że już w starożytności samostanowienie było wartością, do której dążono. Nie ulega wątpliwości, że możliwość decydowania o swoich działaniach daje większe poczucie satysfakcji i więcej spełnienia niż heteronomia, czyli podporządkowanie się obcej dominacji, innymi słowy pozwalanie, aby kierowały nami czynniki zewnętrzne. Można wręcz stwierdzić, że na poziomie jednostki zdolność do wyznaczania sobie pewnych standardów oraz życie zgodnie z nimi stanowi jedną z najwyższych form rozwoju człowieka.

Ten trend filozofii behawioralnej zyskuje w obecnych czasach na znaczeniu, ponieważ jest ściśle powiązany z ochroną praw osobistych. Pojęcie samostanowienia może być niewątpliwie postrzegane jako fundamentalna podstawa wszystkich praw osobistych. We współczesnym świecie, naznaczonym przez międzynarodowe transfery pieniężne i transnarodową wymianę dóbr i usług, coraz większej wagi nabiera poszanowanie dla praw osobistych, a co za tym idzie idei samostanowienia. Zglobalizowane w wymiarze handlowym i gospodarczym społeczeństwo pokazuje swoją „ludzką twarz” w trwałym poszanowaniu dla praw osobistych, ochrony danych osobowych i bezpieczeństwa danych.

Obecnie najważniejszą sprawą dla przedsiębiorstw międzynarodowych jest tworzenie i wprowadzanie koncepcji bezpieczeństwa danych i ochrony danych osobowych w wytwarzane produkty i usługi. Potrzeba ta jest związana z istnieniem ogólnosięwiatowych powiązań gospodarczych oraz konwergencją techniczną, które umożliwiają skuteczniejsze dopasowywanie i przetwarzanie danych osobowych, przez co wzrasta potencjalne ryzyko wykorzystania danych osobowych w nielegalny sposób. Jednocześnie świadomość konsumentów w kwestii przetwarzania ich danych osobowych jest znacznie wyższa niż była zaledwie kilka lat temu. Da się to w szczególności zauważyć przy korzystaniu przez klientów z e-handlu. W handlu elektronicznym skuteczność wcielenia w życie koncepcji bezpieczeństwa danych i ochrony danych osobowych stanowi dodatkowo czynnik konkurencyjności, a przecież gospodarcza wartość informacji ciągle rośnie. Im lepsza ochrona danych klientów, tym wyższe prawdopodobieństwo, że świadomy zagrożenia klient pozostanie lojalny wobec firmy. Potrzeba tu nie tylko ochrony zapobiegającej nadużyciom w wykorzystywaniu danych klienta, ale także ochrony samej firmy przed stratami gospodarczymi wynikającymi z braku lub utraty czynnika produkcji, który tworzą informacje wysokiej jakości.

Równie wysokiego poziomu ochrony wymagają klienci, kontrahenci i pracownicy, jeżeli ich dane, z prawnie uzasadnionych przyczyn, są przesyłane do krajów trzecich. Poszanowanie dla praw człowieka wymaga, aby podmiot przysyłający dane do spółek mających siedzibę za granicą gwarantował ich stałe bezpieczeństwo.

II. Podstawy prawne międzynarodowych transferów danych

Przekazywanie danych osobowych za granicę odbywa się jednak w zupełnie innym środowisku prawnym. Granice państw nie są w stanie zatrzymać przepływu danych; na tychże samych granicach kończy się jednak skuteczność krajowego prawodawstwa. Z braku legislatora o globalnych kompetencjach, który mógłby stawić czoła temu wyzwaniu, na świecie stosuje się wiele różnych koncepcji prawnych, które mają za cel zagwarantowanie skutecznej ochrony danych osobowych. Pomimo, że czynione są starania o zharmonizowanie ogólnosięwiatowych standardów ochrony danych osobowych, obecną sytuację cechuje niejednorodność koncepcji oraz trudne rozgraniczenia prawne. Kraje różnią się między sobą nie tylko filozofią rozwiązań prawnych, ale i stopniem świadomości problemów związanych z ochroną danych osobowych. Niektóre z nich stosują podejście pełnego prawnego uregulowania tych kwestii, co oznacza, że obowiązują w nich ogólne uregulowania ustawowe o ochronie danych osobowych, przewidujące określone wymogi dotyczące gromadzenia, przetwarzania i wykorzystywania danych osobowych przez podmioty publiczne i prywatne. Koncepcje te obowiązują na przykład w Australii, Nowej Zelandii, Chile i Unii Europejskiej. Inne państwa wybierają system uregulowań sektorowych, co oznacza, że obowiązujące w nich przepisy regulują kwestie ochrony danych osobowych w odniesieniu do ich poszczególnych zastosowań, jak na przykład w sektorze finansowym czy telekomunikacyjnym. Przykładem takiego podejścia jest USA, gdzie nie istnieją żadne abstrakcyjne i ogólne uregulowania ustawowe ochrony danych osobowych dotyczące przedsiębiorców jako takich. Istnieją jednak ustawy odnoszące się do poszczególnych sektorów gospodarki, jak np. HIPAA (ustawa o przenoszeniu ubezpieczeń zdrowotnych i odpowiedzialności za nie), ustawa o modernizacji sektora finansowego, ustawa o telekomunikacji lub ustawa o naruszeniach tajemnicy informacyjnej w Kalifornii, które zawierają wymogi dotyczące ochrony danych osobowych w konkretnym sektorze, w którym są stosowane.

Aby uprościć prowadzenie działalności wielonarodowym przedsiębiorstwom i zagwarantować jednolitą ochronę praw człowieka dla wszystkich osób, których dane są gromadzone lub przetwarzane w jednym z krajów członkowskich, Unia Europejska zharmonizowała wymogi dotyczące ochrony danych osobowych na swoim terytorium. Pozostają jednak trudności i otwarte kwestie wynikające z różnych wymogów prawnych dotyczących transferów danych do krajów poza granicami UE i EWG. Dyrektywa UE o ochronie danych osobowych,¹ która została przetransponowana do porządków prawnych krajów członkowskich UE, zawiera szczegółowe regulacje dotyczące przekazywania danych do krajów trzecich, znajdują się one w artykułach 25 i 26. Grupa Robocza Art. 29 opublikowała w 1998 roku dokument roboczy nr 12,² który objaśnia stosowanie tych artykułów, a w szczególności wskazuje, w jaki sposób należy definiować „odpowiedniość” i jak można ją osiągnąć za pomocą samoregulujących instrumentów.

Zgodnie z artykułem 25(1) Dyrektywy UE dane osobowe wygenerowane w UE mogą być przekazywane tylko do takich krajów trzecich, które zapewniają odpowiedni poziom ochrony. Kryteria, które należy brać pod uwagę, aby określić „odpowiedniość”, przywołaną w artykule 25(2) są wyjaśnione w dokumencie roboczym nr 12 Grupy Roboczej Art. 29. W artykule 25(6) stwierdza się, że Komisja Europejska może uznać, że dany kraj zapewnia odpowiedni poziom ochrony stosując procedurę opisaną w artykule 31(2). Jak dotąd, Komisja Europejska uznała za odpowiednie tylko standardy ochrony danych osobowych w Szwajcarii,³ Kanadzie,⁴ Argentynie,⁵ na Guernsey,⁶ i na Wyspie Man⁷ oraz zasady ochrony prywatności „Bezpieczna przystań”⁸ amerykańskiego Departamentu Handlu, jak również transfer rejestru nazwisk pasażerów linii lotniczych do amerykańskiego Biura Celnego i Ochrony Granic.⁹ Jeśli chodzi o tę ostatnią decyzję, w Trybunale Sprawiedliwości Wspólnot Europejskich toczy się obecnie sprawa z pozwu Parlamentu Europejskiego i Europejskiego Inspektora ds. Ochrony Danych Osobowych przeciwko Komisji Europejskiej.¹⁰

Kraje członkowskie muszą się stosować także do negatywnych decyzji Komisji w sprawie odpowiedniego stopnia ochrony danych osobowych w uregulowaniach prawnych kraju trzeciego, na podstawie procedury z artykułu 31(2). Artykuł 25(4) Dyrektywy UE

wymaga, by kraje członkowskie podjęły wszystkie konieczne środki, aby nie dopuścić do przekazania jakichkolwiek danych tego rodzaju do rzeczonego kraju trzeciego. Przekazywanie danych wygenerowanych w UE do krajów, które nie zapewniają odpowiedniego poziomu ochrony danych osobowych, dopuszcza się jedynie w drodze jednorazowego odstępstwa od reguł, zgodnie z artykułem 26(1) Dyrektywy UE (kiedy, na przykład, osoba, której dane dotyczą wyraziła jednoznaczną zgodę na ich przekazanie) lub gdy istnieją inne odpowiednie zabezpieczenia ochrony prywatności, na które powołał się administrator danych, a Państwo Członkowskie wyda zgodę na podstawie artykułu 26(2). Grupa Robocza Art. 29 wydała dokument roboczy nr 114 w celu sprecyzowania wymagań zawartych w artykule 26(1) Dyrektywy. Artykuł ten zawiera wytyczne interpretacyjne dotyczące zastosowania poszczególnych derogacji określonych w artykule 26(1).¹¹ Grupa Robocza wymaga ograniczonego stosowania derogacji, aby zagwarantować przestrzeganie podstawowych praw osób, których dotyczą dane. Inne „odpowiednie zabezpieczenia” mogą mieć formę odpowiednich klauzul umownych lub wiążących regulaminów korporacyjnych, takich jak, np. kodeksy postępowania. Jeszcze inna możliwość to zastosowanie standardowych klauzul umownych, zatwierdzonych przez Komisję zgodnie z punktem 4 artykułu 26, które także muszą zostać uznane przez Państwa Członkowskie za odpowiednie zabezpieczenia.

Opisane zasady prawne są zasadniczo takie same w kilku innych państwach, jak np. w Argentynie,¹² Australii¹³ i Hongkongu,¹⁴ ponieważ wszędzie tam obowiązują podobne przepisy dotyczące „odpowiedniości”.

III. Ocena instrumentów służących do samoregulacji

Powyższe rozważania sprowadzają się do zasady, że dopóki w kraju trzecim brakuje odpowiedniego poziomu ochrony danych osobowych, to na administratorze danych spoczywa zadanie zagwarantowania, aby firma otrzymująca od niego dane zapewniła taki odpowiedni poziom ochrony. W związku z tym obowiązkiem przedsiębiorstwa wielonarodowe muszą zmierzyć się z pytaniem, czy istnieje globalne rozwiązanie dla globalnej firmy, dzięki któremu mogłaby ona spełniać zróżnicowane wymogi prawne, jakie obowiązują w kwestii przepływu danych do krajów trzecich. Tak naprawdę istnieje kilka sposobów, aby poradzić sobie z różnorodnością środowiska prawnego. Wszystkie te rozwiązania są częścią „podejścia opartego na samoregulacji”. Niektóre jednak z instrumentów samoregulacyjnych oferują więcej korzyści niż inne. Prowadzi nas to do pytania, które z opcji samoregulacji będą najbardziej odpowiednim rozwiązaniem dla firmy działającej w skali globalnej.

Pierwsza opcja polega na uzyskaniu zgody osoby, której dotyczą dane, na przekazanie jego/jej danych osobowych do krajów, które nie gwarantują odpowiedniego poziomu ochrony danych, zgodnie z artykułem 26(1)(a) Dyrektywy UE. Ta możliwość wymagałaby jednak intensywnych wysiłków administracyjnych, a przekazywane dane nie obejmowałyby wszystkich klientów, ze względu na dobrowolność udzielania zgody. Nie jest to zatem bardzo skuteczne zabezpieczenie, ponieważ zgody można odmówić i można ją cofnąć.

¹) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Europejskiej z 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, O.J. L 281/31, 23.11.1995; pełen tekst w 16 językach jest dostępny na stronie Komisji Europejskiej poświęconej ochronie danych osobowych pod adresem: http://www.europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm

²) Dokument roboczy: Transfery danych osobowych do krajów trzecich: stosowanie artykułów 25 i 26 Dyrektywy UE o ochronie danych osobowych, dokument roboczy nr 12 z 24 lipca 1994, odnośnie kilku innych dokumentów roboczych dotyczących artykułów 25 i 26, zobacz przypisy 10, 17, 18 i 19.

³) Decyzja Komisji 2000/518/WE z dn. 26.7.2000, Dz.U. Nr L 215/1 z dn. 25.8.2000.

⁴) Decyzja Komisji 2002/2/WE z dn. 20.12.2001 w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych, Dz.U. Nr L 2/13 z dn. 4.1.2002.

⁵) Decyzja Komisji C(2003) 1731 z dn. 30/06/2003 na podstawie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Argentynie, Dz.U. Nr L 168 z dn. 5.7.2003.

⁶) Decyzja Komisji z dn. 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych na Guernsey, Dz.U. Nr L 308, 25.11.2003.

⁷) Decyzja Komisji 2004/411/WE z dn. 28.4.2004 w sprawie właściwej ochrony danych osobowych na Wyspie Man 2004/411/WE, Dz.U. Nr L 151/48 z dn. 30.4.2004.

⁸) Decyzja Komisji 2000/520/WE z dn. 26.7.2000, Dz.U. Nr L 215/7 z dn. 25.8.2000.

⁹) Decyzja Komisji z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych pasażerów lotniczych zawartych w Passenger Name Record (PNR), przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych (ogłoszona pod numerem dokumentu C(2004) 1914), 2004/535/WE, Dz.U. Nr L 235/11 z dn. 06.07.2004.

¹⁰) Sprawy C-317/04 i C-318/04; dokumenty są dostępne w rejestrze spraw na oficjalnej stronie internetowej Trybunału; <http://www.curia.eu.int/de/content/juris/index.htm>.

¹¹) Dokument roboczy nr 114, dostępny na oficjalnej stronie internetowej Grupy Roboczej Art. 29; http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

¹²) Artykuł 12 argentyńskiej ustawy o ochronie danych.

¹³) Zasada ochrony danych nr 9 w ramach ustawy o prywatności z 1988 r.

¹⁴) Artykuł 33 hongkońskiego rozporządzenia w sprawie prywatności.

Druga opcja dla przedsiębiorstw wielonarodowych, by mogły poradzić sobie z wymogami prawnymi, to zawarcie w umowach odpowiednich klauzul. Jednak każda klauzula, której używa się w celu uzyskania odpowiedniego poziomu ochrony danych osobowych, musi zostać zatwierdzona przez stosowną instytucję zgodnie z artykułem 26(2), co wymaga skomplikowanych starań administracyjnych.

Równie dużo wysiłku i czasu zajmą działania administracyjne, w przypadku posłużenia się modelowymi klauzulami¹⁵ proponowanymi przez UE, szczególnie jeśli stanowiłyby one część złożonego systemu umów, chociaż co do reguły zastosowanie klauzul modelowych nie wymagałoby autoryzacji. Zgodnie z postanowieniami sekcji 4 artykułu 26 Państwa Członkowskie muszą podjąć odpowiednie środki, aby zastosować się do tej decyzji Komisji.

Inna możliwość to przyjęcie przez przedsiębiorstwo zasad „Bezpiecznej przystani”,¹⁶ które zapewniają odpowiedni poziom ochrony zgodnie z decyzją Komisji odnoszącą się do artykułu 25(6). W ten stosunkowo prosty sposób można zagwarantować poszanowanie obowiązujących wymogów prawnych. Zasady „Bezpiecznej przystani” są jednak tworzone dla celów zapewnienia odpowiednich zabezpieczeń wyłącznie przy przekazywaniu danych osobowych z UE do USA. Są to standardy postępowania gwarantowane tylko na poziomie bilateralnym. Dlatego zasięg potencjalnego zastosowania tego rozwiązania jest bardzo ograniczony i nie oferuje całościowego rozwiązania problemu w wymiarze globalnym.

Przedsiębiorstwa wielonarodowe mają wreszcie możliwość wprowadzania wiążących reguł korporacyjnych (WRK) zgodnie z artykułem 26(2). Takie wewnętrzne regulacje firmowe wyznaczają korporacyjne standardy postępowania na polu ochrony danych osobowych i bezpieczeństwa danych. Główną zaletą tej możliwości jest fakt, że WRK zawierają ogólnie uznawane zasady dotyczące ochrony danych osobowych, dlatego też odpowiadają w sposób całościowy na wyzwania powstałe w wyniku globalizacji. WRK wystarczają także, aby spełnić aktualne i przyszłe wymagania elektronicznego handlu. Co więcej, mogą dać firmie przewagę konkurencyjną, ponieważ ochrona i bezpieczeństwo danych są znakami charakterystycznymi „usług o najwyższej jakości”. Tego typu regulaminy pozwalają jednocześnie na wprowadzenie jednolitych standardów korporacyjnych pomimo panującej na świecie różnorodności regulacji prawnych dotyczących ochrony danych osobowych. WRK pomagają wreszcie budować mosty międzykulturowe, ponieważ dzięki nim możliwe jest respektowanie różnorodności krajowych przepisów dotyczących prywatności.

Przegląd całej palety środków samoregulacji pokazuje, że jedna z koncepcji wiąże się z korzyściami, które decydują o jej zdecydowanej przewadze w porównaniu do wszystkich innych instrumentów. WRK stanowią zatem najodpowiedniejszy środek samoregulacji, aby uprościć przekazywanie danych osobowych w ramach korporacji w sposób zgodny z wymogami prawnymi dotyczącymi ochrony danych.

IV. Tworzenie i wprowadzanie w życie wiążących reguł korporacyjnych

Podczas opracowywania takiego regulaminu dla spółki czy grupy kapitałowej należy wziąć pod uwagę zarówno stosujące się prawo krajowe wszystkich państw, w których działają spółki, jak również przepisy i wymogi zawarte w dwóch dyrektywach UE poświęconych ochronie danych.¹⁷ Grupa Robocza Art. 29 przedstawiła wspomniany już wcześniej dokument roboczy nr 12, w którym wyjaśnia, jakie konieczne treści muszą zawierać reguły samoregulacyjne mające zapewnić dostateczny stopień ochrony danych. Dokument roboczy nr 74¹⁸ podaje szczegółowe wymogi w sprawie wiążącego charakteru WRK i podstawowych treści, jakie muszą koniecznie uwzględniać. Modelowe klauzule UE mogą posłużyć jako dodatkowe wskazówki co do tego, jakich treści wymaga Komisja Europejska, aby można było mówić o odpowiednim stopniu ochrony.

Aby regulaminy korporacyjne zaczęły obowiązywać wewnętrznie, należy podjąć odpowiednie kroki prawne wprowadzające je w życie – jakie, to zależy od danego przedsiębiorstwa i od przepisów prawa pracy. Również prawo krajowe może wpływać na treść WRK: wewnętrzny krajowy system prawny może ograniczać możliwości włączenia do WRK pewnych postanowień, a może też nakazywać włączenie innych. Z powodu różnic kulturowych i prawnych istniejących pomiędzy spółkami należącymi do globalnej grupy kapitałowej, dyskusje nad treścią uregulowań WRK mogą pochłoniąć większą część czasu i wysiłku przeznaczonego na ich opracowanie. Aby móc przewyższyć te różnice kulturowe, oprócz WRK musi zostać uchwalona, a następnie wprowadzona w życie w całej korporacji międzynarodowej, kompleksowa strategia i polityka ochrony danych. Do wprowadzania w życie wewnętrznych regulacji potrzebna jest w przedsiębiorstwie infrastruktura ochrony danych i środowisko organizacyjne. Z tego powodu zaleca się utworzenie stanowiska dyrektora ds. ochrony danych osobowych, którego zadaniem jest między innymi, dopilnowanie, aby przepisy zostały wprowadzone w życie w całej grupie kapitałowej.

Nadanie wewnętrznym regulaminom spółek czy grupy kapitałowej zewnętrznej mocy obowiązującej wynika wreszcie z właściwego prawa krajowego i może wymagać dodatkowych działań, jak np. ich publikacji. Wprowadzanie przepisów w życie jest również monitorowane zewnętrznie przez właściwy organ nadzorczy do spraw ochrony danych osobowych.

V. Zalecenia dotyczące treści wiążących regulaminów korporacyjnych

W zależności od zadań i zakresu WRK, zalecenia mogą się różnić pomiędzy sobą treścią postanowień. Większość spółek różnicuje zasady przetwarzania danych kadr i danych klientów czy dostawców i nie reguluje tych dwóch typów danych w jednym dokumencie. Z uwagi na inny charakter tych danych osobowych, WRK dotyczące danych kadr muszą uwzględniać dodatkowe kwestie, które z kolei są zbędne w przypadku WRK dotyczących klientów/dostawców. Pomimo to, obu regulaminom można nadać zasadniczo podobną treść.

¹⁷⁾ Dyrektywy 95/46/WE i 2002/58/WE.

¹⁸⁾ Dokument roboczy: Przekazywanie danych osobowych do krajów trzecich: zastosowanie artykułu 26(2) Dyrektywy UE o ochronie danych w odniesieniu do wiążących reguł korporacyjnych dotyczących międzynarodowych transferów danych (*Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*), WP 74 z dn. 3 czerwca 2003.

¹⁵⁾ Dostępne na stronie internetowej Komisji Europejskiej; http://www.europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm.

¹⁶⁾ Dostępne w Departamencie Handlu USA pod adresem internetowym; <http://www.export.gov/safeharbor>.

Po pierwsze, każdy regulamin korporacyjny musi definiować swoje cele i zakres obowiązywania. Aby uniknąć konfliktów pomiędzy systemami prawa, wewnętrzny regulamin musi bezwzględnie określać, w jakim stosunku pozostaje wobec prawa krajowego czy regionalnego i zawierać przepis dotyczący podporządkowania prawu: należy potwierdzić, że przetwarzanie danych osobowych podlega prawu krajowemu lub regionalnemu państwa/stanu, w którym dane były pierwotnie gromadzone i przetwarzane. Można przewidzieć wyjątek dotyczący przekazywania danych w ramach UE lub do krajów, które zapewniają odpowiedni stopień ochrony danych osobowych zgodnie z art. 25 Dyrektywy UE.

Postanowienia regulaminu muszą wskazywać podstawowe zasady przetwarzania danych osobowych oraz zasady bezpieczeństwa danych, które mają być przestrzegane w spółkach, do których stosuje się WRK. Powinny uwzględniać przede wszystkim zasady wskazane w artykułach 6 i 7 Dyrektywy w sprawie ochrony danych, w tym zwłaszcza rzetelne i legalne przetwarzanie, dbanie o to, aby przechowywane dane były prawidłowe i aktualne, oraz ograniczenie dotyczące określonego celu przetwarzania danych. Oprócz tego należy jasno sprecyzować, na jakiej podstawie przetwarzanie lub gromadzenie danych może zostać uznane za uzasadnione zgodnie z WRK.

Regulamin powinien ponadto określać sposób postępowania z danymi wrażliwymi i wskazywać, jakie elementarne kryteria muszą być spełnione, aby mogło dojść do legalnego przekazywania danych zgodnie z WRK. Należy jasno zdefiniować, które dane podlegają szczególnej ochronie, uwzględniając w tej definicji artykuł 8 Dyrektywy w sprawie ochrony danych, ale również specyficzne wymogi przedsiębiorstw, w których regulamin ten będzie obowiązywał. Przetwarzanie danych tego typu powinno mieć ograniczony zakres zgodnie z wymogami Dyrektywy w sprawie ochrony danych.

W odniesieniu do skarg osób, których dane są przetwarzane, reguły muszą wskazywać, jakie prawa przysługują tym osobom i w jaki sposób mogą one je egzekwować. Osoba taka musi mieć zagwarantowane prawo do otrzymania informacji o dotyczących jej danych, które są gromadzone, prawo dostępu do swoich danych, prawo żądania poprawienia lub usunięcia danych, które są nieprawidłowe lub są przechowywane w sposób niezgodny z prawem. Osoba, której dotyczą dane, musi mieć również prawo sprzeciwu wobec bezprawnego przetwarzania danych jako takiego.

Poufność w procesie przetwarzania danych stanowi w tym kontekście równie ważną kwestię. WRK powinny zawierać postanowienie, że dostęp do danych osobowych klientów, potencjalnych klientów, partnerów czy pracowników mogą otrzymać tylko upoważnione osoby. Ta zasada „uzasadnionej potrzeby” przy dostępie dotyczy również pracowników tego samego działu, jeżeli zajmują się różnymi fragmentami bazy danych. Wszyscy pracownicy mający styczność z danymi osobowymi w swojej codziennej pracy powinni zostać zobowiązani do zachowywania poufności, podpisując w momencie podjęcia zatrudnienia odpowiednie oświadczenia.

Ponadto WRK muszą zawierać uregulowania dotyczące określonych przypadków przetwarzania danych, z uwzględnieniem okoliczności występujących w danej grupie kapitałowej czy spółce. Takie szczegółowe reguły mogą dotyczyć przetwarzania danych w imieniu osób trzecich lub z ich udziałem czy też szczególnego trybu postępowania z danymi marketingowymi czy kontaktów z klientem za pomocą środków telekomunikacji. WRK dla działu kadr

mogą przewidywać dodatkowe postanowienia mówiące o tym, w jaki sposób pracownikom wolno korzystać ze środków telekomunikacji, Internetu i Intranetu.

Na koniec, w żadnych WRK nie może zabraknąć postanowień dotyczących konsekwencji ich naruszenia. Sankcje i środki naprawcze muszą być zgodne z przepisami krajowego prawa pracy, a roszczenia często podlegają bezwzględnie obowiązującym wymogom prawodawstwa krajowego. W wielu krajach spółka może nie mieć prawa rozstrząsać swoich instrumentów skierowanych przeciwko pracownikom czy ustalać własnych zasad w sprawie środków naprawczych wobec osób, których dane są przetwarzane. W związku z tym w WRK, które mają obowiązywać w wielu spółkach mieszczących się w różnych krajach, konieczna będzie rezygnacja z postanowień wykraczających poza odniesienie do stosujących się przepisów krajowych.

Zalecane jest włączenie do wszystkich WRK jeszcze jednego rozdziału, na podstawie którego w każdej spółce czy grupie kapitałowej zostanie ustanowiony dyrektor ds. ochrony danych osobowych. Jego kompetencje powinny obejmować nadzorowanie wdrażania WRK. Dyrektor ds. ochrony danych osobowych powinien działać jako niezależna instytucja wewnątrz firmy, do której mogą się zgłaszać wszystkie osoby po konsultacje w sprawach dotyczących ochrony danych, a osoby, których dane są przetwarzane, mogą zgłaszać swoje zażalenia i pytania. WRK powinny określać jego zakres obowiązków i stanowisko w firmie.

VI. Europejska procedura zatwierdzania wiążących reguł korporacyjnych

W kwestii procedury wyrażania zgody na przesyłanie danych na szczeblu wspólnotowym twierdzono, że wnioski o zgodę powinny być składane do urzędu ochrony danych odpowiedniego Państwa Członkowskiego. Kwestia, czy WRK stanowi odpowiednie zabezpieczenie, byłaby rozstrzygana przez każdy urząd z osobna. Procedura ta została jednak uznana za mało wykonalną w przypadku spółek międzynarodowych. Grupa Robocza Art. 29 opracowała w związku z tym w swoim dokumencie roboczym nr 107 procedurę koordynacyjną mającą uprościć zatwierdzenia przez więcej niż jeden krajowy organ ochrony danych.¹⁹ Kolejny dokument roboczy nr 108 określa wymogi związane z zatwierdzaniem WRK w wielu krajach w formie wzorcowej listy kontrolnej.²⁰

Procedura proponowana przez Grupę Roboczą Art. 29 pozwala wnioskodawcy będącemu grupą kapitałową wybrać jeden z kompetentnych organów jako organ koordynujący procedurę: organowi temu są następnie przekazywane wszystkie wymagane dokumenty, w szczególności wszystkie wyjaśnienia i dodatkowe informacje zgodnie z WP 108. Organy uczestniczące w procedurze mogą zmienić wybór organu koordynacyjnego przez wnioskodawcę, jeżeli będą zdania, że inny organ będzie bardziej odpowiedni do sprawowania tej funkcji. Organ koordynacyjny powinien, zgodnie z WP 107, rozpocząć dyskusje z wnioskodawcą o treści projektu WRK, a następnie przedstawić skonsolidowaną wersję do zaopiniowania pozostałym instytucjom. Ich uwagi

¹⁹⁾ Dokument roboczy ustalający procedurę współpracy w sprawie wydawania wspólnych opinii dotyczących odpowiednich zabezpieczeń wynikających z „wiązących reguł korporacyjnych”, WP 107 z dnia 14 kwietnia 2005 r.

²⁰⁾ Dokument roboczy ustalający wzorcowy wniosek o zatwierdzenie wiążących reguł korporacyjnych, WP 108 z dnia 14 kwietnia 2005 r.

powinny zostać uwzględnione w ostatecznej wersji, którą przyjmą wszystkie zaangażowane w procedurę organy.

VII. Wnioski

Pierwsze skoordynowane procedury zatwierdzające, obejmujące wiele krajów UE rozpoczęły się w 2004 roku i zamierzano je sfinalizować w 2005 r.²¹ Cel ten niestety nie został osiągnięty. Postępowania są nadal w toku. Wnioskodawcy musieli przedstawić dodatkowe opracowanie zawierające wszystkie informacje wymagane przez WP 108, które to opracowanie służy jako podstawa dyskusji pomiędzy wszystkimi, uczestniczącymi w procedurze, organami ochrony danych. Ostatecznie powinny one zaowocować wspólnym stanowiskiem w sprawie odpowiedniości postanowień przedmiotowych WRK i umożliwić wszystkim uczestnikom szybkie przystąpienie do postulowanego zatwierdzenia transferów danych.

Dla kwestii samoregulacji szczególne znaczenie ma następujący aspekt: samoregulacja przy pomocy WRK zostanie zaakceptowana przez klientów, pracowników i opinię publiczną tylko wówczas, jeżeli będzie jej towarzyszyć poważne zaangażowanie spółki dotyczące zobowiązań przyjętych przez nią w WRK. Kwestia, w jaki sposób to zaangażowanie może być realizowane zgodnie z przepisami prawa, musi zostać wyjaśniona na podstawie obowiązujących praw krajowych. Opracowywanie takich rozwiązań stanowi wyzwanie dla międzynarodowych spółek i prowokuje dyskusję nad międzynarodową ochroną danych osobowych mającą na celu opracowanie takich procedur i możliwości, które pozwolą spółkom skutecznie wprowadzać w życie ich rozwiązania samoregulacyjne.

Dr Alexander Dix

Berlin Commissioner for Data Protection and Freedom of Information
Berliński Rzecznik Ochrony Danych i Wolności Informacji

*Contribution to a publication
to pay tribute to Dr Ewa Kulesza*

Data Protection and Whistleblowing – The European Response to Sarbanes – Oxley

In a global information society international and – more particularly – European cooperation among Data Protection Commissioners is becoming ever more important. Ewa Kulesza has realized this from the beginning of her two successful terms as the first Polish Inspector General for Personal Data Protection. On numerous occasions, especially when hosting the International Conference of Privacy and Data Protection Commissioners in Wrocław in 2004 and the European Conference of Data Protection Commissioners in Kraków in 2005, she highlighted Poland's central role in this context.

One recent example of how important an effective coordination between European supervisory authorities is can be seen in the issues raised by the U.S. Sarbanes Oxley Act. In response to a number of financial scandals in large U.S. companies, Congress passed this Act in 2002 in order to increase internal transparency and controls, to prevent insider trading and to implement good corporate governance.

The Sarbanes-Oxley Act contains provisions which can increase data security (and thus data protection) inside companies. On the other hand, the legislation requires U.S. and foreign publicly held companies (or foreign subsidiaries of U.S. companies) listed in U.S. stock markets to establish "procedures for the receipt, retention and treatment of complaints... regarding accounting, internal control or auditing matters; and the *confidential*, *anonymous* submission by employees... of concerns regarding questionable accounting or auditing matters."¹ Such procedures are commonly referred to as "whistleblowing hotlines".

The Sarbanes-Oxley Act (commonly abbreviated as "SOX") and this provision in particular raise a number of questions even under U.S. law. Courts in the United States are still dealing with the principal question whether this provision is indeed protection of employees of foreign companies or foreign affiliates of U.S. companies. Recently the U.S. Court of Appeals answered this question in the negative.² Nevertheless, European companies listed in U.S. stock markets as European affiliates of U.S. companies are

²¹ W kilku przypadkach krajowe instytucje ochrony danych udzieliły już zgód krajowych.

¹ Sarbanes-Oxley Act, Section 301 (4).
² 1st Circuit, January 5, 2006.

anxious to comply with SOX since the Securities Exchange Commission (SEC) is threatening them with "delisting" if they don't do so. On the other hand, European data protection authorities and notably the Commission Nationale de l'informatique et des libertés (CNIL) have made it clear from the outset that the European Data Protection Directive has to be observed when complying with SOX.

The CNIL at first issued decisions concerning the French subsidiaries of two U.S. companies stating that their "ethics guidelines" issued to implement SOX were not in line with French data protection law. Consequently, the companies concerned were facing a dilemma: breaking French (and European) law or taking the risk of being delisted at U.S. Stock Exchanges. Talks were being held between the CNIL and the SEC to find a compromise. In Germany a Labour Court ruled that ethics guidelines of a U.S. subsidiary violated German law and – in part even the German Constitution. The case is under appeal to the Federal Labour Court.

Since compliance with SOX is not a national, but an international problem, the Art. 29 Working Party on January 31, 2006 adopted a Working Document.³ The main elements of this common position adopted by European supervisory authorities are:

- While it is legitimate to afford whistleblowers particular protection against reprisals in order to fight illegal transactions such as insider trading and corruption, there is an equal need to afford the incriminated person adequate protection against false accusations.
- Whistleblowing schemes can be justified for compliance with a legal obligation (Art. 7 (c) of the Data Protection Directive) or for the purposes of a legitimate interest pursued by the controller or a third party (Art. 7 (f)). Corporate Governance Codes throughout the European Union and within the OECD demonstrate the need for effective measures to implement better corporate governance in order to ensure the adequate functioning of organisations and to protect the international financial systems.
- Appropriate measures have to be taken to ensure that data collected via whistleblowing hotlines which are inaccurate are erased or rectified. The personal data processed within the scheme should be limited to the data which are strictly necessary and verify the allegations made.
- Clear and complete information about the scheme should be available to data subjects.
- The incriminated person should be informed about the allegations against him or her unless and so long as there is a risk to jeopardize the investigation.
- The incriminated person should have a right of access to the data registered on him except regarding the identity of the whistleblower; however, in case the whistleblower maliciously makes a false statement, the incriminated person may obtain information about the whistleblower's identity.
- Since increasingly external service providers offer their services to run whistleblowing hotlines (e.g. call centers), the Working Party stressed that these service providers themselves have to comply with the principles of Directive 95/46.
- As a rule SOX complaints against the European company should be dealt with inside the EU; only exceptionally data received through a whistleblowing system may be communicated within the group of companies and thus transferred to a third country if the allegation is made against or concerns another legal entity within this group.

- Lastly, if data are to be transferred to a third country – i.e. in most cases to the United States – the provisions of Articles 25 and 26 of Directive 95/46 have to be observed. Either the receiving company has joined the Safe Harbour Scheme, a transfer contract has been concluded or binding corporate rules approved by the competent data protection authorities are in place.

Whistleblowing is not restricted to financial transactions. It may also concern violations of other legal requirements such as environmental protection, safety at work regulations, sexual harassment at the workplace or general grievances in the human resources context. The Working Party has not yet addressed these other circumstances. But the general principles laid down in Working Paper 117 are very likely to be applied beyond the financial auditing context.

Protecting whistleblowers is a major concern for freedom of information. Without whistleblowers a number of severe violations of law and outright scandals would have never come to light, had there not been a person inside an organisation courageous enough to make this public. The Anglo-Saxon legal culture has recognised this early by adopting legislation specifically affording whistleblowers protection (e.g. in the United Kingdom, where – unlike under SOX – whistleblowers can claim confidentiality, not anonymity). However, the incriminated person has also rights which have to be protected, in particular where anonymous allegations are made which later turn out to be incorrect.

European Data Protection Authorities, when adopting Working Paper 116, have taken an important first step to strike a fair balance between the data protection principles and the adequate protection of whistleblowers.

*Artykuł do publikacji
jako wyraz uznania dla dr Ewy Kuleszy*

Ochrona danych i przekazywanie informacji o możliwych nieprawidłowościach – europejska odpowiedź na ustawę Sarbanes – Oxley

W globalnym społeczeństwie informacyjnym coraz bardziej istotna staje się współpraca międzynarodowa, a w szczególności europejska współpraca inspektorów ochrony danych. Jako pierwszy polski Generalny Inspektor Ochrony Danych Osobowych, pani Ewa Kulesza zdawała sobie z tego sprawę już od samego początku jej dwóch udanych kadencji. Podczas wielu okazji, a zwłaszcza podejmując uczestników Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych we Wrocławiu w 2004 r. oraz Konferencji Europejskich Inspektorów ds. Ochrony Danych w Krakowie w 2005 r., podkreślała w tym kontekście niezwykle ważną rolę Polski.

³⁾ Working Paper (WP 117) on the application of EU data protection rules to internal whistleblowing schemes in the field of accounting, account auditing, financial reporting and fight against bribery, financial corruption, banking and financial crime of January 31, 2006.

Niedawnym przykładem tego, jak ważna jest skuteczna koordynacja między europejskimi organami nadzoru, są kwestie podnoszone przez amerykańską ustawę Sarbanes-Oxley. W odpowiedzi na liczne skandale finansowe w dużych przedsiębiorstwach amerykańskich, Kongres przyjął tę ustawę w 2002 r. w celu zwiększenia kontroli i przejrzystości wewnętrznej, zapobiegania wykorzystywaniu poufnych informacji i wprowadzenia właściwych zasad ładu korporacyjnego.

Ustawa Sarbanes-Oxley zawiera postanowienia, które mogą zwiększyć bezpieczeństwo danych (a przez to ich ochronę) wewnątrz przedsiębiorstw. Z drugiej strony, ustawa wymaga od amerykańskich i zagranicznych spółek publicznych (lub zagranicznych podmiotów zależnych firm amerykańskich) notowanych na amerykańskich rynkach giełdowych wprowadzenia „procedur odbioru, rejestracji i obsługi skarg... w zakresie rachunkowości, kontroli wewnętrznej lub audytu; oraz mechanizmów *poufnego, anonimowego* zgłaszania przez pracowników... obaw i wątpliwości w kwestiach rachunkowości i audytu”.¹ Mówiąc o tego typu procedurach, używa się zazwyczaj terminu „linie służące przekazywaniu informacji o możliwych nieprawidłowościach”.

Ustawa Sarbanes-Oxley (skrótowo często określana „SOX”), a w szczególności jej postanowienia, o których mowa powyżej, wywołują liczne pytania i to nawet w obrębie prawa amerykańskiego. Sądy Stanów Zjednoczonych wciąż jeszcze zajmują się podstawowym pytaniem, czy postanowienia te rzeczywiście służą ochronie pracowników przedsiębiorstw zagranicznych lub zagranicznych jednostek powiązanych przedsiębiorstw amerykańskich. Ostatnio amerykański Sąd Apelacyjny odpowiedział na to pytanie przecząco.² Niemniej jednak, przedsiębiorstwom europejskim notowanym na amerykańskich rynkach giełdowych jako europejskie podmioty powiązane przedsiębiorstw amerykańskich zależy na dostosowaniu się do SOX, ponieważ Komisja Papierów Wartościowych i Giełd (SEC) grozi im wykluczeniem z notowań, o ile tego nie uczynią. Z drugiej strony europejskie organy ochrony danych, zwłaszcza zaś Commission Nationale de l'informatique et des libertés (CNIL) od samego początku jasno stwierdziły, że przestrzegając zapisów SOX, konieczne jest jednoczesne uwzględnienie treści europejskiej Dyrektywy w kwestii ochrony danych.

Na przykład CNIL wydała decyzje dotyczące francuskich podmiotów zależnych dwóch przedsiębiorstw amerykańskich, w których stwierdzono, że ich „kodeksy etyki” wydane w celu wdrożenia SOX nie są zgodne z francuskim prawem o ochronie danych. Wskutek tego, przedsiębiorstwa, o których mowa, stanęły wobec dylematu: naruszyć prawo francuskie (i europejskie) lub podjąć ryzyko wykluczenia z notowań na giełdach amerykańskich. Szukając kompromisu, CNIL i SEC podjęły rozmowy. W Niemczech z kolei Sąd Pracy rozstrzygnął, że kodeks etyki amerykańskiego podmiotu zależnego narusza prawo niemieckie, a częściowo nawet niemiecką Konstytucję. Sprawę zaskarżono do Federalnego Sądu Pracy.

Ponieważ zgodność z SOX nie jest problemem krajowym, lecz międzynarodowym, 31 stycznia 2006 r. Grupa Robocza powołana w trybie art. 29 przyjęła dokument roboczy.³

¹⁾ Ustawa Sarbanes-Oxley, art. 301 ust. 4.

²⁾ Okręg nr 1, 5 stycznia 2006 r.

³⁾ Dokument roboczy (WP 117) z dnia 31 stycznia 2006 r. w sprawie zastosowania zasad UE dotyczących ochrony danych do wewnętrznych programów przekazywania informacji o możliwych nieprawidłowościach w zakresie rachunkowości, audytu, sprawozdawczości finansowej i walki z przekupstwem, korupcją finansową oraz przestępczością bankową i finansową.

Główne elementy wspólnego stanowiska przyjętego przez europejskie organy nadzoru są następujące:

- O ile jest zgodne z prawem zapewnianie informatorom ochrony przed represjami w celu zwalczania nielegalnych transakcji, takich jak wykorzystywanie poufnych informacji i korupcja, o tyle równie potrzebne jest, aby inkryminowanej osobie zapewnić odpowiednią ochronę przed fałszywymi oskarżeniami.
- Program przekazywania informacji o możliwych nieprawidłowościach może być uzasadniony w celu zapewnienia przestrzegania zobowiązań (art. 7 lit. c Dyrektywy o ochronie danych) lub dla zagwarantowania realizacji słuszných interesów przez administratora albo osobę trzecią (art. 7 lit. f). Kodeksy ładu korporacyjnego w obrębie Unii Europejskiej i OECD świadczą o potrzebie istnienia skutecznych środków wdrażania ładu nadzoru korporacyjnego w celu zapewnienia odpowiedniego funkcjonowania organizacji oraz ochrony międzynarodowych systemów finansowych.
- Konieczne jest podjęcie odpowiednich środków w celu zapewnienia, że spośród danych zbieranych dzięki liniom służącym przekazywaniu informacji o możliwych nieprawidłowościach, te które są nieściśle, były wymazywane lub korygowane. Przetwarzane w ramach programu dane osobowe powinny ograniczać się wyłącznie do elementów, które są absolutnie niezbędne i które potwierdzają wnoszone zarzuty.
- Osobom, których dotyczą dane, powinno się udostępnić jasne i wyczerpujące informacje o programie.
- Inkryminowana osoba powinna zostać poinformowana o wnoszonych przeciw niej zarzutach, z wyjątkiem sytuacji, gdy może to zagrażać dobru postępowania wyjaśniającego.
- Inkryminowana osoba powinna mieć prawo dostępu do zarejestrowanych na jej temat danych z wyjątkiem danych dotyczących tożsamości informatora; jednakże, w przypadku, gdy działając ze złej woli informator składa fałszywe zeznania, obciążana nimi osoba może otrzymać informacje o jego tożsamości.
- Ponieważ zewnątrzni dostawcy usług coraz szerzej oferują swe usługi w zakresie prowadzenia linii służących przekazywaniu informacji o możliwych nieprawidłowościach (np. centra obsługi telefonicznej), Grupa Robocza podkreśliła, że powyżsi dostawcy usług muszą stosować się do zasad Dyrektywy 95/46.
- Jako zasadę należy przyjąć, że skargi dotyczące SOX wnoszone przeciwko przedsiębiorstwu europejskiemu powinny być rozpatrywane wewnątrz UE, a dane uzyskiwane w ramach programu przekazywania informacji o możliwych nieprawidłowościach jedynie w wyjątkowych przypadkach mogą być przekazywane w obrębie grupy kapitałowej a tym samym do kraju trzeciego, o ile zarzut wniesiony jest przeciwko innemu podmiotowi prawnemu w obrębie grupy bądź też jego dotyczy.
- Jeśli dane mają zostać przekazane do kraju trzeciego – tj. w większości przypadków do Stanów Zjednoczonych – muszą być wówczas przestrzegane postanowienia art. 25 i 26 Dyrektywy 95/46. Albo przedsiębiorstwo otrzymujące dane przystąpiło do programu „bezpiecznej przystani” albo zawarta została umowa transferu informacji albo też istnieją wiążące zasady korporacyjne zatwierdzone przez właściwe organy ochrony danych.

Proces przekazywania informacji o możliwych nieprawidłowościach nie ogranicza się tylko do transakcji finansowych. Może on także dotyczyć naruszania innych wymogów prawnych w sferach takich jak ochrona środowiska, bezpieczeństwo pracy, molestowanie seksualne w miejscu pracy lub generalnie skargi w kontekście spraw personalnych.

Grupa Robocza Art. 29 nie omówiła jeszcze tych innych przypadków, niemniej jednak jest bardzo prawdopodobne, że ogólne zasady wypracowane w dokumencie roboczym nr 117 będą miały zastosowanie również poza obszarem audytu finansowego.

Dla kwestii swobodnego dostępu do informacji ochrona osób przekazujących informacje o możliwych nieprawidłowościach jest problemem podstawowym. Bez takich jednostek w organizacji, wystarczająco odważnych, aby sprawę ujawnić, wiele przypadków poważnego naruszenia prawa oraz zwyczajnych skandali nigdy nie wypłynęłoby na światło dzienne. W anglosaskiej kulturze prawnej, gdzie dosyć wcześnie zauważono tę kwestię, przyjęto ustawodawstwo w sposób konkretny zapewniające informatorom ochronę (np. w Wielkiej Brytanii, gdzie – w przeciwieństwie do SOX – informatorzy mogą żądać poufności, ale nie anonimowości). Niemniej jednak również osoba inkryminowana posiada prawa, które należy chronić, w szczególności zaś w przypadku pojawiania się anonimowych, niepopartych dowodami zarzutów, które później okazują się nieprawdziwe.

Przyjmując dokument roboczy 116, europejskie organy ochrony danych uczyniły pierwszy istotny krok ku znalezieniu rozsądnego złotego środka między zasadami ochrony danych a odpowiednią ochroną osób przekazujących informacje o możliwych nieprawidłowościach.

Prof. Dr Hansjürgen Garstka

Chairman of the European Academy for Freedom of Information and Data Protection
Przewodniczący Europejskiej Akademii Wolności Informacji i Ochrony Danych

Location data: on route to total control?

In the next few years, location data are going to become one of the biggest challenges in respect of data protection. Never before was it possible to determine the whereabouts of a given person if he/she was not under surveillance. New IT and communicational solutions enable to localise people and do even more. Creation and distribution of a location data collection system will soon become necessary for numerous new systems and services. This article discusses issues of location data from the point of view of German law.

1. Prologue: Where art thou, Adam?

People have always dreamt of being able to know where or how long somebody stayed in a given place at any given time. For centuries it was an unreachable dream. Even God Himself – according to chapter 3 verse 9 of the “Book of Genesis” – had to call: “Where art thou, Adam?” to learn Adam and Eve’s location after they have committed the original sin. God did not know that the pair hid in the garden as they had become aware of their nakedness. Therefore, we may say that even the Omniscient had no access to the information on their whereabouts and depended on Adam who would determine his own position by answering to God’s previous question: “I heard thy voice in the garden” (ibid, verse 10).

Obviously, it was much more difficult to determine the location of certain people in the past. It took unbelievable effort to obtain information about their place of stay.

Data could only be collected using traditional scrutiny (which has always been the most expensive method), requiring time and effort of law enforcement agencies.

The situation has substantially changed due to exceptionally accelerated technological progress that has occurred for the last two centuries. Practically, when telegraphic offices came into being in the 30’s of the nineteenth century, it became clear that every person sending a telegram would be forced to reveal not only its content but also his/her place of residence (as opposed to sending letters).

In consequence, secrets concerning the content of information sent by telegraphs, later on via communication media and finally using telecommunication have been covered by such legal regulations as Section 10 of the old communication law laid in 1928.

Another step was introduction of private telephones located in apartments. Although they did not enable to directly determine the whereabouts of the caller yet, it was possible to call back and check the number thanks to the efforts of telephone exchanges.

It also concerned public telephone boxes used by criminals. This way, it was possible to identify the place from which they called and, as a result, determine their whereabouts. Nevertheless, this was not a milestone of criminology (for the purpose of opening investigations or catching suspects).

This level of technology was maintained until the age of computers.

2. Mobile telephony – a milestone in indicating location

The incredible success of mobile telephony in the 90's of the twentieth century had crucial importance for development in the field of location. Small transmitters of mobile telephones and their growing use by all social groups (as opposed to the automatic telephony that had been known, but available only to few privileged groups of people) have enabled more accurate but mostly automatic determination of the whereabouts also of those people who not necessarily used their phones at a given moment, provided that these have been switched on. Due to the rapid evolution of mobile telephony, there is a current trend to create small and more effective transmitters. Certain technologies, such as triangulation using higher number of aerials, have enabled telecommunication to reach the required size that ensures accurate determination of the location of a given telephone user.

The authorisation to use GPS for private purposes (this used to be exclusively a military system in the USA) has been another milestone in the field of determination of location. It used to be applied passively, i.e. the person who held the receiver could determine his/her location.

Another key step in respect of technological development has been the combination of mobile telephony and GPS resulting in utterly new possibilities. Successful logistics companies, which wanted to be able to trace the location of their transport means to manage them appropriately, have been the first (of course, apart from the military) to discover these opportunities. The signals incoming to GPS would be played back in mobile phones and then sent through those to the headquarters. Initially, the idea was widely protested among truck drivers and then by trade unions supporting the drivers, which to some extent contributed to determination of general frames of the currently ongoing debate.

This is also the principal idea of the *Toll-Collect* function used for monitoring of road fee payment by trucks on certain sections of German motorways pursuant to §1 paragraph 1 of the motorway tax law:¹ „for use of German motorways by cars pursuant to Article 2 letter d of the ordinance (...) on payment of amounts due for use of specified roads by trucks (TIR).“

So commonly mentioned *On-Board-Units* are nothing more than devices that constantly receive signals from GPS and forward them via mobile phones to the seat of a given company to the seat of a given company, when the car is located on motorways where fee is required. It is a sophisticated technology, as it assumes comparing GPS-data with

the off-street data. *Toll-Collect* additionally includes another technology: video-surveillance. As a part of the control function of the system, due to automatic observation and analysis of the registered area, not only trucks traffic congestion is controlled but also the whole traffic on motorways is available (e.g. whether cars have their road tax paid).

This way, a technical infrastructure has been established: initially for motorways and, in the future (in specified scope), it is also expected to be established on different roads (legal basis: § 1 paragraph 4 ABMG) in order to control all vehicles. „Transformation“ of data into data actually obliging and indispensable in the subsequent proceedings for enforcement or even further return of the toll – provided for in the legislation but, from the technical point of view impossible to be forced – is – as philosophers might say – possible; the essence of the matter consists in something different: the proceedings every time can be changed this way that any data may be collected but also used for any purposes.

Moreover, it is worth mentioning that further large control systems for car localisation are currently in the preliminary stage.

„eCall“ of the European Commission, developed as a part of 2003 European Road Safety Action Programme, may serve an example here.² It assumes that if there is an accident on a road, all required information concerning a given vehicle will to be automatically sent to an Emergency Centre. This means permanent collection of information on location.

Among American solutions, a relatively well-known solution is a project of insurance companies that considers the possibility of making premiums dependent on the fact that drivers stop more often in danger areas.

3. Location and data protection

Because of their association to people whose whereabouts should be determined, location data relate personally to specific people. Therefore, both their processing and transfer comprise clear interference that breaches the right to informational self-determination.³ This interference is the more intensive, the longer the data are collected.

In the analysis of personal data management pursuant to personal data protection regulations effective in the world, apart from various questions asked about the procedure, it is necessary to see two principal problems of substantial nature:

- Under what conditions can personal data be collected, stored and processed?
- Under what conditions is it possible to use personal data for other purposes, in particular transfer them? The major issue of the discussion includes rights from the point of view of data transfer for the purposes of prosecution and defence against threats if the data have been obtained for completely different purpose.

²⁾ europa.eu.int/comm/transport/road/library/rsap/com_2003_0311_en.pdf

³⁾ The Association of Data Protection dealt with the issues of location data for the first time at the meeting of telecommunication representatives and data protection authorities as a part of the International Conference of Data Protection Commissioners in February 2001 in Bangalore (http://www.datenschutz-berlin.de/doc/int/iwgdpt/locat_de.htm). At that time, the Art. 29 Working Party developed a draft of European guidelines related to data protection (http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf)

¹⁾ Law on payment of fees for use of certain German motorways by trucks with large tonnage (hereinafter: ABMG) of April 5, 2002, BGBl I 2002, 1234.

3.1. Admissibility of location data processing

If we assume that location data are essential to perform certain agreements or services, it should be noted that it is possible to process them only in the required and strictly determined (for that purpose) scope. In relation to mobile telephony, it results from general data protection principles without any explicit regulations in the telecommunication law, though, only within the scope necessary to ensure communication. As the location of a given subscriber should be determined in his/her telephone throughout the whole time when he/she actually remains in a given place, the data that have already been in the telephone can and must be removed or copied in case of a change of a mobile phone.

Consideration of information safety aspects may lead to certain concessions that have to be restricted solely to achieve an assumed objective. If location data are to be further processed – by a longer period or for collection of additional data by other services – it is permissible exclusively upon the basis of data subject's consent.

Today, there are clear provisions in the telecommunication law explicitly stipulating that, in some situations, a given subscriber has to have the right to object to have his/her data processed.

This is similarly in case of the road tolls collected in Germany on certain sections of motorways where location data processing is necessary only for a precisely determined scope. Therefore, initial requirements of data protection commissioners that the system is to be established in such a way to enable its constant operation, also without location data related to certain people, could not have been realised.⁴

The act describes very precisely, what data and for what purposes can be obtained and processed. The problem of the lack of periods the expiry of which obliges to delete the data, unless they may be retained for other purposes than analysis, follows the lack of precise regulation of this question.

Therefore, the previously asked question: „*In what circumstances can law enforcement and security agencies obtain/collect location data*” was subject to discussion first of all consideration in close relation to the right to surveillance. In this case, the primary role was played by the issue of use of tracking devices that, as they are located in cars, enable, in clearly precised scope, to locate the car.

Only a constitutional complaint lodged by person suspected of terrorism, who in the nineties was sentenced for long-year imprisonment, paid attention of lawyers on the new dimension of possibilities of GPS usage. In this specific case, it was possible to track down (and defang) extremely intelligent perpetrators using appropriate devices containing in-built location transmitters. It was possible due to a GPS device secretly installed in the car these people used, which enabled to follow their every move for three months.

Here, the legal basis was an unclear provision developed in the scope of the so-called OrgKG of 1992, § 100. Clause c No. 1 pursuant to which “certain technical means (...) used to determine the whereabouts of the suspect may be used (...) if the object of the investigation is of great importance and if detection of the whereabouts of the perpetrator using other methods has been ineffective or would be considerably hindered.”

In the decision of April 12, 2005⁵, the Federal Constitutional Tribunal avoided providing a direct legal systematisation of issues related to the new aspects of location data. The lodged complaint was denied and the opinion stated that the legal basis in this case was insufficient. However, the Tribunal referred to the threats to law to informative self-determination, obliged legislators to pay special attention to the technical development in the discussed field, and if necessary, prepare and introduce adjusting legal provisions.

The inconsistency with the constitutional so-called “secret surveillance” on the basis of which a detailed profile of person subject to such surveillance may be made was particularly emphasised.

3.2. Data processing incompatible with the purpose for needs of law enforcement and defence agencies

Use of data incompatible with the purpose – their collection and processing – is also a breach of the right to informative self-determination. It was unknown in the times of the first debates regarding personal data that took place in the 70's of the twentieth century but was introduced (even) before the announcement by the German Constitutional Tribunal of the judgement in the case concerning census.

Then, the attention was paid to the necessity of introduction of purpose determination (known as the “finality principle”) to a principal paradigm of the debate on data protection. Introduction of this principle was the main issue of the amendment of the federal data protection law in Germany in 1990.

Constitutional ban of data collection and processing inconsistent with the purpose placed a stop sign before investigation of crimes and fight against hazards.

Even though the legally binding provisions on data protection provide for in turn-point legislation § 14 Clause 2 No. 6 and 7 of the federal act on data protection the right to further – limited by the indispensability of processing – data transmission to the law enforcement and defence agencies and also for purposes of limited investigation of petty offences.

Since many years there have been such legal questions in relation to which the inconsistency with the purpose of data processing also for this purpose was excluded or at least very limited: professional and formal secrecyes such as, on the one hand, medical secrecy and attorney's secrecy and, on the other hand, tax secrecy and other e.g. the right to refuse to testify, lead to a flat prohibition of processing incompatible with the purpose.

⁴) Resolution 62 of the conference of authorities responsible for data protection, October 24-26, 2001 in Münster: “Lkw – motorway toll and general road toll on privately built roads in the territory of Germany,” www.datenschutz-berlin.de/doc/de/konf/62/maut.htm

⁵) Ref. no. 2 BvR 581/01

In relation to communication secrets, the issue has always been ambiguous. On the one hand, protection of state interests has been ensured and, on the other hand, legal restrictions have been observed regarding surveillance. Balance of interests of both sides has been guaranteed by developing comprehensive circumstances of control and by procedural regulations.

Location data in accordance with current technology have been counted to data on circumstances of communication traffic that communication secrecy is subject to communication law, but may be disclosed for criminal investigation purposes under strictly defined conditions. The issue of using automatic telephone data of the former president of Schleswig-Holstein, Uwe Barschel made citizens aware of this situation.

The growing use of mobile phones contributed to in depth debate whether use of data incompatible with the purpose, thus not for telecommunication purposes but for pursuit, should not be subject to the same or similar legal restriction as control (supervision) of telephone content.

The debate resulted, in the effect of many amendments to the German Code of Criminal Proceedings, in development of a model of diversified data use. Inclusion of the regulation of IMSI-Catchers action that, as opposed to legal reasons, is not used to determine the location of a given mobile phone but allow for listening such data, which may be a reason for a motion on installing such tapping, in a much higher degree. During the Toll-Collect's implementation, it became clear for the participants that it could be introduced if use of collected data was restricted only for objectives related to the road tolls.

The decision of the (regional) court of the first instance in Gummersbach made at the testing stage of the project and enabling to make data available in case of truck theft,⁶ brought about an additional stipulation of AMG according to which, by virtue of law, data created in the system in no case could be used for purposes specified in other acts. Without the restriction, the whole system could be doomed to failure.

After the events of the 17 November 2005 in State of Baden-Württemberg, when a car park user after a quarrel over EUR 10 was hit (and eventually died) by a foreign truck, the German Minister of Internal Affairs, Wolfgang Schäuble, initiated the public debate over the material problem related to the purpose of the road database use in official actions related to accidents. The discussed example clearly indicates that road databases should also be provided at the disposal of law enforcement agencies also for the purposes of investigation of the most serious road offences.

Hans Peter Bull, the first Data Protection Commissioner in Germany, a former advocate of restriction of police rights for data processing purposes, said: „If this enables to catch a criminal, law amendment is allowable.”⁷ In this case, he also meant finding a stolen car (because of his views he was not appointed for the second turn of office). To this end it is necessary to change only the road collect but also the whole philosophy of this act. Since most important part of collected personal data needs to be deleted in

a short period of time because they are redundant for the toll purposes, it is necessary to create new legal regulations that would not only enable to obtain data for purposes other than those for which they were collected and hinder their use incompatible with the purpose, but also those that would enable their storage and collection for a longer period of time (e.g. for safety purposes).

Nowadays, telecommunication development goes exactly in this direction. After animated debates concerning in particular competence problems, European Directive have become effective obliging telecommunication employees to store data from six months to one year depending on whether these are needed for own purposes, and to make the data available for criminal investigation purposes.⁸

4. Big Brother: threat of „total control”

In the decision relating to GPS, the Federal Constitutional Tribunal spotted the constitutional limits law in respect of processing of data within the scope of „total control” „together with which a personal profile of a person subject to such control might be prepared.” This would „always be incompatible with the constitution.” Indeed, the court agreed that the questioned control via GPS of a given person (a suspect), does not violate the essence of his right to privacy. Simultaneously, every time the relation between the right to “personal development according to one’s will” indicated by the complainant and the essence of his right to privacy,⁹ emphasised many times by court in recent years – in this case by establishing and processing of the data on the place of stay – comes to existence.

The architecture of the *Toll-Collect* system introducing a video technology, indicates another element in case of which the question: „When are the limits of total control crossed?” reveals a significant aspect of the issue, i.e. connection of location data with other data resources that on the one hand allow for apart from determination of the location also for illustration of behaviour in the place of stay.

Taking into account the fact that video records are in most cases often erased, use of the technology after minute changes in law and „switching” the system into „total control” is appropriate, passing over the possibility to use data with abuse not provided for in the act. Uniting collected data with an information system e.g. of the police or Federal Office for Road Traffic system with the use of existing infrastructure, however, it is possible in the future.

The considerations presented specify the areas of interest that should be subject to discussion during legislative debates to be held in the next few years. In particular, the following issues should be resolved:

1. The top priority is given to construction of a communication and information infrastructure and, additionally, considering the economy principle, the risk related to abuse can be reduced to the minimum only when data are processed in an economical manner.

⁶) Local court in Gummersbach, decision of 21 August 2003 – 10a Gs 239/03.

⁷) Journal of 28 November 2005 p. 3

⁸) A proposal of Directive of the European Parliament and Council on the retention of data generated or processed in connection with the provision of publicly available electronic communication services (21 September 2005), 2005/0182 (COD).

⁹) At the beginning very pointedly in the judgement in the “tapping” case of 3 March 2004, 1 BvR 2378/98.

2. It is unacceptable (*de lege-lata*) to apply obsolete (primary) action procedures by the law enforcement and security agencies to obtain and process location data.
3. In the view of the Federal Constitutional Tribunal actions that make use of GPS must be regulated similarly as in case of telecommunication supervision (control). In any case, it results from the predictable common development of both fields.
4. Communication and information systems that pose a threat of „total control” should be shaped, if possible, in such a way that the use incompatible with the purpose can be eliminated. Technical solutions need to be discussed.
5. In special cases, this type of systems should be made available for pursuit and security purposes. However, there is a need for unambiguous legal regulations that would clearly define situations in which certain data may be made available. Regular use of location data must be excluded as such possibility might „erode” defined constitutional limits.
6. Combination of different control technologies (monitoring) including location data will, in general, refer to the essence personal interests of human being and go beyond constitutional limits for „total control”.

5. Epilogue

To sum up, if there are no circumstances for introducing „total control,” location data processing may always be at the crux of personal rights. Likewise in case of bugging somebody's phone. In individual cases, location data may indicate the activities that fit in the area and, thus, cannot be processed. Thus the circle is closed: Adam was not alone in the garden and, after the original sin Adam and Eve certainly saw themselves not only in a paradisiacal and innocent manner. God's cry: „*Where art thou, Adam?*” would be – pursuant to the German Constitution – inconsistent with the law.

Dane o lokalizacji: na drodze do totalnej kontroli?

W kolejnych latach informacje na temat lokalizacji będą jednym z najważniejszych wyzwań w aspekcie ochrony danych. Nigdy dotychczas nie było możliwości określenia miejsca pobytu danego człowieka, jeżeli nie był on bezpośrednio obserwowany. Nowe rozwiązania w dziedzinie techniki informacyjnej i komunikacji umożliwią lokalizowanie osób, a nawet więcej. Obecnie tworzenie oraz upowszechnianie systemu zbierania danych dotyczących lokalizacji będzie konieczne także dla wielu nowych systemów i służb. W artykule omówiono problematykę danych lokalizacyjnych z punktu widzenia niemieckiego prawa.

1. Prolog: Gdzie jesteście Adamie?

Odwiecznym marzeniem ludzkości było dysponowanie w każdym momencie informacją na temat: *gdzie się ktoś zatrzymał lub jak długo tam przebywał?* Przez tysiące lat wydawało się to niemożliwe do osiągnięcia. Sam Pan Bóg – w myśl rozdziału 3 wiersz 9 „Księgi Rodzaju” – w celu uzyskania informacji o miejscu pobytu Adama i Ewy po popełnieniu grzechu pierworodnego musiał wołać: „gdzie jesteście Adamie”. Nie wiedział bowiem, że

świadomość nagości była powodem ukrycia się obojga w ogrodzie. Można zatem stwierdzić, że nawet sam Wszyszkowiedzący nie miał dostępu do informacji dotyczących miejsca ich pobytu, będąc uzależnionym od tego, czy Adam, wykorzystując jego przekaz informacyjny, ujawni swoje położenie: „Twój głos słyszałem w ogrodzie” (tamże, wiersz 10).

Oczywiste jest, że w przeszłości znacznie trudniejsze było ustalanie miejsca pobytu konkretnych osób. Niewyobrażalna praca musiała zostać włożona, aby zdobyć informacje na temat tego, gdzie zatrzymali się określani ludzie.

Istniała wówczas możliwość uzyskania tych danych wyłącznie metodami klasycznej obserwacji personalnej, które należały i nadal należą do najbardziej kosztownych, wymagających dużego nakładu pracy organów ścigania.

Sytuację tę zmienił zasadniczo postęp technologiczny, jaki dokonał się w niespotykanym dotychczas tempie na przestrzeni ostatnich dwóch stuleci. Praktycznie wraz z pojawieniem się urzędów telegraficznych w latach trzydziestych dziewiętnastego wieku stało się oczywiste, że każda osoba wysyłająca telegram jest zmuszona do ujawnienia urzędnikom nie tylko treści samego telegramu, lecz również danych na temat miejsca zamieszkania (inaczej niż w przypadku wysyłania listów).

W konsekwencji tajemnice dotyczące treści informacji przesyłanych za pomocą telegrafów, w późniejszym zaś czasie środków łączności, a w końcu z wykorzystaniem telekomunikacji zostały objęte uwarunkowaniami prawnymi, takimi jak paragraf 10 starego prawa łączności, który został sformułowany w 1928 roku.

Kolejnym krokiem było wprowadzenie prywatnych telefonów, które znajdowały się w mieszkaniach. Mimo że nie pozwalały jeszcze na bezpośrednie ustalenie miejsca pobytu dzwoniącego, to starania podejmowane w centralach telefonicznych umożliwiały oddzwonienie i sprawdzenie numeru.

Dotyczyło to także publicznych kabin telefonicznych wykorzystywanych również przez sprawców przestępstwa. W ten sposób była możliwa identyfikacja miejsca, z którego dzwonili, a w konsekwencji ustalenie miejsca ich pobytu. Nie był to jednak moment zwrotny w dziedzinie kryminalistyki (dla potrzeb rozpoczęcia śledztwa lub schwytania podejrzanego).

Taki poziom techniki utrzymywał się do czasu wprowadzenia w życie technologii z wykorzystaniem komputerów.

2. Telefonía komórkowa – przełom w dziedzinie określania miejsca pobytu

Fundamentalne znaczenie dla rozwoju dziedziny lokalizacji miał niewyobrażalny sukces telekomunikacji komórkowej w latach dziewięćdziesiątych minionego stulecia. Zajmujące niewiele miejsca urządzenia nadawcze telefonii komórkowej oraz coraz powszechniejsze korzystanie z niej przez wszystkie grupy społeczne (w przeciwieństwie do znanej już wcześniej, lecz dostępnej tylko nielicznym, uprzywilejowanym grupom techniki telefonii automatycznej) umożliwiły dokładniejsze, a przede wszystkim automatyczne określenie miejsca przebywania także tych osób, które nie korzystają w danym momencie ze swoich telefonów komórkowych, pod warunkiem że są one włączone. W związku z rozwojem telefonii komórkowej dominuje obecnie tendencja do

tworzenia coraz to mniejszych, lecz efektywniejszych urządzeń nadawczych. Odpowiednie technologie, np. triangulacja z wykorzystaniem większej liczby anten, pozwoliły telekomunikacji na osiągnięcie wymaganego rozmiaru, który zapewnia precyzyjne określenie miejsca pobytu użytkownika danego telefonu.

Zezwolenie na stosowanie systemu GPS do celów prywatnych (wcześniej system ten był przeznaczony wyłącznie do celów wojskowych USA) jest kolejnym „kamieniem milowym” w dziedzinie określania miejsca pobytu. Wykorzystanie jego jest wprawdzie początkowo pasywne, czyli ten, kto ma urządzenie odbiorcze, może określić swoją własną pozycję.

Kolejnym istotnym krokiem w dziedzinie rozwoju techniki było połączenie telefonii komórkowej z systemem GPS, stwarzające tym samym zupełnie nowe możliwości. Jako pierwsze (poza, oczywiście, wojskiem) odkryły te możliwości dobrze prosperujące na rynku firmy logistyczne, które w każdym czasie chciały znać miejsca pobytu swoich środków transportowych, by móc nimi odpowiednio dysponować. Przychodzące do systemu GPS sygnały były odtwarzane w telefonach komórkowych, a następnie przesyłane przez nie do centrali. Spotkało się to początkowo z licznymi protestami kierowców samochodów ciężarowych (TIR), a następnie występujących w ich obronie związków zawodowych, co przyczyniło się niejako do określenia ogólnych ram toczącej się obecnie dyskusji.

Jest to także myśl przewodnia funkcji *Toll-Collect*, służącej do monitorowania uiszczania opłat drogowych przez samochody ciężarowe na wydzielonych odcinkach niemieckich autostrad zgodnie z § 1 ustęp 1 prawa o podatku drogowym od autostrad:¹ „dla korzystania z autostrad niemieckich przez samochody w myśl artykułu 2 litera d rozporządzenia (...) o uiszczaniu należności za korzystanie z określonych dróg przez samochody ciężarowe (TIR)”.

Powszechnie wymieniane *On-Board-Units* są niczym innym niż urządzeniami, które z jednej strony odbierają nieprzerwanie sygnały z GPS, z drugiej zaś przez telefony komórkowe przekazują je dalej do siedziby firmy, gdy samochód znajduje się na płatnych autostradach. Jest to zaawansowana technika, ponieważ zakłada porównanie danych GPS z danymi z ulicy.

Toll-Collect łączy tę kombinację z kolejną techniką, a mianowicie – wideo nadzorem. W ramach funkcji kontrolnej systemu, dzięki automatycznej obserwacji oraz analizie rejestrowanego obszaru, kontrolowane jest nie tylko natężenie samego ruchu pojazdów ciężarowych, lecz zostaje zobrazowany również cały ruch na autostradach (np. czy samochody mają opłacony podatek drogowy).

Dzięki temu została utworzona infrastruktura techniczna – początkowo na autostradach, a docelowo w przyszłości (w określonym zakresie) przewiduje się również jej utworzenie na innych drogach (podstawę prawną stanowi § 1 ust. 4 ABMG), z przeznaczeniem do kontroli wszystkich pojazdów. Ustawowo przewidziane, ale z technicznego punktu widzenia w żaden sposób niemożliwe do wymuszenia „przekształcenie” danych na dane faktycznie zobowiązujące i niezbędne w późniejszym postępowaniu dla wyegzekwowania lub nawet późniejszego zwrotu opłaty jest – tak powiedzieliby filozofowie

– prawdopodobne; sedno sprawy polega na czymś innym: postępowanie każdorazowo da się w taki sposób zmienić, że wszystkie dane mogą zostać nie tylko pozyskane, ale także wykorzystane dla jakichś celów.

Ponadto należy dodać, że obecnie w fazie przygotowawczej są kolejne duże systemy kontrolne służące do lokalizowania samochodów.

Jako przykład może posłużyć projekt „eCall” Komisji Europejskiej, który został opracowany w ramach „Road Safety Action Plan” z 2003 roku.² Zakłada on, że w sytuacji, kiedy na drodze dojdzie do wypadku, wszystkie wymagane informacje na temat określonego pojazdu powinny zostać automatycznie przesłane do Emergency Centrum. To oznacza ciągle (systematyczne) gromadzenie informacji o miejscu pobytu.

Z rozwiązań amerykańskich dość powszechnie znany jest projekt firm ubezpieczeniowych, które rozważają możliwość uzależnienia składek od tego, czy kierowcy częściej zatrzymują się w niebezpiecznych okolicach.

3. Lokalizacja i ochrona danych

Dane o lokalizacji ze względu na odniesienie ich do ludzi, których miejsca pobytu powinny zostać ustalone, dotyczą personalnie konkretnych osób. W związku z tym zarówno ich przetwarzanie, jak i przekazywanie stanowi jawną ingerencję naruszającą prawo do informacyjnego samostanowienia.³ Ta ingerencja jest tym bardziej intensywna, im dłużej te dane są gromadzone.

Analizując zarządzanie danymi osobowymi na podstawie obowiązujących na świecie zasad dotyczących ochrony danych osobowych, obok stawiania różnego rodzaju pytań odnoszących się do metod postępowania, należy dostrzegać dwa zasadnicze problemy natury materialnej:

- Na jakich zasadach mogą być gromadzone, przechowywane i przetwarzane dane osobowe?
- Pod jakimi warunkami wolno używać danych osobowych do innych celów, a zwłaszcza przekazywać je? Podstawowym zagadnieniem w dyskusji są uprawnienia w aspekcie przekazywania danych dla celów ścigania oraz ochrony przed zagrożeniami, jeśli zostały one pozyskane dla potrzeb realizacji innego rodzaju celów.

3.1. Dopuszczalność przetwarzania danych o lokalizacji

Wychodząc z założenia, że dane o lokalizacji są niezbędne do realizacji określonych umów lub usług, należy stwierdzić, że istnieje możliwość przetwarzania ich wyłącznie w niezbędnym, ściśle określonym – odpowiednio do tego celu – wymiarze. W odniesie-

¹ Prawo o uiszczaniu opłat za korzystanie z wyznaczonych niemieckich autostrad przez samochody ciężarowe o dużym tonażu z 5 kwietnia 2002 r., BGBl I 2002, 1234 (dalej zwane ABMG).

² europa.eu.int/comm/transport/road/library/rsap/com_2003_0311_en.pdf.

³ Stowarzyszenie ochrony danych po raz pierwszy zajęło się problematyką danych o lokalizacji na posiedzeniu przedstawicieli telekomunikacji i organów ochrony danych w ramach Międzynarodowej Konferencji Rzeczników Ochrony Danych w lutym 2001 r. w Bangalore (http://www.datenschutz-berlin.de/doc/int/iwgdpt/locat_de.htm). W tym czasie Grupa Robocza Art. 29 ds. ochrony danych opracowała projekt europejskich wytycznych w zakresie ochrony danych; http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

niu do telefonii komórkowej wynika to z ogólnych zasad ochrony danych – bez dokonania jednoznacznych uregulowań w prawie telekomunikacyjnym, jednakże tylko w wymiarze, który jest niezbędny do zapewnienia łączności. Ponieważ miejsce pobytu abonenta powinno być określone w jego aparacie przez cały czas jego faktycznego przebywania w danym miejscu, wcześniejsze znajdujące się w nim dane mogą i muszą zostać usunięte lub też przepisane przy zmianie aparatu komórkowego.

Rozpatrywanie aspektów bezpieczeństwa informacji może prowadzić do przyjęcia pewnych ustępstw, które muszą ograniczać się ściśle do osiągnięcia zamierzonego celu. Jeżeli dane o lokalizacji mają być w dalszym ciągu przetwarzane – czy to przez dłuższy okres czasu czy też dla pozyskania dodatkowych danych przez inne służby – to jest to dozwolone wyłącznie za zgodą abonenta.

Obecnie w prawie telekomunikacyjnym są jasno sformułowane przepisy, które jednoznacznie wskazują, że abonent w niektórych sytuacjach musi mieć możliwość sprzeciwu wobec przetwarzania tych danych.

Także w przypadku opłat pobieranych w Niemczech na określonych odcinkach autostrad przetwarzanie danych o lokalizacji jest niezbędne wyłącznie w ściśle określonym zakresie. Z tego też względu wstępne wymagania rzeczników ochrony danych osobowych aby system został ukształtowany w taki sposób, by zawsze mógł funkcjonować, również bez danych o lokalizacji dotyczących konkretnych osób, nie mogły być zrealizowane.⁴

Bądź co bądź ustawa opisuje w sposób bardzo szczegółowy, jakie dane i dla jakich celów mogą zostać pozyskiwane oraz przetwarzane. W związku z brakiem dokładnego uregulowania tej kwestii powstaje problem terminów, do upływu których dane muszą być ponownie usunięte, chyba że mogą być one przechowywane dla celów innych niż analiza.

Z tego też względu wcześniej sformułowane pytanie brzmiące: *„Pod jakimi warunkami organy ścigania i bezpieczeństwa mogą pozyskiwać dane o lokalizacji”* zostało poddane pod dyskusję, w pierwszej kolejności, w ścisłym związku z prawem do prowadzenia obserwacji. Główną rolę odgrywało przy tym zagadnienie wykorzystania urządzeń do namierzania, które będąc zamontowane w samochodach pozwalają w ściśle określonym zakresie na ustalenie położenia pojazdu.

Dopiero skarga konstytucyjna osoby podejrzanej o terroryzm, która w latach 90. została skazana na karę wieloletniego pozbawienia wolności, zwróciła uwagę prawników na nowy wymiar możliwości z wykorzystaniem GPS. W tym konkretnym przypadku niezwykle inteligentnych sprawców przestępstwa udało się odnaleźć (i unieszkodliwić) za pomocą odpowiedniego sprzętu z wbudowanymi nadajnikami namierzania. Było to możliwe dzięki potajemnemu zamontowaniu urządzenia GPS w wykorzystywanym przez nich samochodzie, które śledziło każdy ich ruch przez trzy miesiące.

Podstawę prawną stanowił w tym przypadku niejasny przepis opracowany w ramach tzw. OrgKG z 1992 roku, § 100 ust. 1 pkt 1, zgodnie z którym „określone środki techniczne (...)

służące do wykrycia miejsca pobytu podejrzanego mogą zostać zastosowane (...) jeżeli przedmiot ścigania przestępstwa ma duże znaczenie i jeśli wykrycie miejsca pobytu sprawcy innymi sposobami jest mało skuteczne lub byłoby znacznie utrudnione”.

Federalny Trybunał Konstytucyjny w swoim wyroku z 12 kwietnia 2005 r.⁵ uniknął bezpośredniego prawnego usystematyzowania problematyki dotyczącej nowego wymiaru danych o lokalizacji. Złożoną skargę odrzucił, stwierdzając w uzasadnieniu wyroku, że podstawy prawne w prowadzonej sprawie były wystarczające. Jednakże odniósł się także do zagrożeń dla prawa do informacyjnego samostanowienia i zobowiązał ustawodawcę do zwrócenia bacznej uwagi na rozwój techniczny w omawianej dziedzinie, a w razie konieczności do reagowania i wprowadzania korygujących norm prawnych.

W szczególności została podkreślona sprzeczność z Konstytucją tzw. „kontroli totalnej”, na podstawie której można sporządzić szczegółowy profil osoby poddanej obserwacji.

3.2. Niezgodne z przeznaczeniem przetwarzanie danych dla potrzeb organów ścigania i obrony przed zagrożeniami

Niezgodne z przeznaczeniem wykorzystywanie danych – ich pozyskiwanie i przetwarzanie – stanowi także naruszenie prawa do informacyjnego samostanowienia. Nie było ono jeszcze znane w okresie pierwszych debat na temat danych osobowych, które miały miejsce w latach siedemdziesiątych, lecz zostało wprowadzone już przed ogłoszeniem wyroku w sprawie spisu ludności przez Trybunał Konstytucyjny Niemiec.

Wówczas to zwrócono uwagę na konieczność włączenia związku celem, sformułowanego jako „finality principle”, do zasadniczego paradygmatu dyskusji na temat ochrony danych. Wprowadzenie tej zasady było głównym tematem nowelizacji federalnej ustawy o ochronie danych w Niemczech w 1990 roku.

Konstytucyjny zakaz pozyskiwania i przetwarzania danych niezgodnie z celem postawił znak stopu przed ściganiem przestępstw i przed zwalczaniem niebezpieczeństw.

Wprawdzie powszechnie obowiązujące przepisy o ochronie danych przewidują w przełomowych uregulowaniach § 14 ust. 2 pkt 6 i 7 federalnej ustawy o ochronie danych uprawnienie do dalszego – ograniczonego zasadą niezbędności – przesyłania danych do organów ścigania i organów bezpieczeństwa, a także do celów ograniczonego ścigania wykroczeń.

Już od dawna istniały inne materie prawne, przy których niezgodność z celem przetwarzania także dla tego celu była wyłączona lub przynajmniej silnie ograniczona: tajemnice zawodowe i urzędowe, jak na przykład z jednej strony tajemnica lekarska i tajemnica adwokacka, z drugiej zaś tajemnice podatkowe, jak również inne – prawo do odmowy zeznań prowadzą do kategorycznego zakazu przetwarzania niezgodnego z przeznaczeniem.

W odniesieniu do tajemnicy łączności sytuacja od samego początku była dwuznaczna. Z jednej strony bowiem zapewniono ochronę interesów państwowych, z drugiej zaś przestrzegano ograniczeń prawnych w dziedzinie ścigania. Równowaga interesów obu

⁴) Rezolucja 62 konferencji organów odpowiedzialnych za ochronę danych, zorganizowana w dniach 24-26 października 2001 r. w Münster: „Lkw – opłata drogowa na autostradach i ogólna opłata drogowa na prywatnie zbudowanych drogach na terytorium Niemiec”; www.datenschutz-berlin.de/doc/de/konf/62/maut.htm.

⁵) Sygn. akt 2 BvR 581/01.

stron została zapewniona przez opracowanie kompleksowych warunków sprawowania kontroli oraz przez regulacje proceduralne.

Z kolei dane o lokalizacji, stosownie do obecnego stanu techniki, zostały zaliczone do danych o warunkach ruchu komunikacyjnego, które zgodnie z prawem komunikacyjnym podlegają tajemnicy telekomunikacyjnej, ale mogą zostać udostępnione na potrzeby ścigania karnego pod ściśle określonymi warunkami. Wykorzystanie automatycznych danych telefonicznych byłego premiera kraju Schleswig-Holstein Uwe Barschela uświadomiło obywatelom tę sytuację.

Coraz powszechniejsze używanie telefonów komórkowych przyczyniło się do pogłębionej debaty na temat, czy niezgodne z przeznaczeniem, a więc nie dla celów telekomunikacyjnych, lecz dla celów ścigania wykorzystanie danych nie powinno podlegać takim samym lub podobnym ograniczeniom prawnym, jak kontrolowanie treści (nadzorowanie) telefonów.

W wyniku licznych nowelizacji niemieckiego kpk dyskusja ta doprowadziła do opracowania modelu zróżnicowanego systemu wykorzystania danych, włącznie z regulacją działania IMSI-Catchers, która w przeciwieństwie do uzasadnień prawnych nie służy temu, aby ustalić miejsce znajdowania się telefonu komórkowego, lecz w znacznie większym stopniu pozwala na odsłuchanie tych danych, które mogą być podstawą wniosku o założenie podsłuchu. W trakcie wdrażania projektu Toll-Collect, dla uczestniczących w nim stało się jasne, że ten gigantyczny projekt może być wprowadzony w życie, jeżeli korzystanie z pozyskanych danych zostanie ograniczone wyłącznie do potrzeb realizacji celów związanych z opłatami drogowymi.

Podjęta w fazie testowania projektu decyzja sądu pierwszej instancji (rejonowego) w Gummersbach zezwalająca na udostępnienie danych w przypadku kradzieży samochodu ciężarowego (TIR)⁶ doprowadziła do dodatkowego ustalenia AMG, w myśl którego zgodnie z prawem powstałe w systemie dane w żadnym przypadku nie mogą zostać wykorzystane do celów wynikających z innych ustaw. Bez tego ograniczenia cały system mógłby zostać skazany na niepowodzenie.

Po wydarzeniu z 17 listopada 2005 roku w Badenii-Wirtembergii, gdy jeden z użytkowników parkingu po kłótni o 10 Euro został śmiertelnie potrącony przez zagraniczny samochód ciężarowy, Minister Spraw Wewnętrznych Niemiec Wolfgang Schäuble podniósł na forum publicznym istotny problem dotyczący celowości wykorzystania bazy danych drogowych w działaniach urzędowych związanych z tym wypadkiem. Omawiany przykład wskazuje jednoznacznie, że bazy danych drogowych powinny być również oddane do dyspozycji także dla potrzeb ścigania najcięższych przestępstw drogowych.

Hans Peter Bull, pierwszy Federalny Rzecznik Ochrony Danych w Niemczech, niegdyś zwolennik ograniczenia uprawnień policji do przetwarzania danych, powiedział: „Jeżeli możliwe jest poprzez to schwytanie przestępcy, zmiana prawa jest dozwolona”.⁷ W tym przypadku miał również na myśli znalezienie skradzionych samochodów (w związku z tymi poglądami nie wybrano go na drugą kadencję).

Aby to osiągnąć, konieczna jest nie tyle zmiana ustawy o opłatach, lecz zmiana całej filozofii ustawy. Ponieważ istotna część zgromadzonych danych osobowych w bardzo krótkim czasie musi być usunięta, gdyż nie jest już niezbędna do pobierania opłat, powstaje konieczność stworzenia nowych regulacji prawnych, które nie tylko umożliwią wykorzystanie danych dla celów innych niż te, dla których zostały pozyskane oraz nie dopuszczają do zastosowania ich niezgodnie z przeznaczeniem, a także takich, które umożliwią przechowywanie i gromadzenie ich przez dłuższy okres (np. dla potrzeb realizacji celów bezpieczeństwa).

Współcześnie w tym kierunku zmierza właśnie rozwój telekomunikacji. Po ożywionych dyskusjach, zwłaszcza na temat problemów kompetencyjnych, weszła w życie europejska Dyrektywa, która zobowiązuje operatorów telekomunikacji do przechowywania danych od sześciu miesięcy do roku niezależnie od tego, czy są one jeszcze potrzebne dla ich własnych celów, oraz do udostępniania tych danych dla celów ścigania karnego.⁸

4. Big Brother: zagrożenie „kontrolą totalną”

W decyzji odnoszącej się do GPS Federalny Trybunał Konstytucyjny dostrzegł granice konstytucyjne w aspekcie przetwarzania danych o lokalizacji w ramach „kontroli totalnej” „wraz z którą mógłby zostać sporządzony profil osobowy osoby poddanej takiej kontroli”. To byłoby „zawsze niezgodne z Konstytucją”. Sąd jest wprawdzie zdania, że poddana w wątpliwość kontrola za pomocą GPS danej osoby – podejrzanego – nie narusza istoty jego prawa do prywatności. Jednocześnie za każdym razem powstaje związek między prawem do „osobistego rozwoju zgodnie ze swoją wolą” wskazanym przez skarżącego oraz istotą jego prawa do prywatności,⁹ podkreślaną wielokrotnie w ostatnich latach przez sąd – w tym przypadku poprzez ustalanie i przetwarzanie danych o miejscu pobytu.

Architektura systemu *Toll-Collect* wprowadzając technikę wideo wskazuje na kolejny element, który w przypadku pytania: „Kiedy zostają przekroczone granice kontroli totalnej” ujawnia istotny aspekt sprawy, a mianowicie połączenie danych o lokalizacji z innymi zasobami danych, które z jednej strony pozwalają oprócz określenia miejsca pobytu także na zobrazowanie zachowań w miejscu pobytu.

Biorąc pod uwagę fakt, że nagranie wideo w większości przypadków w przeciągu krótkiego czasu jest kasowane, to zastosowanie tej techniki po niewielkich zmianach w prawie oraz „przełączeniu” systemu w położenie „kontrola totalna” – jest właściwe, abstrahując od możliwości wykorzystania danych z nadużyciem nieprzewidzianego przez ustawę. Zespolecie pozyskanych danych z systemem informacyjnym, np. systemem policji lub systemem Federalnego Urzędu ds. Ruchu Drogowego z wykorzystaniem obecnie wprowadzonej infrastruktury, jest jednakże możliwe do wprowadzenia w przyszłości.

⁶) Sąd rejonowy w Gummersbach, decyzja z dn. 21 sierpnia 2003 r. – 10a Gs 239/03.

⁷) Dziennik z dn. 28 listopada 2005 r., str. 3.

⁸) Projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej, 21 września 2005 r., 2005/0182 (COD).

⁹) Początkowo, bardzo dobitnie w wyroku w sprawie „podsłuchu” z dn. 3 marca 2004, 1 BvR 2378/98.

Z przedstawionych rozważań wynikają obszary zainteresowania, które powinny być przedmiotem dyskusji podczas prowadzonych w ciągu kolejnych lat debat ustawodawczych. W szczególności muszą zostać rozstrzygnięte następujące kwestie:

1. Priorytetowe znaczenie ma zbudowanie infrastruktury komunikacyjno-informacyjnej, a ponadto uwzględnienie zasady oszczędności. Tylko bowiem w sytuacji, gdy dane będą przetwarzane oszczędnie, ryzyko związane z nadużyciem może zostać ograniczone do minimum.
2. Nie do przyjęcia (*de lege lata*) jest stosowanie przez organy ścigania i inne organy bezpieczeństwa przestarzałych (pierwotnych) procedur działania w celu pozyskiwania i przetwarzania danych o lokalizacji.
3. W ocenie Federalnego Trybunału Konstytucyjnego działania z wykorzystaniem GPS musi być uregulowane analogicznie, jak w przypadku nadzoru (kontroli) telekomunikacyjnego. Wynika to zresztą z możliwego do przewidzenia wspólnego rozwoju obu obszarów.
4. Systemy komunikacyjno-informacyjne, które kryją w sobie zagrożenie „kontroli totalnej”, powinny być w miarę możliwości tak ukształtowane, aby wyeliminować niezgodne z przeznaczeniem ich wykorzystanie. Rozwiązania technologiczne należy przemyśleć.
5. W wyjątkowych przypadkach tego rodzaju systemy powinny zostać udostępnione dla celów ścigania i bezpieczeństwa. Istnieje jednak potrzeba jednoznacznych uregulowań prawnych, które będą jasno definiowały sytuacje, w których konkretne dane mogą zostać udostępnione. Rutynowe wykorzystywanie danych o lokalizacji musi zostać wyłączone. Bowiem już taka możliwość mogłaby „rozsadzać” wyznaczone konstytucyjne granice.
6. Połączenie różnego rodzaju technik kontroli (monitoringu) z włączeniem danych o lokalizacji będzie – co do zasady – dotyczyć istoty dóbr osobistych człowieka i będzie wykraczało poza konstytucyjne ograniczenia dla „kontroli totalnej”.

5. Epilog

Podsumowując, należy stwierdzić, że jeżeli nie będzie warunków do wprowadzenia w życie „kontroli totalnej”, to przetwarzanie danych o lokalizacji zawsze może dotyczyć „istoty” praw osobistych. Podobnie sprawa wygląda w sytuacji podsłuchu założonego w domu. Dane o lokalizacji mogą w poszczególnych przypadkach wskazywać na działania, które zaliczają się do tego obszaru, a przez to dane o tych działaniach nie mogą zostać przetworzone.

W ten sposób zamyka się krąg: Adam nie był sam w ogrodzie i po grzechu pierwotnym z pewnością Adam i Ewa postrzegali siebie nie tylko w rajsco-niewinny sposób. Wołanie Pana Boga: „*Gdzie jesteś Adamie?*” byłoby przez to – na podstawie niemieckiej Konstytucji – sprzeczne z prawem.

Dr hab. Małgorzata Gersdorf

Uniwersytet Warszawski, Wydział Prawa i Administracji, Polska
University of Warsaw, Law and Administration Faculty, Poland

Ochrona danych osobowych kandydata do pracy

– problem stale dyskusyjny

Uwagi wprowadzające

Problematyka ochrony danych osobowych pracownika zaczęła pojawiać się w opracowaniach popularyzatorskich wraz z wejściem w życie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.¹ W opracowaniach naukowych rozważania na temat konieczności zapewnienia pracownikom ochrony sfery prywatnej były prowadzone w Polsce znacznie wcześniej. Wystarczy przywołać tu podręczniki profesora Macieja Świąćickiego z 1968 r.², by stwierdzić jak dawno i w jak odmiennych warunkach ustrojowych nauka polskiego prawa pracy widziała już ten problem.³ Jest jednak niewątpliwą zasługą powołanej ustawy i działającego z jej upoważnienia Generalnego Inspektora Ochrony danych Osobowych (GIODO), że problematyka ta została doceniona i jest stale obecna w naszym życiu społecznym i gospodarczym. Stale też pracodawcy borykają się z koniecznością wyznaczenia obszaru dozwolonych informacji o pracownikach, które mogą zbierać i przekazywać innym. Problem staje się coraz trudniejszy w związku z udostępnianiem nowych technik gromadzenia i przetwarzania informacji, z wyposażaniem pracownika w nowoczesne narzędzia pracy, które zdolne są do rejestracji informacji obojętnych dla pracodawcy, jednak pracodawca ten może je pozyskać (np. rejestrator GPS).

Niewątpliwie prawo do ochrony prywatności pracownika i jego rodziny jest częścią ogólnego prawa do ochrony danych osobowych obywatela, u którego podstaw leży ochrona prawna godności i życia prywatnego obywatela. Konieczność objęcia szczególną ochroną pracownika wynika z cech charakterystycznych stosunku pracy. Mamy tu bowiem zawsze do czynienia z typowym konfliktem interesów, który – z uwagi na nierównorzędną rolę partnerów – wymaga specjalnej opieki i ingerencji ustawodawcy i który musi zostać rozwiązany przy wyważeniu racji obu stron stosunku pracy. Pracodawcy dążą – co jest naturalne – do lepszego i szybkiego poznania pracownika. Takie dążenia pracodawców wywołują zrozumiałe obawy pracowników i związków zawodowych przed nowymi zmianami. Pracownicy są zainteresowani tym, by informacje o ich sferze życia poza zawodowego nie były zbierane i przetwarzane poza dopuszczalny zakres upoważnienia zawarty w Kodeksie Pracy.

¹⁾ Tj. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.

²⁾ M. Świąćicki, Prawo pracy, Warszawa 1968, s. 170.

³⁾ por. też M.Gersdorf-Giaro, Recenzja pracy Udo Degenera, *Das Fragerecht des Arbeitsgebers gegenueber Bewerber, Berlin 1975*, PiZS 1977/7/82 i nast.; K.Kolasiński, *Problemy prawne przekazu informacji o pracowniku związane ze zmianą zatrudnienia*, PiZS 1978 /4/30 i nast.; M.Gersdorf-Giaro, *Zawarcie umowy o pracę*, Warszawa 1985, s.82.

Bezsprzecznie także prawo do ochrony kandydata na pracownika jest powiązane, czy wręcz wynika z konieczności zabezpieczenia prawa do prywatności. Przypomnijmy, iż dopiero od 2004 r. Kodeks Pracy w art. 22¹ § 1 ogranicza prawo pracodawcy do zadawania pytań. Na marginesie wypada zaznaczyć, iż przepis ten po raz pierwszy w polskim ustawodawstwie pracy normuje pewien wycinek problematyki rokowań między osobą poszukującą pracy, a ewentualnym pracodawcą. Samo istnienie takiego prawa pracodawcy – jako prosta konsekwencja zasady swobody umów – jest bezsporne. Jednakże zawsze za problematyczny uznawano w literaturze przedmiotu zakres tego uprawnienia. Niekorzystna sytuacja na rynku pracy, wysoki wskaźnik bezrobocia powodowały, iż drogowskazem pracodawcy przy stawianiu kandydatom do pracy określonych pytań stawały się w Polsce w latach ostatnich nie oceny gospodarcze, lecz także inne (polityczne, wyznaniowe, rodzinne). Taka praktyka często prowadziła do dyskryminacji w trakcie przyjmowania do pracy.

Konieczność regulacji tej materii prawnej nie podlegała dyskusji. Dyskusyjny był jedynie zakres wprowadzanych ograniczeń. Norma prawna zawarta w przepisie pozwala na podzielenie wszelkich okoliczności dotyczących życia kandydata na pracownika i pracownika na cztery sfery, a mianowicie sferę identyfikacji personalnej; sferę pracy; sferę tajemnicy osobistej i tajemnicy prywatnej. Prawo zadawania pytań kandydatowi do pracy zostało ustawowo ograniczone do dwu sfer życia, a mianowicie do sfery identyfikacji personalnej (lecz bez konieczności podawania nr PESEL) i sfery pracy, pozostawiając pytania należące do sfery prywatnej i sfery tajemnicy osobistej poza obowiązkiem kandydata do udzielenia na nie odpowiedzi, z wyłączeniem sytuacji, w której przepis szczególny na to zezwala. Jako przepis szczególny można przywołać przykładowo wszystkie regulacje, które wśród rygorów selekcyjnych wymieniają brak karalności.

Konkurs a prawo do ochrony danych osobowych kandydata do pracy

W świetle przedstawionego unormowania rodzi się pytanie, czy pracodawca może żądać od kandydata podania innych jeszcze informacji, jeśli ogłosi konkurs na konkretne stanowisko. Z konkursem w prawie pracy mamy wprost do czynienia przy nawiązaniu stosunku pracy z powołania. Zgodnie z art. 68¹ k.p. powołanie może zostać poprzedzone konkursem, choćby przepis szczególny nie przewidywał wymagania zatrudnienia w drodze konkursu. A zatem możliwość zorganizowania konkursu w celu wyłonienia kandydata na powołanie nie wymaga ustawowej podstawy prawnej. Coraz częściej konkursy są ogłaszane przy naborze pracowników na stanowiska związane z umową o pracę. I taka procedura nawiązywania stosunku pracy jest także dopuszczalna. Wynika to z ogólnej zasady swobody doboru pracowników. Powstaje zatem pytanie, czy warunki konkursu organizowanego przez pracodawcę z własnej inicjatywy, bez szczególnej podstawy prawnej, mogą nakazywać udostępnienie innych informacji zamieszczonych w art. 22¹ § 1 k.p. Zagadnienie to nie zostało bliżej omówione w literaturze przedmiotu. *Prima facie* można powiedzieć, iż kandydat przystępujący do konkursu zna jego warunki i dobrowolnie je przyjmuje, w myśl zasady *volenti non fit iniuria*. Jednakże zawsze pozostaną do rozważenia w takim przypadku te poglądy zgłaszane w piśmiennictwie, w myśl których konieczne staje się wyważenie konfliktu dóbr i interesów obu stron, a sama zgoda kandydata na przekazanie informacji naruszających jego prywatność jest konieczną, a nie wystarczającą przesłanką wyłączenia bezprawności podmiotu za-

trudniającego.⁴ Zawsze też można zastanawiać się, czy ogłoszenie konkursu na obsadzenie stanowiska na podstawie umowy o pracę lub nawet powołania, w sytuacji gdy przepis szczególny nie ustanawia takiego warunku zatrudnienia, nie ma na celu w tym przypadku jedynie obejścia prawa statuującego ochronę prywatności osoby ubiegającej się o pracę. W tym kontekście warto też rozważyć w przyszłości moc wiążącą postanowień układowych odnoszących się do zakresu danych osobowych kandydatów do pracy przyjmowanych z konkursu. W pierwszym rzędzie należałoby odpowiedzieć na pytanie, czy układy zbiorowe pracy, jako źródła prawa pracy, mogą wprowadzać konkurs i warunki jego przeprowadzenia inne niż zawarte w art. 22¹ § 1 k.p.

Zbieranie i przetwarzanie danych o kandydatach na pracowników – jak długo?

Przypomnijmy, iż zasadą jest rejestracja zbioru danych osobowych u Generalnego Inspektora Ochrony Danych Osobowych. Jednakże zbiór danych osobowych pracowników przetwarzany przez pracodawcę nie musi być rejestrowany, co wynika z art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych. W myśl normy prawnej, w przepisie tym zawartej, z obowiązku rejestracji zbioru danych zwolnieni są m.in. administratorzy danych przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się. Nie oznacza to, że zbiór ten nie podlega innym obowiązkom wynikającym z ustawy, a przede wszystkim obowiązkowi należytego zabezpieczenia danych osobowych.

Ustawie podlega także kreowanie zbioru danych osobowych kandydatów do pracy w procesie rekrutacji. A zatem, jeśli przyszły pracodawca tworzy bazę danych o kandydatach ustawa o ochronie danych osobowych znajduje pełne zastosowanie już na etapie tworzenia bazy. Wszelkie bowiem informacje o kandydacie mają przymiot danych osobowych w rozumieniu art. 6 ustawy o ochronie danych osobowych. Przyszły pracodawca musi zatem respektować zasady zbierania danych wyrażone w art. 26 ustawy. Zgodnie z tym przepisem administrator danych (pracodawca) przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

- 1) przetwarzane zgodnie z prawem;
- 2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
- 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
- 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Ponadto powinien respektować obowiązki nałożone na niego przez rozdział 6 wspomnianej ustawy.

W związku z przedstawionymi przepisami powstaje pytanie, czy i jak długo prowadzący nabór do pracy może przechowywać informacje o kandydatach, którzy zgłosili się do pracy? Czy może np. zostawić sobie „w szufladzie” dane osobowe kilku wybranych osób, które potencjalnie spełniają jego wymagania, ale które nie mogły już być zatrud-

⁴ Por. A. Drozd, *Prawo podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, Warszawa 2004, s. 100 i nast. i cyt. tam literatura.

nione w danym momencie? Odpowiedź na postawione pytania jest zasadniczo negatywna. Nie ma możliwości zbyt długiego przetwarzania zbioru danych osobowych sporządzonego w okresie rekrutacji. Warta zaznaczenia w tym kontekście jest wynikająca z art. 26 ustawy o ochronie danych osobowych zasada ograniczenia czasowego przechowywania danych osobowych. Dane osobowe kandydatów mogą być zatem dostępne tylko przez okres do momentu osiągnięcia celu ich zbierania. *Ad casum* celem tym jest przyjęcie do pracy osób wytypowanych w trakcie rekrutacji i ewentualnie okres ten może zostać przedłużony o czas, w jakim kandydaci mogą zaskarżyć decyzje podjęte przez podmiot zatrudniający np. zarzucając mu dyskryminację w przyjmowaniu do pracy. Nie może być zatem tak, że pracodawcy nie rejestrując zbioru ewentualnych kandydatów do pracy, nadal, po rekrutacji, ten zbiór zachowują. Takie działania pracodawców są w praktyce dość częste, jeśli nie nagminne. Być może warto byłoby ocenić rozmiary tego zjawiska.

Protecting the Personal Data of Prospective Employees – an ever-controversial issue

Introductory Remarks

The issues surrounding the protection of personal data began to appear in popularising studies together with the introduction of the Act on the Protection of Personal Data¹ on the 29th August 1997. Scholarly studies deliberating the issue of the need to guarantee employees a level of protection of their private sphere were undertaken in Poland a great deal earlier. It is enough to mention the textbooks of Professor Maciej Świąćicki from 1968² to see how long ago and in what kind of differing political climate Polish scholarly work on Labour Law took place and how the problem was tackled.³ However, it is without doubt largely thanks to the above-mentioned Act and the introduction of the Inspector General for the Protection of Personal Data (GIODO), authorised by the Act that this issue is appreciated and constantly under discussion in our social and economic lives. Employers still have to wrestle with the necessity of defining the area and scope of legal information on employees that they can collect, process and pass on to others. This problem is becoming more difficult to cope with due to the fact that employers have access to new technological tools for collecting and processing of information and employees make use of modern tools that allow the logging of information which is not necessarily important to the employer, although the employer is able to retrieve this data (for example, GPS logging).

Without doubt, the right of the employee to protect his/her own privacy and the privacy of his/her family is part of the general law on the protection of a citizen's personal data, at the heart of which lies the legal protection of citizen's dignity and private life.

The need for the employee to be protected results from the particular nature and characteristics of employment relations between the employer and employee. There is, to a certain extent, a conflict of interests here resulting from an inequality between the two parties. Due to this fact special care and direct intervention from the legislators is needed in order to resolve this inequality by weighing up both sides of these employment relations. The employer, naturally, is always striving for methods of getting to know the employee as speedily and as effectively as possible. This desire as well as any legal amendments or procedural changes that take place is something that both employees and trade unions naturally fear. Employees are concerned that information about their non-professional lives will not be collected and processed beyond what is authorised by the Labour Code.

The right to the protection of personal data of a prospective employee is indisputable and is not only directly linked to, but stems from the necessity for the protection of privacy. It is worth noting that not until 2004 did Article 22¹ § 1 of the Labour Code restrict the rights of the employer to ask questions. It is also worth mentioning that this regulation, for the first time in Polish legislation on employment, regulates one aspect of the issue of negotiation between those seeking employment and the future employer. The very existence of these employer's rights – as a simple consequence of the principle of freedom of contract – is unquestionable. However, the scope of these powers has always been a problematic issue in the literature of the subject. An unfavourable situation in the employment market and a high level of unemployment have led to a situation where in recent years in Poland the milestone for asking a potential employee questions has not been economic factors but a host of others, for example, political, religious or family-related factors. This practice often leads to discrimination in the process of recruitment and employment.

The necessity for this legal matter to be regulated is indisputable. However, the scope of the restrictions that have been introduced is debatable. The legal standard that is found in the regulations permits the division of all the circumstances that concern the life of a prospective employee or employee into four spheres. These are: the sphere of personal identification; working sphere; sphere of personal secrecy; sphere of private secrecy. The right to ask a prospective employee questions is statutorily restricted to two spheres of life, that is the sphere of personal identification (without the necessity of giving one's PESEL identification number) and the working sphere. This means that questions regarding the other two sphere of personal secrecy and private secrecy do not have to be answered by the prospective employee, other than in situations where a particular rule permits it. A particular rule could, for example, be all regulations which within the selection procedure include mention of the lack of a criminal record.

Competitions and the Rights of Prospective Employees for the Protection of Personal Data

In the light of the afore-mentioned standards, a question arises if the employer can demand that the prospective employee gives other additional information if a competition for a particular position is announced. When it comes to such competitions within labour law we are directly dealing with the establishment of employment relations as a form of selection. In accordance with Article 68¹ of the Labour Code selection can be preceded by a competition, although the regulation does not define such employment

¹) Law Gazette 2002 No. 101, 926.

²) M. Świąćicki, *Prawo pracy*, Warsaw 1968, p.170.

³) see also: M. Gersdorf-Giario, Review of Udo Degener, *Das Fragerecht des Arbeitsgebers gegenueber Bewerbern*, Berlin 1975, PiZS 1977/7/82 and also, K. Kolasinski, *Problemy prawne przekazu informacji o pracowniku związane ze zmianą zatrudnienia*, PiZS 1978/4/30, and also, M. Gersdorf-Giario, *Zawarcie umowy o pracę*, Warsaw 1985, p. 82.

requirements by competition. Therefore, the possibility of organising a competition in order to select a prospective employee does not require a statutory basis in law. Competitions are announced with increasing regularity when recruiting potential employees for positions with employment contracts. This kind of procedure of establishing employment relations is also admissible. It results from the principle of freedom of employee selection. A question arises if the conditions of the competition organised by the employer of his/her own initiative, without particular legal foundation, can require that the employee make available information other than that given in Article 22¹ § 1 of the Labour Code. The problem has not been discussed in detail in the literature. It can be said *prima facie* that the prospective employee who decides on entering a competition for a particular post knows the conditions of the competition and freely accepts them according to the principle *volenti non fit iniuria*. However, in this situation it is worth considering the opinions found in the literature, the intention being that there is a need to weigh up the conflict of the rights and interests of both parties. The consent alone of the prospective employee for divulging information that impinges on his/her privacy is not a sufficient but necessary factor to negate the unlawful nature of the employing institution.⁴ One can always deliberate whether the announcement of a competition for a particular position with an employment contract or selection in a situation where a particular rule does not regulate the conditions of employment is simply a way of circumventing the statutory law which protects the privacy of an individual seeking employment. In this context, it is also worth considering the binding power of ruling of agreement relating to the scope of personal data of prospective employees being employed through competition. One needs to, firstly, clarify whether collective employment agreements, as a source of labour law, can initiate competitions and the conditions in which they are carried out differently from what is included in Article 22¹ § 1 of the Labour Code.

Collecting and Processing Data on Prospective Employees – How Long?

It is worth remembering that in principle an employer should register personal data files with the Inspector General for the Protection of Personal Data (GIODO). However, such files including employees' personal data that are processed by employers do not have to be legally registered which follows from Article 43 (1), point 4 of the Act on the Protection of Personal Data. The idea behind the legal standard as put forward in this regulation is that some people are exempt from the registration of data files. This includes controllers processing data, those providing services for them employed on civil legal contract, as well as people associated with them or students. This does not mean that the data file is not subject to other obligations following from the Act or the appropriate security measures and protection of the personal data found therein. The creation of file of personal data on prospective employees as part of the recruitment process is also subject to the Act. Therefore, should a future employer create a database on prospective employees, the Act on the Protection of Personal Data can be applied in full at this phase of database development. All information about prospective employees has the attribute of personal data in the understanding of Article 6 of the Act on the Protection of Personal Data. A future employer must respect the principles

of collecting data as expressed in Article 26 of the Act. In accordance with this regulation, a data controller (the employer) who processes data should make every effort to protect the interests of the individuals whose data is concerned and, in particular, is obliged to ensure that the data is:

- 1) processed in accordance with the law;
- 2) collected for a predetermined goal in accordance with the law and is not released for additional processing which is inconsistent with these goals;
- 3) correct with regards to content and appropriate in relation to the goals required for processing;
- 4) stored in a form which allows the identification of the individual whose personal data it is and stored no longer than it is necessary for the completion of the intended initial goals of the processing.

Furthermore, the employer should respect the responsibilities imposed on him/her by Chapter 6 of the afore-mentioned Act.

An important question beckons in relation to the above-mentioned regulations: can someone who is recruiting prospective employees keep hold of information on candidates who have applied for the job and how long can they hold this information? Can a recruiter file a candidate's personal information "in a drawer" if the prospective employee meets his/her requirements but cannot at this point of time be employed? The answer to both questions is without doubt in the negative. There is absolutely no possibility for personal data, which has been collected during the recruitment process, to be processed for an excessively long period of time. It is worth noting the principle of time restriction concerning the storage of personal data resulting from Article 26 of the Act on the Protection of Personal Data. The personal data of prospective employees can only be available up to the moment that the initial goal of collecting this data is achieved. The *ad casum* goal is the hiring of a new member of the personnel selected through the process of recruitment. This time scale can be extended if need be, for prospective employees to appeal against the decision undertaken by the employing company (on the grounds of, for example, discrimination). However, there is no possibility for an employer, who has created a database of information on prospective employees, to keep hold of this database after the recruitment process has come to an end. In practice, such a situation is quite common, if not very common. It would be noteworthy, therefore, to ascertain the scale of this phenomenon.

⁴⁾ A. Drozd, *Prawo podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, Warsaw 2004, p. 100.

Billy Hawkes

Data Protection Commissioner, Ireland
Rzecznik Ochrony Danych, Irlandia

Data Protection: the experience of a small EU Member State

Introduction

Ar scáth a chéile a mhaireann na daoine.

This Irish proverb – it roughly translates as “People live in one another’s shadow” – offers interesting insights into the challenges surrounding data protection, especially in a small and fairly thinly populated country like Ireland.

Irish people value their privacy – particularly in relation to the State. But they are also (notoriously!) sociable, with lots of inter-personal contact, not only within families and work-places, but with relative strangers in such environments as the pub. Despite this sociability, Irish people are quite good at keeping aspects of their personal lives private. The challenge for data protection is to respect and reinforce this preference, while also acknowledging the inevitability of increased data flows arising from the use of new technologies – notably the mobile phone where Irish usage surpasses that of most other EU countries.

How important is Privacy?

Privacy advocates (including data protection commissioners) repeatedly assert the importance of privacy in society. But we also know that people attach importance to other issues than can sometimes be – or appear to be – hard to reconcile with privacy. Obvious examples include security, ease of communication and electronic payment systems.

In order to get an objective view on this, we recently commissioned a survey from a professional market research company.

Is privacy important?	important	very important
Crime Prevention	7%	91%
Personal Privacy	9%	89%
Consumer protection	12%	85%
Workplace equality	11%	82%
Ethics in public office	14%	78%

The results of the most recent survey, carried out in November 2005, show that privacy is ranked as very important by Irish people – second in importance only to crime prevention. The results also showed that the importance of privacy had increased since the last comparable survey was carried out in 2002.

Privacy most important in relation to:

1. Financial records
2. Medical Records
3. PPS Number
4. Credit Card Details
5. Telephone No.
6. Home Address
7. Date of Birth
8. Marital Status

The survey was also interesting in revealing the **relative** importance that people attach to privacy in relation to different aspects of their lives. It is interesting that financial records – which are not regarded as “sensitive” personal information under data protection law – top the list of people’s concerns about privacy. It is also interesting that people are concerned about the confidentiality of their PPS number (the most common identifier used in the public service).

The survey also revealed unhappiness in relation to unsolicited direct marketing (especially “cold calling” by telephone) – 52% of respondents indicated that they were “not at all happy” with such intrusive marketing.

Promoting Privacy Awareness

As surveys show that Irish people value their privacy, a key challenge for the Commissioner’s Office is how to get across the message that the law gives them strong rights in this area. In order to promote such awareness, we have been running a publicity campaign on buses, trains etc. drawing attention to people’s rights to data privacy. This campaign has had some success – one out of 4 persons interviewed for the public awareness survey had seen the advertisements.

We have also been trying to increase awareness among young people. Data protection is included in the Business Studies curriculum, which many secondary students study. A data protection module is also due to be introduced shortly into the Civil, Political and Social Education curriculum, which most secondary students take.

The relative lack of data protection awareness among less educated people is also being targeted, both through the public advertising campaign and through focussed activity with Citizens Information Centres.

Despite these activities, it is clear that much remains to be done to increase data protection awareness in the general population.

International Activity

As a small EU Member State, it is a tremendously useful and enriching experience to be able to draw on the combined wisdom of colleagues in forums such as the Article 29 Committee. Being an advocate for privacy is oftentimes a lonely and isolating experience. Especially at times – such as in recent years – when the right to privacy has often seen to be brushed aside in pursuit of what are seen as more pressing priorities such as State security, it is at least comforting to regularly meet up with peers who are facing the same pressures. The collective will of the privacy and data protection commissioners to insist that privacy is not a luxury to be brushed aside can give a much-needed morale boost to individual commissioners, as they return to their countries to again “take up the cudgels” on behalf of the right to privacy.

The entry of 10 new Member States from the Eastern part of Europe has brought a welcome new and fresh perspective to bear on the work of the EU in the area of data and privacy protection. As memories fade in “old” Europe of the State’s capacity, left unchecked, to invade the “personal space” in a way that undermines any reasonable concept of democracy, the new Member States brought with them fresh memories of the violence to personal dignity that can be inflicted by systems that do not have privacy built in as a foundation of an acceptable way of living. Following the initial and inevitable “bedding down” period, their experience is likely to weigh more heavily on EU deliberations in a way that can only enhance their depth and credibility. This has been very obvious in the case of the Police Working Party which has been guided so ably by the distinguished Data Protection Commissioner from Poland, Dr. Ewa Kulesza.

But even more important are the thoughtful and insightful Opinions and Working Papers that the Article 29 Committee produces. For a small Member State with limited resources for research, these provide an essential aid to interpreting the right to privacy as it applies in new contexts. In themselves, the Opinions also represent an invaluable resource to others who seek a balancing privacy-related view to the alternative securocratic or technocratic agendas being urged upon them. The value of the Opinions in alerting key players – the European Parliament, national Parliaments, the general public – to the often unnoticed privacy issues that lie hidden in many policy initiatives cannot be underestimated.

While membership of the Article 29 Working Group is a crucial forum for a commissioner from an EU Member State, the activities of the Article 29 Working Group are further enriched by the contributions from the broader family of privacy commissioners in other European States and further afield. These provide an essential broadening experience to what might sometimes seem the excessively EU-centric attitude of Article 29.

Outside the ‘family’ of Data Protection Commissioners, there is the broader family of democratic nations who attach value to privacy as a crucial component of a democratic society but choose to achieve it in a different way. While many may see in the EU model an ideal of privacy protection, it is essential to be open to other ideas of how to achieve privacy protection in a democratic society. Examples from the United States, such as California’s Information Practices Act, show that there are alternative ways of approaching data protection which might usefully be considered in Europe.

The Future?

George Orwell’s book 1984 predicted the possibility of a totalitarian state where even people’s thoughts would not be private. Fortunately, that prediction has not come true but there is no doubt that the advances in technology have been a double edged sword. We have more access to information than ever but when we use technology such as e-mail or the Internet we can sometimes be leaving ourselves open to exposure.

The increased risk of terrorist attacks has led to stringent measures being taken to protect the public. Travellers are more keenly vetted and the use of biometrics to check identity has been seen as intrusive by some. Although we will hopefully never have an Orwellian state, increased security measures will see us disclosing more personal information about ourselves.

Nobody knows what new technological advances will have been made in 30 years time. 30 years ago nobody would have imagined that we could carry a personal phone in our pocket or that we could use the computer to send letters that would arrive immediately. However, technological advances should not interfere with our basic right to privacy of our personal information – we are still a democracy.

The challenge for data protection commissioners is to insist on the right to privacy as a fundamental of a democratic society, while recognising that people’s views of what constitutes invasion of privacy can vary over time. Many people are willing to surrender some of their privacy, in exchange for better service either from private companies or from the State. As long as this is an informed choice, with appropriate safeguards, data protection commissioners should not “get in the way”, as it were, of what people want.

This paper started with a quote from the wisdom of an ancient Irish proverb. A more modern ‘prophet’, Bob Geldof, also had something to say about the threat to privacy in his song “Someone’s Looking at You”. His rather sardonic view of the subject neatly captures the ambiguities involved in protecting privacy:

*On a night like this I deserve to get kissed at least once or twice
You come over to my place screaming blue murder, needing someplace to hide.
Well, I wish you'd keep quiet,
Imaginations run riot,
In these paper-thin walls.
And when the place comes ablaze with a thousand dropped names
I don't know who to call.
But I got a friend over there in the government block
And he knows the situation and he's taking stock,
I think I'll call him up now
Put him on the spot, tonight.*

*They saw me there in the square when I was shooting my mouth off
About saving some fish.
Now could that be construed as some radical's views or some liberals' wish.*

And it's so hot outside,
And the air is so sweet,
And when the pressure drop is heavy I don't wanna hear you speak.
You know most killing is committed at 90 degrees.
When it's too hot to breathe
And it's too hot to think.

There's always someone looking at you.
S-s-s-s-someone.
They're looking at you.

And I wish you'd stop whispering.
Don't flatter yourself, nobody's listening.
Still it makes me nervous, those things you say.
You may as well
Shout it from the roof
Scream it from your lungs
Spit it from your mouth
There's a spy in the sky
There's a noise on the wire
There's a tap on the line
And for every paranoid's desire...

There's always Someone
looking at you.
S-s-s-s-someone looking at you...
They're always looking at you.

(written by Bob Geldof – taken from the album "The fine art of surfacing")

Ochrona danych: doświadczenia małego Państwa Członkowskiego Unii Europejskiej

Wstęp

Ar scáth a chéile a mhaireann na daoine.

To przysłowie irlandzkie, które w tłumaczeniu brzmi: „Ludzie żyją w cieniu innych” – daje interesujący pogląd na kwestie dotyczące ochrony danych, zwłaszcza w małym i dość słabo zaludnionym kraju, jakim jest Irlandia.

Irlandczycy cenią sobie swoją prywatność, zwłaszcza w relacjach z państwem. Jednakże są również (z natury!) towarzyscy, utrzymują wiele interpersonalnych kontaktów, nie tylko w kręgu swojej rodziny czy miejscu pracy, ale także w takim miejscu, jak pub. Mimo to potrafią zachować w dużym stopniu swoją prywatność w pewnych dziedzinach

życia osobistego. Wyzwaniem dla ochrony danych jest więc respektowanie i umacnianie tych preferencji, przy jednoczesnym uznaniu nieuchronności obiegu danych wynikającej z rozwoju nowych technologii – zwłaszcza telefonii komórkowej. Liczbą użytkowanych telefonów Irlandia przewyższa bowiem większość państw Unii Europejskiej.

Jak ważna jest prywatność?

Zwolennicy prywatności (wliczając komisarzy ochrony danych) regularnie podkreślają znaczenie prywatności w społeczeństwie. Jednakże wiemy również, że ludzie przywiązują wagę do innych spraw, które niekiedy mogą być – bądź wydają się – trudne do pogodzenia z prawem do prywatności. Oczywiście tego przykłady to środki bezpieczeństwa oraz wygoda w korzystaniu z systemów komunikacji i elektronicznych systemów płatności.

W celu obiektywnego spojrzenia na tę sprawę, niedawno zleciliśmy przeprowadzenie ankiety przez profesjonalną firmę zajmującą się badaniem rynku.

Czy prywatność jest ważna?		
	ważna	bardzo ważna
Zapobieganie przestępczości	7%	91%
Prywatność osobista	9%	89%
Ochrona konsumenta	12%	85%
Równość w miejscu pracy	11%	82%
Etyka w urzędach publicznych	14%	78%

Wyniki ostatniego sondażu przeprowadzonego w listopadzie 2005 r. wskazują, że dla Irlandczyków prywatność jest bardzo ważna – sklasyfikowana została na drugim miejscu, zaraz po zapobieganiu przestępczości. Rezultaty te odzwierciedlają również fakt, że od czasu ostatniego sondażu przeprowadzonego w 2002 r. przywiązują oni coraz większą wagę do prywatności.

Najważniejsze dziedziny ochrony prywatności

1. Dane finansowe
2. Dane medyczne
3. Numer PPS
4. Dane na karcie kredytowej
5. Numer telefonu
6. Adres domowy
7. Data urodzenia
8. Stan cywilny

Sondaż ten był interesujący również z innego względu. Ujawnił bowiem, że ludzie przywiązują **relatywną** wagę do prywatności w różnych dziedzinach ich życia. Na przykład dane finansowe, które nie należą w regulacjach prawnych dotyczących danych osobowych do kategorii danych „szczególnych”, znalazły się na czele listy. Ciekawie

wy jest również fakt, że ludzie martwią się o poufność numeru PPS (powszechny identyfikator stosowany w służbie publicznej).

Sondaż ten ujawnił ponadto, że Irlandczykom nie podoba się stosowanie metod „niezamawianego” marketingu bezpośredniego (zwłaszcza „nagabywanie” telefoniczne – 52% ankietowanych odpowiedziało, że „w ogóle nie byli zadowoleni” ze stosowania wobec nich takiej formy natrętnego marketingu).

Kształtowanie świadomości w sferze ochrony prywatności

Według przeprowadzonych sondaży, Irlandczycy cenią sobie prywatność. Podstawowym wyzwaniem dla Biura Komisarza jest zatem znalezienie sposobu dotarcia do społeczeństwa z informacją, że w tej dziedzinie zostały ustanowione solidne podstawy prawne. W celu kształtowania tej świadomości prowadzimy kampanię publiczną w autobusach, pociągach itd. Staramy się zwrócić uwagę ludzi na przysługujące im prawo do prywatności. Kampania ta odniosła pewien sukces – jedna na cztery pytane osoby zauważyła plakaty informacyjne.

Staramy się również kształtować świadomość w tej dziedzinie wśród młodych ludzi. Zajęcia poświęcone zagadnieniom ochrony danych są włączone do programu nauczania na temat biznesu, który wybiera wielu uczniów szkół średnich. Ponadto wkrótce zajęcia z tej dziedziny zostaną włączone do programu nauczania na temat edukacji obywatelskiej, politycznej i społecznej, w którym uczestniczy większość uczniów szkół średnich.

Publiczne kampanie reklamowe oraz działania ośrodków informacyjnych (Citizens Information Centres) są również ukierunkowane na pogłębianie wiedzy z zakresu ochrony danych wśród mniej wykształconych obywateli.

Mimo podjęcia tych kroków, jest jeszcze wiele do zrobienia w dziedzinie kształtowania świadomości społeczeństwa na temat ochrony danych.

Działalność międzynarodowa

Ponieważ Irlandia jest niewielkim Państwem Członkowskim UE, niezwykle ważnym i wzbogacającym doświadczeniem jest dla nas możliwość czerpania z wiedzy kolegów dzięki udziałowi w działaniach, na przykład, Grupy Roboczej Art. 29. Promowanie prawa do prywatności oznacza często działanie w pojedynkę. Zwłaszcza w czasach – takich jak ostatnie lata – kiedy prawo do prywatności często jest odsuwane na bok ze względu na priorytety, do których należy m.in. bezpieczeństwo państwa. Pociągającym jest przynajmniej fakt, że można spotykać się regularnie z kolegami, którzy borykają się z podobnymi trudnościami. Kolektywne dążenie komisarzy ochrony prywatności i danych, by stać na stanowisku, że prywatność nie jest luksusem, który można odłożyć na bok, może w takim stopniu wpłynąć na morale poszczególnych komisarzy, że po powrocie do kraju podejmą wysiłek na rzecz ochrony prawa do prywatności.

Przystąpienie 10 nowych Państw Członkowskich ze wschodniej części Europy przyczyniło się do nowego spojrzenia na działania UE w dziedzinie ochrony danych i ochrony prywatności. Ponieważ w „starej” Europie wspomnienia dotyczące uprawnień państwa – pozostawionych bez kontroli – do ingerowania w „prywatną przestrzeń” jednostki w

sposób, który przekracza jakiegokolwiek rozsądne granice demokracji, są coraz słabsze, nowe Państwa Członkowskie przedstawiają świeże przykłady naruszania godności osobistej przez systemy, dla których prywatność nie jest fundamentalną wartością. Ich doświadczenia będą miały prawdopodobnie duży wpływ na obrady UE i to w sposób, który może tylko zwiększyć słuszność przyjmowanych rozwiązań. Było tak w przypadku Grupy Roboczej ds. przetwarzania danych osobowych w sektorze policji kierowanej bardzo umiejętnie przez dr Ewę Kuleszę, wybitnego Inspektora Ochrony Danych z Polski.

Jednak ważniejsze są rozsądne oraz wnikliwe opinie i dokumenty Grupy Roboczej Art. 29. Dla małego Państwa Członkowskiego, które ma ograniczone środki na prowadzenie badań, stanowią one znaczną pomoc w interpretacji prawa do prywatności, kiedy jest ono stosowane w nowym kontekście. Same w sobie opinie te stanowią nieocenione źródło dla tych, którzy szukają zrównoważonego spojrzenia na kwestie dotyczące prywatności w stosunku do alternatywnego podejścia z punktu widzenia ochrony czy technokratycznego potraktowania tematu, do czego się ich zachęca. Nie można nie doceniać wartości tych dokumentów we wskazywaniu tak istotnym organom, jak Parlament Europejski, krajowe parlamenty czy wreszcie społeczeństwo – często niezauważanych kwestii dotyczących prywatności, które są ukryte w wielu inicjatywach ich polityki.

Grupa Robocza Art. 29 to zasadnicze forum dla komisarzy z Państw Członkowskich UE, rozwijające również współpracę z komisarzami do spraw prywatności z innych państw europejskich i nie tylko. Dzięki temu zyskuje się nowe, szersze spojrzenie na zagadnienie prywatności, wykraczające poza nadmiernie eurocentryczny punkt widzenia, ograniczający się jedynie do krajów UE.

Poza „rodziną” komisarzy ochrony danych, istnieje także duża grupa państw demokratycznych, które przywiązują wagę do prywatności jako podstawowego wyznacznika społeczeństwa demokratycznego, jednakże wybierają inną drogę osiągnięcia celu. Tymczasem wiele osób postrzega model obowiązujący w Unii Europejskiej jako idealny. Ważne jest jednak to, aby być otwartym na nowe pomysły dotyczące ochrony prywatności w społeczeństwie demokratycznym. Przykłady można zaczerpnąć ze Stanów Zjednoczonych. Ustawa obowiązująca w Kalifornii („Information Practices Act”) wskazuje, że istnieją alternatywne sposoby podejścia do tego zagadnienia, które z pożytkiem można rozważyć w Europie.

Jaka przyszłość?

W książce „Rok 1984” George Orwell przewidział możliwość powstania państwa totalitarnego, w którym nawet ludzkie myśli nie byłyby prywatne. Na szczęście przewidywania te nie sprawdziły się, ale bez wątpienia postęp w rozwoju technologii to „miecz obosieczny”. Mamy większy dostęp do informacji niż kiedykolwiek dotychczas, jednak kiedy korzystamy z takich technologii, jak e-mail czy Internet, niekiedy sami się narażamy.

Większe zagrożenie atakami terrorystycznymi spowodowało wprowadzenie bardziej rygorystycznych procedur w celu ochrony społeczeństwa. Osoby podróżujące są dokładniej kontrolowane, natomiast stosowanie biometrii do sprawdzania tożsamości przez niektórych jest traktowane jako niepożądane zjawisko. Chociaż, miejmy nadzieję, nigdy nie będziemy żyć w państwie orwellowskim, zwiększone środki bezpieczeństwa spowodują, że będziemy ujawniać więcej danych osobowych.

Nikt nie może przewidzieć, jaki postęp technologiczny nastąpi za 30 lat. 30 lat temu nikt nie wyobrażał sobie, że będzie nosił osobisty telefon w kieszeni albo, że będzie mógł korzystać z komputera, czy też wysyłać listy, które natychmiast dotrą do adresata. Przy tym jednak rozwój technologii nie powinien kolidować z naszym podstawowym prawem do prywatności danych osobowych – ciągle mamy demokrację.

Wyzwaniem dla komisarzy ochrony danych jest domaganie się, aby prawo do prywatności stanowiło fundament społeczeństwa demokratycznego. Należy jednocześnie zauważyć, że z biegiem czasu poglądy ludzi na to, co jest naruszeniem ich prywatności, mogą się zmieniać. Wiele osób jest gotowych zrzec się części swojej prywatności w zamian za lepsze usługi świadczone przez przedsiębiorstwa prywatne bądź też państwo. Jak długo jest to świadomy wybór, z odpowiednimi środkami zabezpieczenia, komisarze ochrony danych nie powinni „wchodzić w drogę”, gdyż tego właśnie oczekują ludzie.

Wystąpienie swe rozpocząłem cytatem – starym irlandzkim przysłowiem. Zakończę odniesieniem do piosenki. Współczesny „prorok” Bob Geldof miał również coś do powiedzenia na temat zagrożenia prywatności w swoim utworze „Someone’s Looking at You” [„Ktoś patrzy na Ciebie”]. Jego, raczej sardoniczne, spojrzenie na tę kwestię trafnie oddaje niejasności, które dotyczą ochrony prywatności.

*W taką noc zasługuję na jeden lub dwa pocałunki
Przychodzisz do mnie krzycząc jak opętana, szukasz schronienia.
Wolałbym żebyś była cicho,
Wyobraźnia szaleje,
A ściany są tu cienkie jak papier.
A gdy rozpalasz to miejsce rzucając tysiące imion
Nie wiem do kogo dzwonić.
Ale mam przyjaciela w rządowym bloku
On zna sytuację i potrafi ją ocenić,
Chyba zadzwonię do niego
Wyjaśnię mu to dziś wieczorem.*

*Widzieli mnie tam, na placu, gdy krzyczałem
O ratowaniu ryb.
Czy to można uznać za radykalne poglądy albo za życzenia liberała.
Na dworze jest tak gorąco,
A powietrze tak przyjemne,
A kiedy spada ciśnienie nie chcę cię już słuchać.
Wiesz, większość morderstw popełnia się przy 30 stopniowym upale.
Kiedy jest za gorąco żeby oddychać
I za gorąco by myśleć.*

*Zawsze jest ktoś kto patrzy na ciebie.
Ktoś.
Oni patrzą na ciebie.*

*Przestań wreszcie szeptać.
Nie łudź się i tak nikt nie słucha*

*Ale i tak to co mówisz denerwuje mnie.
Możesz równie dobrze
Wykrzyczeć to stojąc na dachu
Wykrzyczeć to z płuc
Wypluć to z ust
Na niebie jest szpieg
Na linii jest szum
Jest podsłuch na linii
Jest coś dla każdego paranoika...*

*Zawsze jest ktoś, kto patrzy na ciebie
Ktoś patrzy na ciebie...
Oni zawsze patrzą na ciebie.*

Słowa: Bob Geldof – z albumu „The fine art of surfacing” [„Sztuka utrzymywania się na powierzchni”]

Peter J. Hustinx

European Data Protection Supervisor
Europejski Inspektor Ochrony Danych

A Framework in Development: Third Pillar and Data Protection

Introduction

During her period in office as the first Polish Inspector General for Personal Data Protection, Dr Ewa Kulesza displayed a great sense for international relations. This went beyond a close cooperation with colleagues in the middle and Eastern Europe. Just a short selection of events to illustrate: I had the pleasure of being invited for a visit to Warsaw in May 2004, the first month of Poland's full membership of the European Union. In September 2004, the Polish Inspector General hosted the 26th International Conference on Privacy and Personal Data Protection in Wroclaw. In April 2005, she hosted the annual Spring Conference of European Data Protection Commissioners in Krakow. In May 2006, shortly before the end of her second term, she will be hosting a conference in Warsaw on "Public Security and Data Protection", at which many European colleagues will be present again.

This certainly suggests a special interest for a subject that also featured prominently both in Wroclaw and in Krakow. The key documents adopted at these conferences have influenced developments in Europe. It is appropriate therefore to give a brief overview of developments in a publication that intends to be a tribute to Dr Ewa Kulesza and her contributions to data protection.

Third Pillar

The term "Third Pillar" refers to the pillar structure of the European Union, introduced in the Treaty of Maastricht (1992). At that stage, it dealt with the cooperation in the field of justice and home affairs. This cooperation was restructured in the Treaty of Amsterdam (1997). The progressive establishment of an "area of freedom, security and justice" became an objective of the First Pillar, and provisions on visas, asylum, immigration and judicial cooperation in civil matters are now laid down in Title IV of the EC Treaty. The objective to provide citizens with a high level of safety within an area of freedom, security and justice, especially by developing common action in the field of police and judicial cooperation in criminal matters, remained as the Third Pillar in Title VI of the EU Treaty. The activities in the area of freedom, security and justice as a whole have picked up speed after the conclusions of the European Council of Tampere (1999). A new five-year programme was adopted in November 2004 as the Hague Programme. This will, no doubt, lead to a further increase of activities, also in the Third Pillar.

At this point, it is important to realize that the Third Pillar suffers from a number of structural problems. Firstly, any action in this pillar is intergovernmental and can thus only come about, if Member States are unanimous. This means that decision making is not easy and often leads to a weak compromise. Secondly, the role of the European Parliament is still limited. Under Article 39 of the EU Treaty, the Parliament only has the right to be consulted, and the Council is free to ignore and sometimes even to act without the opinion of the Parliament, if it wants to do so. Thirdly, the judicial control by the Court of Justice is also incomplete. Under Article 35 of the EU Treaty, the Court does not have jurisdiction insofar as the maintenance of law and order and the safeguarding of internal security are at stake. Fourthly, the implementation of the EU rules on the national level is problematic, and can often not be enforced or challenged before the courts. Finally, there is a great lack of transparency, and relevant information often comes late and only piecemeal. Most of these problems would be solved by the Constitutional Treaty, but this is not a reality for the near future.

When it comes to the advisory role of data protection authorities, present arrangements are also unsatisfactory. The European Commission has confirmed that it feels bound by Article 28(2) of Regulation (EC) 45/2001 to consult the European Data Protection Supervisor (EDPS) when it adopts a proposal for legislation with an impact on the protection of personal data, but its right of legislative initiative is shared with Member States not bound by such an obligation. Arrangements for a systematic input from national data protection authorities are even less adequate. It is for this reason that the European Conference of Data Protection Commissioners adopted a resolution in Wroclaw in September 2004 to request the setting up of a joint forum on data protection in the Third Pillar to ensure a systematic input from their side in decision making.

As to general provisions on data protection, it should be noted that Directive 95/46/EC does not apply, since activities such as those provided for by Title VI of the EU Treaty have been excluded in Article 3(2). The Council of Europe's Convention 108 has been ratified by all Member States of the EU, but its provisions apply only indirectly to the Union itself under Article 6 of the EU Treaty. Convention 108, although considered as too general for specific use, has been referred to in several instruments as a relevant standard for data protection in the Third Pillar. This happened first in the Schengen Convention (1990), also in the Europol Convention (1995) and finally in the Council Decision setting up Eurojust (2002). Schengen was incorporated in the EU framework by the Treaty of Amsterdam, but Europol and Eurojust developed in the Third Pillar at different stages. Each of these instruments contained specific measures on data protection, only applicable in that context and not necessarily consistent with each other. The absence of general rules in the Third Pillar was a problem in each case.

Exchange of data

The need for a common framework of rules has become more evident in recent years due to an increasing interest for exchange of personal data between law enforcement authorities in different Member States. Apart from specific incidents, suggesting lack of cooperation and exchange of information, this follows from a simple logic. Police and judicial cooperation in criminal matters is approaching a stage in which exchange of data and direct access to data "across borders" are becoming more and

more essential for law enforcement in "high profile" areas. It is for this reason that the Hague Programme has put a great emphasis on the exchange of data under the principle of "availability". This means that information that is available to certain authorities in a Member State must also be provided to equivalent authorities in other Member States.

It is emphasized in the Hague Programme that such arrangements should be subject to adequate safeguards for data protection. It is not hard to see that law enforcement in different Member States will become more interrelated and mutually dependent, when it comes to verification of compliance with rules on fair and lawful collection, data quality, security etc. Adequate rules on data protection, followed by good practices, will thus build "trust" between authorities in different countries and contribute to better cooperation across borders in criminal matters. It is clear that adequate common standards on data protection will be more than safeguards in these cases; they should also be considered as essential conditions for effective cooperation.

There have been quite a few initiatives in recent years, both in and outside the EU framework, to promote the exchange of police information between different countries. In June 2004, Sweden proposed a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States. In May 2005, seven Member States signed a Convention in Prüm (Germany) on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. It introduces *inter alia* measures to improve information exchange for DNA and fingerprints, and is open for any other Member State to join. The aim is to incorporate the Convention into the legal framework of the EU. This comes in addition to other initiatives, such as proposals for a second generation Schengen Information System (SIS II), and recently also a proposal for a Framework Decision on the exchange of information under the principle of availability, as a general follow up to this part of the Hague Programme. These different initiatives are not necessarily consistent, nor has a consistent approach to data protection been guaranteed as yet.

Data protection

After their meeting in Wrocław, in September 2004, the European Data Protection Authorities continued their work on data protection in the Third Pillar. At the Spring Conference in Krakow, in April 2005, this resulted in the adoption of a position paper on Law Enforcement and Information Exchange in the EU, setting out the main elements of a general legal framework for data protection in the Third Pillar. The position paper was annexed to a Declaration with a clear message. It emphasized, first of all, that initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection. The Declaration also emphasized that a set of rules applicable to law enforcement activities should be consistent with the current level of data protection in the First Pillar. The standard of data protection found in Directive 95/46/EC should therefore serve as a basis for the development of appropriate rules in the Third Pillar.

The European Commission made good use of the input provided in the Krakow Declaration and the position paper. In October 2005, it adopted a proposal for a Framework

Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This proposal follows the approach of Directive 95/46/EC in many ways and the position paper is referred to at different points in the explanatory memorandum. The proposal is now subject of discussion in a working group of the Council and in the LIBE Committee of the European Parliament. The EDPS published an opinion in December 2005. The European Conference adopted the opinion shortly after the meeting in January 2006 under Polish presidency. Both welcome the proposal of the Commission and support its main lines, but suggest improvements on various details. It is quite likely that many of these suggestions will be taken up by the European Parliament. Both the Parliament and the Council are presently dealing with the proposal as an urgent priority.

Taking a closer look at the present state of play, it should be noted first that the need for rules on data protection in the Third Pillar does not seem to be contested or doubted any longer. The European Parliament has called for a Commission proposal many times, but the Council has been much more reluctant so far. It is fair to assume that the discussions about data exchange in general and the principle of availability more specifically have led to a change of mind in most circles in the Council. However, the fact that the Framework Decision can only be adopted by unanimity should give reason for some caution as to its final content and timing.

A more relevant issue at this stage is the scope of the proposal. According to Article 1(1), the proposal intends to determine "common standards" to ensure the protection of personal data in the course of activities of police and judicial cooperation in criminal matters. According to Article 3(1), the proposal shall apply to "the processing of personal data (.....) by a competent authority for the purpose of prevention, investigation, detection and prosecution of criminal offences". It follows from these provisions that the proposed Framework Decision has two main characteristics: it sets common standards and it applies to all processing for the purpose of criminal law enforcement, even if the data concerned have not been transmitted or made available by authorities in other Member States.

The opinions of the EDPS and the European Conference have underlined the importance of these characteristics. This approach would result in a legal framework for data protection in the Third Pillar that fully complements the present legal framework in the First Pillar. This would also be the case for "purely domestic" situations, and this might give rise to difficult discussions in the Council. However, it should be emphasized that any limitation to "data that are transmitted or made available to authorities in other Member States" would make the field of application of the Framework Decision particularly unsure and uncertain, which would be contrary to its essential objective. Harm would be done to the legal certainty of individuals. Under normal circumstances, one never knows in advance if personal data will be relevant for an exchange with competent authorities in other Member States. It would also be difficult to use different standards, distinguishing on the basis of the origin of personal data. This would most certainly lead to great practical problems in the context of the principle of availability and the abolishment of internal borders for the exchange of law enforcement data.

In the recent opinion, the Legal Service of the Council has concluded that Articles 30, 31 and 34(2)(b) of the EU Treaty provide for the necessary legal basis to allow the Council

to adopt the Framework Decision on the protection of personal data covering also processing of data in purely domestic situations. This means that it is up to the Council to decide to what extent it wishes to use its competence under these provisions.

Another issue of scope is whether the proposal should also apply to Europol and Eurojust. It should be noted first that the Framework Decision under Article 34(2)(b) of the EU Treaty can only be adopted for the purpose of approximation of the laws and regulations of the Member States and therefore as a matter of principle cannot be directed to bodies like Europol and Eurojust. At the same time, it is desirable that the rules that presently apply to them are made fully consistent with the new rules, as soon as possible. This could also be an occasion for some horizontal harmonization. In the case of SIS II, it is already assumed that the proposed Framework Decision will be part of the general framework ("*lex generalis*") after its adoption.

The substance of the proposal raises many other interesting issues – commented upon in the opinions of the EDPS and the European Conference – but a further discussion would exceed the scope of this article.

Availability

The EDPS has recently also issued an opinion on the Commission proposal for a Framework Decision on the exchange of information under the principle of availability. The opinion calls for a better analysis of the principle, and for a more cautious and gradual introduction, starting with one type of data (not six as proposed by the Commission), indirect access (using index data of information that is not available online) and a hit/no-hit system, which would allow for more control of the exchange of information than a system based on direct access. It is in any case essential that the availability principle is complemented by the adequate data protection rules in the Third Pillar.

As to the need for the better analysis, the scope of the principle should be clarified, by adding a clear and precise definition of the data that will be considered "available", and as a first option, the principle should be limited to information that is controlled by competent authorities. It is not so clear whether data outside the control of these authorities and only accessible for them under certain circumstances, should be considered as "available" for potential sharing with authorities in other Member States.

Further analysis would also be crucial for the concept of "index data": a basic distinction needs to be made between "meta data" about available information on a category level, and "flagging data" that refer to available information on an individual level. The opinion also makes a number of observations on "direct access". It should be clear that unconditional interconnection of databases has to be avoided, if only because an international network of databases would be hard to control and supervise. Finally, the opinion discusses a number of limitations and conditions for the exchange of DNA data, the subject that is dealt with prominently, but not in a fully satisfactory manner, in the Prüm Convention.

The proposal for the Framework Decision on availability has not been the subject of a discussion in the Council so far. This is why the EDPS opinion also comments on other

approaches and suggests a gradual introduction of the principle that combines a number of positive elements.

Final remarks

This brief overview is probably sufficient to illustrate that many activities are presently taking place to come to an adequate framework for data exchange and data protection in the Third Pillar. The input from data protection authorities at different levels has played an important part in this debate and this will hopefully continue so in the near future. In any case, it is clear that contributions from Poland have left visible traces and that Dr Ewa Kulesza deserves thanks for her role in that context.

There is of course more to say, both on a personal and on a substantive level. However, it is my privilege to reserve some of that for another occasion, most probably the next conference in Warsaw, during which I will have the pleasure to speak again.

Ramy rozwoju: trzeci filar i ochrona danych

Wstęp

W okresie pozostawania na stanowisku, jako pierwszy polski Generalny Inspektor Ochrony Danych Osobowych, dr Ewa Kulesza wykazała się wielkim wyczuciem w kwestiach kontaktów międzynarodowych. Wykraczało to daleko ponad bliską współpracę z kolegami ze środkowej i wschodniej Europy. Przytoczmy choćby, jako ilustrację, krótką listę wydarzeń.

W maju 2004 r. miałem przyjemność gościć w Warszawie, a był to pierwszy miesiąc pełnego członkostwa Polski w Unii Europejskiej. We wrześniu 2004 r. polski Generalny Inspektor podejmował uczestników 26 Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych we Wrocławiu. W kwietniu 2005 r. dr Kulesza organizowała doroczną Wiosenną Konferencję Europejskich Inspektorów Ochrony Danych w Krakowie. W maju 2006 r., na krótko przed zakończeniem swojej drugiej kadencji, dr Kulesza gościć będzie w Warszawie konferencję „Bezpieczeństwo Publiczne i Ochrona Danych”, na której ponownie pojawi się wielu europejskich współpracowników.

Z pewnością świadczy to o szczególnym zainteresowaniu tematem, który zajmował także poczesne miejsce zarówno w Krakowie, jak i we Wrocławiu. Przyjęte podczas tych konferencji kluczowe dokumenty wpłynęły na zachodzące w Europie przemiany. W publikacji, która w swojej intencji zamierza być wyrazem uznania dla dr Ewy Kuleszy i jej wkładu w kwestie ochrony danych, wypada zatem przedstawić krótki przegląd powyższych przemian.

Trzeci filar

Termin „trzeci filar” odnosi się do struktury Unii Europejskiej wprowadzonej w „Traktacie z Maastricht” (1992). Na ówczesnym etapie dotyczył on współpracy na polu spra-

wiedliwości i spraw wewnętrznych. Na mocy „Traktatu Amsterdamskiego” (1997) współpracę tę poddano restrukturyzacji. Stopniowe ustanowienie „przestrzeni wolności, bezpieczeństwa i sprawiedliwości” stało się celem pierwszego filaru, zaś postanowienia w zakresie wiz, azylu, imigracji i współpracy sądowej w sprawach cywilnych zostały obecnie opracowane w tytule IV „Traktatu WE”. Cel, jakim jest zapewnienie obywatelom wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, zwłaszcza przez rozwój wspólnych działań w dziedzinie współpracy policyjnej i sądowej w sprawach karnych, pozostał jako trzeci filar w tytule VI „Traktatu UE”. Działania w obszarze wolności, bezpieczeństwa i sprawiedliwości jako całość uległy intensyfikacji po ustaleniach szczytu Rady Europejskiej w Tampere (1999). W listopadzie 2004 r. przyjęto nowy pięcioletni „Program Haski”. Ponad wszelką wątpliwość doprowadzi on do dalszego wzrostu aktywności, również w trzecim filarze.

Ważne jest, by w tym miejscu zdać sobie sprawę z faktu, iż trzeci filar boryka się z wieloma strukturalnymi problemami. Po pierwsze, wszystkie działania w tym filarze odbywają się na płaszczyźnie międzyrządowej i skutkiem tego mogą mieć miejsce tylko w przypadku jednomyślności Państw Członkowskich. Oznacza to, że podejmowanie decyzji nie jest łatwe i często prowadzi do słabych kompromisów. Po drugie, rola Parlamentu Europejskiego wciąż pozostaje ograniczona. Na mocy art. 39 „Traktatu UE”, Parlamentowi przysługuje tylko prawo wydawania opinii, Rada zaś może tę opinię zignorować lub czasem nawet – jeśli sobie tego życzy – działać bez jej zasięgnięcia. Po trzecie, kontrola sądowa sprawowana przez Trybunał Sprawiedliwości także jest niepełna. Na mocy art. 35 „Traktatu UE”, w sprawach dotyczących utrzymania prawa i porządku oraz ochrony bezpieczeństwa wewnętrznego, Trybunał nie jest organem właściwym. Po czwarte, problematyczna jest kwestia wdrażania zasad UE na poziomie krajowym; często nie da się jej egzekwować lub kwestionować przed sądem. Na koniec, bardzo brakuje przejrzystości, a istotne informacje często pojawiają się późno i tylko fragmentarycznie. Większość problemów rozwiązałby traktat konstytucyjny, jednak nie jest to kwestia najbliższej przyszłości.

Jeśli chodzi o rolę doradczą organów ochrony danych, aktualne ustalenia również nie są satysfakcjonujące. Komisja Europejska potwierdziła, że przyjmując wniosek legislacyjny mający wpływ na ochronę danych osobowych, na mocy art. 28 ust. 2 Rozporządzenia (WE) 45/2001, czuje się ona zobowiązana do konsultowania się z Europejskim Inspektorem Ochrony Danych (EDPS); jej prawo do podejmowania inicjatyw ustawodawczych dzieli z nią jednak niezobligowane do takich konsultacji Państwa Członkowskie. Jeszcze bardziej nieadekwatne są ustalenia dotyczące systematycznego wkładu ze strony krajowych organów ochrony danych. Z tego właśnie powodu, we wrześniu 2004 r., podczas europejskiej konferencji inspektorów ochrony danych we Wrocławiu, przyjęto rezolucję wzywającą do ustanowienia w trzecim filarze wspólnego forum ds. ochrony danych, w celu zapewnienia z ich strony systematycznego wkładu w podejmowanie decyzji.

Odnosnie do ogólnych postanowień w sprawie ochrony danych należy zauważyć, że nie ma zastosowania Dyrektywa 95/46/WE, ponieważ przedmiotowe działania objęte tytułem VI „Traktatu UE” zostały wyłączone w art. 3 ust. 2. „Konwencja nr 108” Rady Europy została ratyfikowana przez wszystkie Państwa Członkowskie UE, jednak jej postanowienia stosują się do samej Unii tylko pośrednio, na mocy art. 6 „Traktatu UE”. Choć „Konwencję nr 108” uznaje się za zbyt ogólną do konkretnych zastosowań, od-

woływało się do niej wiele instrumentów, uznając ją za ważny standard w sprawie ochrony danych w trzecim filarze. Miało to miejsce najpierw w „Konwencji z Schengen” (1990), podobnie w „Konwencji o Europolu” (1995) i w końcu w decyzji Rady powołującej Eurojust (2002). Schengen włączono w ramy UE na mocy „Traktatu Amsterdamskiego”, natomiast rozwój w trzecim filarze Europolu i Eurojustu przebiegał na różnych etapach. Każdy z tych instrumentów zawierał konkretne środki dotyczące ochrony danych, stosowalne tylko w tym kontekście i niekoniecznie ze sobą zgodne. W każdym z tych przypadków problemem był brak w trzecim filarze zasad ogólnych.

Wymiana danych

W ostatnich latach, z powodu rosnącego zainteresowania wymianą danych osobowych między organami ścigania w różnych Państwach Członkowskich, potrzeba wspólnych ram i zasad staje się coraz bardziej oczywista. Oprócz konkretnych incydentów, które sugerowałyby brak współpracy i wymiany informacji, wynika to z czystej logiki. Współpraca policyjna i sądowa w sprawach karnych zbliża się do fazy, w której wymiana danych i bezpośredni dostęp do danych „ponad granicami” stają się kwestią coraz bardziej zasadniczą dla ścigania przestępczości w obszarach o „wysokim znaczeniu”. Z tego właśnie powodu „Program Haski” tak wielki nacisk położył na wymianę danych w ramach zasady „dostępności”. Oznacza to, że informacje dostępne pewnym organom Państwa Członkowskiego muszą być także przekazane równoważnym organom innych Państw Członkowskich.

W „Programie Haskim” kładzie się nacisk na to, by ustalenia takie podlegały odpowiednim zabezpieczeniom w zakresie ochrony danych. Nietrudno jest zauważyć, że w kwestiach dotyczących weryfikowania zgodności z zasadami uczciwego i zgodnego z prawem zbierania danych, jakości tych danych, bezpieczeństwa itp., ściganie przestępczości w różnych Państwach Członkowskich stanie się coraz bardziej wzajemnie powiązane i od siebie zależne. Odpowiednie zasady ochrony danych, w ślad za którymi pojawiają się dobre praktyki, zbudują w ten sposób „zaufanie” między organami w różnych krajach i przyczynią się do lepszej współpracy transgranicznej w sprawach karnych. Jest oczywiste, że w tego typu sprawach odpowiednie wspólne standardy ochrony danych będą stanowić więcej niż tylko zabezpieczenie; należy je także postrzegać jako zasadnicze warunki skutecznej współpracy.

W ostatnich latach, zarówno w obrębie, jak i poza Unią Europejską, pojawiło się całkiem sporo inicjatyw promujących wymianę informacji policyjnych między różnymi krajami. W czerwcu 2004 r. Szwecja zaproponowała decyzję ramową w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ochrony porządku publicznego Państw Członkowskich. W maju 2005 r. siedem Państw Członkowskich podpisało w Prüm (Niemcy) Konwencję w sprawie pogłębienia współpracy transgranicznej, szczególnie w dziedzinie walki z terroryzmem, przestępczością międzynarodową i nielegalną imigracją. Wprowadza ona, między innymi, środki służące poprawie wymiany informacji na temat DNA i odcisków palców; przystąpienie do niej jest otwarte dla wszystkich pozostałych Państw Członkowskich. Celem jest włączenie Konwencji do ram prawnych UE. Inicjatywa ta pojawia się obok innych, takich jak, np. wnioski w sprawie drugiej generacji „Systemu informacyjnego Schengen” (SIS II) oraz ostatnio także wniosek dotyczący decyzji ramowej w sprawie wymiany informacji w ramach zasady dostępności jako ogólnego następstwa stosownej części „Programu

Haskiego". Owe różne inicjatywy niekoniecznie są ze sobą zgodne, ani też nie zagwarantowano, jak dotąd, spójnego podejścia do kwestii ochrony danych.

Ochrona danych

Po spotkaniu we Wrocławiu we wrześniu 2004 r., europejskie organy ochrony danych kontynuowały prace nad ochroną danych w trzecim filarze. Podczas wiosennej konferencji w Krakowie, w kwietniu 2005 r., zaowocowało to przyjęciem stanowiska w sprawie ścigania przestępstw i wymiany informacji w UE, rozpoczynając prace nad głównymi elementami ogólnych ram prawnych ochrony danych w trzecim filarze. Niosąc wyraźne przesłanie, stanowisko to zostało dołączone do deklaracji. Przede wszystkim kładzie ono nacisk na fakt, że inicjatywy zmierzające do poprawy ścigania przestępstw w UE, takie jak, np. zasada dostępności, powinny być wprowadzane wyłącznie na podstawie odpowiedniego systemu uzgodnień w sprawach ochrony danych, gwarantującego wysoki i równorzędny standard ochrony danych. Deklaracja kładzie także nacisk na to, że zbiór zasad mających zastosowanie do działań związanych ze ściganiem przestępczości powinien odpowiadać obecnemu poziomowi ochrony danych w pierwszym filarze. Standard ochrony danych znajdujący się w Dyrektywie 95/46/WE powinien zatem służyć jako podstawa rozwijania stosownych zasad w trzecim filarze.

Wkład krakowskiej deklaracji oraz dokumentu zawierającego stanowisko został przez Komisję Europejską należycie wykorzystany. W październiku 2005 r. przyjęła ona wniosek dotyczący decyzji ramowej w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Propozycja ta w wielu kwestiach podąża za stanowiskiem Dyrektywy 95/46/WE, a wiele punktów uzasadnienia zawiera odsyłacze do dokumentu określającego to stanowisko. Wniosek jest obecnie tematem dyskusji grupy roboczej Rady oraz komitetu LIBE Parlamentu Europejskiego. Opinia EIOD została opublikowana w grudniu 2005 r. Konferencja europejska przyjęła opinię wkrótce po spotkaniu w styczniu 2006 r., w czasie sprawowania przewodnictwa przez Polskę. Oba organy z zadowoleniem witają propozycję Komisji oraz popierają jej główne zarysy, ale proponują też w różnych szczegółach ulepszenia. Jest całkiem możliwe, że wiele z tych sugestii zostanie podjętych przez Parlament Europejski. Zarówno Parlament, jak i Rada zajmują się obecnie wnioskiem, traktując go jako priorytet.

Przyglądając się bliżej obecnemu stanowi rzeczy, należałoby, po pierwsze, zauważyć, że nikt nie wydaje się już podważać lub poddawać w wątpliwość potrzeby istnienia zasad dotyczących ochrony danych w trzecim filarze. Parlament Europejski wiele razy apelował o wniosek Komisji, jednak Rada, jak dotychczas, zajmowała stanowisko dużo bardziej nieprzychylnie. Należy przyjąć, że dyskusje na temat wymiany informacji w ogóle, a na temat zasady dostępności w szczególności, doprowadziły do zmiany zapartytowań w większości kręgów w Radzie. Jednakże fakt, że przyjęcie decyzji ramowej może nastąpić tylko jednogłośnie, powinien stanowić powód do zachowania pewnej rozwagi odnośnie ostatecznej zawartości oraz terminu tejże decyzji.

Na obecnym etapie ważniejszą kwestią jest zakres wniosku. Zgodnie z art. 1 ust. 1, wniosek winien określić „wspólne standardy” w celu zapewnienia ochrony danych osobowych w trakcie działań związanych z policyjną i sądową współpracą w sprawach karnych. Zgodnie z art. 3 ust. 1, wniosek będzie miał zastosowanie do „przetwarzania

przez właściwy organ danych osobowych (...) dla celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania”. Z postanowień tych wynika, że proponowana decyzja ramowa posiada dwie charakterystyczne cechy: wyznacza wspólne standardy i ma zastosowanie do wszelkiego rodzaju przetwarzania danych dla celów ścigania przestępstw karnych, nawet jeśli rozpatrywane dane nie zostały przekazane lub udostępnione przez organy innego Państwa Członkowskiego.

Opinie EIOD oraz konferencji europejskiej podkreślają znaczenie tych charakterystyk. Podejście takie skutkowałoby ramami prawnymi ochrony danych w trzecim filarze, które w pełni uzupełniłyby obecne ramy prawne pierwszego filaru. Tak samo byłoby w sytuacjach „czysto krajowych”, co w Radzie mogłoby prowadzić do trudnych dyskusji. Trzeba jednak podkreślić, że wszelkie ograniczanie się do „danych, które są przekazywane lub udostępniane organom innego Państwa Członkowskiego” mogłoby uczynić pole zastosowania decyzji ramowej szczególnie wątpliwym i niepewnym, co stałoby w sprzeczności z jej zasadniczym celem. Spowodowałoby to szkodę dla pewności prawnej osób fizycznych. W zwykłych okolicznościach nikt nie potrafi określić z wyprzedzeniem, czy dane osobowe będą przedmiotem wymiany informacji z właściwymi organami innych Państw Członkowskich. Trudno byłoby też posługiwać się różnymi standardami, różnicując je na podstawie pochodzenia danych osobowych. Najprawdopodobniej prowadziłyby to do wielkich trudności praktycznych w kontekście zasady dostępności oraz zniesienia granic wewnętrznych odnośnie wymiany danych związanych ze ściganiem przestępstw.

W swojej niedawnej opinii Służba Prawna Rady stwierdziła, że art. 30, 31 i 34 ust. 2 lit. b „Traktatu UE” stanowią niezbędną podstawę prawną umożliwiającą Radzie przyjęcie decyzji ramowej w sprawie ochrony danych osobowych, obejmującej także przetwarzanie danych w sytuacjach czysto krajowych. Oznacza to, że decyzja odnośnie tego, w jakim zakresie Rada zamierza korzystać ze swych kompetencji wynikających z tych postanowień, należy do samej Rady.

Inną związaną z zakresem kwestią jest pytanie, czy wniosek powinien stosować się także do Europolu i Eurojustu. Należy po pierwsze zauważyć, że decyzja ramowa na mocy art. 34 ust. 2 lit. b „Traktatu UE” może zostać przyjęta jedynie w celu zbliżania przepisów ustawowych i wykonawczych Państw Członkowskich i dlatego zasadniczo nie może być kierowana do ciał takich jak Europol oraz Eurojust. Jednocześnie pożądane jest, aby przepisy mające do nich obecnie zastosowanie zostały tak szybko, jak to tylko możliwe, w pełni dostosowane do nowych zasad. Byłaby to także okazja do harmonizacji horyzontalnej. W przypadku SIS II zakłada się już, że po jej przyjęciu wnioskowana decyzja ramowa będzie stanowiła część zasad ogólnych („*lex generalis*”).

Treść wniosku prowadzi do wielu innych interesujących kwestii, do których komentarz znajduje się w opiniach EIOD oraz konferencji europejskiej, jednak dalsza dyskusja na ten temat wykraczałaby poza zakres niniejszego artykułu.

Dostępność

EIOD wydał też ostatnio opinię w sprawie wniosku Komisji dotyczącego decyzji ramowej w sprawie wymiany informacji w ramach zasady dostępności. Opinia wzywa do lepszego przeanalizowania zasady i do ostrożniejszego oraz stopniowego jej wpro-

wadzenia, rozpoczynając od jednego rodzaju danych (a nie sześciu, jak proponowała Komisja), dostępu pośredniego (wykorzystując odnośniki do informacji, które nie są dostępne przez Internet) i systemu potwierdzania lub wykluczania, który pozwalałby na większą kontrolę wymiany informacji niż system oparty na dostępie bezpośrednim. Kwestią zasadniczą jest w każdym razie uzupełnienie zasady dostępności odpowiednimi zasadami ochrony danych w trzecim filarze.

Jeśli chodzi o potrzebę lepszej analizy, należałoby wyjaśnić kwestię zakresu zasady dostępności przez dołączenie jasnej i precyzyjnej definicji danych, które należy uznawać za „dostępne”; jako pierwszą opcję można by przyjąć, że zasada ta powinna być ograniczona do informacji znajdujących się pod kontrolą właściwych organów. Nie jest zbyt jasne, czy dane leżące poza obszarem kontroli tych organów i udostępnione im tylko w szczególnych okolicznościach, powinny być uznawane za „dostępne” w celu potencjalnego dzielenia się nimi z organami innych Państw Członkowskich.

Dalsza analiza miałaby zasadnicze znaczenie również dla koncepcji „odnośników”; konieczne jest podstawowe rozróżnienie między „meta danymi” dotyczącymi dostępnych informacji na poziomie kategorii oraz „danymi wskaźnikowymi” odnoszącymi się do dostępnych informacji na poziomie indywidualnym. W opinii zawarto także szereg spostrzeżeń na temat „dostępu bezpośredniego”. Powinno być oczywiste, że należy unikać bezwarunkowego wzajemnego połączenia baz danych, już choćby dlatego, że międzynarodową sieć baz danych trudno byłoby kontrolować i nadzorować. Na koniec, opinia przedstawia omówienie licznych ograniczeń i warunków dotyczących wymiany danych na temat DNA, stanowiących zasadniczą część Konwencji z Prüm, jednak nieuregulowanych w niej w zadowalający sposób.

Jak dotąd wniosek dotyczący decyzji ramowej w sprawie dostępności nie był jeszcze tematem dyskusji Rady. Z tego też powodu opinia EIOD przedstawia również komentarz do innych podejść oraz sugeruje, aby zasada, która niewątpliwie łączy w sobie wiele pozytywnych elementów, była wprowadzana stopniowo.

Uwagi końcowe

Niniejszy krótki przegląd prawdopodobnie wystarczy do zilustrowania mnogości podejmowanych obecnie działań w celu wypracowania odpowiednich ram wymiany i ochrony danych w trzecim filarze. W debacie tej istotną rolę odegrał wkład organów ochrony danych różnych szczebli i można mieć nadzieję, że w najbliższej przyszłości będzie podobnie. W każdym razie jest oczywiste, że w rozwoju tym w sposób trwały zapisał się wkład wniesiony przez Polskę, a dr Ewie Kuleszy, za jej rolę w tym kontekście, należą się szczególne wyrazy podziękowania.

Oczywiście, zarówno na poziomie osobistym, jak i w kwestiach dotyczących samego meritum, jest jeszcze wiele wartych omówienia zagadnień, jednak moim przywilejem jest, choć część z nich zachować na inną okazję, którą będzie najprawdopodobniej następna konferencja w Warszawie, w czasie której ponownie będę miał przyjemność wygłaszać odczyt.

Dr hab. Małgorzata Jaśkowska

Naczelny Sąd Administracyjny, Wydział Informacji Sądowej, Polska
The Supreme Administrative Court, Court Information Department, Poland

Skarga na bezczynność w zakresie dostępu do informacji publicznej

I. W polskim systemie prawnym funkcjonuje zarówno prawo do informacji, jak i prawo do ochrony danych osobowych. Pierwsze z nich wynika wyraźnie z art. 61 Konstytucji RP z dnia 2 kwietnia 1997 r.¹ oraz z ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (powoływanej dalej jako udip).² Drugie natomiast znajduje swoją podstawę w art. 51 Konstytucji oraz w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (powoływanej dalej jako uodo).³ Pomiędzy tymi dwoma prawami mogą zachodzić różnego typu relacje, może też dochodzić między nimi do pewnych konfliktów. Podobna sytuacja ma miejsce również w innych systemach prawnych, przy czym ustawodawcy przyjmują dla rozwiązywania takich problemów różne rozwiązania, w tym rozwiązania organizacyjne. I tak w niektórych państwach europejskich organy powołane do ochrony danych osobowych wyposażane są również w kompetencje w zakresie ochrony prawa do informacji. Taką regulację przyjęto np. na Węgrzech, gdzie powołany został Parlamentarny Rzecznik Ochrony Danych i Wolności Informacji, czy też w niektórych landach niemieckich. W Berlinie funkcjonuje np. Rzecznik Ochrony Danych i Wolności Informacji, a w Brandenburgii Rzecznik Ochrony Danych i Dostępu do Informacji. Z kolei w innych systemach prawnych funkcje te ulegają rozdeleniu.

W Polsce przyjęto to drugie rozwiązanie. Do zadań Generalnego Inspektora Ochrony Danych Osobowych nie należy bowiem ochrona wolności informacyjnej ani koordynowanie działań w tym zakresie. Brak jest też innego centralnego organu posiadającego tego typu kompetencje. Spowodowało to w konsekwencji, iż dostęp do informacji publicznej został w wielu przypadkach utrudniony, bądź też dochodzi do jego nadużyć. Nie oznacza to jednak, iż zagadnienie dostępu do tej informacji znajduje się całkowicie poza sferą zainteresowania Generalnego Inspektora Ochrony Danych Osobowych. Świadczy o tym m.in. zorganizowane 12 maja 2003 r., w ramach Akademii Ochrony Danych, międzynarodowe seminarium „Ochrona Danych Osobowych a dostęp do informacji publicznej”. Pośród wielu omawianych wówczas zagadnień znalazło się również zagadnienie dostępu do informacji publicznej w orzecznictwie Naczelnego Sądu Administracyjnego. Poniższe opracowanie stanowi rozwinięcie i kontynuację tez przedstawionych w tym zakresie na forum przedmiotowej konferencji.

¹) Dz.U. Nr 78, poz. 483 ze sprost.

²) Dz.U. Nr 112, poz. 1198 ze zm.

³) Dz.U. 2002 r. Nr 101, poz. 926 ze zm.

II. Jak już zaznaczono powyżej w Polsce kwestie dostępu do informacji publicznej i ochrony danych osobowych regulowane są w odrębny sposób. Pierwszym z nich poświęcona jest ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, drugim ustawa o ochronie danych osobowych. Jednocześnie pierwsza z tych ustaw wskazuje na sytuacje, w których kwestia ochrony danych osobowych może być przesłanką udzielenia odmowy informacji. Zgodnie z art. 22 tej ustawy w przypadku odmowy udzielenia informacji z uwagi na ochronę danych osobowych służy powództwo do sądu powszechnego. Oznacza to w konsekwencji, iż decyzję wydawaną na podstawie art. 16 ustawy, w której powołano się na ochronę danych osobowych, podejmuje organ, do którego zwrócono się o udzielenie informacji, a kontroluje ją sąd powszechny. Sąd ten może badać rozstrzygnięcie nie tylko w zakresie jego legalności, ale także merytorycznej zasadności przesłanek odmowy udostępnienia informacji. Orzeczenie jego, stwierdzające prawo do uzyskania dostępu do informacji publicznej, będzie stanowić podstawę do jej udzielenia, a nie jak w przypadku wyroku sądu administracyjnego podstawę do ponownego rozpatrzenia sprawy. W sprawach tych wyłączona zostaje właściwość Generalnego Inspektora Ochrony Danych Osobowych, jako organu ochrony danych (art. 18 ust. 3 w zw. z ust. 1 pkt 2 uodo oraz art. 22 udip). Jednocześnie jednak osoba sprawująca funkcję publiczną nie może skutecznie sprzeciwić się przekazywaniu dotyczących jej informacji publicznych (*a contrario* art. 32 ust. 1 pkt 8 w zw. z art. 23 ust. 1 uodo).⁴

Zakres i tryb kontroli decyzji administracyjnych w sprawie udostępniania lub odmowy udostępniania informacji publicznej, niewyłączonej spod kompetencji sądów administracyjnych przez art. 22 udip, normują szczegółowo przepisy postępowania sądowo-administracyjnego, tj. ustawy z dnia 30 sierpnia 2002 r. prawo o postępowaniu przed sądami administracyjnymi (powoływanej dalej jako ppsa).⁵ Wyłączna właściwość tych sądów odnosi się do przypadków beczynności podmiotów zobowiązanych do udzielenia informacji publicznej.⁶

W tym miejscu należy wskazać na najistotniejsze przesłanki dopuszczalności wniesienia skarg na beczynność w zakresie udzielania informacji publicznej, które wynikają z przepisów ppsa a pozostają w ścisłym związku z rozwiązaniami przyjętymi na gruncie ustawy o dostępie do informacji publicznej. Podstawowymi przesłankami dopuszczalności postępowania sądowo-administracyjnego są przede wszystkim: istnienie przedmiotu zaskarżenia tj. aktu i czynności mieszczących się w zakresie kontroli sądów administracyjnych i aktu zaskarżenia, czyli pisma procesowego uruchamiającego postępowanie.⁷ W odniesieniu do pierwszej z nich podstawę prawną skargi na beczynność w zakresie dostępu do informacji publicznej stanowi art. 3 §2 pkt 8 ppsa w związku z art. 3 §2 pkt 4 ppsa. Natomiast rolę pisma spełnia skarga uprawnionego podmiotu. Stwierdzenie przez sąd istnienia przedmiotu zaskarżenia i aktu jego zaskarżenia

umożliwia badanie właściwych przesłanek dopuszczalności skargi. Przez przesłanki te rozumie się określone w ustawie warunki formalne, tj. wymagania co do samej zawartości skargi jako pisma procesowego, a także inne ustawowo określone wymagania, jakie muszą być spełnione, aby pisma te mogły być rozpatrywane przez sąd. Dotyczy to po pierwsze kręgu osób uprawnionych do ich wniesienia, wymogów formalnych samych pism procesowych oraz trybu ich wnoszenia. Wśród przesłanek tych można wyróżnić też przesłanki negatywne, których istnienie skutkuje niedopuszczalnością uruchomienia postępowania sądowo-administracyjnego pomimo spełnienia pozostałych warunków.

Skarga na beczynność powinna być przede wszystkim wniesiona przez odpowiedni podmiot dysponujący legitymacją procesową. Na tle ustawy o dostępie do informacji publicznej będzie nim zarówno wnioskodawca jak i prokurator, Rzecznik Praw Obywatelskich oraz organizacja społeczna w zakresie jej statutowej działalności, w sprawach dotyczących interesów prawnych innych osób, o ile brała ona udział w postępowaniu administracyjnym (art. 50 §1 ppsa). Ta ostatnia sytuacja może w istocie dotyczyć beczynności organu w postępowaniu odwoławczym. Do czasu wydania decyzji o odmowie trudno jest bowiem mówić o postępowaniu administracyjnym, które gwarantuje w art. 31 ustawy z dnia 14 czerwca 1960 r. kodeks postępowania administracyjnego⁸ [zwany dalej kpa – przypis red.] udział organizacji społecznej, a w przypadku wydania decyzji nie można już w zasadzie mówić o beczynności. Może więc ona dotyczyć jedynie beczynności organu odwoławczego po wniesionym odwołaniu. Skarga na beczynność winna być wniesiona do wojewódzkiego sądu administracyjnego właściwego ze względu na siedzibę organu, do którego zwrócono się o udzielenie informacji, a więc organu, którego beczynność jest przedmiotem zaskarżenia. Składa się ją, zgodnie z art. 54 §1 ppsa, za pośrednictwem organu, którego beczynność została zaskarżona. Skarga taka winna spełniać wymogi pisma procesowego, określone w art. 46 ppsa. Zgodnie z nim każde pismo powinno zawierać: oznaczenie sądu, do którego jest skierowane, imię i nazwisko lub nazwę stron, ich przedstawicieli ustawowych i pełnomocników, oznaczenie rodzaju pisma, osnovę wniosku lub oświadczenia, podpis strony albo jej przedstawiciela ustawowego lub pełnomocnika, wymienienie załączników. Jeżeli pismo strony jest pierwszym pismem w sprawie, powinno ponadto zawierać oznaczenie miejsca zamieszkania, a w razie jego braku adresu dla doręczeń lub siedziby stron, ich przedstawicieli ustawowych czy pełnomocników oraz przedmiotu sprawy. Do pisma należy dołączyć pełnomocnictwo, jeżeli przedtem nie zostało ono złożone. Należy dołączyć również odpisy i odpisy załączników w celu doręczenia ich stronom, a ponadto jeżeli w sądzie nie złożono załączników w oryginale, po jednym odpisie każdego załącznika do akt sądowych. Ponadto skarga winna spełniać warunki wymienione w art. 57 §1 ppsa, tj. w tej omawianej sytuacji wskazywać na beczynność w zakresie rozpatrzenia konkretnego wniosku i określać organ, którego beczynność zaskarżono. Warunkiem wniesienia skargi jest także uiszczenie wpisu. Wynosi on obecnie 100 zł na podstawie §2 pkt 6 rozporządzenia Rady Ministrów z dnia 16 grudnia 2003 r. w sprawie wysokości oraz szczegółowych zasad pobierania wpisu w postępowaniu przed sądami administracyjnymi.⁹

Jeżeli skarga nie spełnia warunków formalnych pism procesowych przewodniczący wzywa strony do ich uzupełnienia w terminie 7 dni pod rygorem odrzucenia skargi. Dotyczy to

⁴) G. Sibiga, *Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych*, Samorząd Terytorialny 2003 r. nr 11, s.10.

⁵) Dz.U. Nr 153, poz. 1270 ze zm.

⁶) M. Jaśkowska, *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002 r. s.71 czy S. Szuster, *Komentarz do art. 21 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej*, Dz.U. 2001 r. Nr 112, poz. 1198 / Lex/el 2003, inaczej K. Nowacki, M. Mucha, *Problemy regulacji prawnej dostępu do informacji w Polsce*, Przegląd Sądowy 2002 r. nr 2 s. 24, którzy dopuszczają wniesienie powództwa do sądu powszechnego o ustalenie obowiązku udzielenia informacji publicznej w przypadku beczynności podmiotu nienależącego do systemu administracji publicznej.

⁷) Por. T. Woś, *Postępowanie sądowo-administracyjne*, Warszawa 1999 r. s. 91.

⁸) Dz.U. 2000 r. Nr 98, poz. 1071 ze zm.

⁹) Dz.U. Nr 221, poz. 2193.

również wezwania do uiszczenia wpisu, o ile nie dotyczy to wpisu stałego (a taka sytuacja zachodzi w przypadku skarg na bezczynność) i skargi nie wnosi adwokat czy radca prawny.

Natomiast w związku z faktem, iż skarga dotyczy bezczynności, nie obowiązuje w tym zakresie żaden termin do jej wniesienia. Odnosi się to do wszystkich podmiotów wnoszących przedmiotową skargę.¹⁰

Przy rozpatrywaniu przesłanek dopuszczalności skargi powstaje jednak pytanie, czy w przypadku skarg na bezczynność obowiązuje wymóg wcześniejszego wyczerpania środków zaskarżenia. Temu też zagadnieniu chciałabym poświęcić dalszą część opracowania.

III. Postępowanie w sprawie dostępu do informacji publicznej może zakończyć się bądź udzieleniem takiej informacji, bądź odmową jej udzielenia. W pierwszym przypadku udzielenie informacji dokonywane jest w formie czynności materialno-technicznej,¹¹ co nie budzi już wątpliwości ani w literaturze ani w orzecznictwie. Nie ma tu zastosowania ustawa kodeks postępowania administracyjnego, a ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej zawiera jedynie fragmentaryczne uregulowania w tym zakresie, wskazując m.in. obowiązek oznaczania informacji danymi podmiotu udostępniającego i wytwarzającego informację (art. 12 udip), czas załatwienia sprawy (art. 13 udip), częściowo też sposób i formę udostępnienia danych (art. 14 udip). Natomiast odmowa udzielenia dostępu do informacji publicznej i umorzenie postępowania o jej udzielenie następuje w drodze decyzji administracyjnej (art. 16 udip).

Ten zróżnicowany sposób zakończenia postępowania o udzielenie informacji spowodował pojawienie się, zarówno w literaturze jak i orzecznictwie, rozbieżnych poglądów odnośnie m.in. do warunków dopuszczalności skargi na bezczynność w przedmiotowym zakresie z uwagi na wyczerpanie środków zaskarżenia. Obecnie reprezentowane są cztery stanowiska co do dopuszczalności takiej skargi. Pierwsze trzy uzależniają dopuszczalność skargi do sądu administracyjnego od wcześniejszego wniesienia środka zaskarżenia na drodze administracyjnej, przy czym za taki środek przyjmuje się bądź zażalenie, bądź wezwanie do usunięcia naruszenia prawa, bądź alternatywnie jeden z tych środków. Według reprezentantów czwartego stanowiska skarga na bezczynność w zakresie informacji publicznej do sądu administracyjnego nie musi być poprzedzona żadnym środkiem zaskarżenia na drodze administracyjnej.

Zwolennicy pierwszego stanowiska uważają, iż warunkiem wniesienia skargi jest uprzednie złożenie zażalenia do organu wyższego stopnia, zgodnie z art. 37 kpa, chyba że bezczynny jest minister w odniesieniu do którego nie służy obrona na drodze administracyjnej. Pogląd taki został zaprezentowany m.in. w wyroku Naczelnego Sądu Administracyjnego z dnia 18 marca 2005 r. sygn. akt OSK 1209/04. Podkreślono w nim, że

ustawa „Prawo o postępowaniu przed sądami administracyjnymi” przyjmuje jako obowiązującą regułę, iż droga sędow-administracyjna jest dopuszczalna po wykorzystaniu środków obrony na drodze administracyjnej. Wyjątek od tej reguły ma miejsce jedynie wówczas, gdy na drodze postępowania administracyjnego nie służy żaden środek zaskarżenia lub gdy tak stanowi przepis szczególny. Na tle ustawy o dostępie do informacji publicznej, w świetle rozwiązań przyjętych w art. 13 i 16 ustawy, obronę przed bezczynnością organu należałoby przyjąć przez zobowiązanie organu do wydania decyzji, a tym samym zastosowania środków obrony przed bezczynnością zgodnie z art. 37 kpa. Przesłanką zatem wniesienia skargi do sądu administracyjnego na bezczynność w zakresie nieudzielenia informacji publicznej jest złożenie zażalenia do organu stopnia wyższego, chyba że skarga dotyczy ministra.

Powyższy pogląd wydaje się jednak trudny do zaakceptowania. Prawa do zażalenia, w przypadku milczenia organu w zakresie złożonego wniosku o udostępnienie informacji, nie da się bowiem wyprowadzić z przedmiotowej ustawy ani w drodze wykładni gramatycznej, ani celowościowej, ani systemowej. Po pierwsze ustawa ta nie przewiduje wyraźnie żadnego środka zwalczania bezczynności. Nie można też tego środka poszukiwać w przepisach kodeksu postępowania administracyjnego. Ustawa o dostępie do informacji publicznej ma bowiem na celu przede wszystkim zagwarantować wnioskodawcy dostęp do informacji, który jest prawem wynikającym z art. 61 Konstytucji. Zasadą jest więc udzielenie informacji, natomiast odmowa ma charakter wyjątku. Jak zaś podkreślono powyżej, udzielenie informacji następuje w formie czynności materialno-technicznej, a odmowa w drodze decyzji. Tymczasem w art. 16 ust. 2 ustawy ustawodawca dokonał wyraźnego odesłania do przepisów kpa jedynie w odniesieniu do decyzji wydawanych (zgodnie z ust. 1) w razie odmowy udzielenia informacji i umorzenia postępowania w przypadku określonym w art. 14 ust. 2. Nie dokonał takiego odesłania w stosunku do całego postępowania zmierzającego do udzielenia informacji. Podkreśla to A. Knopkiewicz wskazując, iż użycie w art. 16 ustawy wyrazów „do decyzji” służyć miało również wyłączeniu stosowania reguł kodeksu do faz postępowania, poprzedzających wydanie decyzji w sprawie odmowy udostępnienia informacji lub umorzenia postępowania.¹² Jeżeli wolą ustawodawcy byłoby stosowanie norm kodeksu postępowania administracyjnego do całego postępowania, to znalazłoby to wyraźne odzwierciedlenie w treści ustawy o dostępie do informacji publicznej. Taką techniką redagowania przepisów posługuje się bowiem prawodawca w innych ustawach, w których nakazuje co do zasady stosowanie kodeksu do całych postępowań, a nie jedynie do decyzji.¹³ Jak podkreśla też A. Knopkiewicz w tej sytuacji mamy do czynienia z kolizją ogólniejszej i wcześniejszej normy z art. 1 pkt 1 kpa w związku z art. 16 udip z normą szczególną i późniejszą zawartą w art. 16 ust. 2 udip. W takim zaś przypadku za stosowaniem kpa dopiero od momentu wydawania decyzji przemawiają dwie reguły kolizyjne, *lex specialis derogat legi generali* i *lex posterior derogat legi priori*. Uzasadnienia niestosowania tego kodeksu do postępowania przed wydaniem decyzji o odmowie lub umorzeniu można upatrywać również w tym, iż wolą prawodawcy jest odformalizowanie tego postępowania.¹⁴ Pewnym paradoksem byłoby zresztą uzależnianie skargi strony, która domaga się informacji, od żądania od niej wcześniejszego ubiega-

¹⁰ Por. M. Jaśkowska w: M. Jaśkowska, M. Masternak, E. Ochendowski, *Postępowanie sędow-administracyjne*, wyd. 2 Warszawa 2005 r., s. 132.

¹¹ M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej, Informatyzacja administracji*, Wrocław 2005 r., s. 85, A. Knopkiewicz, *Tryby udostępniania informacji publicznej*, RPIES 2004 r. nr 4 s. 97 i d., R. Stefanicki, *Ustawa o dostępie do informacji publicznej, wybrane zagadnienia w świetle orzecznictwa sądowego*, PIP 2004 r. nr 2, s. 109, por. też wyrok NSA z 20 czerwca 2002 r. sygn. akt II S.A./Lu 507/02 czy wyrok WSA w Warszawie z dnia 17 lutego 2004 r. sygn. akt II SAB 424/03 oraz wyrok NSA z dnia 18 marca 2005 r. sygn. akt OSK 1209/04.

¹² A. Knopkiewicz, *Tryby op. cit.*, s. 103.

¹³ Por. np. art. 22 ustawy o ochronie danych osobowych, czy art. 80 (z zastrzeżeniem art. 81) ustawy z dnia 15 grudnia 2000 r. o ochronie konkurencji i konsumentów, Dz.U. 2003 r. Nr 86, poz. 804 ze zm.

¹⁴ A. Knopkiewicz, *Tryby op. cit.*, s. 103 i d.

nia się na drodze administracyjnej o odmowę udzielenia takiej informacji. Jak wskaza-
no w wyroku NSA z dnia 17 lutego 2004 r. sygn. akt II SAB 424/03 „nie można skarżą-
cej czynić zarzutu niewykorzystania środka zaskarżenia, o którym mowa w art. 37 kpa.
Skarżąca domagając się od organu wyższego stopnia (...) podjęcia działań określo-
nych w art. 37 §2 kpa, w istocie domagałaby się wydania decyzji negatywnej, co
pozostaje w oczywistej sprzeczności z jej żądaniem.”

Należy również podkreślić, iż gdyby ustawodawca zamierzał rozciągnąć przepisy ko-
deksu postępowania administracyjnego w szerszym stopniu na postępowanie w spra-
wie dostępu do informacji publicznej, to uczyniłby to w sposób wyraźny. Nic nie stało
bowiem na przeszkodzie, aby określając w art. 13 ustawy skutki nieudzielenia infor-
macji w terminie wskazał dodatkowo środek zaskarżenia w postaci zażalenia. W prze-
pisie tym znalazły się przecież inne szczegółowe unormowania, związane ze sposobem
poinformowania wnioskodawcy o powodach opóźnienia. Nie można zaś domniemywać,
co wydaje się wynikać z powoływanego wyroku NSA z dnia 18 marca 2005 r. sygn. akt
OSK 1209/04, odwołującego się w swojej argumentacji do art. 13 ustawy, iż artykuł
ten jest niejako wstępem do wydania decyzji o odmowie udzielenia informacji, stąd
jego konsekwencją jest prawo do zażalenia na bezczynność organu. Po pierwsze nawet
na tle art. 13 udiip ustawodawca podkreśla, iż postępowanie winno zmierzać do udzie-
lenia informacji, a nie jej odmowy. Zgodnie z art. 13 ust. 2 powiadomienie musi bo-
wiem dotyczyć nie tylko powodów opóźnienia, ale i terminu w jakim udostępni się
informację. Po drugie, ponieważ cały czas mamy na tym etapie do czynienia z postępo-
waniem w sprawie czynności materialno-technicznej, tym bardziej nie można wypro-
wadzać z przedmiotowego przepisu prawa do zażalenia. Jest to o tyle istotne, iż w
zasadzie wszystkie procedury administracyjne przyjmują, że prawo do zażalenia służy,
gdy ustawa wyraźnie tak stanowi. Nie bez znaczenia jest również fakt, iż ustawa o
dostępie do informacji publicznej w swoich założeniach zmierza do szybkiego załatwie-
nia sprawy, upraszczając postępowanie oraz skracając w stosunku do kpa istniejące
terminy, w tym terminy rozpatrywania środków zaskarżenia. Rzuca to w konsekwen-
cji na sposób dokonywania wykładni przedmiotowej ustawy i oznacza, iż nawet w razie
wątpliwości nie należy ich rozwiązywać na drodze przedłużania postępowania poprzez
jego uzależnianie od nieprzewidzianych w tejże ustawie wymogów formalnych.

Według drugiego stanowiska złożenie skargi na bezczynność w zakresie dostępu do
informacji publicznej jest uzależnione od wyczerpania środka zaskarżenia, obowiązek
ten ma jednak charakter alternatywny. Wnioskodawca może bowiem skorzystać za-
równo z zażalenia jak i wezwania do usunięcia naruszenia prawa, które wynika z art.
52 §3 bądź 4 ppsa. Pogląd taki został zaprezentowany w wyroku Wojewódzkiego Sądu
Administracyjnego w Opolu z dnia 27 maja 2004 r. sygn. akt II SAB/Op 1/04¹⁵ oraz w
postanowieniu NSA z dnia 8 lipca 2005 r. sygn. akt OSK 1682/04. W wyroku WSA w
Opolu wskazano, iż w tej złożonej sytuacji, gdy wnioskodawca oczekuje pozytywnego
załatwienia wniosku, ale jednocześnie może liczyć się z odmową lub pismem o nienale-
żeniu sprawy do informacji publicznych, należy przyjąć, że wyczerpano środki zaskarże-
nia zarówno wtedy, gdy wnioskodawca przed wniesieniem skargi złożył zażalenie w try-
bie art. 37 §1 kpa, wymagane w odniesieniu do skargi na bezczynność, polegającą na
niewydaniu decyzji (...) jak i wtedy, gdy... wezwał organ do usunięcia naruszenia pra-

wa, co jest wymagane przy bezczynności organu w zakresie czynności materialno-
technicznych (art. 52 ppsa).¹⁶ W postanowieniu NSA podkreślono natomiast, iż w kon-
kretnej sprawie należy badać intencje wnioskodawcy, a więc sprawdzić, czy domaga
się on działań w trybie art. 37 §2 kpa, czy też czynności materialno-technicznej. W tym
drugim przypadku skarga winna być poprzedzona wezwaniem do usunięcia naruszenia
prawa wniesionym na podstawie art. 52 §4 ppsa.

Wskazane wyżej argumenty, przemawiające przeciwko uzależnianiu dopuszczalności
skargi od zażalenia składanego w trybie art. 37 kpa, wydają się aktualne także w
odniesieniu do tezy o możliwości jego wnoszenia jako alternatywnego środka zaskar-
żenia. Stąd należy tu w istocie odpowiedzieć na pytanie, czy dopuszczalność przedmio-
towej skargi warunkowana jest złożeniem wezwania do usunięcia naruszenia prawa,
niezależnie od tego, czy środek ten miałby charakter alternatywny z zażaleniem w
trybie art. 37 kpa, czy też nie.

W literaturze zwraca się uwagę, iż skargę na bezczynność w zakresie informacji pu-
blicznej można wnieść w zasadzie po wezwaniu organu do usunięcia naruszenia prawa.
Pogląd taki reprezentuje m.in. K. Klonowski. Twierdzi on, iż w przypadku skargi na
bezczynność organu w zakresie pozostałych postanowień oraz aktów i czynności okre-
ślonych w art. 3 §2 pkt 4 ppsa, wniesienie skargi należy poprzedzić wezwaniem na
piśmie właściwego organu w terminie czternastu dni od dnia, w którym skarżący do-
wiedział się lub mógł się dowiedzieć o wydaniu aktu lub podjęciu innej czynności – do
usunięcia naruszenia prawa.¹⁷ Zdaniem M. Bernaczyka, M. Jabłońskiego i K. Wygody,
jeżeli milczenie jest związane z zachowaniem organu władzy (podmiotu publicznego
zobowiązanego w trybie udiip) to przed wystąpieniem do sądu administracyjnego nale-
ży wezwać go do usunięcia naruszenia prawa. Jest to bezwzględna przesłanka, której
spełnienie warunkuje wniesienie skargi do sądu administracyjnego. W sytuacji nato-
miast, w której zobowiązany nie należy do kategorii organów władzy publicznej (oraz
innych podmiotów publicznych) zainteresowanemu przysługuje prawo wniesienia po-
wództwa o ustalenie obowiązku udzielenia informacji do sądu powszechnego.¹⁸ Pozo-
stawiając na marginesie kwestię rozróżnienia drogi sądowej w zależności od organu,
która nie wydaje się znajdować uzasadnienia na tle ustawy o dostępie do informacji
publicznej, należy wskazać, iż teza o uzależnieniu skargi na taką bezczynność od we-
zwania do usunięcia naruszenia prawa nie ma obecnie podstawy w art. 52 ppsa. Jest
ona w istocie powtórzeniem stanowiska, jakie znajdowało oparcie w starych przepi-
sach postępowania sądowo-administracyjnego. Na tle art. 34 ust. 3 ustawy z dnia 11
maja 1995 r. o Naczelnym Sądzie Administracyjnym,¹⁹ jeżeli ustawa nie przewidywała
środków odwoławczych w sprawie będącej przedmiotem skargi, należało przed wnie-
sieniem jej do sądu zwrócić się do właściwego organu z wezwaniem do usunięcia naru-
szenia prawa. Termin do wniesienia takiej skargi rozpoczynał przy tym bieg po upływie
trzydziestu dni od dnia doręczenia wezwania. Oznaczało to, iż na tle ustawy o NSA
wezwanie do usunięcia naruszenia prawa nie było związane z żadną konkretną formą
działania czy bezczynności administracji publicznej, lecz stanowiło konsekwencję bra-

¹⁶⁾ J.w. s. 84.

¹⁷⁾ K. Klonowski, *Bezczynność organu w postępowaniu sądowo-administracyjnym*, Samorząd Terytorialny 2004
r. nr 4, s.31-32.

¹⁸⁾ M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn*, op. cit., s. 86-87.

¹⁹⁾ Dz.U. Nr 74, poz. 368 ze zm.

ku w ustawie szczególnej środków odwoławczych. Tymczasem przepisy ustawy prawo o postępowaniu przed sądami administracyjnymi regulują tę kwestię odmiennie.

Stąd trudno się zgodzić ze stanowiskiem przedstawionym w pierwszej części wyroku Naczelnego Sądu Administracyjnego z dnia 18 marca 2005 r. sygn. akt OSK 1209/04. Mimo iż ostatecznie opowiedziano się w nim w odniesieniu do skargi na bezczynność w zakresie informacji publicznej za uzależnieniem jej dopuszczalności od wniesienia zażalenia w trybie art. 37 kpa, jednak we wstępnej części uzasadnienia przedstawiono ogólne możliwości zwalczania bezczynności. W wyroku tym podkreślono przede wszystkim, iż ppsa przyjmuje jako obowiązującą regułę, że droga postępowania przed sądami administracyjnymi jest dopuszczalna tylko po wykorzystaniu środków zaskarżenia na drodze administracyjnej. Te środki zaskarżenia przewiduje kpa lub przepisy szczególne. W razie, gdy przedmiotem zaskarżenia jest wykonywanie administracji publicznej w innych formach prawnych, do których nie stosuje się przepisów kpa, obowiązek wyczerpania obrony regulują przepisy ppsa. Przewidują one w art. 52 §3 i 4 środek zaskarżenia w postaci wezwania do usunięcia naruszenia prawa. Ma on zastosowanie również w odniesieniu do bezczynności.

Wydaje się jednak, iż przeciwko tej tezie, nie tylko w odniesieniu do bezczynności w zakresie informacji publicznej, ale także szerzej, w stosunku do aktów i czynności dotyczących uprawnień i obowiązków wynikających z przepisów prawa,²⁰ przemawia zarówno wykładnia językowa, jak i celowościowa. Po pierwsze należy jednak zaakcentować, iż udzielenie informacji publicznej jest czynnością, o której mowa w art. 3 §2 pkt 4 ppsa, dotyczy bowiem zarówno prawa wynikającego z art. 61 Konstytucji, jak i sprecyzowanego przedmiotową ustawą o dostępie do informacji publicznej. Stąd też środka zaskarżenia w odniesieniu do tych aktów należy poszukiwać w art. 52 §3, a nie §4 ppsa. Po drugie trzeba zgodzić się z poglądem, iż art. 52 ppsa wyraża ogólną zasadę uzależnienia drogi postępowania sądowo-administracyjnego od wykorzystania środków obrony administracyjnej. Z jego treści wynika jednak, iż ma to miejsce wówczas, gdy takie środki zaskarżenia przysługują: bądź na podstawie kpa, bądź przepisów szczególnych, czy też ppsa. Ponieważ ustaliliśmy już brak tego typu środków w ustawie o dostępie do informacji publicznej, a w odniesieniu do aktów i czynności, o których mowa w art. 3 §2 pkt 4 ppsa – brak ich jest w kodeksie postępowania administracyjnego, należy przeanalizować pod tym względem art. 52 §3 ppsa. Warto w związku z tym podkreślić, iż w świetle wykładni językowej art. 52 §3 ppsa odnosi się do skarg na akty i czynności, a nie na bezczynność w zakresie wydawania aktów. Taki sposób rozumienia tego przepisu wynika zresztą z dalszej jego części. Przepis ten wskazuje bowiem wyraźnie, iż skargi takie można wnieść po uprzednim wezwaniu na piśmie właściwego organu – w terminie czternastu dni od dnia, w którym skarżący dowiedział się lub mógł się dowiedzieć o wydaniu aktu lub podjęciu innej czynności – do usunięcia naruszenia prawa. Oznacza to, iż środek ten w jednoznaczny sposób wiąże się z aktywnością organu, a nie jego bezczynnością. Trudno w tej mierze zaakceptować stanowisko H. Knysiak-Molczyk, iż art. 52 §3 ppsa ma zastosowanie do bezczynności, nie odnosi się natomiast do niej w zakresie terminu przewidzianego w dalszej części tego artykułu.²¹ Przeciwko takiej wykładni przemawia bowiem językowe rozumienie tego

przepisu. Wydaje się zresztą, iż w momencie, gdy ustawodawca dąży do uzależniania zaskarżania bezczynności od wniesienia środka zaskarżenia, czyni to w sposób wyraźny, jak np. w art. 37 kpa, czy w art. 101a ust. 1 w związku z art. 101 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym,²² art. 88 ust. 1 i 87 ust. 4 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym,²³ art. 91 ust. 1 w związku z art. 90 ust. 4 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa²⁴ bądź art. 45 ust. 1 w związku z art. 44 ust. 4 ustawy z dnia 5 czerwca 1998 r. o administracji rządowej w województwie.²⁵ Za wskazanym wyżej sposobem rozumienia art. 52 §3 ppsa przemawia też treść art. 53 §2 ppsa. Zgodnie z nim, jeżeli organ milczy po wezwaniu do usunięcia naruszenia prawa w stosunku do aktu, to można po upływie określonego terminu wnieść skargę. W tej sytuacji ustawodawca powiązał wyraźnie dopuszczalność skargi z milczeniem organu po wniesieniu wezwania. Oznacza to, iż takie konsekwencje, nawet na gruncie ppsa, zostały przewidziane w stosunku do bezczynności określonego rodzaju. Nie można więc domniemywać, iż brak ujęcia bezczynności w art. 52 §3 ppsa jest tylko pewną niedoróbką legislacyjną. Uwagi te mają zresztą również znaczenie przy wykładni art. 52 §4 ppsa, który także nie może być odnoszony do bezczynności.

Warto zresztą podkreślić, iż w orzecznictwie NSA nie przyjmuje się wezwania do usunięcia naruszenia prawa, ani innej formy obrony na drodze administracyjnej jako bezwzględnej reguły. W przeciwnym bowiem przypadku w odniesieniu do bezczynności ministra, w której to sytuacji wyłączony jest warunek wniesienia zażalenia, przyjmowano by istnienie takiego środka. Uznaje się natomiast, iż na bezczynność tego organu można wnieść bezpośrednio skargę do sądu administracyjnego.²⁶

Nie bez znaczenia jest także w tym przypadku istota skargi na bezczynność i sposób składania skarg do sądu administracyjnego. Skarga ta nie zmierza bowiem jeszcze w istocie do określonego rozstrzygnięcia, a jedynie do rozpatrzenia wniosku. Nieco inne znaczenie ma ona w przypadku informacji publicznej, gdzie dodatkowo wchodzi jednak w grę wymienione wyżej przesłanki szybkości postępowania i jego odformalizowania. Składanie skarg do sądu za pośrednictwem organu administracji publicznej i możliwość samokontroli w postaci wydania aktu czyni zadość postulatowi umożliwienia wcześniejszej obrony na drodze administracyjnej. Jak podkreśla bowiem K. Klonowski, uwzględnienie w całości skargi przy zaskarżaniu bezczynności organu ma specyficzny charakter. Polega ono, odmiennie niż przy skardze na akt, nie na uchyleniu zaskarżonej decyzji w całości lub w części i orzeczeniu w tym zakresie co do istoty sprawy zgodnie z zarzutami skargi, lecz na podjęciu zaniechanych wcześniej czynności niezbędnych dla załatwienia sprawy lub rozstrzygnięcia w sprawie.²⁷ Wydaje się to przemawiać przeciwko stawianiu dodatkowych warunków utrudniających szybkie rozpatrzenie skargi na bezczynność, wtedy kiedy nie czyni tego wyraźnie ustawa. Skarga na bezczynność winna bowiem zmierzać do jak najszybszego przynaglenia organu do rozpatrzenia wniosku skarżącego.

²²⁾ Dz.U. 2001 r. Nr 142, poz. 1591 ze zm.

²³⁾ Dz.U. 2001 r. Nr 142, poz. 1592 ze zm.

²⁴⁾ Dz.U. 2001 r. Nr 142, poz. 1590 ze zm.

²⁵⁾ Dz.U. 2001 r. Nr 80, poz. 872 ze zm.

²⁶⁾ Wyrok NSA z dnia 29 sierpnia 2000 r. sygn. akt I SAB 52/00, czy wyrok NSA z dnia 3 listopada 1999 r. sygn. akt I SAB 156/99. Odmienny pogląd zaprezentowany w postanowieniu NSA z dnia 17 października 1997 r. sygn. akt IV SAB 31/97, spotkał się z krytyczną glosą B. Adamiak, OSP 1998 r. nr 10, poz. 185.

²⁷⁾ K. Klonowski, *Bezczynność* op. cit., s.33.

²⁰⁾ Por. M. Jaśkowska w: M. Jaśkowska, M. Masternak, E. Ochendowski, *Postępowanie* op. cit., s.130.

²¹⁾ Por. T. Woś, H. Knysiak-Molczyk, M. Romańska, *Prawo o postępowaniu przed sądami administracyjnymi*, Komentarz, Warszawa 2005 r. s. 88.

Należy podkreślić również, iż pod wpływem prawa europejskiego, w którym przywiązuje się szczególną rolę do terminowości i szybkości postępowania, wprowadzono do polskiego systemu prawa instytucje mające przeciwdziałać przewlekłości postępowania. Jedną z nich jest skarga na naruszenie prawa strony do rozpoznania sprawy w postępowaniu sądowym bez nieuzasadnionej zwłoki.²⁸ Oznacza to, iż kwestia terminowości i szybkości traktowana jest w naszym prawie jako szczególna wartość. Rozważając kwestię uzależniania drogi sądowej od wyczerpania środków obrony na drodze administracyjnej, należy mieć więc także na uwadze ten aspekt zagadnienia.

IV. Złożenie skargi na bezczynność powoduje wszczęcie postępowania sądowo-administracyjnego. Wywołuje ono stan zawisłości sprawy, co stanowi ujemną przesłankę dopuszczalności skargi w tej samej sprawie. Złożenie skargi nakłada na organ obowiązek jej przekazania sądowi wraz z aktami sprawy i odpowiedzią w terminie 15 dni od dnia jej otrzymania (art. 21 pkt 1 udip) bądź rozważenia możliwości samokontroli. Zgodnie bowiem z art. 54 §3 ppsa organ, którego działanie lub bezczynność zaskarżono, może w zakresie swojej właściwości uwzględnić skargę w całości do dnia rozpoczęcia rozprawy. Przy tym, w związku z charakterem skargi, jej uwzględnienie polegać może na rozpatrzeniu wniosku, a więc na udzieleniu informacji publicznej bądź wydaniu decyzji o odmowie jej udzielenia. W razie dokonania samokontroli sąd winien umorzyć postępowanie, a strona może ewentualnie skarżyć decyzję o odmowie udzielenia informacji, w zależności od przesłanek tej odmowy i po wyczerpaniu środków zaskarżenia.

W przypadku nieprzekazania akt lub niewykonania innych obowiązków sąd dysponuje możliwościami dyscyplinującymi organ. Może on przede wszystkim, na podstawie art. 55 §1 ppsa, na wniosek skarżącego orzec o wymierzeniu organowi grzywny. Jeżeli zaś organ nie przekazał sądowi skargi, mimo wymierzenia grzywny, sąd może na żądanie skarżącego, zgodnie z art. 55 §2 ppsa, rozpatrzyć sprawę na podstawie nadesłanego odpisu skargi, gdy stan faktyczny i prawny przedstawiony w skardze nie budzi uzasadnionych wątpliwości. Zdaniem S. Szustera, które należy w tym przypadku w pełni podzielić, ze względu na specyfikę spraw z zakresu udostępniania informacji publicznych oraz liczne mankamenty konstrukcyjne ustawy, rozwiązanie to nie będzie miało większej roli w praktyce.²⁹ Taką rolę może spełniać natomiast sygnalizacja. O rażących przypadkach naruszenia przez organ wspomnianych obowiązków, skład orzekający lub prezes sądu zawiadamia bowiem organy właściwe do rozpatrywania petycji, skarg i wniosków (art. 55 §3 ppsa).

Artykuł 21 pkt 2 udip nakłada na sądy administracyjne obowiązek rozpatrzenia sprawy w terminie 30 dni od dnia otrzymania przez sąd od organu, którego bezczynność zaskarżono, akt sprawy wraz z odpowiedzią na skargę. Jak wskazuje S. Szuster, bezskuteczny upływ tego terminu nie będzie rodził jednak skutków materialno-prawnych w postaci przyznania racji skarżącemu. Wskazuje on jedynie intencję ustawodawcy, aby maksymalnie skrócić okres oczekiwania w tych sprawach.³⁰ Upływ tego terminu może mieć jednak znaczenie przy skardze na opieszałość sądu.

W wyniku wniesionej skargi sąd może ją odrzucić, umorzyć postępowanie, oddalić lub uwzględnić. Przy czym w przypadku skargi na bezczynność odrzucenie może nastąpić po pierwsze z uwagi na brak przedmiotu zaskarżenia, a więc gdy skarga nie będzie dotyczyć w istocie bezczynności w zakresie informacji publicznej, czy innych form działania objętych zakresem kognicji sądu administracyjnego, a wynikających z art. 3 ppsa. Odrzucenie będzie też miało miejsce w przypadku nieuzupełnienia w wyznaczonym terminie, mimo wezwania, braków formalnych skargi, w tym nieuiszczenia wpisu. Z uwagi na specyfikę skargi i brak w tym zakresie szczególnych wymogów w grę nie będzie wchodzić odrzucenie z powodu przekroczenia terminu do wniesienia skargi, czy niewyczerpania środków zaskarżenia. Odrzucenie następuje w formie postanowienia, które może być wydane na posiedzeniu niejawnym. Przysługuje od niego skarga kasacyjna.

Umorzenie postępowania może nastąpić w przypadku ustania bezczynności, wycofania skargi lub innej bezprzedmiotowości postępowania. Również i to orzeczenie zapada w formie postanowienia, które może zostać podjęte na posiedzeniu niejawnym. Służy od niego skarga kasacyjna.

Oddalenie skargi na bezczynność następuje w formie wyroku, gdy skarga ta jest nieuzasadniona, a więc np. organ udzielił przed jej wniesieniem stosownej informacji, czy podmiot, do którego się zwrócono z wnioskiem nie był dysponentem danej informacji i poinformował o tym wnoszącego wniosek. Od wyroku takiego służy skarga kasacyjna.

Uwzględnienie skargi na bezczynność, w oparciu o art. 149 ppsa, nastąpi w sytuacji, gdy sąd uzna skargę za uzasadnioną. Będzie ono polegać w tym przypadku na zobowiązaniu organu do rozpatrzenia określonego wniosku w wyznaczonym terminie (por. wyrok NSA z dnia 20 czerwca 2002 r. sygn. akt II SAB 113/02 czy z 30 października 2002 r. sygn. akt II SAB 181/02). Na tym etapie sąd nie może bowiem rozstrzygać o sposobie rozpatrzenia wniosku, tzn. czy ma ono nastąpić poprzez udzielenie informacji, a więc czynność materialno-techniczną, czy też odmowę w drodze decyzji. Od takiego wyroku służy skarga kasacyjna.

Skargi kasacyjne służą na równych prawach uczestnikom postępowania sądowo-administracyjnego, tj. skarżącemu, organowi, którego bezczynności dotyczyła skarga, prokuratorowi oraz Rzecznikowi Praw Obywatelskich. Powinny one odpowiadać wymogom pisma procesowego, wskazanym powyżej, a w odniesieniu do treści spełniać warunki z art. 176 ppsa. W związku z tym powinny także zawierać oznaczenie zaskarżonego orzeczenia ze wskazaniem, czy jest ono zaskarżone w całości, czy w części, przytoczenie podstaw kasacyjnych i ich uzasadnienie, a także wniosek o uchylenie lub zmianę orzeczenia z oznaczeniem zakresu żadanego uchylenia lub zmiany. Podstawą skargi kasacyjnej może być przy tym, zgodnie z art. 174 ppsa, naruszenie prawa materialnego przez błędną jego wykładnię lub niewłaściwe zastosowanie albo naruszenie przepisów postępowania, jeżeli uchybienie to mogło mieć istotny wpływ na wynik sprawy. Naruszenie przepisów postępowania musi jednak dotyczyć tych z nich, które stosuje sąd administracyjny, a więc przepisów ppsa. Respektowaniu podstaw kasacyjnych służy przymus adwokacko-radcowski. Zgodnie z art. 175 ppsa skarga kasacyjna powinna być bowiem sporządzona przez adwokata czy radcę prawnego, chyba że sporządza ją sędzia, prokurator, notariusz, profesor, dr habilitowany nauk prawnych będący stroną, jej przedstawicielem lub pełnomocnikiem, albo gdy skargę wnosi prokurator lub Rzecznik Praw Obywatelskich. Sprawą wymagającą rozważenia

²⁸) Wprowadzona ustawą z dnia 17 czerwca 2004 r. o skardze na naruszenie prawa strony do rozpoznania sprawy w postępowaniu sądowym bez nieuzasadnionej zwłoki, Dz.U. Nr 179, poz. 1843.

²⁹) S. Szuster, *Komentarz do art. 21 op. cit.*

³⁰) J.w.

jest natomiast kwestia, czy skarga taka może być wnoszona przez rzecznika patentowego – w sprawach własności przemysłowej bądź doradcę podatkowego w sprawach zobowiązań podatkowych. Wydaje się jednak, iż regulacje te mogą – po pierwsze – jak na gruncie ustawy z dnia 30 czerwca 2000 r. prawo własności przemysłowej,³¹ stanowić *lex specialis* w odniesieniu do informacji publicznej i zawierać w tym zakresie szczególne reguły dostępu. W takim więc przypadku sprawa nie będzie się toczyć na podstawie ustawy o dostępie do informacji publicznej. Po drugie regulacje te mogą zawierać pewne rodzaje tajemnic, stanowiące wyjątek od jawności administracyjnej np. w zakresie tajemnicy skarbowej.³² W tym przypadku przedmiotem sprawy nie będzie jednak zobowiązanie podatkowe lecz dostęp do informacji. Nie będzie więc możliwy na gruncie ustawy o dostępie do informacji udział rzecznika patentowego czy doradcę podatkowego. Nie bez znaczenia jest również fakt, że ta ostatnia sytuacja może mieć miejsce dopiero w przypadku skargi na decyzję o odmowie udzielenia informacji, a nie w przypadku skargi na bezczynność w zakresie dostępu do tej informacji.

W wyniku złożonych skarg sąd może odrzucić skargę kasacyjną, gdy nie spełnia ona warunków formalnych, umorzyć postępowanie np. w wyniku jej cofnięcia, oddalić skargę kasacyjną, gdy uzna ją za nieuzasadnioną bądź ją uwzględnić i w zależności od sytuacji uchylić zaskarżony wyrok czy postanowienie, znieść postępowanie w zakresie dotkniętym nieważnością i przekazać je do ponownego rozpatrzenia, bądź samemu rozstrzygnąć sprawę, a także uchylić zaskarżone orzeczenie i odrzucić skargę lub umorzyć postępowanie. Czyni to w drodze wyroku bądź postanowienia (np. odrzucenie skargi kasacyjnej). W przypadku skargi kasacyjnej, wnoszonej od postanowienia, orzeczenie NSA przyjmie zawsze formę postanowienia.³³

W przypadku uwzględnienia skargi na bezczynność można wnieść następnie, po wezwaniu organu do usunięcia naruszenia prawa, skargę na niewykonanie wyroku sądu. W trybie art. 154 §1 ppsa sąd administracyjny może wówczas wymierzyć organowi grzywnę lub orzec o istnieniu lub nieistnieniu uprawnienia czy obowiązku, jeżeli pozwala na to charakter sprawy oraz niebudzące uzasadnionych wątpliwości okoliczności jej stanu faktycznego lub prawnego. Także i w tym przypadku, z uwagi na specyfikę spraw, rozwiązanie takie będzie trudne do zastosowania. Sąd administracyjny nie jest bowiem władny do wyegzekwowania od organu udzielenia określonej informacji publicznej.

Egzekwowanie obowiązku udzielenia informacji publicznej możliwe jest w istocie jedynie w oparciu o art. 23 udip. Kto więc wbrew ciążącemu na nim obowiązkowi nie udostępnił informacji publicznej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. W sprawie tej właściwy jest sąd powszechny. Grzywna ta nie jest jednak tożsama z grzywną, o której mowa w art. 154 ppsa. Stąd żądanie skargi ukarania osoby, która nie udostępniła informacji publicznej, jest niedopuszczalne w postępowaniu przed sądem administracyjnym. Możliwa jest

także odpowiedzialność dyscyplinarna, porządkowa albo rozwiązanie stosunku pracy z winy pracownika.

Complaint against inaction within the domain of access to public information

I. The right to information as well as the right for the protection of personal data both function in the Polish legal system. The former is a direct result of Article 61 of the Constitution of the Republic of Poland of 2 April 1997¹ as well as the Act on the Access to Public Information of 6 September 2001 (hereafter AAPI).² One can find the basis of the former right in Article 51 of the Constitution as well as in the Act on the Protection of Personal Data (hereafter APPD).³ There are variety of legal relations concerning these rights that overlap, furthermore, there are also a number of legal conflicts that result in their interaction. An analogous situation can be found in the legal systems of other states, although legislators in other countries use different solutions to solve these conflicts including organisational solutions. Some European states have created personal data protection authorities whose job it is also to protect one's right to access to information. These kinds of regulations have been adopted, for example, in Hungary where a Parliamentary Commissioner for Data Protection and Freedom of Information has been appointed and also in some German states (Lande). In Berlin there is a Commissioner for Data Protection and Freedom of Information and in Brandenburg a Commissioner for Data Protection and Access to Information operates. In turn, in other legal systems these two functions are separated.

In Poland, the second solution has been adopted. The Inspector General for the Protection of Personal Data (GIODO) is not responsible for the protection of freedom of information or the coordination of any action within this scope. There is no central authority which possesses this kind of power or jurisdiction in Poland. Therefore, this means that access to public information is in many cases hampered or, in fact, this access is abused. However, this does not mean that the issue of access to information is found completely outside the interests of the Inspector General for the Protection of Personal Data. Evidence of this can be found in the fact that an international seminar on "Protection of Personal Data and Access to Public Information" was organised on 12 May 2003 by the Academy of Data Protection. Among the variety of topics discussed, there were many issues concerning the access to public information in the judicial decisions of the Supreme Administrative Court. The study below constitutes a development and continuation of the propositions put forward in this field at the above-mentioned international conference.

³¹ Dz.U. 2003 r. Nr 119, poz. 1117 ze zm. – por. art. 181, 207 ust.1 czy 251.

³² Por. rozdział VII, w szczególności art. 293 i n. ustawy z dnia 29 sierpnia 1997 r. ordynacja podatkowa, Dz.U. 2005 r. Nr 8, poz. 60 ze zm.

³³ Szerzej na temat orzeczeń NSA – M. Jaśkowska, M. Masternak, E. Ochendowski, Postępowanie op. cit., s.191 i d.

¹ Law Gazette No. 78, 484 with corrections.

² Law Gazette No. 112, 1198 with amendments.

³ Law Gazette of 2002 No. 101, 926 with amendments.

II. As previously noted, the issues of access to public information and protection of personal data are regulated in differing and separate ways in Poland. The second issue is dealt with through the Act of 6 September 2001 on the Access to Public Information. The former is dealt with through the Act on Protection of Personal Data. Concurrently, the first of these two acts indicates situations in which the question of protection of personal data can be a factor in meeting with a refusal for giving out information. In accordance with Article 22 of this Act in cases where there is a refusal for giving out information owing to protection of personal data legal action can be taken in a common court. In consequence, this means that a decision issued on the basis of Article 16 of the Act, in which the protection of personal data is called upon, is taken by the authority from which information is requested, but is controlled by a common court. This court is able to investigate the settlement not only in terms of its legality but also the matter of the legitimacy of the premise behind the refusal to make information available. The court ruling ascertaining the rights to obtain access to public information will constitute a basis for providing this information and not, as in the case of a sentence of an administrative court, the basis for reconsidering the case. In such cases, the jurisdiction of the Inspector General for the Protection of Personal Data is excluded as the authority for the Protection of Personal Data (Article 18 (3) in relation to Article 18 (3), point 2 of the APPD and Article 22 of the AAPI). Concurrently however, an individual in public office cannot successively question the legality of having public information about them being made available (*a contrario* Article 32 (1), point 8 and Article 23 (1) of the APPD).⁴

The scope and way of controlling administrative decisions in the case of making public information available or not allowing access to public information not excluded from the jurisdiction of administrative courts through Article 22 of the AAPI, are regulated in detail by the provisions of judicial-administrative proceedings, that is the Act of 30 August 2002 on the Law of Proceedings before Administrative Courts (hereinafter referred to as LPAC).⁵ The exclusive jurisdiction of these courts is related to examples of inaction by entities that are responsible for making public information available.⁶

At this point it is worth pointing out the most crucial factors in relation to the admissibility of lodging complaints against inaction in the scope of making public information available, which result from the regulations of the LPAC but remain in direct relation to the solutions established on the grounds of the Act on the Access to Public Information. The basic premises of admissibility of judicial-administrative proceedings are, above all, the existence of a subject of prosecution, that is an act found in the bounds of an administrative court and the bill of indictment, in other words, a pleading setting the legal proceedings in motion.⁷ With reference to the first of these, the legal basis of

a complaint against inaction concerning access to public information is Article 3 §2, point 8 of the LPAC in relation to Article 3 §2, point 4 of the LPAC. The pleading is the complaint put forward by an eligible entity. The assertion before court that there is a subject of prosecution and a bill of indictment allows for the investigation of the appropriate premises in the admissibility of complaint. These premises are understood as the formal conditions that are required in the contents of the complaint, that is in the pleading, as well as other statutory-defined requirements that need to be fulfilled in order for the pleading to be considered by a court. To begin with, this concerns the people authorised to lodge complaints, the formal requirements of the pleading itself as well as the way in which it is filed. Amongst these premises, negative premises can also be distinguished. Their existence leads to inadmissibility of setting judicial-administrative proceedings in motion despite fulfilment of the remaining conditions.

A complaint against inaction can be, above all, filed by an appropriate entity possessing the lawsuit authorisation. On the basis of the Act on the Access to Public Information, these can be both the petitioner as well as the prosecuting attorney, the Ombudsman for Civic Rights as well as social organisations working within their statutory bounds in cases concerning the legal interests of other people insofar as they have taken part in administrative proceedings (Article 50 §1 of the LPAC). This situation can, in essence, apply to the inaction of an authority in the appeal proceedings. To the moment of the issue of a decision of refusal, it is difficult to speak of the administrative proceedings which guarantee the participation of a social organisation in Art. 31 of the Act on the Code of Administrative Procedure of 14 June 1960.⁸ When the decision is issued, one can, in principle, no longer speak of inaction. It can, therefore, apply only to inaction of an appealing authority after an appeal has been lodged. A complaint against inaction should be filed to the Regional Administrative Court, which is appropriate as it is the headquarters of the authority to which one turns in asking for information, and therefore it is the authority whose inaction is the subject of the complaint. The complaint is lodged, in accordance with Article 54 §1 of the LPAC, in mediation with the authority which is the subject of the complaint. The complaint should fulfil the conditions of a pleading as defined in Article 46 of the LPAC. In accordance with this Article, every pleading should include: the designation of the court to which the pleading is referred to, the forename and surname or name of both parties, their legal representatives and plenipotentiaries, identification of the kind of pleading it is, the structure of the petition or declaration, signatures of the party or their representatives or plenipotentiaries, annexes. If the pleading of the party concerned is the first of its kind, it must also include identification of the place of residence or, if this is not included, a correspondence address or the address of the headquarters of the parties concerned, their legal representatives or plenipotentiaries, as well as the subject of the case. Power of attorney or proxy must be included in the pleading if it has not been documented beforehand. Also, certified copies of the pleading and all annexes must be included in order for them to be presented to all parties concerned. Moreover, if the original annexes have not been filed in court, then one copy of each annex must be deposited in the judicial acts. Furthermore, the claim should fulfil the requirement defined in Article 57 §1 of the LPAC, that is in the afore-mentioned situation, inaction has to be clearly defined in order for the particular petition to be investigated and in

⁴) G. Sibiga, *Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych* [Access to public information and the right to privacy of the individual and their personal data], Local Authority 2003, No. 11, p. 10.

⁵) Law Gazette No. 153, 1270 with amendments.

⁶) M. Jaśkowska, *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego* [Access to public information in light of the rulings of the Supreme Administrative Court], Toruń 2002, p. 71 or S. Szuster, *Commentary to Article 21 of the Act of the 6 September 2001 on the Access to Public Information*, Law Gazette 2001, No. 112, 1198/Lex/el 2003), K. Nowacki, M. Mucha, *Problemy regulacji prawnej dostępu do informacji w Polsce* [Problems of legal regulation of access to information in Poland], Court Review 2002, No. 2, p. 24. They allow for action to be brought against someone in a common court in order for a decision to be reached whether there is a responsibility for making public information available in cases where an entity guilty of inaction does not belong to the public administration.

⁷) T. Woś, *Postępowanie sądowoadministracyjne* [Judicial-administrative Proceedings], Warsaw 1999, p. 91.

⁸) Law Gazette 2000, No. 98, 1071 with amendments.

order to determine which authority is charged with inaction. A condition for lodging a complaint is paying a fee, which currently stands at PLN 100, on the basis of §2, point 6 of the Regulation by the Council of Ministers dated 16 December 2003 on the amount and the detailed rules governing the fees of legal proceedings before administrative courts.⁹

If a complaint does not fulfil the formal requirements of a pleading, then the judge calls both parties to give them seven days in which to do so under penalty of dismissal of the complaint. This applies to both the call to pay the necessary fee, insofar as it does not apply to a permanent fee (this applies in cases of complaints against inaction) and when the complaint is not lodged by a solicitor or lawyer.

However, when the situation pertains to complaints that concern inaction then there is no deadline for the submission of the complaint. This applies to all entities lodging complaints.¹⁰

While investigating the premises of admissibility of the complaint, a question arises whether in cases of complaints against inaction there is a requirement for all means of charging to be exhausted. This issue is the topic of the next section.

III. Legal proceedings concerning access to public information can come to a conclusion with this access being given or being denied. In the first case, the access to information is given in the form of technical and material action,¹¹ which is not questioned by either the literature or by the body of rulings in Poland. There is no application here of the Act on the Code of Administrative Procedure and the Act on the Access to Public Information of 6 September 2001 contains only fragmentary regulations on this matter, indicating, amongst other things, the duty to mark who and where the information is taken from and for whom the information is being made available (Article 12, AAPI), the timescale for settling the issue (Article 13, AAPI), and also partly the way and form of making the information or data available (Article 14, AAPI). However, the refusal to make public information available and the discontinuation of legal proceedings for the access to information take place by administrative decision (Article 16 of the AAPI).

These varied ways of bringing proceedings for the access to public information to a close have given rise to, both in the literature and in the jurisprudence, a discrepancy of opinion concerning, amongst other things, the conditions for admissibility of complaints against inaction in a subjective scope owing to the exhaustion of means of charging. Four positions are currently represented in respect to admissibility of such complaints. The first three make the admissibility of the complaint before an admini-

strative court dependent on an earlier submission of means of charging by administrative action, while these means can be taken as a complaint or a call to remove the given infringement of the law or alternatively one of these means. According to representatives of the fourth position, a complaint against inaction concerning public information put before an administrative court does not have to be preceded by any means of charging by administrative action.

Supporters of the first position believe that a requirement for lodging a complaint against inactivity is the prior lodging of an appeal before a higher authority, in accordance with Article 37 of the Code of Administrative Procedure (CAP), unless inaction is lodged against a minister in which case the defence against this complaint is not undertaken by administrative routes. This opinion has been put forward in, amongst others, a ruling by the Supreme Administrative Court of 18 March 2005, Reg. No. OSK 1209/04. It was highlighted in this ruling that the Law on Legal Proceedings within Administrative Courts accepts the binding principle to be that the administrative judicial route is admissible after all means of defence on the administrative route have been exhausted. The exception to this principle occurs only when during administrative proceedings there is no means of charging or if a particular ruling determines this course. On the backdrop of the Act on Access to Public Information in light of solutions accepted in Articles 13 and 16 of the Act, defence of inaction by an authority should be accepted as the obligation of the authority to issue a decision thereby using means of defence against inaction in accordance with Article 37 of the CAP. Therefore, a premise for the lodging of a complaint against inaction before an administrative court in the sphere of not giving access to public information is the lodging of an appeal to a higher authority, unless the complaint relates to a minister.

The above-mentioned opinion may seem difficult to accept. The right to lodge an appeal in cases where an authority remains silent in cases where an application is submitted to make information available is difficult to introduce into the subject of the Act, by simple grammatical interpretation, purposeful or systematic explanation. Firstly, the Act does not provide any clear instrument or means for combating inaction. Furthermore, these means cannot be found in the Code of Administrative Procedure. The Act on Access to Public Information, above all, guarantees that the applicant has access to information, which is his right following from Article 61 of the Constitution. The governing principle is making information available whereas refusal to make information available is seen as an exception to the principle. As has been highlighted above, making information available occurs in the form of technical and material action and a refusal occurs through decision. However, in Article 16 (2) of the Act, the legislator makes a clear reference to the CAP only in reference to decisions issued (in accordance with Article 16 (2)) when there is a refusal to making information available and a discontinuation of proceedings in the cases defined in Article 14 (2). The legislators have not made such a reference to the proceedings of making information available. This is highlighted by A. Knopkiewicz who notes that the use of "to the decision" in Article 16 of the Act also serves to exclude the use of the rules of the Code on phases of the proceedings that precede the issue of a decision concerning the refusal to make information available or the discontinuation of proceedings.¹² If the intention of the

⁹ Law Gazette 2000. No. 98, 1071 with amendments.

¹⁰ M. Jaśkowska in M. Jaśkowska, M. Masternak, E. Ochendowski, *Postępowanie sądowoadministracyjne* [Judicial-administrative Proceedings], edition 2, Warsaw 2005, p. 132.

¹¹ M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej, Informatyzacja administracji* [Public Information Bulletin, Implementing Information Technology in Administration], Wrocław 2005, p. 85; A. Knopkiewicz, *Tryby udostępniania informacji publicznej* [Methods of making public information available], RPIES 2004, No. 4, p. 97; and R. Stefanicki, *Ustawa o dostępie do informacji publicznej, wybrane zagadnienia w świetle orzecznictwa sądowego* [Act on Access to Public Information, selected problems in light of judicial rulings], PiP 2004, No. 2, p. 109; also Supreme Administrative Court ruling of 20 June 2002, Reg. No. II S.A./Lu 507/02; also ruling of the Regional Administrative Court in Warsaw of 17 June 2004, Reg. No. II SAB 424/03 and the ruling of the Supreme Administrative Court of 18 March 2005, Reg. No. OSK 1209/04.

¹² A. Knopkiewicz, *Tryby* [Methods] *quot.*, p. 103.

legislator was the compliance with the rules of the Code of Administrative Procedure for the whole proceedings mentioned above then this would be clearly stated in the Act on Access to Public Information. This technique of editing the rules and regulations is also practiced by legislators in other Acts in which there are requirements to apply the code to the whole procedure and not just one of the decisions.¹³ A. Knopkiewicz also highlights that in this situation we are dealing with a conflict of the more general and earlier norms of Article 1 (1) of the CAP in relation to Article 16 of the AAPI and the more detailed and later norms included in Article 16 (2) of the AAPI. In this situation, on the other hand, two rules of conflict for the use of the CPA only after the moment a decision is issued are manifest: *lex specialis derogate legi generali* and *lex posterior derogate legi priori*. The justification of not applying this code to proceedings before the issue of a decision on the refusal of access to information or discontinuation can be also found in the fact that the will of the legislator is a reduction of formalities within these proceedings.¹⁴ There would be a paradox if the complaint of a party wanting access to information was dependent on the demand to require from them a prior application by administrative routes of a refusal to make information available. As indicated in the Supreme Administrative Court ruling of the 17 February Reg. No. II SAB 424/03, "the charging party cannot be accused of not using means and instruments of prosecution of which there is mention in Article 37 of the CAP. By requiring that a higher authority undertakes the necessary action as stipulated in Article 37 (2) of the CAP, the charging party in essence requiring that a negative decision be issued, which is obviously in contradiction to its demands".

It also needs to be pointed out that if the legislators wished for the regulations of the Code of Administrative Procedure to be stretched to cover a more wider scope, for example, proceedings on access to public information, then they would have clearly undertaken so. There were no barriers in the way when, in Article 13 of the Act giving the consequences of not making information available until a specific point in time, the legislators also indicated the additional instruments of prosecution in the form of an appeal. There are, of course, other detailed norms found in this regulation which are related to the way in which applicants are informed about the reasons for any delay. One cannot, however, assume from the Supreme Administrative Court ruling of 18 March 2005 Reg. No. OSK 1209/04 referring in its argumentation to Article 13 of the Act, that this article is to some extent an introduction to the issue of a decision on the refusal of access to information, hence the consequence of it is the right to lodge an appeal against the inaction of an authority. Firstly, even on the backdrop of Article 13 of the AAPI, the legislators have highlighted the fact that the proceedings should aim towards giving access to information and not refusing it. In accordance with Article 13 (2), the notice must not only concern the reasons for any delay, but also give a deadline when the information can be made available. Secondly, due to the fact that at this particular phase, we are still dealing with proceedings concerning material and technical action, then we cannot introduce a subjective regulation of the law to the appeal. This is important as in principle all administrative procedures assume that the right to lodge an appeal serves to be in force when the act constitutes this fact. It is not

without meaning that the principles of the Act on Access to Public Information are to aim towards the quick settling of all issues, by simplifying proceedings as well as shortening all deadlines in relation to the CAP including deadlines for the examination of applications on the means of charging. In consequence, this has an impact on the way in which a subjective interpretation of the Act is undertaken and it also means that even when there is doubt, these issues cannot be solved by extending the proceedings by making them dependent on unforeseen formal requirements found in this Act.

According to the second position, the lodging of complaints against inaction in relation to access to public information is dependent on the exhaustion of means of charging, but this obligation has an alternative nature. The applicant can make use of the right to lodge an appeal as well as the call to remove the infringement of the law, which follows from Article 52 §3 and §4 of the LPAC. This opinion is represented by a ruling of the Regional Administrative Court in Opole of 27 May 2004 Reg. No. II SAB/Op 1/04¹⁵ as well as ruling by the Supreme Administrative Court of 8 July 2005 Reg. No. OSK 1682/04. The Opole ruling indicated that in a complex situation where an applicant expects a positive settlement to the application, but is also prepared for refusal or a decision in that the information does not belong to the public domain it must be accepted that the means of charging have been exhausted both when an applicant lodges an appeal through Article 37 §1 of the CAP before lodging complaints, which is required with reference to complaints against inaction consisting in the non-issue of a decision and also when an applicant has called for the authority to remove the infringement of the law, which is required when an authority is guilty of inaction in the scope of material and technical action (Article 52 of the LPAC).¹⁶ In the Supreme Administrative Court ruling it was highlighted that in specific cases the intentions of the applicant need to be examined, thus, checked whether the applicant demands action on the basis of Article 37 §2 of the CAP or material and technical action. In the latter case, a complaint should be preceded by a call to remove the infringement of the law submitted on the basis of Article 52 §4 of the LPAC.

The above-mentioned arguments which appeal against the dependency of the admissibility of a complaint to the lodging of an appeal on the basis of Article 37 of the CAP appear to be current in relation to the proposition concerning the possibility of submitting an alternative means of charging. Hence, the question has to be answered whether the admissibility of the subjective complaint is determined by the submission of a call to remove the infringement of the law irrespective of whether the means are alternative to the complaint on the basis of Article 37 of the CAP or not.

The literature draws attention to the fact that a complaint against inaction concerning access to public information can in essence be filed after the authority has been called to remove the infringement of the law. This opinion is advocated by, amongst others, K. Klonowski. He claims that in cases of complaints against inaction of an authority in the scope of the remaining regulations as well as the acts and actions defined in Article 3 §2 (4) of the LPAC, the filing of a complaint should be preceded by a call in writing to the relevant authority within fourteen days from the day on which the charging party found out or was able to find out about the issue of an appropriate act or the underta-

¹³) For example, Article 22 of the Act on Protection of Personal Data or Article 80 (with reservation to Article 81) of the Act on the Competition and Consumer Protection of the 15 December 2000, Law Gazette 2003, No. 86, 804 with amendments.

¹⁴) A. Knopkiewicz, Tryby [Methods] quot., p. 103.

¹⁵) The Opole Regional Administrative Court and Supreme Administrative Court 2005 2/5/33.

¹⁶) The Opole Regional Administrative Court and Supreme Administrative Court 2005 2/5/33, p. 84.

king of another action, that is the removal of the infringement.¹⁷ According to M. Bernaczyk, M. Jabłoński and K. Wygoda, if silence is related to the behaviour of a state authority (a public entity obligated to the AAPI) then prior to an appearance before an administrative court, it should be called to remove the infringement of the law. This is an unconditional premise, whose fulfilment determines the possibility of lodging complaints before an administrative court. However, in a situation where the entity is not a state institution (or another type of public authority) the interested party has the right to file a suit before a common court in order to ascertain the responsibility for making the information available.¹⁸ We should set aside the issue of differentiating the judicial course of action taken which depends on the authority that does not find justification in light of the Act on Access to Public Information, and point out that the proposition concerning the dependency of the complaint against this type of inaction on the call to remove the infringement of the law has no legal basis in Article 52 of the LPAC. In essence, it is a revision of the position which found its basis in the old regulations of judicial-administrative proceedings. Pursuant to Article 34 (3) of the Act on the Supreme Administrative Court of 11 May 1995,¹⁹ if the act does not stipulate the means of appeal in the case which is the subject of the complaint, then before the filing of it before the court, one must address the relevant authority with a call to remove the infringement of the law. The deadline for the filing of this complaint begins its course after thirty days from the day of servicing the call. This means that in the light of the Act of the Supreme Administrative Court, the call to remove the infringement of the law is not related to any specific form of action or inaction of public administration, but constitutes a consequent lack in the act of particular means of appeal. Meanwhile, this issue is regulated differently by the law on administrative court procedure.

Therefore, it is difficult to agree with the position presented in the first part of the ruling of the Supreme Administrative Court of 18 March 2005 Reg. No. OSK 1209/04. Despite the fact that ultimately the ruling, in relation to complaints against inaction relating to public information, is dependent on the admissibility of lodging an appeal on the basis of Article 37 of the CAP, the introductory part of the justification presents the general ways in which to combat inaction. It was highlighted in this ruling that, above all, the binding principle of the LPAC is that the way proceedings before an administrative court take place is admissible only after taking advantage of all means of prosecution through administration. These means of prosecution are stipulated in the CAP or other detailed regulations. In cases when the object of prosecution is the exercise of public administration in different legal forms under which the CAP is not applied, the obligation to make complete use of defence is regulated by the LPAC. The means of prosecution are stipulated in Article 52 §3 and §4 in the form of a call to remove the infringement of law. It is also applicable in reference to inaction.

However, it seems that contrary to this proposition, not only in reference to inaction within the domain of public information, but also in a wider context in relation to acts and action concerning powers and obligations stemming from legal regulations,²⁰ is the simple linguistic interpretation as well as purposeful explanation. Firstly, one needs to

highlight the fact that making public information available is an action mentioned in Article 3 §2, point 4 of the LPAC. This concerns both the law following from Article 61 of the Constitution as well as the specific subjective Act on Access to Public Information. Therefore, the means of prosecution in relation to these acts can be found in Article 52 §3 and not §4 of the LPAC. Secondly, one must agree with the opinion that Article 52 of the LPAC presents the general principle of making the judicial-administrative procedure dependent on making full use of administrative defence. It follows from the subject matter therein that this takes place when these means of prosecution are entitled to be used either on the basis of the CAP or through specific regulation, or even through the LPAC. Since we have established that there is lack of such means in the Act on Access to Public Information, and in relation to acts and actions mentioned in Article 3 §2, point 4 of the LPAC the lack is in the Code of Administrative Procedure, then there is a need to re-examine Article 52 §3 of the LPAC in this matter. It is worth highlighting that in the light of the linguistic interpretation, Article 52 §3 of the LPAC relates to the complaints against acts and actions and not inaction in the scope of the issue of acts. This manner of interpreting this regulation results from points made clear later in the regulation. It does not indicate clearly whether such complaints can be lodged after a prior call in writing to the relevant authority is made in forty days from the day on which the charging party found out or was able to find out about the issue of the act or undertaking of another action to the removal of the infringement of the law. Therefore, these means in no ambiguous way relate to the activity of the authority and not its inaction. In this case, it is difficult to accept the position of H. Knysiak-Molczyk as Article 52 §3 of the LPAC relates to inaction and not to the scope of the deadline stipulated in the later parts of the article.²¹ In contradiction to this interpretation there is a simple linguistic understanding of this regulation. It seems that the moment in which the legislator is striving at making the charge of inaction dependent on the submission of means of charging, they do so in a clear manner as in, for example, Article 37 of the CAP, or Article 101a (1) in relation to Article 101 (3) of the Act of 8 March 1990 on Local Self-Government,²² Article 88 (1) and 87 (4) of the Act of 5 June 1998 on Provincial Self-Government,²³ Article 91 (1) in relation to Article 90 (4) of the Act of 5 June 1998 on Regional Self-Government²⁴ or Article 45 (1) in relation to Article 44 (4) of the Act of 5 June 1998 on Regional Government Administration.²⁵ In the above-mentioned way of understanding Article 52 §3 of the LPAC, we must also consider Article 53 §2 of the LPAC. In accordance with it, if an authority is silent after being called to remove an infringement of the law in relation to an act, then one can lodge a complaint after a specified deadline. In this situation, the legislators made the admissibility of the complaint dependent on the silence of the authority after the issue of a call to remove the infringement. This means that these consequences, even on the basis of the LPAC, are stipulated in relation to the inaction of a specific kind. One cannot, therefore, presume that the lack of depiction of inaction in Article 52 §3 of the LPAC is a certain legislative fault. These remarks are of considerable importance in the interpretation of Article 52 §4 of the LPAC, which also does not necessarily have to be related to inaction.

¹⁷⁾ K. Klonowski, *Bezczynność organu w postępowaniu sądowoadministracyjnym* [Inaction of authorities in Judicial-administrative proceedings], Local Authority 2004, No. 4, p. 31-32.

¹⁸⁾ M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn* [Bulletin], quot., p. 86-87.

¹⁹⁾ Law Gazette No. 74, 368 with amendments.

²⁰⁾ M. Jaśkowska in: M. Jaśkowska, M. Masternak, E. Ochendowska, *Proceedings*, quot. p. 130.

²¹⁾ T. Woś, H. Knysiak-Molczyk, M. Romański, *Prawo o postępowanie przed sądami administracyjnymi* [Law on Proceedings in Administrative Courts], Commentary, Warsaw 2005, p. 88.

²²⁾ Law Gazette 2001, No. 142, 1591 with amendments.

²³⁾ Law Gazette 2001, No. 142, 1592 with amendments.

²⁴⁾ Law Gazette 2001, No. 142, 1590 with amendments.

²⁵⁾ Law Gazette 2001, No. 80, 872 with amendments.

It is worth highlighting that in the judicial decisions of the Supreme Administrative Court there is no provision for a call to remove the infringement of the law or any other form of defence through administration as an unconditional rule. In other cases, in relation to inaction of a minister in which case the condition of lodging an appeal is excluded, the existence of other means would be accepted. However, the recognition of inaction of this authority can be filed directly through a complaint before the administrative court.²⁶

It is not without meaning that in this case also the essence of the complaint against inaction is the way in which the complaint is put before the administrative court. This complaint does not yet aim towards a specified resolution, but only an examination of the application. It has a somewhat different meaning in relation to public information where, additionally, the afore-mentioned premises of the speed of the proceedings and reduction of formalities have a part to play. Lodging complaints before a court via a public administration authority and the possibility of self-investigation in the form of acts satisfies the postulates that allow for the earlier defence by administration. As K. Klonowski highlights, the complete consideration of the complaint when accusing the authority of inaction has a very particular nature. This consists in, unlike complaints against acts, not on reversing an appealed decision in full or in part and the ruling of the essence of this case in accordance with the charges of it, but in undertaking the essential actions that were earlier forsaken in order to bring the case to a conclusion or resolve it.²⁷ This seems to appeal against the case for setting additional requirement that would hamper the speedier handling of a complaint against inaction in situations when the Act does not make this apparent. The complaint against inaction should aim at forcing the authority into investigating and resolving the charge as soon as possible.

It needs to be also highlighted that under the influence of European law, which is particularly attached to the role of punctuality and the quickness of proceedings, Polish law has introduced institutions aiming to counteract the lengthiness of proceedings. One of these institutions is the complaint against infringement of the right of a party to hear a case in court without due delay.²⁸ This means that the issue of punctuality and the speed has particular value in Polish law. Considering the issue of dependency of the courts on the exhaustion of means of defence through administration, one should also be aware of this aspect of the problem.

IV. Lodging a complaint against inaction induces a commencement of judicial-administrative proceedings. This causes a state of dependence of the case which constitutes a negative premise of the admissibility of the complaint in the same case. The lodging of a complaint imposes a responsibility on the authority to pass it on to a court together with the case files and the responsibility to give a reply within fifteen days from the day it is received (Article 21 (1) of the AAPI) or the consideration of the possibility of self-investigation. In accordance with Article 54 §2 of the LPAC, the authority whose

activities are questioned or which is charged with inaction, can in the scope of its own jurisdiction consider the entire complaint from the day the case begins. At the same time, in connection with the nature of the complaint, its consideration can consist of the investigation of the application, that is making the public information available or deciding to refuse access. If self-investigation ensues, the court should discontinue legal proceedings and the party, if need be, can question the negative decision concerning access to information depending on the premises of the refusal and after exhaustion of all charging means.

In the event where the case files have not been passed on or in case of non-execution of other responsibilities, the court has the ability to discipline the authority. The court can, on the basis of Article 55 §2 of the LPAC and at the complaints request, rule that a fine be measured out to the authority. However, if the authority does not pass on the complaint to the court, despite imposing a fine, the court can investigate the case on the basis of a description of the complaint if the actual and legal status depicted in the complaint does not come under question on the request of the charging party and in accordance with Article 55 §2 of the LPAC. According to S. Szuster, whose opinion it is well worth considering, due to the particular nature of the case in the scope of access to public information as well as the many shortcomings of the structure of the Act, the above-mentioned solution will not actually perform a great function in practice.²⁹ This function can be fulfilled through signalling. The deciding members of the hearing or the chairman of the court inform the relevant authorities responsible for investigating petitions, complaints and application (Article 55 §3 of the LPAC) when there are cases of glaring infringements by an authority in relation to the above-mentioned responsibilities.

Article 21 (2) of the AAPI imposes on administrative courts an obligation to investigate cases within thirty days from the day the court receives the case files together with a reply to the complaint from the authority that is charged with inaction. As S. Szuster notes, the ineffective lapse of this deadline will not give rise to material and legal effects by acknowledging the charging party is right. The intention of the legislators is made clear here, which is, in fact, to shorten the waiting time of these cases as much as possible.³⁰ The lapse of this deadline can have an important meaning in complaints against tardiness of the court.

As a result of the filed claim, a court can reject the complaint, discontinue legal proceedings, dismiss or consider the complaint. At the same time, in the case of complaints against inaction, rejection can take place firstly due to lack of an object of charge, that is when the complaint does not apply in essence to inaction in the scope of public information or other forms of action covered by the scope of an administrative court following from Article 3 of the LPAC. Rejection can also take place when the formal conditions of the complaint, despite a call to do so, have not been fulfilled in the allotted time, this includes the non-payment of a fee. Owing to the particular nature of the complaint and the lack of detailed requirements in this scope, rejection due to exceeding the deadline for the filing of a complaint or the non-exhaustion of charging means do not come into play here. Rejection comes in the form of a ruling decision, which can be given at a closed session. An appeal against a complaint can be used here.

²⁶ The ruling of the Supreme Administrative Court of 29 August 2000 Reg. No. I SAB 52/00, the ruling of the Supreme Administrative Court of 3 November 1999 Reg. No. I SAB 156/99. A differing position is represented in the decision of the Supreme Administrative Court of 17 October 1997 Reg. No. IV SAB 31/97, which was criticised by B. Adamiak, OSP 1998 No. 19, 185.

²⁷ K. Klonowski, *Inaction*, quot. p. 33.

²⁸ The introduction of the Act of 17 June 2004 on complaints against infringement of the right of the party to hear a case by the court without due delay, Law Gazette No. 179, 1843.

²⁹ S. Szuster, *Commentary to Article 21*, quot.

³⁰ S. Szuster, *Commentary to Article 21*, quot.

The discontinuation of legal proceedings can ensue in the event of the inaction ceasing, the withdrawal of the complaint or other irrelevancy of the proceedings. Likewise, this ruling is given in the form of a decision, which can be taken at a closed session. An appeal against the complaint serves this aim.

The dismissal of a complaint against inaction follows in the form of a verdict when the complaint is unfounded, that is when, for example, an authority made the relevant information available before its submission or when an institution which is asked to make information available is not the holder of this information and has informed the applicant of this matter. An appeal against the complaint serves this verdict.

The consideration of a complaint against inaction on the basis of Article 149 of the LPAC follows in situations when the court rules that the complaint is unfounded. In this case, this consists of the obligation of the authority to investigate the given application by an appointed time (see the ruling of the Supreme Administrative Court of 20 June 2002 Reg. No. II SAB 113/02 or 30 October 2002 Reg. No. II SAB 181/02). At this point in the proceedings, the court cannot decide on the manner the application should be investigated, that is, whether it can be settled through giving access to the relevant information through material and technical action or a refusal by decision. An appeal against the complaint serves this ruling.

Appeals serve all participants of judicial-administrative proceedings equally, that is, the charging or prosecuting party, the authority against which the complaint against inaction is being filed, the public prosecutor and Ombudsman for Civic Rights. The appeals should meet the formal requirements of pleading given above, and also fulfil the conditions of Article 176 of the LPAC. In relation to this, the complaints should also contain the necessary designations of the claims against the ruling, indicating whether the charge is questioned in full or in part, the basis of the appeal and its justifications as well as the application for the reversal or amendment of the ruling indicating the scope of the reversal or amendment. The basis for the appeal can be, in accordance with Article 174 of the LPAC, the infringement of material law through an incorrect interpretation or its improper application, or the infringement of the procedural regulations if the error had a significant influence on the result of the case. The infringement of procedural regulations should apply to those which are applied in administrative courts, that is the regulations of the LPAC. Respecting the principles of appeal is an obligation of solicitors/lawyers. In accordance with Article 175 of the LPAC, an appeal against a complaint should be drawn up by a solicitor or lawyer, unless it was drawn up by a judge, public prosecutor, notary public, professor, doctor of law of who is the party concerned, or its representative or plenipotentiary, or if the complaint is filed by the public prosecutor or Ombudsman for Civic Rights. However, the issue that needs to be addressed and resolved is if a complaint can be put forward by a patent officer in cases of industrial property or a tax advisor in cases of tax liabilities. It seems that the regulations can firstly, on the basis of the Act of 30 June 2000 on Industrial Property Regulations,³¹ constitute a *lex specialis* in relation to access to public information and include particular regulations concerning access to information. In this situation, the case will not proceed on the basis of the Act of Access to Public Information. Secondly,

these regulations can include particular confidential information, which is deemed an exception to the transparency of administration, for example, in the scope of treasury secrets.³² In this case, the object of the case will not be tax liability but the access to information. Therefore, the participation of a patent officer or tax advisor will not be possible on the basis of the Act on Access to Public Information. It is not without meaning that this final situation can take place only when a complaint against decision on refusal of access to information is given and not in the case of a complaint against inaction in the scope of access to information.

As a result of the filing of complaints, the court can reject an appeal if it does not fulfil the formal requirements, it can discontinue the legal proceedings as a result of, for example, their withdrawal, dismiss the appeal if the court regards it as unfounded, or it can be taken into consideration, and, depending on the situation, reverse the sentence or decision, annul the proceedings due to their invalidity and pass them on to be re-considered, or it can settle the proceedings itself, as well as reject the complaint and discontinue the legal proceedings. It does this through verdict or ruling decision (for example, the rejection of appeal). In the case of an appeal against the complaint submitted to the decision, the ruling of the Supreme Administrative Court always takes the form of a decision.³³

In the event of considering a complaint against inaction, after calling for the authority to remove the infringement of the law, a party can subsequently submit a complaint against non-fulfilment of a court ruling. Through Article 154 §1 of the LPAC, the administrative court is able to impose a fine or rule on the existence or non-existence of powers or responsibilities if this is permitted by the nature of the case and the unquestionable circumstances of its actual or legal status. Also owing to the nature of the case, this kind of solution will be difficult to apply. An administrative court is not empowered to force the authority to make the relevant public information available.

Executing the obligation to make public information available is possible as a matter of fact only on the basis of Article 23 of the Act. Whoever does not grant access to public information, despite the responsibility to do so, can be subject to a fine, restriction of liberty or deprivation of liberty for up to a year. The common court is competent authority in this scope. The fine is not identical to the fine mentioned in Article 154 of the LPAC. Hence, the demand to punish a party that has not made public information available is inadmissible in proceedings before an administrative court. In this situation, disciplinary responsibility, regulatory responsibility or termination of employment for that cause is possible.

³²⁾ See chapter 7, in particular Article 193 of the Act of 29 August 1997 on Tax Ordinance, Law Gazette 2005 No. 8, 60 with amendments.

³³⁾ More on Supreme Administrative Court decisions can be found in M. Jaśkowska, M. Masternak, E. Ochendowski, Proceedings, quot., p. 191.

Monika Krasińska

Dyrektor Departamentu Skarg,
Biuro Generalnego Inspektora Ochrony Danych Osobowych, Polska
Director, Complaints Department,
Bureau of the Inspector General for Personal Data Protection, Poland

Współpraca Generalnego Inspektora Ochrony Danych Osobowych z organami ścigania

Prawa i wolności osób, których danymi posługuje się szereg podmiotów z sektora publicznego i prywatnego zostały poddane reżimowi nie tylko prawa administracyjnego i cywilnego, ale również prawa karnego. O docenieniu przez ustawodawcę wartości i dóbr chronionych ustawą o ochronie danych osobowych świadczy niewątpliwie uregulowanie w niej bezpośrednio odpowiedzialności karnej (art. 49-54 ustawy). Znaczenie tej regulacji podkreśla wyróżnienie odrębnej kategorii przestępstw przeciwko ochronie danych osobowych ściganych z oskarżenia publicznego a nie prywatnego. Rodzi to daleko idące konsekwencje w życiu społeczno - gospodarczym dla podmiotów łamiących prawo ale i obowiązki po stronie organów odpowiedzialnych za przestrzeganie w państwie praworządności. I tak obowiązkiem Generalnego Inspektora Ochrony Danych Osobowych jest złożenie zawiadomienia o popełnieniu przestępstwa w razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie (art. 19 ustawy). Natomiast w takich sytuacjach organy ścigania, tj. Policja i prokuratura, są obligowane sprawę rzetelnie wyjaśnić, zabezpieczyć zgromadzone dowody i podjąć wszelkie działania celem pociągnięcia sprawcy do odpowiedzialności karnej, w przeciwnym przypadku respektowanie przepisów o ochronie danych osobowych staje się jedynie iluzoryczne.

Wieloletnia praktyka Generalnego Inspektora Ochrony Danych Osobowych wskazuje jednak na odmienną koncepcję pojmowania przez organy ścigania czynów zabronionych z ustawy o ochronie danych osobowych, bagatelizowania jej fundamentalnych zasad lub wręcz braku świadomości istnienia tej ustawy. Jest to zjawisko niebezpieczne. Postawa organów ścigania utrwała bowiem w podmiotach dopuszczających się naruszeń poczucie ich bezkarności a w konsekwencji godzi także w poczucie bezpieczeństwa obywateli, których prawa są naruszane. Wyrazem powyższego mogą być ujawniane w corocznych sprawozdaniach Generalnego Inspektora składanych przed Sejmem wyniki postępowań prowadzonych przez prokuratury na skutek złożonych zawiadomień o popełnieniu przestępstwa. Spośród skierowanych w ciągu 8 lat prawie 400 zawiadomień jedynie w kilkudziesięciu przypadkach sprawy znalazły finał przed sądem powszechnym, zaś orzeczenia o ukaraniu sprawców przestępstw stanowią znikomy procent zapadłych rozstrzygnięć. W pozostałych przypadkach postępowania były umarzane. Najczęściej podawaną przyczyną takiej decyzji procesowej była znikoma społeczna szkodliwość czynu, brak danych uzasadniających popełnienie przestępstwa, czy

też brak znamion czynu zabronionego. Wskazywano ponadto na niemożność ustalenia sprawcy czynu. Niejednokrotnie sprawcy przestępstw w ogóle nie byli poddawani ocenie prawno – karnej, albo Generalny Inspektor nie był informowany o podjęciu jakichkolwiek wobec nich działań.

Przedstawiciele wymiaru sprawiedliwości wychodząc z góry przyjętej błędnej tezy, iż doszło do nieznacznego jedynie naruszenia reguł życia społecznego, często odmawiali w ogóle wszczęcia postępowania, przy czym ocena zasadności przedstawianych przez Generalnego Inspektora zarzutów była dokonywana w oparciu o niekompletny materiał dowodowy a nawet z wyłącznym wykorzystaniem interpretacji ustawy prezentowanej przez podmioty, wobec których były kierowane zawiadomienia. Lakoniczność przedstawianych uzasadnień ujawniająca zarówno braki w ustaleniu przebiegu zdarzeń oraz nieznajomość nie tylko przepisów o ochronie danych osobowych ale i własnych procedur, świadczyła w wielu sytuacjach wyłącznie o próbie szybkiego „pozbycia się sprawy”. Reakcją Generalnego Inspektora było sygnalizowanie nieprawidłowości Ministrowi Sprawiedliwości pełniącemu jednocześnie funkcję Prokuratora Generalnego. I chociaż na jego polecenie ponownie analizowano niemal każdy ze zgłoszonych przypadków naruszeń, wynik przeprowadzonych po raz kolejny postępowań przygotowawczych nie różnił się od zakwestionowanych wcześniej przez Generalnego Inspektora ustaleń. Co ciekawe, przy tych samych stanach prawnych i faktycznych prokuratury wydawały sprzeczne ze sobą postanowienia – raz to przyjmując, iż czynu nie popełniono, a następnie, że czyn wprawdzie został popełniony, ale nie zawierał ustawowych znamion czynu zabronionego.

Niezrozumienie organu do spraw ochrony danych osobowych budziła w wielu przypadkach uporczywość prezentowania przez prokuratury stanowisk, które nie tylko nie znajdowały uzasadnienia w świetle ustawy, ale wręcz były sprzeczne z zasadami logicznego rozumowania. Trudno bowiem za racjonalne uznać przykładowo, iż zestaw danych w postaci imienia, nazwiska, adresu i pełnionej funkcji nie stanowi danych osobowych, a więc informacji pozwalających na identyfikację ich właściciela, czy też przyjąć za uzasadnione, iż pozostawienie w miejscu powszechnie dostępnym dokumentacji medycznej nie jest przejawem niewłaściwego zabezpieczenia danych sensytywnych w niej zawartych. Prokuratury – oceniając słuszność kierowanych przez Generalnego Inspektora zawiadomień o przestępstwie – kierowały się nierzadko oceną indywidualnego odczucia doznanej krzywdy pokrzywdzonych i ich wolą jak najszybszego zakończenia postępowania (np. gdy toczyło się przez kilka lat), które to okoliczności nie mają znaczenia dla bytu przestępstw z ustawy o ochronie danych osobowych ściganych z urzędu, a mogłyby ewentualnie wpływać tylko na wymiar kary i ocenę stopnia społecznego niebezpieczeństwa. Niepokój budzi także od lat marginalizowanie faktu popełnienia przestępstwa z ustawy o ochronie danych osobowych wobec prowadzenia przez organy ścigania spraw o takim ciężarze gatunkowym jak chociażby rozboje, czy włamania. Tymczasem, w polskim systemie prawa, nie został wprowadzony podział na ustawy „ważne” i „mniej ważne”. Konstytucja RP zagwarantowała równość aktom prawnym o tej randze, w związku z czym każde przestępstwo powinno być ścigane w równym stopniu.

Brak należytej reakcji organów powołanych do ścigania przestępstw na wystąpienia Generalnego Inspektora Ochrony Danych Osobowych znacznie zatem utrudniał prowadzenie skutecznej polityki w zakresie ochrony danych osobowych. Szczególnie firmy marketingowe, wobec których postępowania umarzano, kontynuowały proceder nielegalnego przetwarzania danych osobowych, wskazywały fałszywe źródła ich pozyska-

nia, bądź też w ogóle nie dopełniały spoczywających na nich obowiązków informacyjnych. W rezultacie na przestrzeni ostatnich lat do Biura Generalnego Inspektora wpływało wiele skarg osób, których prawa zostały naruszone nie tylko poprzez przesyłanie niezamawianej korespondencji o charakterze marketingowym ale i przesyłkę z nadrukami przypominającymi dokumenty urzędowe wzywające ich do zapłaty określonych sum pieniężnych tytułem bliżej nieokreślonych zobowiązań. Niskim stopniem społecznej szkodliwości uzasadniane bywały także czyny osób odpowiedzialnych za nieprawidłowe zabezpieczenie danych w instytucjach operujących danymi milionów obywateli, takich jak banki, czy telefonie, a więc w instytucjach, które kształtują swój wizerunek, jako podmioty zaufania publicznego i na których z tego tytułu spoczywają szczególne obowiązki. U podstaw takich rozstrzygnięć znajdował się często brak wiedzy w zakresie istnienia rozporządzeń wykonawczych do ustawy o ochronie danych osobowych, a zobowiązujących do wprowadzenia dodatkowych procedur każdego administratora danych, np. co do danych przetwarzanych w systemach informatycznych.

Nie ulega wątpliwości, że instrumenty prawno-administracyjne, jakimi dysponuje Generalny Inspektor Ochrony Danych Osobowych w zwalczaniu praktyk nieuczciwych administratorów danych, są o wiele mniejsze niż te, w które wyposażone zostały na podstawie odrębnych przepisów Policja i prokuratura. Uzasadnione zatem jest oczekiwanie organu administracji publicznej na skorzystanie właśnie z tych narzędzi ochrony prawnej przez ww. podmioty w sytuacjach, gdy kończy się zakres administracyjnych możliwości ustalenia okoliczności sprawy i stwierdzenia naruszenia przepisów. Szczególnie istotne znaczenie ma to w przypadku doniesień o popełnieniu przestępstwa przez firmy, które przetwarzają dane osobowe bez żadnych podstaw prawnych na terytorium RP a wskazują jako adres swojej siedziby miejsca egzotyczne, w których brak jakichkolwiek regulacji z zakresu ochrony danych osobowych, co w konsekwencji uniemożliwia podejmowanie przez Generalnego Inspektora skutecznych wobec nich działań. Jednak szereg postępowań prokuratur koncentruje się na ograniczeniu zbadania takich spraw wyłącznie do ustaleń i dowodów przedstawianych przez Generalnego Inspektora, a w rezultacie do umorzenia postępowania bądź odmowy jego wszczęcia. W przekonaniu wielu prokuratorów prowadzących postępowania częściowe wykonanie przepisów z ustawy o ochronie danych osobowych jest wystarczającym argumentem za usprawiedliwieniem zarzucanych czynów. Taka interpretacja obowiązującego prawa u przedstawicieli organów ścigania rodzi niepokój co do poziomu praworządności w Polsce.

Zdarzają się oczywiście przypadki, gdy prokuratury w sposób niemal wzorcowy podejmują szereg czynności mających na celu rzetelne zbadanie sprawy i wykazują się dużą wiedzą z zakresu ochrony danych osobowych, ale takie sytuacje nie stanowią niestety reguły.

Współpracę Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami organów ścigania na przestrzeni ostatnich lat trudno zatem uznać za zadawalającą.

W obliczu przypadków umarzania wszczętych postępowań przygotowawczych albo w ogóle ich nie podejmowania rodzi się pytanie, w jaki sposób osoby, których danymi posługują się nieuczciwi administratorzy mogą mieć realnie zapewnione poczucie bezpieczeństwa. Dane osobowe, są tymczasem coraz cenniejszym towarem, wykorzystywanym przez podmioty funkcjonujące w obrocie gospodarczym, wobec czego istnieje

potrzeba coraz intensywniejszej ich ochrony. Nie jest ona jednak możliwa bez należytego współdziałania organów ścigania z Generalnym Inspektorem Ochrony Danych Osobowych. Nie można dopuścić do tego, aby ustawa o ochronie danych osobowych w zakresie obejmującym jej przepisy karne traktowana była w sposób lekceważący. Przepisy, których się nie stosuje zaczynają bowiem być traktowane jako przepisy martwe i zbędne, co prowadzi do osłabienia systemu ochrony porządku prawnego RP.

Cooperation between the Inspector General for Personal Data Protection and prosecuting bodies

The rights and freedoms of data subjects' whose data are used by the entities both from public and private sector are subject not only the provisions of administrative and civil law but also penal law. The high position of value and goods protected by Polish Act on the Protection of Personal Data confirms that there is penal responsibility (art. 49-54 of the Act) provided for directly in this Act. The above mentioned position results from the fact that all crimes against data protection are prosecuted upon public accusation and not prosecuted upon private accusation. This brings the important consequences in economic and social life for entities breaking the law and also the duties for authorities responsible for upholding the law in the state. And so, the duty of Inspector General for Personal Data Protection is to inform a proper prosecuting body, enclosing the evidence confirming his/her suspicions, about committing the crime when he finds out that the action or failure in duties of the head of an organisational unit, its employee or any other natural person fulfilled the attributes of the crime (Article 19 of the Act). In such situations the Police and the prosecuting bodies are obliged to clear up the case reliably, to secure the evidences and to undertake all activities the aim of which is to bring the perpetrator to penal responsibility, otherwise observance of legal provisions concerning the data protection becomes illusory.

Long-term policy of the Inspector General for Personal Data Protection indicates that the prosecuting bodies represent the different way of understanding of forbidden acts described in data protection Act and they trivialise fundamental principles of this Act or even show the lack of awareness of existence of this Act. This is a dangerous phenomenon. The attitude of prosecuting bodies convinces the entities violating the data protection provisions that they will still avoid penal responsibility and also strikes at the security's sense of the citizens whose rights are violated. Those facts find their confirmation in annual reports of the Inspector General for Personal Data Protection presented for Diet (the Lower Chamber of Polish Parliament). From those reports it results that during the last 8 years the Inspector General informed about the committing the crime in 400 cases and only dozens cases find their final in the court, whereas the sentence condemning the offenders constitute insignificant percentage of all sentences. In the rest of cases there were taken decisions on discontinuance of legal proceedings. The most common reason of such decisions was insignificant noxiousness of an act to society, the lack of data confirming the committing of the crime or the lack of attributes of forbidden act.

In many cases offenders will not subject to the penal assessment at all or the Inspector General was not informed about any activities undertaken against such offenders.

The representatives of jurisdiction, standing on the grounds of incorrect thesis adopted in advance according to which there were only insignificant violations of principles of social live, often refused to institute proceedings. It needs to be noted that the assessment of grounds of charges presented by the Inspector General was carried out on the basis of not fully completed evidence, or even with the exclusive use of interpretation of data protection Act presented by the entities against whom the notification about committing the crime were addressed. Laconism of presented reasons for the decision demonstrates not only the shortages in establishments on facts but also the ignorance of both provisions concerning the data protection and their own legal procedures, which only demonstrated the attempt of quick "disposal of the case". The reaction of the Inspector General was the addressing such incorrectness to the Minister of Justice who is also the General Public Prosecutor. Though on his order evidence almost in every case was re-analysed, the result of activities conducted once more did not show any difference with comparison to previous findings having been questioned by the Inspector General. What is interesting, in the same factual and legal state of affairs the prosecuting bodies issued contradictory decisions – at the beginning stating that the act was not committed or after intervention the Minister of Justice that the act was committed but did not include the legal attribute of the crime.

The Polish DPA could not agree with the positions of the prosecuting bodies, which not only did not find the confirmation in provisions of the data protection act but also were directly contradictory with the rules of logical reasoning. For example it is hard to agree that the set of data composed of first name, surname, and address and carried out function is not personal data, and in such a way is not information allowing for identification of their owner. It is also impossible to accept that leaving the medical documentation containing sensitive data in publicly available place is not an example of inadequate protection of such data. The prosecuting bodies – assessing the notifications – often acted by assessing the individual fillings of injured party and his/her will to have the proceedings concluded as quickly as possible (e.g. when the proceedings took several years). The above mentioned circumstances are irrelevant for existence of crimes described in data protection Act which are prosecuted upon public accusation, and could potentially influence the sentencing and assessment of the degree of noxiousness of an act to society. The fact that prosecuting bodies for many years reduced the meaning of crimes from the data protection Act in comparison with proceedings carried out in such cases like burglary or robbery is also worrying. It needs to be stressed that in the Polish legal system there is no division into acts "important" and "less important". The Polish Constitution guaranteed the equality for the legal acts of the same level what causes that every crime should be prosecuted with the same engagement.

The lack of proper reaction of prosecuting bodies on the addresses of the Inspector General made carrying out the efficient data protection policy even more difficult. Especially the marketing companies against whom the proceedings were discontinued have been continuing the illegal personal data processing, inter alia by showing false sources of data, or by not fulfilling the information obligation. In result it needs to be pointed out that the Inspector General has received many complaints from the persons

whose rights has been violated not only by sending not ordered marketing correspondence but also sending the documents similar to the official documents calling for paying specific amount of money because of vaguely described obligations. The prosecuting bodies often justify with a low degree of noxiousness of an act to society the acts of persons responsible for incorrect protection of personal data in entities dealing with data of millions citizens such as banks or phone operators – entities which should be treated as public trust institutions. The reason of such decisions was first of all lack of knowledge of the existence of law enforcement provisions to the data protection Act which oblige the data controller to introduce the additional procedures for example when the data are proceeded in computer system.

There are no doubts that the administrative instruments with which the Inspector General is empowered to suppress the practices of dishonest data controllers, are much smaller than those in which the Police and prosecuting bodies are empowered. The Polish DPA could expect that prosecuting bodies and Police will make use from their legal tools, where the powers of administrative authority are not sufficient to establish all the facts and establish that there was violation of legal provisions. It has a special importance in the cases of notifications against the entities which process personal data without any legal basis on the Polish territory and indicate an address of their registered seat in some exotic places in which there is no legal provisions concerning the data protection at the moment which makes any efficient activities of the Inspector General almost impossible. In many of such cases the prosecuting bodies do not make any findings other than those made by the Inspector General and the result is that the proceedings are discontinued or even not instituted. For many prosecutors the partial observance of obligations resulting from the data protection Act is a sufficient argument for justifying the violation. Such interpretation of legally binding provisions presented by the prosecutors brings the anxiety about the level of legality in Poland.

There are of course some cases in which the prosecuting bodies almost outstandingly undertake some activities which aim at examining the case reliably is to resource the case and show high level of knowledge of data protection regulations, but such situations are unfortunately an exception.

It is rather difficult to recognise the co-operation between the prosecuting bodies and the Inspector General to be satisfactory during the last few years.

In the face of discontinued proceedings or not instituted at all one may rise a question in which way persons whose data are used by dishonest data controllers, can have the sense of the security assured. Personal data are in the meantime more and more precious good (the subject of treat) used by the entities functioning in economic relations, which means that the personal data need more intensive protection. This protection is not possible without proper co-operation between the prosecuting bodies and the Inspector General. It must not be allowed that the data protection Act in scope of its penal provisions is treated disrespectfully. The legal provisions being not in use in practice start to be treated as dead provisions which leads to weakening of legal order in Poland.

Immanuel Kant and Implementation of the EU Data Protection Directive

February 12, 2004 was the two hundredth anniversary of the death of the great philosopher Immanuel Kant, who was born and spent almost his entire life in the formerly Prussian city of Königsberg, which is now the Russian city of Kaliningrad and is situated on Poland's northern border. As one of the leading European thinkers in data protection law, Professor Ewa Kulesza also has close ties to the data protection community in Germany. It is thus appropriate to ask what, if any, lessons Kant's philosophy may hold for interpretation of the EU Data Protection Directive 95/46/EC (referred to herein as the "Directive"), in particular with regard to improving its implementation in the Member States.

I. Directive 95/46 and its Implementation

Many EU directives take the form either of "minimum harmonization" directives, i.e. they leave it to the Member States to adopt more stringent standards than those in the directive, or "maximum harmonization" directives, i.e. they provide for a more or less uniform European standard in a particular field. However, Directive 95/46 falls neither wholly into one camp nor the other. The legal basis of the Directive was Article 100a of the Treaty of Rome (currently Article 95 of the Amsterdam Treaty), which provides for the adoption of "measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market" and mandates "a high level of protection" in matters concerning consumer protection.² However, the Directive does not set forth a single uniform standard of data protection, and cannot be regarded as a "maximum harmonisation" directive. Rather, it both sets forth minimum standards which all Member States must fulfil (e.g. regarding the restriction of data transfers to third countries without an adequate level of data protection), and allows them leeway in determining how such standards are to be met (e.g. Article 5 explicitly allows the Member States to 'determine more precisely the conditions under which the processing of personal data is lawful'³). The Directive could thus be said to contain a mixture of both maximum and minimum rules. This means that there is a bandwidth

between which Member State must stay in implementing the Directive: on the one hand, they must make their laws 'equivalent' to each other and to the protections of the Directive (the minimum),⁴ but at the same time must not adopt provisions which impede data flows with other Member States (the maximum).⁵

Directive 95/46 provides for mechanisms designed to motivate the Member States to comply with their data protection obligations and make violations of their implementation duties less likely. For example, Member States must notify the Commission if they make use of certain derogations in implementing the Directive⁶ and when they approve the use of contractual clauses for international data transfers.⁷ The existence of the Article 29 Working Party, in which all the Member States participate, is also intended to lead to a more harmonised approach to data protection and to make it less likely that individual Member States will implement the Directive in ways which are substantially at variance from each other. Finally, the Commission is supposed to report to the Council and European Parliament at regular intervals concerning implementation of the Directive.⁸

II. Experience with Implementation of the Directive

On May 15, 2003 DG Internal Market of the European Commission published its "First Report on the Implementation of the Data Protection Directive (95/46/EC)".⁹ The Report is divided into two sections: the first is the Report itself, which describes the process under which it was written, identifies the main issues, relates the results to the Commission's upcoming Work Program, and then draws some general conclusions. The second, and lengthier, document, is entitled "Analysis and Impact Study on the Implementation of Directive EC/95/46 in Member States", which goes into considerable detail about Member State law. The Commission has also published the results of questionnaires sent to the Member States and the national data protection authorities.

While finding that the Directive has achieved its major objectives, the Report also finds a number of instances in which it has been inadequately transposed by the Member States; examples include Articles 4, 7, 8.1, 10, 13, and 26 (see p. 12). The Commission thus states that it "considers that some of the issues that have emerged and which are here only the subject of a preliminary analysis need to be further analyzed and may need in due course to be the subject of a proposal to revise the Directive" (p. 9). The Report concludes with the outline of a "work programme for a better implementation of the data protection directive" over the years 2003-2004, which states that the Commission will hold a series of bilateral discussions with Member States and data protection authorities in order to ensure increased harmonization of national data protection law. There is thus no doubt that, despite the undoubted overall success of the Directive, there are a number of important deficiencies with regard to its implementation in the Member States.

¹ Mr. Kuner is a partner in the international law firm Hunton & Williams, Brussels, and is Chair of the International Chamber of Commerce (ICC) Task Force on Privacy and Data Protection; ckuner@hunton.com.

² See regarding the legal basis for the Directive U Dammann and S Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997) 64-65.

³ See Directive, Recital 9, which states 'whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; ...whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive...'

⁴ Recitals 8-9.

⁵ See Art 1(2), stating that 'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

⁶ E.g. Art 8(6) (regarding sensitive data).

⁷ Art 26(3).

⁸ Art 33.

⁹ Commission document COM(2003) 265 final. Quotations and page citations in this article refer to the official printed version of the report, ISBN 92-894-5378-8.

In considering implementation of Directive 95/46, it is important to construe the term “implementation” liberally to include not only the letter of a Member State’s data protection law, but many other types of instruments as well, both formal and informal. Such things as the practice of data protection authorities, interpretative statements issued by them, administrative practice, etc. may have a substantial impact on how effective an implementing national rule is in realizing the Directive’s goals. The Commission’s report goes into great detail about differences in implementation in the actual national data protection law, but has less information about informal practices which may greatly affect the efficiency and effectiveness of the national data protection regime.

The author is aware of many instances where Member States have interpreted in contradictory ways, or where a Member State has imposed administrative burdens in a way that would seem to contravene the spirit if not the letter of the Directive, such as the following:

- A company is investigated simultaneously by two data protection authorities in neighboring Member States. Each DPA examines the same database, which is hosted outside the EU but may be accessed in each of the countries. One DPA finds that the database does not result in the processing of personal data, while the other finds that the same database does in fact process personal data.
- When filing copies of the EU-approved standard contractual clauses with a national data protection authority, the DPA requires that the signature for each of the data importers be notarized, and that the notarization be deposited with the DPA. There are over seventy data importers that have signed the contract around the world, and notarization of each of their signatures is a complex operation that must be performed in accordance with the national civil procedure law of each data importer’s country. In addition, in order for the notarizations to be recognized in the EU, an “apostille” must be issued by the appropriate authority in each non-EU country of the data importers under the terms of the Hague Legalization Convention, a process which in some countries can take months.

These are just two examples of Member States applying national interpretations of the Directive, which, if not explicitly violating its letter, do seem to raise questions about violating its spirit. And this is where Kant comes in.

III. Kant and Implementation of the Directive

Kant’s writings are notoriously dense and complex, and scholars of philosophy will hopefully forgive the superficiality of their characterization here. Nevertheless, his precepts do hold important lessons which, when applied to the present situation surrounding implementation of the Directive, help to demonstrate the necessity of taking a European rather than a purely nationalistic approach to interpretation of important provisions.

Kant’s most famous maxim was the “categorical imperative”, which had several formulations,¹⁰ perhaps the most well-known of which is “handle so, als ob die Maxime

deiner Handlung zum allgemeinen Naturgesetz werden sollte”,¹¹ or in a rough English translation, “act so that the expressions of your action should become a general law of nature”. Kant’s aim was to derive ethical rules from logic, and to free them from what he saw as the imperfect restrictions of experience. Greatly simplified, the categorical imperative requires that ethical rules be tested by determining whether elevating them to a general law or rule would produce an inherent contradiction; if this is the case, then the rule is invalid.¹² The categorical imperative does not take into account external empirical factors or ethical principles that derive from external sources, but solely whether the consequences of the action would produce a contradictory result. In applying it to implementation of the Directive, one should thus not take into account considerations such as whether implementation would be too burdensome or expensive.

The categorical imperative is easier to understand if one applies it to the two examples stated above relating to implementation of Directive 95/46:

Example One: Member State A implements a fundamental principle of Directive 95/46 (such as the definition of personal data) in one way, while Member State B implements the same term in a completely opposite way. The maxim to be tested would thus be “in implementing the Directive, Member States should interpret important terms as they like without any regard to how they are interpreted in other Member States”.

Example Two: Member State A places complex conditions on the filing of model contractual clauses for data transfer which derive from its own national civil procedure law and require a considerable amount of time and resources to satisfy. In this case the maxim to be tested under the categorical imperative would be “in implementing Community legislation meant to provide for harmonization, Member States may impose their own national legal requirements on such implementation no matter how complex”.

It could be objected that applying the categorical imperative to evaluate national implementation of the Directive is inappropriate, since the Directive is not an ethical rule as such, and implementation has to be judged based on empirical factors that fall outside of the purely logical test that Kant has constructed. However, the Directive does contain rules of conduct that can be analogized to ethical rules. Moreover, a number of important basic policies underlie the directive; for instance, the European Court of Justice has emphasized that one of the inherent purposes of the Directive is to “ensure the free movement of personal data between Member States through the harmonization of national provisions on the protection of individuals with regard to the processing of such data”.¹³ There is no reason why it should not be possible to evaluate a particular implementation of the Directive and determine if it is inherently contradictory in light of these policies, which is precisely the test that Kant set forth in the categorical imperative.

¹¹ Ibid., p. 75.

¹² An example cited by Kant would be the proposed rule that “if things are not going well for me in life, then in order to avoid further pain I should commit suicide”. This would mean in effect that I would be killing myself for the egotistical reason that I do not want to suffer pain, i.e., I would be destroying myself out of love for myself, which is an inherent contradiction.

¹³ Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk* (2003), para. 39.

Applying the categorical imperative to these two situations leads to the following results:

Example One: The maxim “in implementing the Directive, Member States should interpret important terms as they like without any regard to how they are interpreted in other Member States” would lead to a situation in which Member States implemented the Directive as they wished, without any view to harmonizing it with implementations in other Member States. However, harmonization or at least close equivalence is inherent in the definition of a Directive, as pointed out by the European Court of Justice. Thus, this attitude contains an inherent contradiction, and Member States should actively keep abreast as to how the Directive is implemented elsewhere and strive for a harmonized implementation.

Example Two: Here the maxim to be tested is “in implementing Community legislation meant to provide for harmonization, Member States may impose their own national legal requirements on such implementation no matter how complex”. This rule suffers from the same defects as the first one, since the Directive’s goal of harmonization inherently implies that Member States will at least minimize the imposition of national legal requirements that make harmonization more difficult, which is impossible if they have free reign to impose their own national requirements as they would like. There are other problems with this maxim (such as the fact that it would make use of the clauses overly expensive and difficult to use, particularly for small and medium-sized enterprises), but these are empirical factors that should, strictly speaking, not be taken into account when applying the categorical imperative.

IV. Conclusions

EU law allows a considerable amount of freedom for Member States to implement Data Protection Directive 95/46 with regard to their particular legal and cultural circumstances. It is thus particularly difficult to state with certitude that a particular implementation violates the Directive. At the same time, the increased size of the Union means that traditional methods for determining whether a Member State implementation violates the Directive are in most cases no longer useful. The long road of the Commission complaining to a Member State, issuing a reasoned opinion, then finally taking the Member State before the Court of Justice for improper implementation can take years and in the end provides little useful relief.

Kant’s categorical imperative provides a useful logical framework for testing the inherent compatibility of an implementing national rule with the basic policy that underlies it. National legislators and DPAs would do well to keep it in mind and exercise self-restraint in implementation of the Directive, by taking into account not only their own national situations, but the possible implications of converting their national rules into rules of general application that would apply around the EU. If the result of this test is that the rules would become unworkable if applied universally or would lead to an absurd result or an inherent contradiction, then this is a strong indication that the rule may violate at least the spirit of the Directive. It is precisely such unconventional thinking that is needed to provide new mechanisms for ensuring that EU data protection legislation takes into account not only national characteristics, but also the cross-border nature of the Directive from which it derives.

Immanuel Kant a implementacja Dyrektywy Unii Europejskiej o ochronie danych

Christopher Kuner¹

12 lutego 2004 roku minęła dwusetna rocznica śmierci wielkiego filozofa Immanuela Kanta, który urodził się i spędził niemal całe życie w byłym pruskim mieście Königsberg, obecnie rosyjskim Kalingradzie, leżącym w pobliżu północnej granicy Polski. Profesor Ewa Kulesza, która jest jednym z głównych specjalistów europejskich w sprawach regulacji prawnych odnoszących się do ochrony danych, utrzymuje bliskie kontakty ze środowiskiem niemieckim zajmującym się tą problematyką. Dlatego też stosowne wydaje się postawienie pytania, jakie wnioski można wyciągnąć, jeśli w ogóle jest to możliwe, z filozofii Kanta odnośnie interpretacji Dyrektywy Unii Europejskiej dotyczącej ochrony danych osobowych – 95/46/WE (zwanej dalej Dyrektywą), zwłaszcza w zakresie usprawniania jej implementacji w Państwach Członkowskich.

I. Dyrektywa 95/46 i jej implementacja

Wiele dyrektyw UE przyjmuje formę unormowań „minimalnej harmonizacji”, pozostawiając Państwom Członkowskim możliwość przyjmowania bardziej rygorystycznych norm niż te, które zostały ujęte w danej dyrektywie, bądź też unormowań „maksymalnej harmonizacji”, ustanawiając bardziej lub mniej jednolite normy europejskie w określonej dziedzinie. Jednak Dyrektywa 95/46 nie należy w całości do żadnej z wymienionych grup. Jej podstawę prawną stanowi artykuł 100a „Traktatu rzymskiego” (obecnie artykuł 95 „Traktatu amsterdamskiego”), który zakłada podjęcie „działań mających na celu upodobnienie warunków ustanowionych przez prawo, przepisy bądź działania administracyjne w Państwach Członkowskich dla utworzenia i funkcjonowania rynku wewnętrznego” i nakazuje zapewnienie „wysokiego poziomu ochrony” w sprawach dotyczących ochrony praw konsumenta.² Dyrektywa nie przedstawia jednak jednolitej normy odnoszącej się do ochrony danych, nie można zatem traktować jej jako Dyrektywy „maksymalnej harmonizacji”. Jest raczej wykładnią minimalnych norm, według których muszą postępować wszystkie Państwa Członkowskie (np. dotyczących ograniczenia przekazywania danych do państw trzecich bez zapewnienia odpowiedniego poziomu ochrony tych danych). Pozostawia ponadto swobodę w spełnianiu tych norm (np. art. 5 wyraźnie zezwala Państwom Członkowskim na „szczegółowe określanie warunków legalności przetwarzania danych osobowych”³). Można więc stwierdzić, że Dyrektywa zawiera zasady zarówno maksymalne, jak i minimalne. Oznacza to, że między krajami członkowskimi istnieje pewien przedział, w obrębie którego państwa te muszą działać, wprowadzając Dyrektywę w życie: z jednej strony muszą uchylać ustawy, które będą „równoważne” w stosunku do siebie i do przepisów zawartych w Dyrekty-

¹ Ch. Kuner jest współnikiem w międzynarodowej firmie prawniczej Hunton & Williams, Bruksela. Jest też przewodniczącym Grupy Zadaniowej ds. Ochrony Danych w Międzynarodowej Izbie Handlu (ICC Task Force).

² Patrz: Dyrektywa U. Dammann i S. Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997), 64-65.

³ Patrz: Dyrektywa, pkt 9, który mówi, że: „Państwa Członkowskie będą zatem mogły określić w swoim ustawodawstwie ogólne warunki regulujące legalność procesu przetwarzania danych; (...) w granicach wspomnianego marginesu swobody działania oraz zgodnie z prawem Wspólnoty mogą wystąpić rozbieżności we wdrażaniu Dyrektywy...”

wie (minimum),⁴ z drugiej zaś nie wolno im przyjąć przepisów, które utrudnią przepływ danych do innych Państw Członkowskich (maksimum).⁵

Dyrektywa 95/46 ustanawia mechanizmy, które mają motywować kraje członkowskie do przestrzegania zobowiązań wiążących się z ochroną danych i spowodować, że mniej prawdopodobne będzie naruszenie zasad wprowadzania tej Dyrektywy w życie. Na przykład Państwa Członkowskie muszą poinformować Komisję o przypadkach naruszeń w dziedzinie implementacji Dyrektywy⁶ i zatwierdzania klauzul umownych dotyczących międzynarodowego transferu danych.⁷ Istnienie Grupy Roboczej Art. 29, w której pracach uczestniczą wszystkie kraje członkowskie, ma również na celu przyjęcie zharmonizowanego stanowiska w sprawie ochrony danych oraz wyeliminowanie prawdopodobieństwa, że poszczególne Państwa Członkowskie wprowadzą Dyrektywę każde w inny sposób. Poza tym Komisja ma regularnie składać raporty Radzie i Parlamentowi Europejskiemu w sprawie implementacji Dyrektywy.⁸

II. Doświadczenie wynikające z wprowadzania Dyrektywy

15 maja 2003 roku Dyrekcja Generalna ds. Rynku Wewnętrznego Komisji Europejskiej opublikowała „Pierwszy raport w sprawie wprowadzania Dyrektywy o ochronie praw osobowych (95/46/WE)”⁹ [„First Report on the Implementation of the Data Protection Directive (95/46/EC)”]. Jest on podzielony na dwie części. Pierwszą stanowi sam raport, w którym opisano proces jego powstawania, przedstawiono główne tematy, porównano rezultaty z opracowywanym programem roboczym Komisji, a następnie podano ogólne wnioski. W drugiej, dłuższej części dokumentu zatytułowanej „Analizowanie i badanie wpływu na implementację Dyrektywy WE/95/46 w Państwach Członkowskich” („Analysis and Impact Study on the Implementation of Directive EC/95/46 in Member States”) szczegółowo omówiono prawo obowiązujące w Państwach Członkowskich. Komisja opublikowała również wyniki kwestionariuszy wysłanych do Państw Członkowskich i organów zajmujących się w poszczególnych państwach ochroną danych osobowych.

Raport dowiódł, że Dyrektywa osiągnęła główne zamierzone cele. Podaje jednak także wiele przypadków, kiedy była ona nieodpowiednio przetransponowana przez kraje członkowskie, np. art. 4, 7, 8.1, 10, 13 i 26 (patrz s. 12). Komisja stwierdziła zatem, że „niektóre kwestie, które się pojawiły i są przedmiotem jedynie wstępnej analizy, należy dokładnie zbadać, by w odpowiednim czasie, gdy zaistnieje konieczność, wprowadzić zmiany do Dyrektywy” (s. 9). Raport kończy zarys „programu pracy służącego usprawnieniu implementacji Dyrektywy o ochronie danych osobowych” w latach 2003-2004, zgodnie z którym Komisja ma przeprowadzić wiele dwustronnych rozmów z Państwami Członkowskimi oraz z przedstawicielami organów zajmujących się ochroną danych. Celem tych dyskusji ma być lepsza harmonizacja prawa krajowego dotyczącego ochrony danych. Bez wątpienia, mimo sukcesu Dyrektywy, jest jeszcze wiele słabych punktów odnośnie jej implementacji w Państwach Członkowskich.

⁴) Pkt 8-9.

⁵) Patrz: art. 1 (2) stwierdzający, że „państwa członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych pomiędzy państwami członkowskimi ze względów przewidzianych w ust. 1”.

⁶) Np. Art. 8 (6) (dot. szczególnej kategorii danych).

⁷) Art. 26 (3)

⁸) Art. 33.

⁹) Dokument Komisji COM (2003) 265 (wersja końcowa). Cytaty w tym artykule zostały zaczerpnięte z oficjalnej drukowanej wersji raportu, ISBN 92-894-5378-8.

Omawiając implementację Dyrektywy 95/46, należy interpretować termin „implementacja” liberalnie, by zawierał on nie tylko literę prawa o ochronie danych osobowych w Państwach Członkowskich, ale również wiele innych typów instrumentów – zarówno formalnych, jak i nieformalnych. Takie zagadnienia, jak stosowana praktyka organów do spraw ochrony danych osobowych, opracowane przez nie interpretacje, postępowanie administracyjne itd. mogą mieć istotny wpływ na to, jak skuteczne będą przepisy państwowe w realizowaniu założeń Dyrektywy. Raport Komisji szczegółowo opisuje różnice w ich implementacji w krajowym prawie o ochronie danych. Zawiera jednak mniej informacji dotyczących nieformalnych praktyk, które mogą mieć ogromny wpływ na sprawność i skuteczność krajowych unormowań do spraw ochrony danych.

Autor jest świadomy wielu przypadków sprzecznych interpretacji dokonanych przez Państwa Członkowskie bądź też nakładania przez nie ograniczeń administracyjnych w sposób, który – wydawałoby się – narusza „ ducha”, jeśli nie literę Dyrektywy, np.:

- Firma jest badana jednocześnie przez dwa organy ochrony danych w sąsiadujących Państwach Członkowskich. Każdy z nich bada tę samą bazę danych znajdującą się poza UE, ale dostęp do niej jest możliwy w obu krajach. Wyniki jednego z organów są jednak takie, że dane osobowe nie są przetwarzane, podczas gdy drugi stwierdza, że w tej samej bazie danych faktycznie dane osobowe są przetwarzane.
- Podczas katalogowania kopii zatwierdzonych przez UE standardowych klauzul umownych w krajowych organach ochrony danych organy te wymagają, aby podpis każdego importera danych był poświadczony notarialnie, a dokumenty złożone w depozycie w organach ochrony danych. Jest ponad siedemdziesięciu importerów danych, którzy podpisali umowy na świecie. Przy tym poświadczenie notarialne każdego podpisu to skomplikowana operacja, którą należy przeprowadzić zgodnie z obowiązującymi krajowymi cywilnymi procedurami prawnymi w każdym z państw importera danych. Co więcej, aby potwierdzenie to zostało uznane przez UE, musi być wydane przez odpowiednie organy w każdym kraju (certyfikat poświadczenia zwany „apostille”), który nie należy do UE, zgodnie z warunkami Konwencji Haskiej. Proces ten może w niektórych krajach trwać kilka miesięcy.

Są to tylko dwa przykłady zastosowania w Państwach Członkowskich krajowych interpretacji Dyrektywy, które jeśli wyraźnie nie naruszają litery prawa, to wydają się poruszać kwestie dotyczące naruszania „ ducha” Dyrektywy. I tutaj właśnie wchodzi Kant.

III. Kant a implementacja Dyrektywy

Teksty Kanta są bardzo hermetyczne i skomplikowane, mam więc nadzieję, że filozofowie wybaczą mi powierzchowne ich potraktowanie. Można jednak na tej podstawie wyciągnąć z nich ważne wnioski, które zastosowane do obecnej sytuacji odnoszącej się do implementacji Dyrektywy wskazują na konieczność przyjęcia europejskiego, a nie czysto nacjonalistycznego stanowiska w sprawie interpretacji ważnych przepisów.

Najbardziej znana maksyma Kanta brzmi „imperatyw kategoryczny”.¹⁰ Wynika z niego kilka zasad. Być może najbardziej znaną jest „handle so, als ob die Maxime deiner Handlung zum allgemeinen Naturgesetz werden sollte” („postępuj tak, aby twe działania stały się powszech-

¹⁰) Więcej na temat przedstawianych tu koncepcji patrz: R. Ludwig, *Kant für Anfänger: Der kategorische Imperativ*, 1995.

nym prawem natury”).¹¹ Celem Kanta było czerpanie zasad etycznych z logiki i uwolnienie ich od tego, co postrzegał jako niedoskonałe ograniczenia doświadczenia. W znacznym uproszczeniu, imperatyw kategoryczny Kanta zakłada testowanie zasad etycznych w odniesieniu do prawa powszechnego lub zasady te będą w swoistej sprzeczności; jeśli ma miejsce taka sytuacja, to dana zasada jest nieważna.¹² Imperatyw kategoryczny nie uwzględnia zewnętrznych czynników empirycznych lub zasad etycznych, które wywodzą się ze źródeł zewnętrznych, lecz jedynie rozpatruje, czy konsekwencją działania będzie sprzeczny rezultat. Odnosząc ten punkt widzenia do implementacji Dyrektywy, nie należy zatem brać pod uwagę takich czynników, jak uciążliwość implementacji czy zbyt duży jej koszt.

Imperatyw kategoryczny łatwiej zrozumieć, jeśli zastosuje się go do dwóch przykładów odnoszących się do wprowadzania Dyrektywy 95/46.

Przykład pierwszy. Państwo Członkowskie A wprowadza podstawową zasadę Dyrektywy 95/46 (np. definicję danych osobowych) w jeden sposób, podczas gdy państwo B wprowadza ją zupełnie inaczej. Maksyma, która ma być sprawdzona, brzmiałaby wówczas tak: „przy wprowadzaniu Dyrektywy Państwa Członkowskie powinny interpretować ważne terminy tak jak chcą, nie zwracając uwagi na to, jak są one interpretowane w innych Państwach Członkowskich”.

Przykład drugi. Państwo Członkowskie A stawia kompleksowe warunki dotyczące katalogowania wzorcowych klauzul umownych w sprawie przekazywania danych, które wynikają z cywilnej procedury prawnej tego państwa i w związku z tym potrzebuje ono znacznie więcej czasu i środków, aby je wypełnić. W tym przypadku maksyma imperatywu kategorycznego będzie brzmiała: „przy wprowadzaniu legislacji Wspólnoty, która ma zapewnić harmonizację, Państwa Członkowskie mogą narzucać własne prawne wymagania dotyczące implementacji, nieważne przy tym, jak kompleksowe”.

Mogą pojawić się opinie, że zastosowanie imperatywu kategorycznego w ocenie krajowego sposobu wprowadzania Dyrektywy jest niewłaściwe, gdyż nie jest ona zasadą etyczną samą w sobie, a implementację należy oceniać na podstawie czynników empirycznych, które nie podlegają czysto logicznemu testowi, który skonstruował Kant. Jednakże Dyrektywa zawiera zasady zachowania, które można porównać do zasad etycznych. Poza tym, kilka istotnych podstawowych zasad tkwi u podstaw Dyrektywy, np. Europejski Trybunał Sprawiedliwości podkreślił, że jednym z nieodłącznych celów Dyrektywy jest „zapewnienie swobodnego przepływu danych osobowych między Państwami Członkowskimi przez harmonizację krajowych przepisów dotyczących ochrony osób w związku z przetwarzaniem tych danych”.¹³ Nie ma zatem powodu, dla którego ocena poszczególnych implementacji Dyrektywy nie byłaby możliwa, zwłaszcza ustalenie, czy nie jest ona sprzeczna wewnętrznie w świetle tej polityki, a to stanowi dokładny test, który Kant ujął w imperatywie kategorycznej.

Zastosowanie imperatywu kategorycznego w tych dwóch przypadkach prowadzi do następujących wniosków:

Przykład pierwszy. Stwierdzenie: „przy wprowadzaniu Dyrektywy Państwa Członkowskie powinny interpretować istotne warunki tak jak chcą, nie biorąc pod uwagę, jak są one interpretowane w innych Państwach Członkowskich” – doprowadziłoby do sytuacji, że państwa te wprowadzałyby Dyrektywę tak jakby chciały, nie zważając na to, by zharmonizować ją z innymi Państwami Członkowskimi. Harmonizacja jednak lub przynajmniej dążenie do niej są wbudowane w definicję Dyrektywy, na co zwrócił uwagę Europejski Trybunał Sprawiedliwości. Zatem stanowisko to zawiera wewnętrzną sprzeczność, a Państwa Członkowskie powinny aktywnie śledzić, jak Dyrektywa jest wprowadzana w życie w innych krajach i dążyć do zharmonizowanej implementacji.

Przykład drugi. Stwierdzenie, które ma być testowane, brzmi: „przy wprowadzaniu we Wspólnocie legislacji, która ma zapewnić harmonizację, Państwa Członkowskie mogą narzucać własne prawne wymagania dotyczące implementacji, nieważne przy tym, jak kompleksowe”. Zasada ta ma takie same wady, jak pierwsza, gdyż cel Dyrektywy w sprawie harmonizacji narzuca wymóg, by Państwa Członkowskie przynajmniej minimalizowały wprowadzanie krajowych wymagań prawnych, które utrudniają harmonizację. Nie jest to natomiast możliwe w przypadku, gdy mają wolną rękę co do narzucania własnych krajowych wymagań, tak jak chcą. Istnieją też inne problemy z tym związane (np. stosowanie klauzul byłoby nadmiernie kosztowne i trudne w praktyce, zwłaszcza dla małych i średnich przedsiębiorstw), ale są to czynniki empiryczne, które nie powinny być, ściśle mówiąc, brane pod uwagę przy odnoszeniu ich do imperatywu kategorycznego.

IV. Wnioski

Prawo UE zezwala Państwom Członkowskim na znaczną swobodę we wprowadzaniu w życie „Dyrektywy o ochronie danych osobowych 95/46”, biorąc pod uwagę szczególne prawne i kulturowe uwarunkowania. Jest więc niezwykle trudno określić z całą pewnością, że poszczególne implementacje naruszają przepisy Dyrektywy. Jednocześnie większa liczba członków Unii sprawia, że tradycyjne metody określania, czy implementacja w Państwach Członkowskich narusza Dyrektywę, są najczęściej bezużyteczne. Procedura składania przez Komisję zażalenia do Państwa Członkowskiego, żądania racjonalnej opinii, a w końcu stawiania Państwa Członkowskiego przed sądem za nieprawidłową implementację może trwać lata i w końcu także okaże się mało użyteczna. Imperatyw kategoryczny Kanta daje użyteczne, logiczne podstawy do sprawdzania kompatybilności narodowych przepisów wprowadzanych do dziedziny polityki ochrony danych, która leży u jej podstaw. Narodowi legislatorzy oraz władze zajmujące się ochroną danych osobowych powinni o tym pamiętać przy implementacji Dyrektywy, biorąc pod uwagę nie tylko sytuację ich w kraju, ale również prawdopodobne implikacje przekształcania przepisów obowiązujących w ich kraju w przepisy powszechnie stosowane, które będą miały zastosowanie w całej UE. Jeśli okaże się, że przepisy te nie nadają się do uniwersalnego zastosowania bądź będą sprzeczne, jest to wówczas wyraźny znak, że mogą one naruszyć przynajmniej ducha Dyrektywy. Jest to tak niekonwencjonalny sposób myślenia, że należy stworzyć nowe mechanizmy, by mieć pewność, że legislacja w dziedzinie danych osobowych w UE uwzględnia nie tylko narodowe cechy, ale również międzynarodowy charakter Dyrektywy, z której się wywodzi.

¹¹) Ibidem, p. 75.

¹²) Przykładem cytowanym przez Kanta byłaby następująca zasada: „Jeśli nie układa mi się w życiu, aby uniknąć bólu, powinienem popełnić samobójstwo”. Oznacza to, że zabiłbym się z egoistycznych powodów, ponieważ nie chcę cierpieć, tj. zniszczyłbym się z miłości do samego siebie, co jest wewnętrzną sprzecznością.

¹³) Sprawy: C-465/00, C-138/01 i C-139/01 *Österreichischer Rundfunk* (2003), § 39.

Citizens' awareness level and data protection education activity in the field of privacy and data protection across the EU

Introduction

The citizens' awareness concerning the personal data protection goes out mainly from the accomplishment of the national data protection (DP) law, eventually from the international legislation and legal documents which regulate the processing and use of personal data. Further, it can be information, which the citizen obtains from the websites of the data protection authorities executing the supervision over the processing of personal data, information from media (mainly from TV, radio or newspapers), from the direct or indirect contacts with data controllers from state or private sector and at last but not least also from experience obtained in the course of using information and communication technologies and electronic services.

In the course of writing this article I will try to find answers to the following questions:

- What does the citizens' legal awareness relating to his/her privacy with regard to the processing of personal data consist of?
- What affects awareness?
- What is the level of citizens' awareness and how do they exercise it?
- How to raise citizens' awareness?
- What are the trends for future?

Some of the opinions, theses and the basic part of figures were taken from the sources noted in the footnotes on a particular page.

Legal instruments of personal data protection

Through the 70's – 80's of the past century, above all in connection with the wide introduction of computing techniques, several current EU Member States adopted acts on personal data protection. We can speak about the first legal regulations in which the basic duties and requirements on data controllers when processing personal data were specified, the rights of data subjects were stipulated and the supervisory authorities were introduced, who in case of breaching the law were empowered to impose remedies or financial sanctions. These acts were adopted gradually and also their legislative level was different. With the objective to remove these differences at the beginning of

80's the Council of Europe in close cooperation with Member States adopted the Convention for the protection of individuals with regard to automatic processing of personal data No. 108/1981 ETS (hereinafter only "Convention 108").

The purpose of Convention 108 is to secure in the territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). Gradually this document (together with the additional protocol to the Convention 108) became the "legal standard" when the application of principles of this convention into the national legislation became criteria for assessment of adequate level of data protection in the third countries.

Next significant international legal document adopted by the EP in October 1995 was the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and free movement of such data (hereinafter only "Directive 95/46 EC").

The main intention of the Directive 95/46 EC was to set up the conditions for free movement of data within the framework of European Community, as well as the transfer of data into the third countries and to enlarge the scope of powers of personal data processing principles also on non-automated processing or non-automated data files. New EU Member States in a pre-accession period harmonized the national law to the above-said Directive. The Directive 95/46 became an assessment criterion, when the level of DP law in Member States was negotiated as well.¹

Except the legislative documents mentioned above, the European Commission issued further documents e.g. Decisions, from which the DPA enforces the uniform practices into the process of handling personal data (e.g. Commission Decision of 15 June 2001 on standard contractual clauses for transfer of personal data to the third countries, under Directive 96/46/EC). In compliance with the above-mentioned decision, the controllers are obliged to elaborate the contract concerning the processor, when transferring the data into the third country.

The special Eurobarometer focused on data protection² brings assessment of the EU citizens awareness concerning the data protection issues.

Opinion of the UE citizens concerning the level of DP awareness

On finding opinion to the level of data protection awareness the requested respondents answered the following question (1):

"Do you tend to agree or tend to disagree that people's awareness about personal data protection in (OUR COUNTRY) is low?" The answers were as follows:

¹⁾ First report on the implementation of the Data Protection Directive 95/46/EC, Brussels, 15.5.2003, COM(2003) 265 final.

²⁾ This opinion poll has been carried out at the request of Directorate General Internal Market Unit E4 – Media and data protection in September 2003.

As you can see on Diagram No. 1 on average more than two-thirds of EU citizens (70%) tended to agree that awareness of personal data protection in their country was low. As it has been seen on numerous occasions in other parts of the country analysis in this diagram, this average figure conceals a wide spread of opinion ranging from 57% in Austria to 83% in France.

The same spread of opinion is also seen in the constituent figures making up the EU15 average, 15% of those tended to disagree with the statement. Amongst these figures are figures of 9% or less in Ireland, France and Portugal and figures of 27% in Austria.

A similar range is seen in those respondents who answered Don't know and here the results vary from 8% in Luxembourg to 26% in Spain.

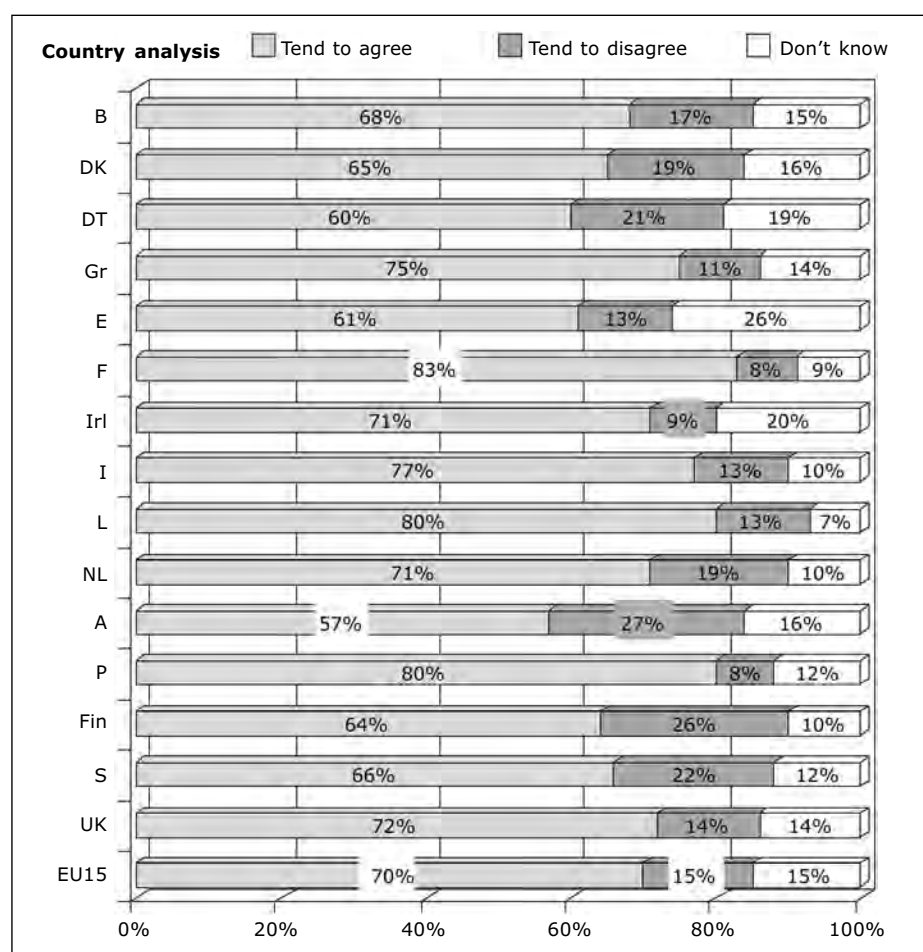


Diagram No. 1

The Slovak DP authority in close cooperation with this institute for research of public opinion carried out the survey concerning the data protection issue. Such survey was executed 6 times in: 1999, 2000, 2001, 2002, 2003 and 2005. 1300 respondents, who

represented 75 % of the population, participated in the survey. The statistical accuracy of the result, when 1266 forms were evaluated was 1-2,75 0%.The sample was composed in such a way that corresponded with the socio-demographic, educational, professional and age structure of the population. From this survey I chose the similar diagram which illustrated the growth of citizens' awareness. The Slovak respondents answered the question:

"Do you know your rights concerning the personal data protection resulting from Act on personal data protection?"

Development of the data subjects' legal awareness concerning the DP law between 1999 and 2005 shows Diagram No. 2

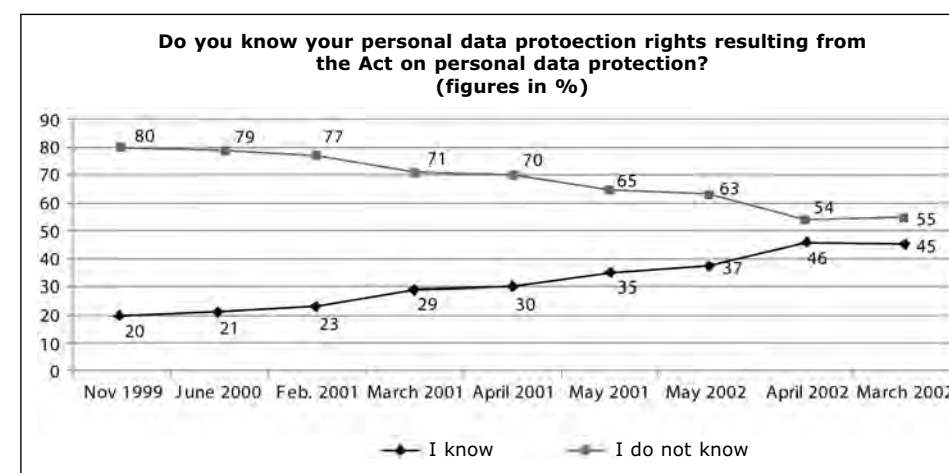


Diagram No. 2

Extraordinary awareness of their rights which relate to this problem present the respondents with university education – till 76%, then businessmen 63% and employees 61%. From categories divided by age the persons most conscious are between 40 and 49 years old (till 58%). The most legal awareness among Slovak citizens was determined in the citizens of Bratislava and Trnava (54%). As the level of education is upgraded, the legal awareness develops. The difference between respondents with university education and with basic education is 47%.

The results from the question (1) on Diagram No. 1 confirm also the answers concerning the existence of an independent supervisory authority and its tasks, which was the next question (3) included in the survey:

„Before today, had you heard or not about independent authorities monitoring the application of data protection laws, hearing complaints from individuals and imposing sanctions on law breakers?"

The next diagram shows the results of this question:

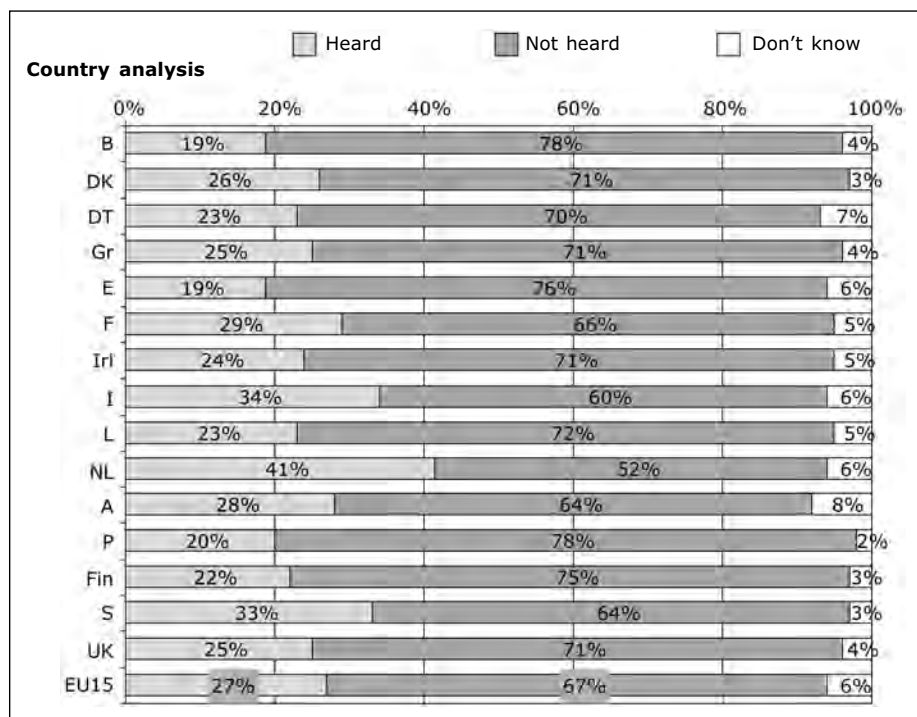


Diagram No. 3

The level of knowledge about existence of these independent authorities was low across the European Union and two-thirds (67%) of the EU citizens were not aware of their existence !!

Exercise of data subject's right

The following set of diagrams (No. 4 ÷ No. 7) illustrated in which way the EU citizens manifest their awareness practically, i.e. how they exercise their rights resulting from national DP law or other international legal regulations (Directive 95/46/EC).

According to the Article 12 of Directive 95/46/EC or corresponding paragraph from national DP law, the data controllers are obliged to respect the principle to keep data up-to-date. In practice that means that the citizen/ data subject has the right of access to his/her personal data, to ask for correction of inaccurate data or their deletion. To assess data subject's awareness concerning the application of principle of Article 12 of Directive 95/46/EC, the following question (4) was used:

"Before today, had you heard or not about laws granting individuals access to personal data held by others and the right to correct or remove data which are inaccurate or have been obtained unlawfully?"

On average 32% of EU15 citizens had heard about these laws, although this figure included numbers as disparate as 13 % in Greece and 53 % in Italy.

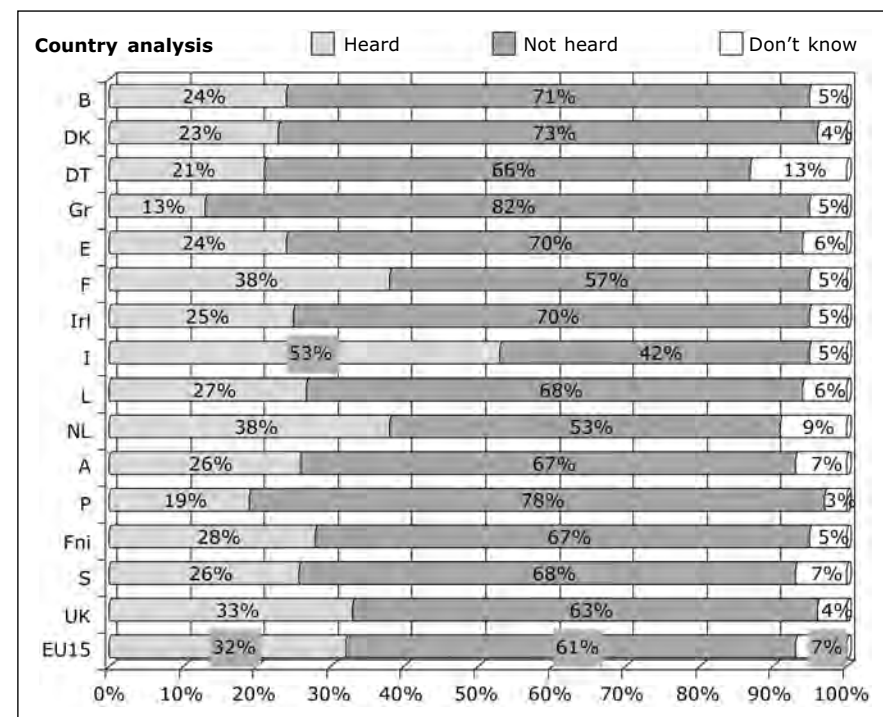


Diagram No. 4

The Slovak citizens were requested to give answer to the following, similar question (5):

"Did you take advantage to exercise your legal right to seek information on your processed personal data as well as transcription of processed data or deletion of such data?"

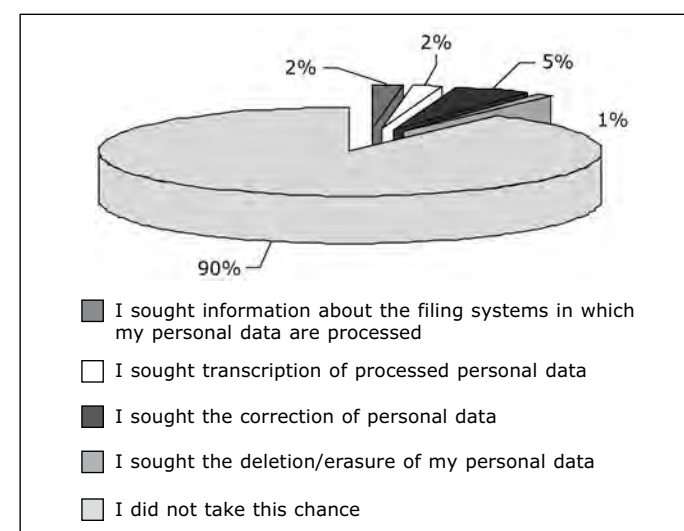


Diagram No. 5

To refuse his/her consent for the processing of data and to object against the use of data belongs to the right of individuals stipulated in Article 14 of Directive 95/46/EC. The further question (6) concerns the awareness of data subjects, if they are familiar with this right.

"Before today, had you heard or not about the need to have your agreement for someone to use your personal information and your right to oppose some uses?"

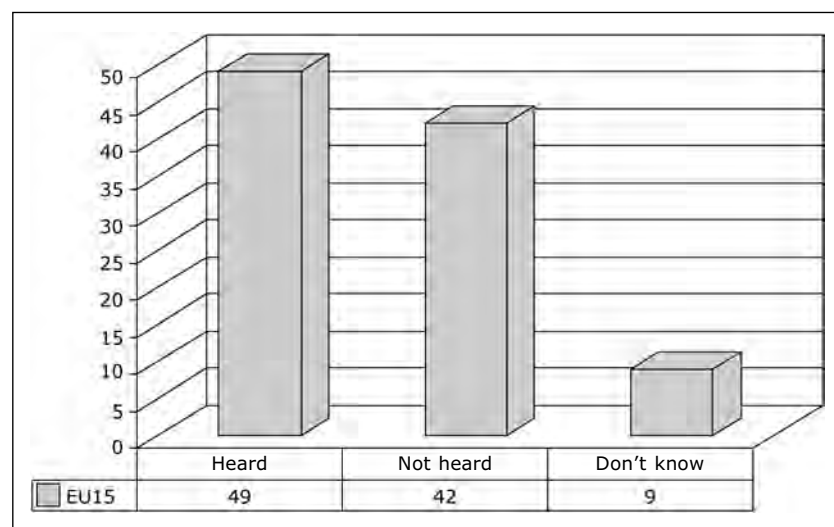


Diagram No. 6

On average, across the European Union, 49% of citizens had heard about the need to provide agreement for someone to use their personal information and their right to oppose some uses compared with the 42% who had not heard of this. However, these broad averages, once again, hide major differences between countries.

The right to refuse his/her consent for transfer of personal data to controller/(processor) in a country which is not a member of EU. In the globalized economy increasingly more data are subject to transfer between states. There is no problem from the point of data protection principles when the recipient country is a EU Member State. In case of the third country, which does not guarantee the adequate level of data protection, the consent of data subject is a necessary condition for such data transfer. The fulfilment of this condition was the idea for the following question (Diagram No. 7).

"Do you tend to agree or tend to disagree that (NATIONAL) organisations that keep personal information should not be allowed to transfer it without your consent to similar organisations in a country which is not a member of the European Union?"

82% on average of EU15 tended to agree with this statement. This high position of the EU citizens also express certain non-confidence with the legislation in the third countries.

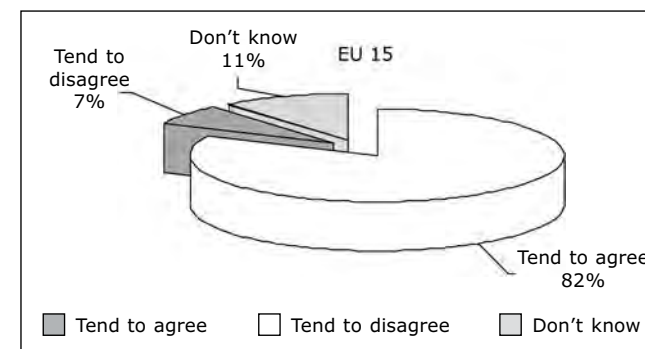


Diagram No. 7

Relation between the data subjects and data controllers

During this survey also the opinion of the EU citizens concerning the behaviour of data controllers was investigated. Attention was particularly paid to the provision of information to data subjects as well as the trust to the correct handling of personal data. The following question was included into the poll.

"The following organizations may keep personal information about us. Do you trust these organizations to use this information in a way you think acceptable?"

The result you can see on Diagram No. 8.

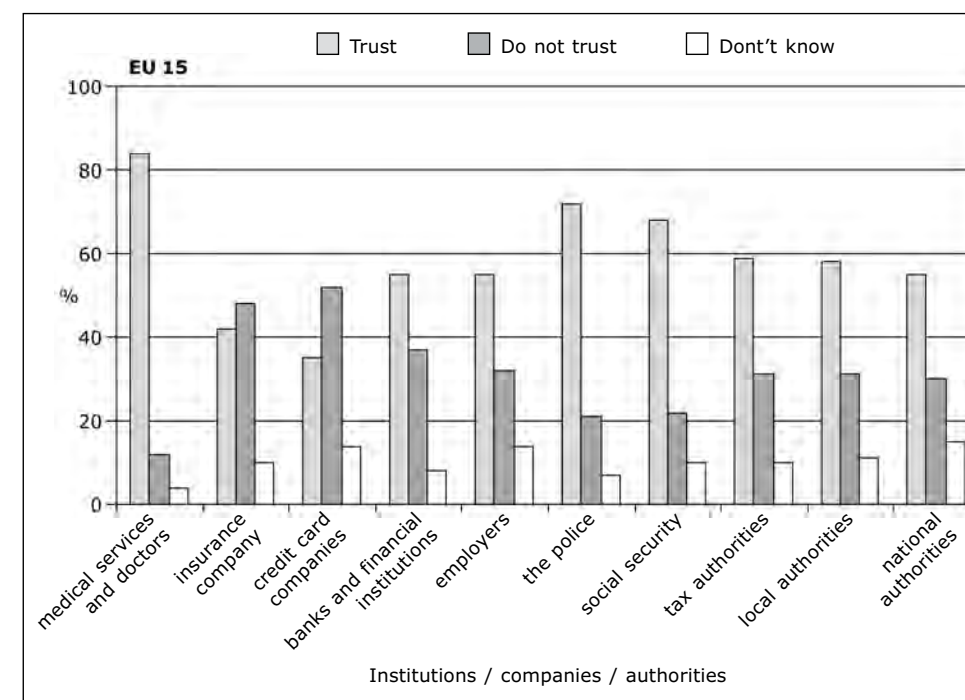


Diagram No. 8

Medical services and doctors were held in particularly high regard by EU15 citizens on the issue of the correct use of personal information. On average – 84% of EU citizens trusted the medical profession in this way, followed by the police forces which across the Europe earned the trust of nearly three out of four (72%) EU respondents, who believed that they would use personal data held about citizens in an acceptable way. The 69% trust of EU citizens in social security bodies took third place in this survey.

The trust to the use of personal information held by tax authorities, state and local authorities on average is at intervals from 55% to 59%. Credit card companies are less trusted than insurance companies and 52% of the EU poll did not trust them (in case of insurance companies this figure was 48%).

Tools for the protection of data and privacy

The next area involved in this survey concerns the use and security of electronic communication services (namely using Internet services and its influence on protection of citizens' privacy).

A lot of personal data are collected when people are on the Internet. In the course of the last years the citizens found out that using the Internet and related services mainly electronic mail and also others application can not only seriously damage the integrity of databases as well as the function of computers and software, confidentiality of correspondence, but also cause unchecked leakage of personal data without awareness of concerned persons, i.e. who use these means.

On this account the service providers as well as producers of software started to offer products to customers, which can raise the safety and security of communication, prevent or reduce the possible misuse of databases, unauthorized acquisition of personal data, mail addresses and identification of computers connected to the world wide network.

In connection to this issue, the respondents involved in the survey answered the following question (9):

"Have you heard of tools or technologies limiting the collection of PD (such data)? And, if so, have you ever used these technologies?"

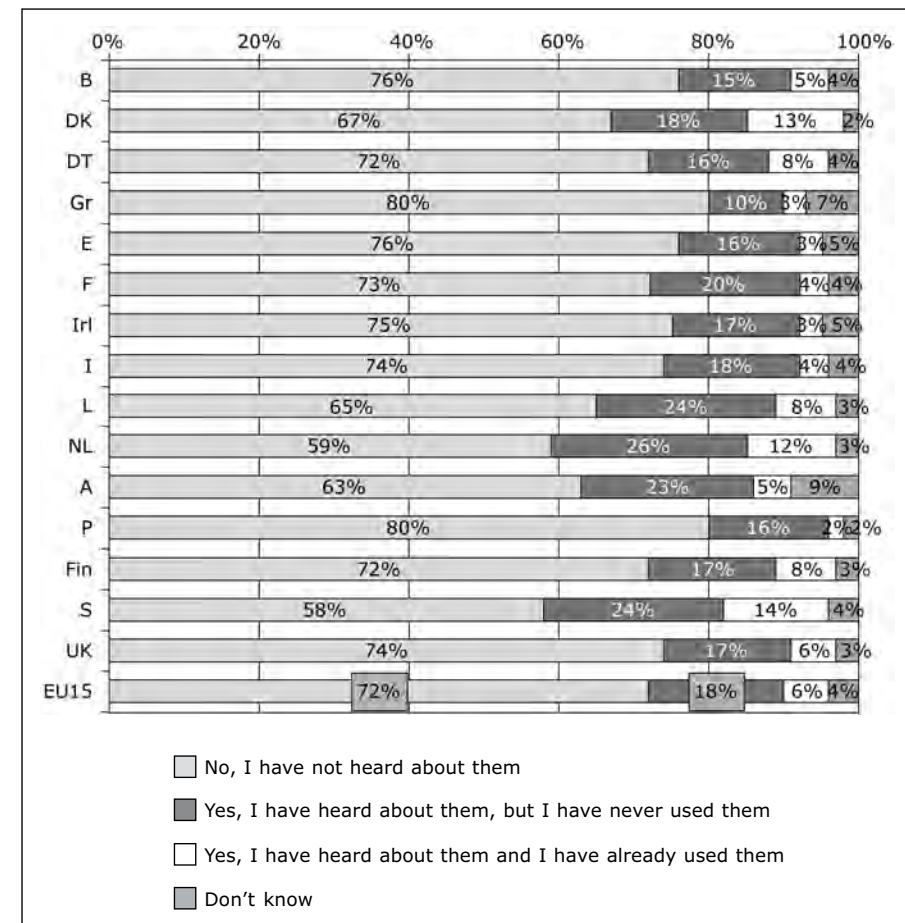


Diagram No. 9

72 % of EU citizens had never heard about these tools or technologies, but this average figure hides substantial variations by country. In Greece, the figure rises to 80%, while in computer-literate Sweden the figure is only 50%.

To give the fuller picture, the figures for those who have heard of the tools but have never used them should perhaps be aggregated with those who have not only heard of them, but already use them. Accordingly, in Sweden, this total knowledge and use figure is 38%, while in Greece it is only 13%.

On the related question (10): **"Why have you never used these tools or technologies?"**

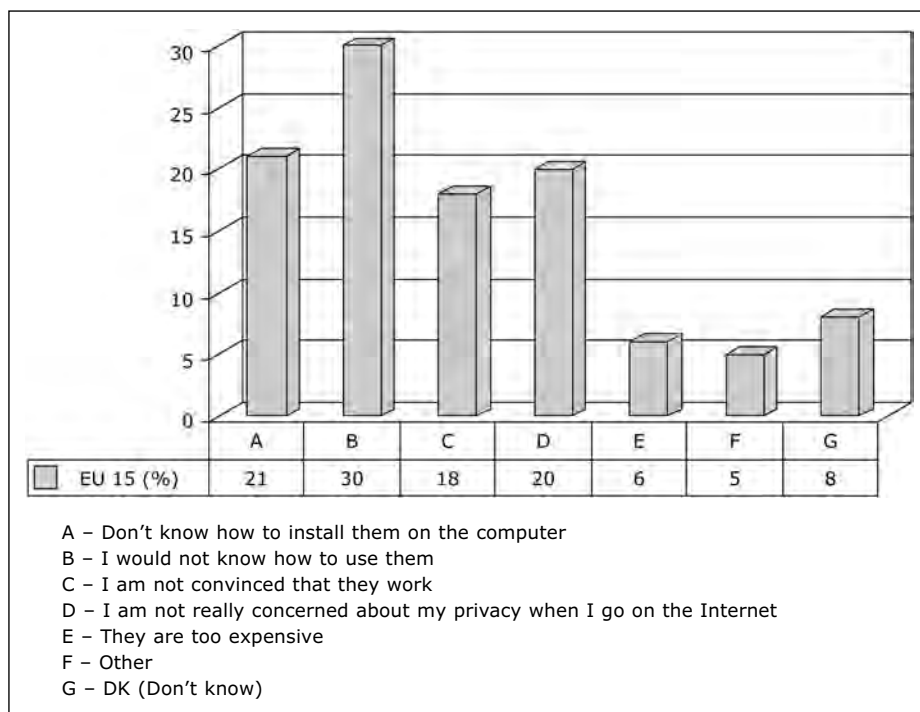


Diagram No. 10

The polled EU citizens answered in the following way: 18% of the total poll (C) who had heard about these tools but had never used them were then asked why?

The first two most often cited reasons were based upon concerns over technology. The prime reason (B) cited by 30% of this group was that they would not know how to use them. The second (A) technological reason concerned the inability to install them on the computer and was quoted by 21% of the poll.

Lack of concern about basic privacy issues was cited by 20% of the EU15 sample (D). Cost was not a major determining factor and was cited only by 6% of the poll (E).

Education activities in the field of data protection and privacy

The previous pictures from the Eurobarometer provide a certain view on the level of citizens' awareness in the EU Member. It is necessary to say that the citizens' awareness in the field of data protection does not correspond to the efforts, which the DPA in the EU Member States in the field of education and edification made.

On the base of the questionnaires obtained from DPA in the new Member States as well as from annual reports when the educational activities concern the data subjects (citizens), the following forms of communication and information provision are going on.

- Through the website of the DPAs. At present time, Internet except TV is the most frequently used source of information. From the practical point of view of citizens the most visited part of DPA websites is the part, where the frequently asked qu-

estions are illustrated, further binding position of the DPA concerning the investigated matter, information on rights of data subjects, information on procedure how to file a complaint etc.

- Telephone information is the next, frequently used service, by means of which the DPA Office provides the citizens with answers to the questions asked by the public and tutorial concerning the complaints.
- Information provided by the DPA office in written form (by post or e-mail) concerns the answer to the question asked by the public and also different written documents e.g. information bulletin for the citizens, annual report on activities of DPA Office and status of data protection matter, opinion of the DPA concerning the data subjects when providing their personal data to data controller etc.

The next diagram shows the view on the form of provision of consultation (communication of information) to the citizens by DPA in some of the EU Member States:

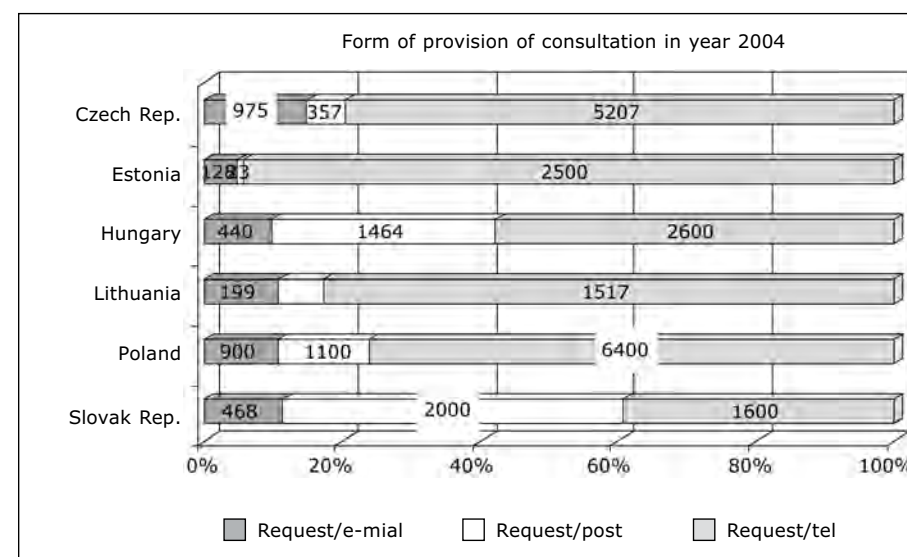


Diagram No. 11

- Provision of information to public via media (TV, radio, press and information agencies) concerning the activities of DPA and its Office, organization of conferences and seminars, legislative initiatives of DPA, issued opinions and binding position of the DPA focused on up-to-date investigated cases, when the DP law was breached, answers and explanations to the questions and complaints of citizens mediated through a journalist or representatives of television.

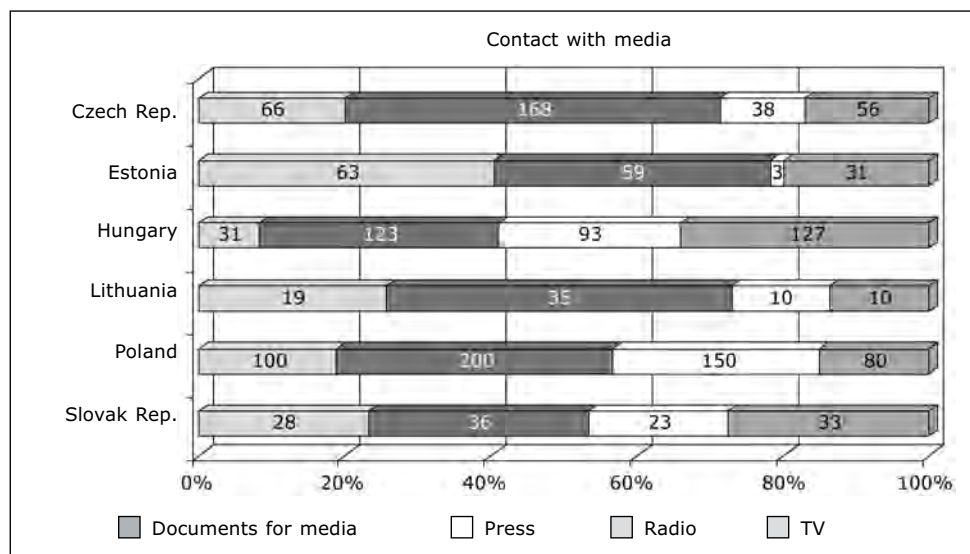


Diagram No. 12

What are the possible directions to raise the citizens' awareness?

- To raise the interest of data subject in data protection issue (to this point there is an interesting initiative of the T-PD, which suggests issuing with a support of the Council of Europe common guidelines concerning the rights of data subject as well as declaring the date 28 January 2006 as a Data Protection Day (on the 25th anniversary of opening the Convention 108/1981 ETS for signature),
- to change the passive role of data subject on data protection issue (in a current condition of globalization to delegate the responsibility for privacy and data protection to the data subject – in line with the main ideas contained in Professor Poullet report on conference on the rights and responsibilities of data subjects,³
- to incorporate the data protection topic into the regular school education system, mainly for young people/ students (aged between 10-15) who are very skillful in using computers and IT, but their awareness about data protection matter is very low, even there is no at all,
- to address the data controllers in particular in private sector and self-government to inform the clients, customers and citizens about the adopted privacy policy e.g. via Internet or billboard,
- to improve the citizens' awareness concerning the advantage, availability and use of tools supporting security of electronic communication and protection of privacy,
- to continue initiatives adopted at the International Conference on Privacy and Personal Data Protection – namely to start the collaboration in common experts group within the framework of PETTEP.⁴

³) Contribution of Prof. Poullet: Making data subjects aware of their rights and capable of protecting themselves, DP(2004) Report POULLET, Council of Europe.

⁴) 26th International Conference on Privacy and Personal Data Protection, Wrocław, 14 September 2004, Resolution on a Draft ISO Privacy Framework Standard.

Poziom świadomości obywateli a działania edukacyjne na temat ochrony danych osobowych w kontekście ochrony prywatności i danych w Unii Europejskiej

Wstęp

Źródłem wiedzy obywateli na temat ochrony danych osobowych są krajowe unormowania prawne, ustawodawstwo międzynarodowe oraz dokumenty prawne regulujące przetwarzanie i wykorzystywanie danych osobowych. Ponadto, informacje w tej dziedzinie obywatele mogą znaleźć na stronach internetowych organów ochrony danych nadzorujących przetwarzanie danych osobowych, a także uzyskać z mediów (głównie telewizji, radia i gazet), jak również dzięki bezpośrednim bądź pośrednim kontaktom z administratorami danych z sektora państwowego i prywatnego, a w końcu z doświadczeń zdobytych podczas korzystania z technologii informacyjnych i komunikacyjnych oraz serwisów elektronicznych.

Pisząc ten artykuł, próbowałem znaleźć odpowiedź na następujące pytania:

- Co składa się na świadomość prawną obywateli dotyczącą ich prywatności w związku z przetwarzaniem danych osobowych?
- Co ma wpływ na tę świadomość?
- Jaki jest poziom świadomości obywateli i jak z niej korzystają?
- Jak zwiększyć poziom świadomości obywateli?
- Jakie są trendy dotyczące przyszłości?

Niektóre opinie i tezy oraz większa część danych została zaczerpnięta ze źródeł podanych w przypisach.

Instrumenty prawne ochrony danych osobowych

W latach 70.-80. ubiegłego wieku, przede wszystkim w związku z powszechnym wprowadzaniem technik komputerowych, kilka obecnych Państw Członkowskich UE przyjęło ustawy o ochronie danych osobowych. Możemy zatem mówić o pierwszych prawnych regulacjach określających podstawowe zadania i wymagania stawiane organom kontroli w dziedzinie przetwarzania danych. Ponadto określono w nich prawa podmiotów oraz ustalono organy nadzorcze, które w przypadkach łamania prawa były uprawnione do stosowania odpowiednich środków lub nakładania sankcji finansowych. Regulacje te były przyjmowane stopniowo, różniły się przy tym poziomem legislacyjnym. W celu zniwelowania tych różnic na początku lat 80. Rada Europy, przy ścisłej współpracy z Państwami Członkowskimi, przyjęła „Konwencję o ochronie osób w związku

z automatycznym przetwarzaniem danych osobowych nr 108/1981 ETS” (zwaną dalej „Konwencją 108”).

Konwencja 108 miała na celu zapewnienie każdej osobie na terytorium każdej ze stron, niezależnie od narodowości czy miejsca zamieszkania, respektowania jej praw i fundamentalnych wolności, a zwłaszcza prawa do prywatności w związku z automatycznym przetwarzaniem danych osobowych („ochrona danych”). Dokument ten stopniowo (wraz z dodatkowym protokołem do Konwencji 108) stał się „standardem prawnym”, a zastosowanie zasad Konwencji w ustawodawstwie krajowym było kryterium poziomu ochrony danych w państwach trzecich.

Kolejnym ważnym międzynarodowym dokumentem prawnym przyjętym w październiku 1995 roku przez Parlament Europejski była Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (zwana dalej „Dyrektywą 95/46/WE”).

Główną intencją Dyrektywy 95/46/WE było ustanowienie warunków swobodnego obiegu danych w ramach Wspólnoty Europejskiej, jak też transferu danych do państw trzecich oraz zwiększenie zakresu obowiązywania zasad dotyczących przetwarzania danych osobowych, tzn. również w sferze nieautomatycznego przetwarzania i nieautomatycznych zbiorów danych.

Nowe Państwa Członkowskie UE w okresie przedakcesyjnym dostosowały krajowe regulacje do wspomnianej Dyrektywy. Stała się ona kryterium oceny poziomu regulacji ochrony danych w Państwach Członkowskich.¹

Oprócz wspomnianych wcześniej dokumentów legislacyjnych, Komisja Europejska wydała kolejne, np. decyzje, na podstawie których organ ochrony danych (DPA) egzekwuje stosowanie jednolitych praktyk odnośnie danych osobowych (np. decyzja Komisji z 15 czerwca 2001 roku o standardowych klauzulach umownych dotyczących transferu danych osobowych do państw trzecich zgodnie z Dyrektywą 96/46/WE). Zgodnie ze wspomnianą decyzją w przypadku transferu danych do państwa trzeciego organ kontroli jest zobowiązany do opracowania umowy dotyczącej podmiotu przetwarzającego dane.

„Eurobarometer” dokonał oceny poziomu świadomości obywateli UE w kwestiach związanych z ochroną danych.²

Opinia obywateli UE dotycząca poziomu świadomości w dziedzinie ochrony danych

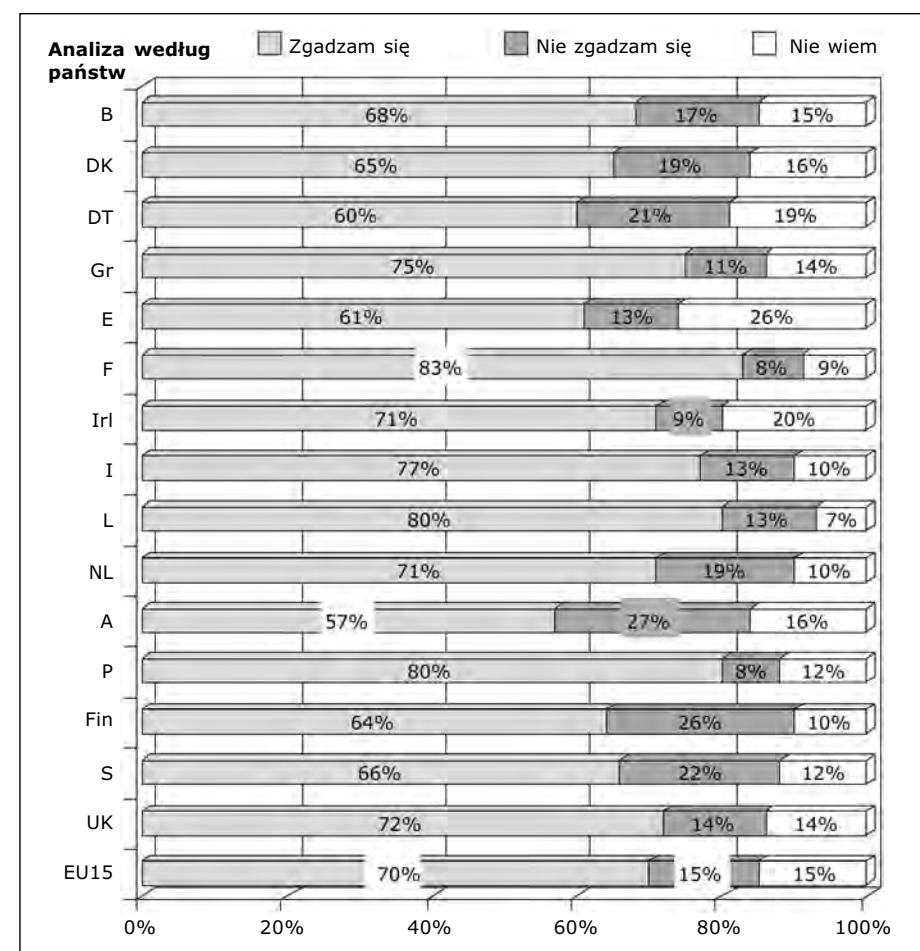
W celu uzyskania opinii na temat poziomu ochrony danych osobowych respondenci odpowiadali na następujące pytanie (1):

„Czy zgadza się Pan/Pani z twierdzeniem, że poziom świadomości o ochronie danych osobowych w (NASZYM KRAJU) jest niski?”. Uzyskano następujące odpowiedzi:

Jak wynika z wykresu 1, średnio ponad 2/3 obywateli UE (70%) zgodziło się ze stwierdzeniem, że poziom świadomości na temat ochrony danych osobowych jest niski. Przy wielu okazjach analizowania tego wykresu można było zauważyć, że średnie wyniki nie oddają dużej rozpiętości sięgającej od 57% w Austrii do 83% we Francji.

Tę samą rozpiętość można zauważyć, analizując średnie wyniki uzyskane w 15 państwach UE – 15% pytanych nie zgadzało się z tym stwierdzeniem, przy czym wartości te wynosiły od 9% lub mniej w Irlandii, Francji i Portugalii do 27% w Austrii.

Podobnie przedstawiał się rozkład odpowiedzi respondentów, która brzmiała: *nie wiem*. W tym przypadku wyniki wynosiły od 8% w Luksemburgu do 26% w Hiszpanii.



Wykres nr 1

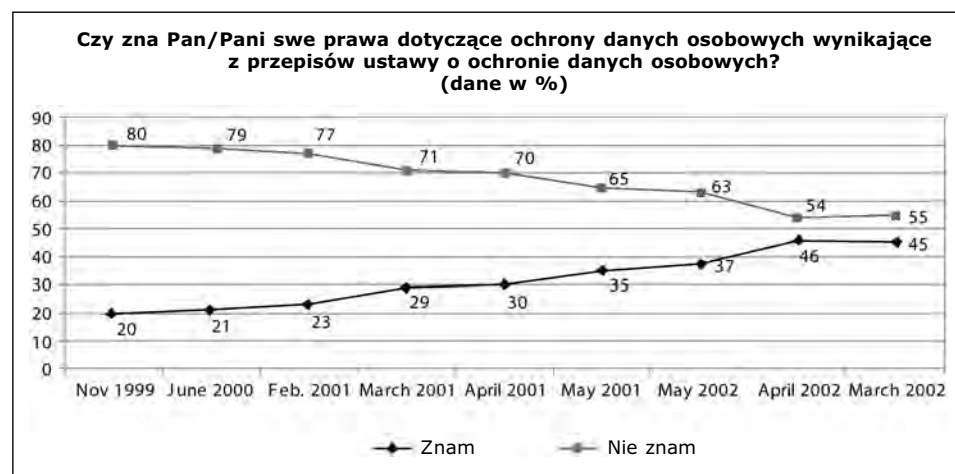
¹⁾ Pierwszy raport dotyczący wprowadzenia dyrektywy o ochronie danych 95/46/WE. Bruksela, 15.5.2003 r., COM (2003) 265 (wersja końcowa).

²⁾ Omawiane badanie opinii publicznej zostało przeprowadzone na wniosek Dykcji Generalnej Rynek Wewnętrzny, Sekcja E4 – Media a ochrona danych, we wrześniu 2003 r.

Słowacki organ ochrony danych, przy ścisłej współpracy z instytutem do spraw badania opinii publicznej, przeprowadził badanie dotyczące kwestii ochrony danych. Było ono prowadzone często, mianowicie sześć razy w następujących latach: 1999, 2000, 2001, 2002, 2003 i 2005. Wzięło w nim udział 1300 respondentów reprezentujących 75% populacji. Dokładność statystyczna wyników, przy ocenie 1266 formularzy, wyniosła 1-2,75 0%. Badanie uwzględniało czynniki socjo-demograficzne, wykształcenie, zawód i wiek respondentów. Z badania wybrałem podobny wykres ilustrujący wzrost poziomu świadomości społeczeństwa. Respondenci odpowiadali na pytanie:

„Czy zna Pan/Pani swe prawa dotyczące ochrony danych osobowych wynikające z przepisów ustawy o ochronie danych osobowych?”

Zmiany poziomu świadomości w dziedzinie regulacji prawnych przyjętych w latach 1999-2005 przedstawia wykres 2.



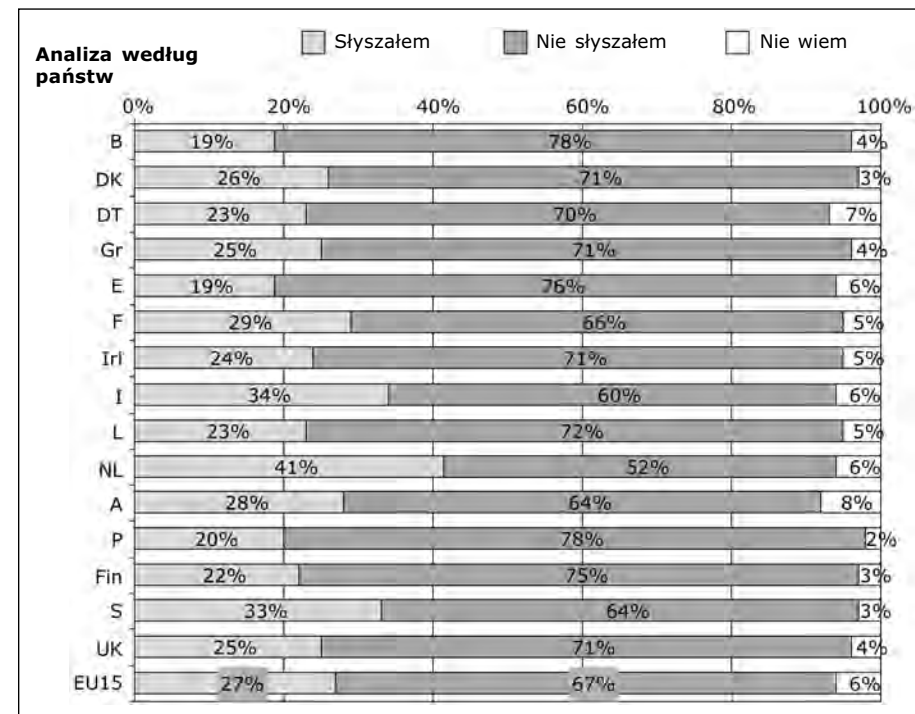
Wykres nr 2

Wyjątkowo świadomi swoich praw są respondenci z wyższym wykształceniem – 76%, następnie biznesmeni – 63% i osoby pracujące – 61%. Pod względem kategorii wiekowej na pierwszym miejscu uplasowali się respondenci w przedziale wiekowym 40-49 lat (58%). Najwyższy poziom świadomości reprezentowali obywatele Bratysławy i Trnavy (54%). Ponieważ wyższy jest poziom edukacji, wzrasta także stopień świadomości prawnej. Różnica między respondentami z wyższym wykształceniem i wykształceniem podstawowym wyniosła 47%.

Wyniki uzyskane na podstawie odpowiedzi na pytanie (1) na wykresie 1 potwierdzają również odpowiedzi na pytanie dotyczące istnienia niezależnego organu nadzorczego i jego zadań (3):

„Czy słyszał/a Pan/Pani o niezależnym organie monitorującym stosowanie prawa o ochronie danych, rozpatrującym zażalenia jednostek i nakładającym sankcje na łamiących prawo?”

Odpowiedzi na to pytanie przedstawia kolejny wykres.



Wykres nr 3

Poziom wiedzy w Unii Europejskiej na temat niezależnych organów był niski, a 2/3 (67%) obywateli UE nie wiedziało o ich istnieniu!

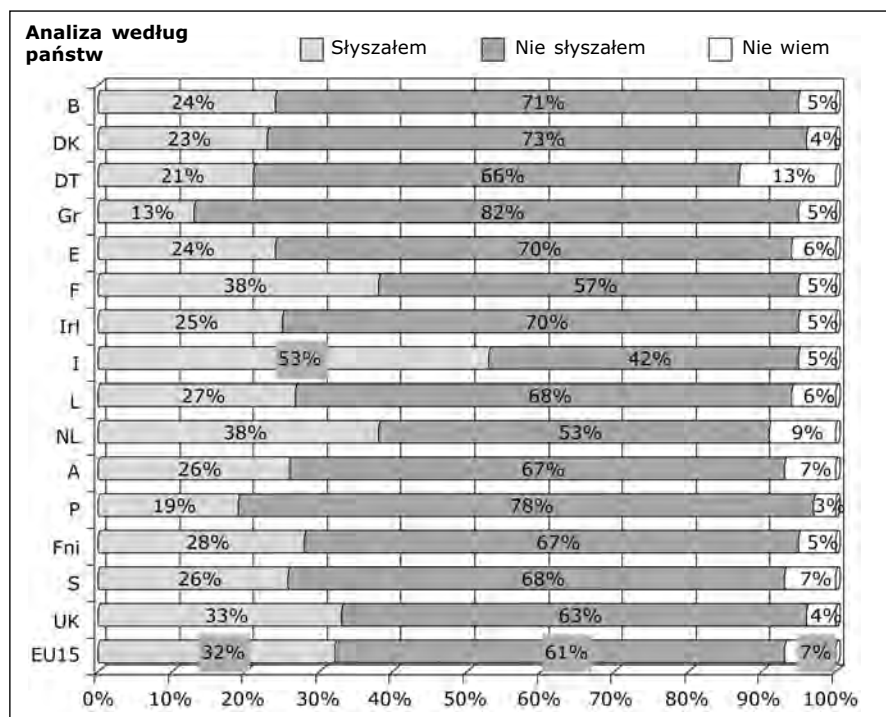
Korzystanie podmiotu, którego dane dotyczą, z przysługujących mu praw

Kolejne wykresy (4-7) ilustrują, w jaki sposób obywatele UE postępują w praktyce, tzn. czy wiedzą, jak korzystać z przysługujących im praw wynikających z przepisów prawnych dotyczących ochrony danych lub innych międzynarodowych regulacji (Dyrektywa 95/46/WE).

Administratorzy danych są zobowiązani – zgodnie z art. 12 Dyrektywy 95/46/WE lub z odpowiednim przepisem krajowego ustawodawstwa o ochronie danych – do przestrzegania zasady uaktualniania danych. W praktyce oznacza to, że obywatel, którego dane dotyczą, ma prawo dostępu do swoich danych osobowych, tzn. może poprawić niewłaściwe dane bądź je usunąć. W celu oceny poziomu świadomości podmiotu, którego dane dotyczą, dotyczącej stosowania zasady wynikającej z art. 12 Dyrektywy 95/46/WE, zadano następujące pytanie (4):

„Czy słyszał/a Pan/Pani o regulacjach prawnych przyznających jednostce prawo dostępu do danych osobowych będących w posiadaniu innych oraz prawo do poprawienia bądź usunięcia danych, które są niewłaściwe lub zostały uzyskane bezprawnie?”

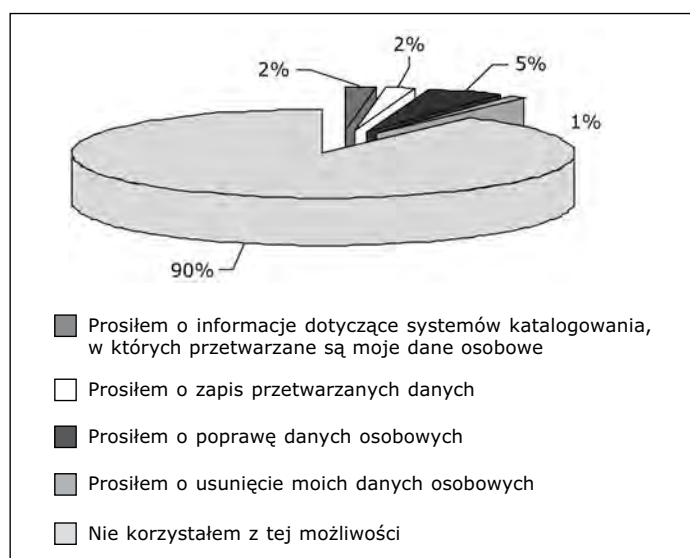
Średnio 32% respondentów z 15 państw UE słyszało o tych regulacjach, jednak wyniki są bardzo rozbieżne – 13% w Grecji i 53% we Włoszech.



Wykres 4

Obywatele słowacy zostali poproszeni o odpowiedź na podobne pytanie (5):

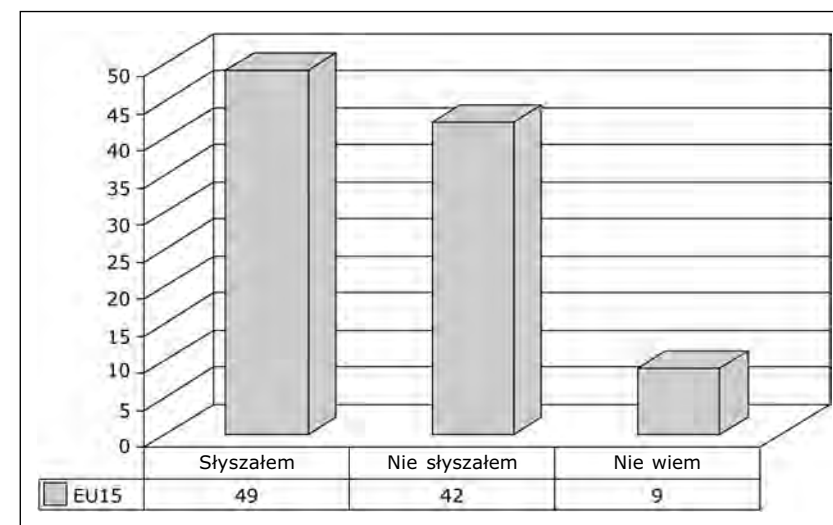
„Czy skorzystał/a Pan/Pani ze swego prawa do uzyskania informacji dotyczących przetwarzanych danych osobowych, jak też zapisu przetwarzanych danych lub usunięcia tych danych?”



Wykres 5

Jednostka ma prawo nie wyrazić zgody na przetwarzanie danych oraz prawo do sprzeciwu wobec korzystania z tych danych zgodnie z art. 14 Dyrektywy 95/46/WE. Kolejne pytanie (6) dotyczyło wiedzy podmiotu o przysługującym mu prawie.

„Czy wiedział/a Pan/Pani, że osoba, która chce korzystać z Pańskich danych osobowych musi mieć Pana/Pani zgodę oraz że ma Pan/Pani prawo nie wyrazić zgody na korzystanie z tych danych?”

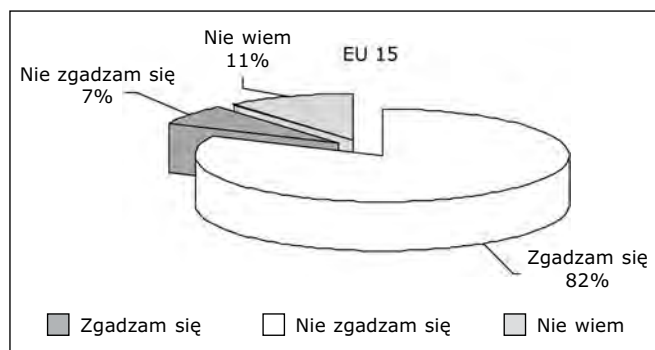


Wykres 6

Przeciętnie w Unii Europejskiej 49% obywateli słyszało o konieczności posiadania zgody podmiotu, którego dane dotyczą, na użytkowanie jego danych i o prawie sprzeciwu wobec wykorzystywania jego danych, natomiast 42% nie słyszało o tym prawie. Jednak przedstawione średnie wyniki po raz kolejny świadczą o dużych różnicach między państwami.

Prawo do niewyrażenia zgody na transfer danych osobowych do administratora danych do kraju, który nie jest członkiem UE. W zglobalizowanej gospodarce coraz więcej danych podlega transferowi między państwami. Z punktu widzenia zasad ochrony danych nie ma problemu, kiedy państwo odbiorca jest Państwem Członkowskim UE. W przypadku państwa trzeciego, które nie gwarantuje dostatecznego poziomu ochrony danych, zgoda podmiotu jest warunkiem koniecznym do przeprowadzenia transferu. Spełnienie tego warunku zrodziło następne pytanie (wykres 7).

„Czy zgadza się Pan/Pani, aby (KRAJOWYM) organizacjom, które posiadają dane osobowe, nie wolno było przekazywać tych danych bez Pana/Pani zgody podobnym organizacjom w państwie, które nie jest członkiem Unii Europejskiej?”



Wykres 7

82% respondentów z 15 badanych państw UE dało twierdzącą odpowiedź. Dane te świadczą o braku zaufania do poziomu regulacji prawnych w państwach trzecich.

Relacje między podmiotami danych a administratorami danych

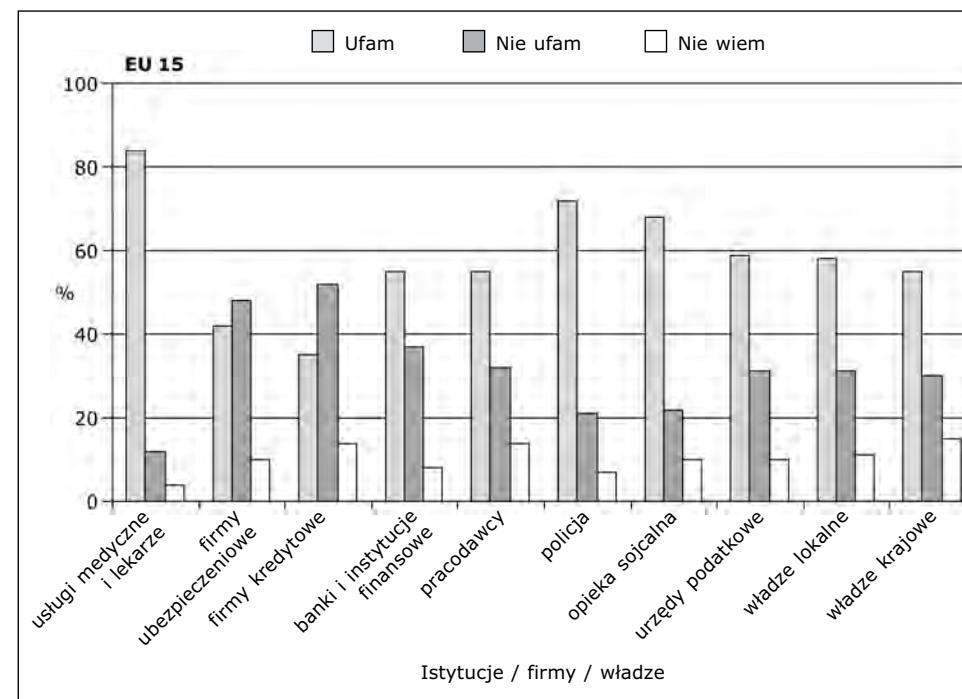
Podczas przeprowadzania tego sondażu badano również opinie obywateli UE dotyczące zachowania się administratorów danych. Zwrócono szczególną uwagę na zapewnienie informacji podmiotom, których dane dotyczą, jak też na zaufanie, co do prawidłowego wykorzystania danych osobowych. W badaniu zadano pytanie:

„Następujące organizacje mogą przechowywać informacje osobowe na nasz temat. Czy ufa Pan/Pani tym organizacjom odnośnie korzystania z tych informacji w odpowiedni sposób?”

Wyniki ilustruje wykres 8.

Sfera usług medycznych oraz lekarze zostali szczególnie wysoko ocenieni w 15 państwach UE odnośnie właściwego wykorzystywania danych osobowych. Średnio 84% obywateli UE zaufało profesjom medycznym w tej dziedzinie, drugie miejsce zajęła policja, która zyskała zaufanie prawie u $\frac{3}{4}$ (72%) respondentów. Uważali oni, że policja korzysta z danych osobowych o obywatelach w akceptowalny sposób. 69% uzyskały instytucje opieki społecznej, plasując się na trzecim miejscu.

Zaufanie do organów podatkowych, władz państwowych i lokalnych w kwestii używania danych osobowych wyniosło średnio od 55% do 59%. Mniej osób ma zaufanie do firm kredytowych niż do firm ubezpieczeniowych, a 52% respondentów nie miało do nich zaufania (w przypadku firm ubezpieczeniowych wartość ta wynosiła 48%).



Wykres 8

Narzędzia służące do ochrony danych i prywatności

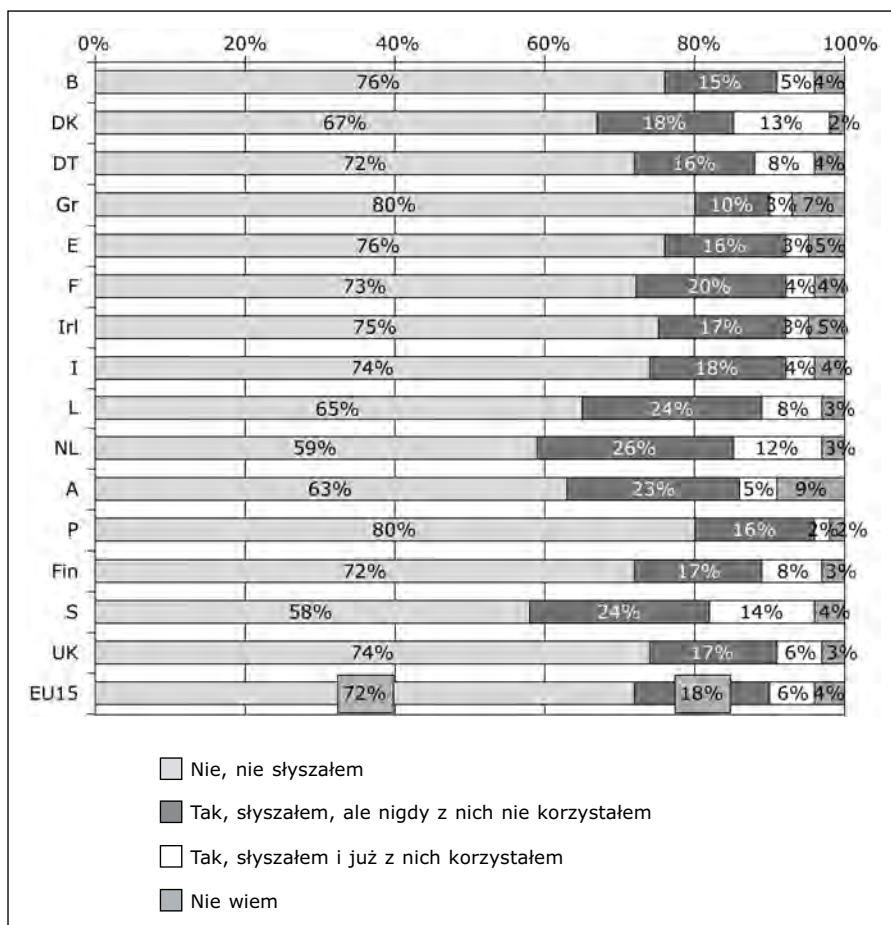
Kolejna badana dziedzina dotyczyła korzystania z elektronicznych środków łączności (z usług internetowych oraz ich wpływu na ochronę prywatności obywateli).

Podczas korzystania z Internetu uzyskuje się wiele danych osobowych. W ciągu ostatnich kilku lat obywatele zauważyli, że korzystanie z Internetu i podobnych serwisów, głównie poczty elektronicznej oraz innych aplikacji, może nie tylko poważnie naruszyć integralność baz danych, wpłynąć na działanie komputera i oprogramowania, ale spowodować także wydostanie się danych osobowych bez świadomości osób, które korzystają z tych środków.

Z tego powodu zarówno dostawcy usług, jak i producenci oprogramowania oferują klientom produkty, które mogą zwiększyć bezpieczeństwo w dziedzinie łączności, zapobiec niewłaściwemu korzystaniu z baz danych oraz bezprawnemu pozyskiwaniu danych osobowych i adresów poczty elektronicznej lub ograniczyć te działania, a także uniemożliwić identyfikację komputerów podłączonych do sieci www.

W związku z tą kwestią respondenci uczestniczący w badaniu odpowiedzieli na następujące pytanie (9):

„Czy słyszał/a Pan/Pani o narzędziach i technologiach ograniczających zbieranie danych osobowych? Jeśli tak, czy kiedykolwiek stosował/a Pan/Pani te technologie?”

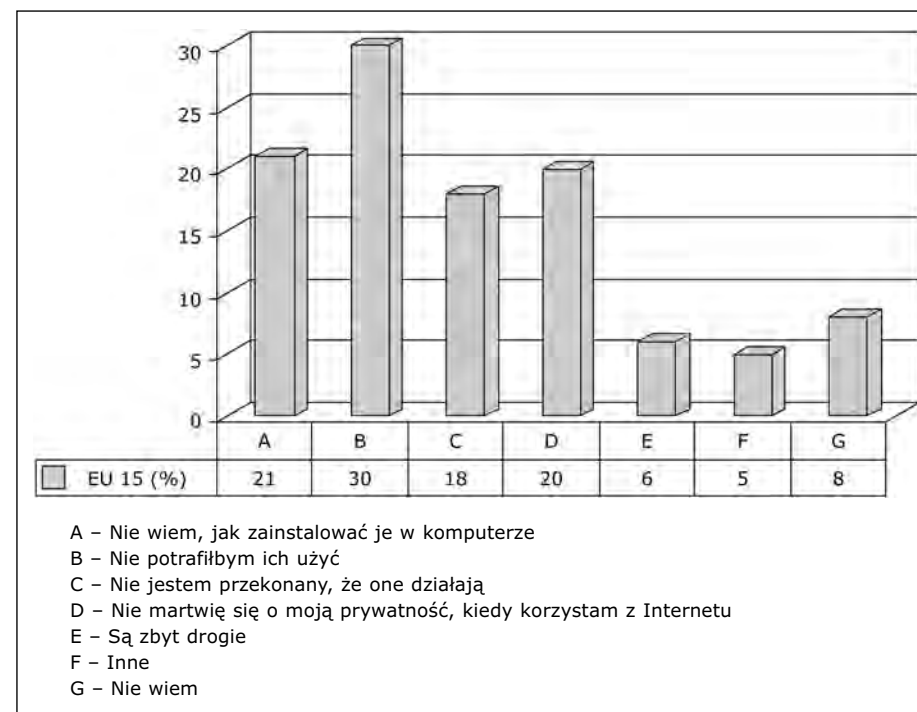


Wykres 9

72% obywateli UE nigdy nie słyszało o tych narzędziach i technologiach, ale średnia ta nie wykazuje znacznych różnic między poszczególnymi państwami. W Grecji liczba ta stanowi 80%, podczas gdy w rozwiniętej pod względem informatycznym Szwecji tylko 50%.

By uzyskać pełny obraz wyniki dotyczące osób, które słyszały o tych narzędziach, ale nigdy z nich nie korzystały, być może należałoby zsumować z tymi, które odnoszą się do osób, które nie tylko o nich wiedzą, ale też z nich korzystają. Odpowiednio w Szwecji znajomość i korzystanie z tych narzędzi zadeklarowało 38%, podczas gdy w Grecji tylko 13%.

Związane z tą kwestią pytanie (10) brzmiało: „**Dlaczego nigdy nie korzystał/a Pan/Pani z tych narzędzi lub technologii?**”



Wykres 10

Biorący udział w ankiecie obywatele UE odpowiedzieli w następujący sposób: 18% ogólnej liczby ankietowanych udzieliło odpowiedzi C, czyli słyszało o tych narzędziach, ale z nich nie skorzystało. Zapytano ich dlaczego.

Dwa główne powody dotyczyły spraw związanych z technologią. Podstawowym powodem (B) podanym przez 30% ankietowanych był brak umiejętności korzystania z nich. Drugi (A) powód dotyczył braku umiejętności zainstalowania tych narzędzi w komputerze – odpowiedzi takiej udzieliło 21% pytanych.

20% respondentów wykazało brak zainteresowania kwestiami dotyczącymi prywatności (D). Koszty nie były czynnikiem decydującym i zostały podane tylko przez 6% respondentów (E).

Działania edukacyjne w sferze ochrony danych i prywatności

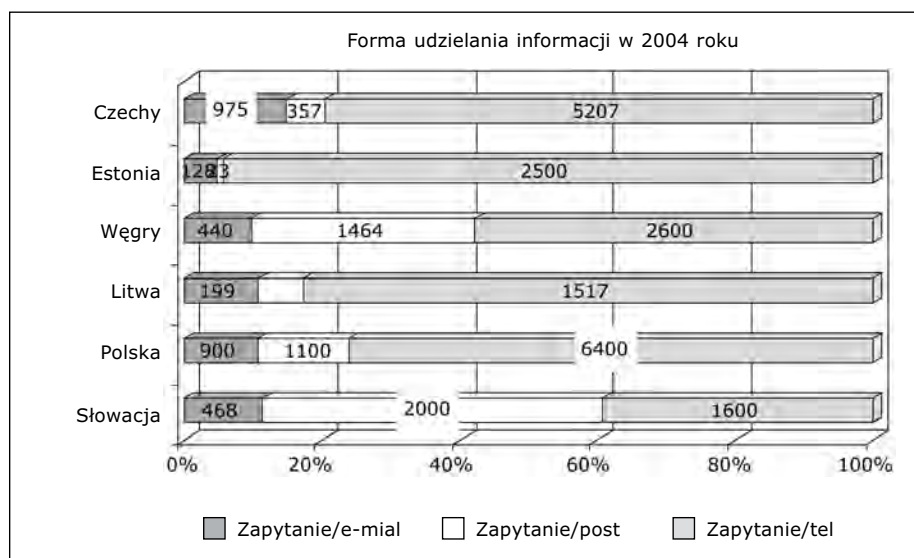
Dane uzyskane w wyniku badań przeprowadzonych przez „Eurobarometer” dają nam pewne spojrzenie na poziom świadomości obywateli w Państwach Członkowskich UE. Należy przy tym dodać, że poziom ten nie koresponduje z wysiłkami, które podejmują w Państwach Członkowskich UE DPA w dziedzinie edukacji i oddziaływania na społeczeństwo.

Na podstawie kwestionariuszy uzyskanych z DPA w nowych Państwach Członkowskich, jak również rocznych raportów z działalności edukacyjnej, którą są objęte podmioty danych (obywatele), można wyróżnić następujące formy przekazywania informacji.

- Strona internetowa DPA. Obecnie Internet, poza telewizją, jest źródłem informacji, z którego korzysta się najczęściej. Z praktycznego punktu widzenia, najczęściej odwiedzaną zakładką strony internetowej jest ta, która dotyczy najczęściej zadawanych pytań, wiążącego stanowiska DPA w danej sprawie, informacji odnoszących się do praw przysługujących podmiotowi danych, informacji, jak składać skargi itd.
- Informacje telefoniczne. Jest to kolejna, często stosowana metoda, za pomocą której Biuro DPA udziela odpowiedzi na pytania obywateli oraz udziela wskazówek w przypadku zażaleń.
- Informacje udzielane przez Biuro DPA w formie pisemnej (przesyłane zwykłą pocztą bądź elektroniczną). Są to odpowiedzi na pytania zadane przez społeczeństwo. Zawarte są także w różnych drukowanych publikacjach, np. w biuletynie informacyjnym opracowywanym dla obywateli, w raporcie rocznym z działalności Biura DPA i o sytuacji w dziedzinie ochrony danych, w opiniach DPA w sprawie przekazywania danych osobowych organowi kontroli danych przez podmioty danych.

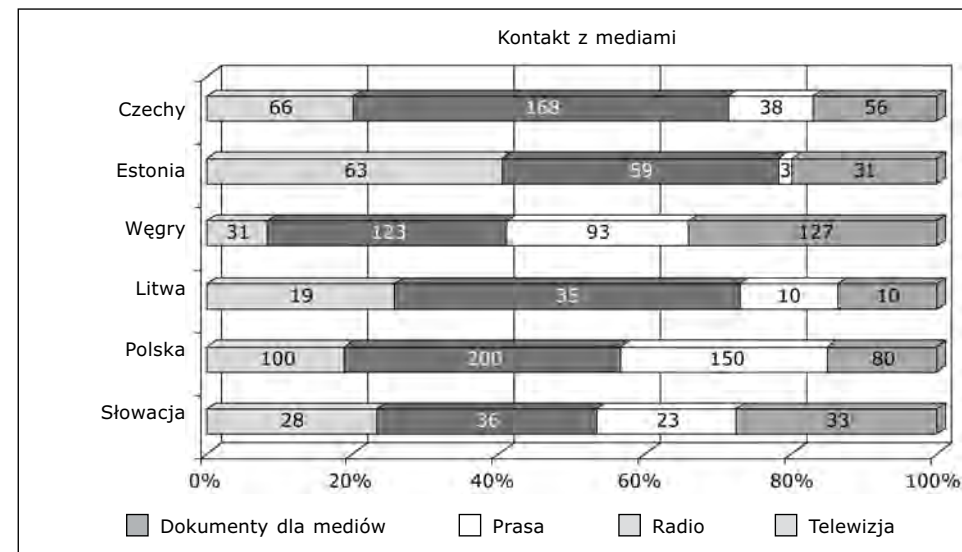
Kolejny wykres przedstawia formę konsultacji – udzielania informacji społeczeństwu przez DPA w kilku Państwach Członkowskich UE.

Formy konsultacji w 2004 roku:



Wykres 11

- Informacje przekazywane z wykorzystaniem mediów (telewizji, prasy i agencji informacyjnych). Dotyczą czynności podjętych przez DPA i jego Biuro, organizowanych konferencji i seminariów, inicjatyw legislacyjnych DPA oraz wydanych opinii i wiążących stanowisk DPA w aktualnie prowadzonych sprawach, kiedy miało miejsce naruszenie prawa, a także odpowiedzi i wyjaśnień dotyczących kwestii spornych i skarg obywateli przekazanych przez dziennikarza bądź przedstawicieli telewizji.



Wykres 12

Jakie działania można podjąć, by zwiększyć poziom świadomości obywateli?

- Zwiększyć zainteresowanie podmiotu, którego dane dotyczą, kwestią ochrony danych (w tej dziedzinie powstała interesująca inicjatywa T-PD, która zakłada opracowanie przy wsparciu Rady Europy wspólnych wytycznych dotyczących praw podmiotu, którego dane dotyczą, a także ogłoszenie 28 stycznia 2006 roku Dniem Ochrony Danych (w 25. rocznicę podpisania Konwencji 108/1981 ETS).
- Uaktywnić podmiot w kwestii ochrony danych (w obecnych warunkach globalizacji przekazać odpowiedzialność za ochronę prywatności i ochronę danych podmiotowi danych – zgodnie z głównymi założeniami zawartymi w raporcie profesora Poulléta przedstawionym na konferencji dotyczącej praw i obowiązków podmiotów danych).³
- Włączyć tematy z zakresu ochrony danych do programu nauczania, zwłaszcza uczniów (w wieku 10-15 lat), którzy bardzo umiejętnie posługują się komputerem, jednak poziom ich świadomości w dziedzinie ochrony danych jest bardzo niski a wiedza zerowa.
- Zwrócić się do organów kontroli danych, zwłaszcza w sektorze prywatnym i samorządowym, o informowanie klientów i obywateli o przyjętej polityce w dziedzinie prywatności, np. za pomocą Internetu bądź przez plakaty informacyjne.
- Podnieść poziom świadomości obywateli na temat zalet, dostępności i możliwości korzystania z narzędzi zwiększających bezpieczeństwo komunikacji elektronicznej i ochronę prywatności.
- Kontynuować inicjatywy przyjęte na Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych w celu nawiązania współpracy w grupach eksperckich w ramach PETTEP.⁴

³⁾ Artykuł prof. Poulléta: „Making data subjects aware of the rights and capable of protecting themselves”. DP (2004) Report POULLET, Rada Europy.

⁴⁾ 26 Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych, Wrocław, 14 września 2004 r., Rezolucja w sprawie projektu standardu ochrony prywatności ISO.

Data protection in the Republic of Lithuania

I. LEGISLATION

The grounds for the data protection are established in the Constitution of the Republic of Lithuania (1992) and in the Law on Legal Protection of Personal Data (1996). The Article 22 of the Constitution of the Republic of Lithuania:

The private life of an individual shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other intercommunications shall be inviolable. Information concerning the private life of an individual may be collected only upon a justified court order and in accordance with the law. The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life and from encroachment upon their honor and dignity.

The new version of the Law on Legal Protection of Personal Data of the Republic of Lithuania was adopted in 2003 and on 1 July 2003 this Law came into force. It was passed in order to achieve fine-tuning with the EU acquis. Additionally the Law establishes the conditions of the personal data processing for the purposes of evaluation of a person's solvency and management of his/her debt, regulates the cases, in which the State Data Protection Inspectorate shall carry out the prior checking. The English version of this Law is available on the website www.ada.lt.

The recent amendment of the Law (the Law was adopted by Sejm on 13 April 2004) concerning prior checking came into force on 24 April 2004. The Law narrowed the scope of the prior checking to the processing of sensitive personal data by automated means for the purposes of internal administration or in the cases specified in Article 10 and paragraph 2(6) and (7) of Article 5 of this Law; where the data controller intends to process public data files by automated means unless the laws and other legal acts specify the procedure for disclosure of the data.

The Law on Electronic Communications, transposing Directive 2002/58/EC into national law, was adopted on 15 April 2004 and came into force on 1 May 2004.

The supplements of Administrative Code, foreseeing administrative liability for unlawful processing of personal data and violation of privacy protection in the scope of electronic communications, were adopted on 22 April 2004. The Administrative Code defines various monetary penalties in cases of the infringement of the Law on Legal Protection of Personal Data.

The new version of the Penal Code, which came into force on 1 May 2003, established penal liability for unlawful collection of information about private life of individual, the disclosure and use of such information. The unlawful collection of information about

private life of individual, the disclosure and use of such information is punished by public works or fine, or confinement, or arrest, or imprisonment up to three years. The penal liability for such criminal offences is also for legal entity.

In February 2000 Lithuania signed and in 2001 ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108). On 8 November 2001 Lithuania signed and on 18 December 2003 ratified Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108) regarding Supervisory Authorities and Transborder Data Flows.

On 23 June 2003 Lithuania signed the Council of Europe Convention on Cybercrime. On 8 March 2004 the Parliament of the Republic of Lithuania ratified the Convention drawn up on the basis of Article K.3 of Treaty on European Union, on the use of information technology for customs purposes. On 15 July 2004 the Government of the Republic of Lithuania appointed the Inspectorate as a responsible authority for the independent supervision of personal data entered in the Customs Information System, ensuring that processing and use of personal data stored in the Customs Information System would not violate rights of concerned persons.

On 22 April 2004 the Parliament of the Republic of Lithuania ratified the Convention based on Article K.3 of the Treaty on European Union, on the establishment of the European Police Office (Europol Convention). On 28 June 2004 the Government of the Republic of Lithuania appointed the Inspectorate as a responsible authority for the independent supervision of the permissibility of the input, the retrieval and any communication of personal data to Europol by the Republic of Lithuania and for examination whether this doesn't violate the rights of the data subject.

On 20 May 2003 by the Governmental Resolution No. 624 the State Data Protection Inspectorate was assigned as the institution responsible for the independent supervision of the legitimacy of the processing of personal data in the national Schengen Information System.

II. DATA PROTECTION ISSUES

1) Case on Alcohol and Tobacco

At the beginning of May 2004 the adviser of the President *ad interim* of the Republic of Lithuania referred to the Inspectorate with the request to examine if the biggest supermarkets do not violate the Law on Legal Protection of Personal Data when requesting the personal identity documents and inputting the first seven numbers of customer's identification number from it into cash register.

The Law on Alcohol Control, which came into force on 1 May 2004, provided that it shall be prohibited to sell alcoholic beverages to individuals who are under 18 years of age; the persons who sell alcoholic beverages shall have the right, and if there are any suspicions that the person is younger than 18 years old, are obliged to request, that the individual who is buying alcohol products present a document attesting his age; if the person doesn't present a document attesting his age, sellers of alcohol products must refuse to sell him these products. The same provisions on selling tobacco products are in the Law on Tobacco Control.

The supermarkets started to request the personal identity documents from all citizens in order to make sure that alcohol or tobacco products were not sold to the customer who was a minor.

In May 2004 the Inspectorate carried out checking if the requirements of the Law on Legal Protection of Personal Data were not violated while selling alcohol beverages and tobacco products and found no violations motivating that the supermarkets did not process personal data and one supermarket used the first numbers of personal identification number for the only purpose – to estimate the age of a person and it was impossible directly or indirectly to identify the person, according to them.

2) Case of Special Investigation Service

At the beginning of 2004 Parliamentary Committee on National Security and Defence informed the Inspectorate about the possible violations of the Law on Legal Protection of Personal Data in the Special Investigation Service.

The Law on Prevention of Corruption establishes the restrictions for the gathering and use of the information about a person seeking or holding a position at a state or municipal institution; the decision to request the Special Investigation Service for information about a person shall be made by the head of an institution or a state politician that intends to appoint or that has appointed the person.

During the inspection it was detected that personal data were provided for the persons who were not entitled the right to receive such information and other violations of personal data processing were detected: Special Investigation Service processed sensitive data without executing prior checking, unlawfully collected information from some institutions, did not notify the Inspectorate on the cases of automated processing of personal data. The Inspectorate instructed the Special Investigation Service to eliminate the detected violations during the set time. The Special Investigation Service appealed against the instruction of the Inspectorate to the Court. The main issue was related with the application of the Law especially what concerns the processing of structured filing system by non-automatic means. Special Investigation Service contested the Inspectorate's right established in the Article 32 paragraph 1 subparagraph 5 of the Law on Legal Protection of Personal Data to make recommendations and give instructions to data controllers with regard to personal data processing and protection while the Service was not a data controller. The court overruled this argument saying that data controller is a legal or natural person which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes of the processing of personal data are determined by laws or other legal acts, the data controller and/or the procedure for its appointment may be designated by laws or other legal acts. Processing of data is any operation, which is performed upon personal data such as collection, recording, accumulation, storage, classification, grouping, combination, alteration (supplementing or rectifying), disclosure, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction or any other operation or a set of operations. The court founded that the Service by fulfilling its task in preventing the corruption area and processing the personal data became data controller. There was an argument made by the Service that the Law on Legal Protection of Personal Data is not applicable to the activities of the Service while

the Article 1 paragraph 5 of the Law states that when personal data are processed for the purposes of State security or defence, this Law shall apply insofar as other laws do not provide otherwise. The court overruled this saying that there is no reason to allege that the Law on Legal Protection of Personal Data is not applicable. The only absolute exception established in the Law on Legal Protection of Personal Data is that the Inspectorate shall have no right to monitor processing of personal data in courts.

3) Cases of use of personal identification number

The personal identification number is a unique sequence of digits assigned for person's identification, collection of data about him, and ensuring of interaction between state registers and information systems. Personal identification number assigned to a person is unique and unalterable. Frequently, data controllers collect personal code from data subject not for the purpose of identification, but in order to keep this data, although it is not used for any other purposes for which it was collected.

The Inspectorate receives more and more notifications from persons on collection of personal identification number for discount and client loyalty cards of shops and pharmacies. After examination of persons' complaints the Inspectorate has detected that data controllers process excessive data – personal identification number and has drawn up Protocols of Administrative Offences which are examined in Court.

On 23 July 2004, the Chairman of the Parliament of the Republic of Lithuania organized round-table discussion about the use of personal identification number and the Director of the State Data Protection Inspectorate participated there. The research "Implementation of Human Rights in Lithuania" made in 2004 by Human Monitoring Institute was considered there. The attention was drawn to the excessive use of personal identification numbers in Lithuania. Institute noted that there were about 560 legal acts in force in Lithuania (including amendments and supplements) regulating the use of personal identification number. It was agreed unanimously that legal base on the use of identification numbers should be revised and also that public should be informed wider that a person could realize his right to give consent or to object to processing of his identification number or other data.

Also in 2004 the Inspectorate received a complaint disputing the lawfulness of personal data processing by one joint-stock company (hereinafter – Company X). The requestor claimed that Company X offering a card of benefits requires providing PIN. During the investigation it was established that Company X presenting the loyalty card's blank (hereinafter referred to as Blank) to be filled in by person, requires indicating the following data: name, surname, PIN, gender, place of residence, telephone number, electronic mail address. The Company X processes the PINs of the clients, although the PIN is not used for any specific purpose, it is not needed for accomplishment neither the paying of taxes nor any other purposes. It was established that the processing purpose of data to be filled in the Blank, is to calculate the number of scores grantable for the persons who fulfil payment (carry out transactions) by loyalty cards at the chain stores managed by Company X and to disperse the information about the commercial events and promotions carried out in the trading centre to the card owner. But according to the Buyer's card general usage rules, item 4.3 points out, that Company X card owner presenting the card for the first time and paying for the purchases at Company X stores, will be granted the discount of 10% of total estimated value of

the purchase. Thus the purpose of processing of data to be filled in the form is not only calculation of scores gained and sending the information related to promotions carried out in the trading process, to the card owner, but also application of payoffs for the Company X loyal customers. It was established that Company X customers' personal data have been processed for the direct marketing and discount granting purposes. Company X performs processing of one type of excessive personal data – clients' PIN. With regard to Buyers' loyalty cards, adopted by Company X and general usage rules, item 4.6, the card owner will be informed with his consent about topical novelties, promotions and special offers by e-mails, SMS and post. Company X does not introduce the information to the client about his right to object that his personal data might be processed for the direct marketing purpose.

For these violations a protocol of administrative offences was issued to Company X director. The Court imposed a penalty of 600 Lt to Company X director.

The legislation of the Republic of Lithuania on the personal data protection in the state registers was examined by the PHARE project experts. The conclusion was that the legislation on the state registers concerning the data protection complies with the EU *acquis*, nevertheless the permission for legal persons indicated in Art. 7 paragraph 3 subparagraph 4 Law on Legal Protection of Personal Data is quite extensive. With respect to the number of legal persons which are allowed to use the PIN, this provision leads less to a restriction but rather to an extension of the use of the PIN.

At present, the draft Law on Legal Protection of Personal Data amending the Article 7 is prepared and sent for approximation to other state institutions and non-governmental organisations.

4) Case of disclosure of excessive personal data

State Data Protection Inspectorate carried out investigation relating to activities of Anticorruption Commission under the Parliament of the Republic of Lithuania investigating possible corruption cases of several Members of Parliament; telephone numbers and calling content were made public in the mass media then. In August 2004 Inspectorate received 5 complaints of these citizens, whose data were made public.

Inspectorate, after examination of the complaints, concluded that the Anticorruption Commission under the Parliament of the Republic of Lithuania, acting independently without interference of the Parliament Office of the Republic of Lithuania is data controller, since the criminal case comprising the personal data has been transferred not through the Parliament Office of the Republic of Lithuania. Therefore, the Protocol of Administrative Offences was drawn up to the Chairwoman of Anticorruption Commission who transferred excessive personal data to the media while delivering information about a citizen under suspicion and also protocol of witness interrogatory.

First instance court decided to dismiss an administrative case against the Chairwoman of Anticorruption Commission of the Parliament of the Republic of Lithuania on the ground of absence of the fact of administrative law violation.

After an appeal against decision of the first instance court, the Lithuanian Supreme Administrative Court by its decision acknowledged that the first instance court properly resolved the

issue on the subject being liable for violations indicated in the Protocol of Administrative Offences. According to the Law on Legal Protection of Personal Data of the Republic of Lithuania *"Data controller – a legal or natural person which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes of the processing are determined by laws or other legal acts, the data controller and (or) the procedure for his appointment may be designated by laws and other legal acts. Data processor – a legal or natural person, not employee of the data controller, processing personal data on behalf of the data controller. The data processor and (or) the procedure for its appointment may be designated by laws or other legal acts."* Lithuanian Supreme Administrative Court, regarding the definitions provided by Law on Legal Protection of Personal Data of the Republic of Lithuania, concluded that the Chairwoman of the Anticorruption Commission of the Parliament of the Republic of Lithuania cannot be considered either data processor or data controller because the above-indicated attributes of data controller and data processor do not apply to her and therefore she is not subject to liabilities of breach of norms of Law on Legal Protection of Personal Data of the Republic of Lithuania indicated in the Protocol of Administrative Offences. The Law of the Parliament Anticorruption Commission does not indicate directly implication of obligations prescribed for members of the Anticorruption Commission for processing personal data in the sense of the Law on Legal Protection of Personal Data of the Republic of Lithuania. Administrative penalties can be imposed only for disregard of clearly unambiguously formulated prohibitions.

5) Cases of unsolicited communications

Within the period of August 2004 till December 2005 Inspectorate received 12 complaints concerning unsolicited communications by e-mail. Inspectorate faces certain problems in examination of this kind of complaints, as it is difficult to identify the sender because unsolicited communications are usually sent from the Internet cafe not retaining the information about a sender or other people's data have been used. In four cases Inspectorate could not trace actual offender, as it was impossible to identify the sender; in 1 case – there were not detected violations of Law on Legal Protection of Personal Data of the Republic of Lithuania, 8 protocols of Administrative Offences were drawn up for the enterprises which had been sending electronic mail messages to a citizen without having his prior consent, 1 instruction was given to the enterprise.

Inspectorate received a complaint on unsolicited communications sent from 49 Internet pages and a certain IP number. The complaint indicated that the owner of the 49 Internet pages addresses and the controller is an enterprise operating in the Republic of Lithuania. During the inspection of this enterprise it was detected that the enterprise was provided with another IP number, different from that indicated in the complaint. During the investigation director of the enterprise stated that there are no registered Internet pages on behalf of the enterprise as indicated in the complaint. On the Internet page of the enterprise there are its requisites placed, therefore, on its behalf other persons could register Internet pages. From publicly available Internet data base www.ripe.net it was detected that the IP number, indicated in the complaint belonged to the Russian Federation RTCOMM networks, therefore Inspectorate had no opportunity to detect who actually was the Internet service provider of the indicated Internet pages and the virtual electronic mail server, who might verify whether the enterprise paid for the creation of Internet pages and use of electronic mail server; that is to confirm that this enterprise was engaged in direct marketing activity.

6) Problems of personal data processing for historical purposes

Since 1 January 2005, the Law on Documents and Archives of the Republic of Lithuania came into force and persons carrying out historical research faced the problem of accessibility to documents. In compliance with the Law on Documents and Archives of the Republic of Lithuania, access to the documents of the National Documentary Fund which contain information on a person's private life, as well as to the structured sets of personal data, transferred to the state archives, shall be limited for a period of 50 years after the person's death, and in the event of failure to establish this fact – for a period of 100 years after the creation of the said documents. Consequently, certain problems occurred of how historical research should be interpreted, since the Law on Legal Protection of Personal Data of the Republic of Lithuania does not foresee any specific provisions on the carrying out historical research, although it determines provisions on carrying out scientific research. In accordance with the Law on Legal Protection of Personal Data of the Republic of Lithuania, personal data are processed if persons carrying out scientific research obtain data subject's consent. Without data subject's consent personal data may be processed for the purposes of scientific research only if the State Data Protection Inspectorate, which must carry out a prior checking, has been duly notified. For this issue, there were meetings organized with the representatives of the Department of Archives, historians in order to resolve the pending problems. Presently, recommendations are being prepared on the processing of personal data while conducting historical research and also recommendations on filling the form of notification for prior checking while processing personal data for the purposes of historical research. In addition, the Law on Legal Protection of Personal Data of the Republic of Lithuania will be amended and supplied with separate specific provisions on the processing of personal data for the purposes of historical research.

7) Investigation of the Ministry of Interior

On 11 April 2003 the Chairman of the Sejm Provisional Investigation Commission for legality examination of publicly announced charges by the Minister of Interior to Commissar General of the Police and his suspension and certification referred to Inspectorate, asking to investigate the legality of personal data processing, validity of passwords usage and data security in the databases of the Ministry of Interior (hereinafter referred to as MI) and the Police Department. After examination in MI and its Informatics and Communications Department, it was set that in the database "Residents" personal data were stored without a legal processing aim. In addition, search engine was created which allowed without legal basis, to join, group personal data, relating them to a person's relatives, neighbours, means of transport. Personal data were given (giving possibility to connect to databases) to data receivers without personal data contracts and without setting the aim of data usage. Data subject was not informed about processing his personal data. Data protection organizational means were improperly implemented. MI was given an order to make a plan of the offences, indicated in the inspection report, removal within 1 month and coordinate it with Inspectorate. This plan is coordinated with Inspectorate and confirmed, however, its implementation is delayed.

After examination offences were not set in the Police Department. It is stated in examination conclusions that the Police Department collects, stores, processes and

uses information in special central purpose systems on operative activity purpose. The Police Department is not directly assigned to control if officers purposefully and legally use MI central database, and according to the Order No. 343 "On checking and checkout order of central data bank users of the Ministry of Interior" of the Minister of Interior of 5 May 1999, the heads of Police Commissariats and heads of MI and its structural divisions are responsible for legality and purposefulness of central database usage by police officers.

In the same year the Inspectorate carried out a direct inspection on the lawfulness of the data processing in the Social Insurance Fund Board (hereinafter – Institution). The inspection established that this institution daily transferred personal data of all persons of the Republic of Lithuania, who had social insurance (except those, who had military rank) to the law enforcement institutions, which carried out operational activities. Personal data of the above-mentioned persons are being transferred in the "Oracle materialized view" or "Oracle snapshot" way by transferring partial copy of the data base. "Partial" means that not all elements of personal data being kept in the data base are transferred. The law enforcement institutions receive the list of all persons (except those, who have military rank), who are in the data base of this Institution, even those persons who, at that moment, are not objects of the operational activities, but not all elements of their personal data.

III. INITIATIVES OF THE STATE DATA PROTECTION INSPECTORATE

The State Data Protection Inspectorate has taken new initiatives to assist individuals with protecting their privacy or otherwise manage their personal information.

The Inspectorate initiates different measures for raising the level of data subjects' awareness of their rights and realisation of those rights is not sufficient. The representatives of the Inspectorate take part in the public discussions in the TV, radio programmes on data protection issues, write articles in the daily newspapers and magazines. Also the informational poster "Be interested", familiarizing people with their right to data protection was issued and 100 posters were posted up in different cities at the bus stations cases. The educational documentary film "Right to Know" on data protection was created and demonstrated on national television, in order to make more people familiar with data protection and data subjects' rights. Also the school pupils' essays competition on data protection matters was organised. The Inspectorate received a number of essays from the schools from different parts of Lithuania. The best works were awarded.

The conference "E-commerce and data protection". Currently, handling the issues pertaining to the information society development in Lithuania, the greater significance acquires the protection of personal data. The Internet and the opportunities offered by it involves more and more public activity spheres, increasing the scope of personal data collected and processed on the Internet. The person in electronic space tends to be especially perceptible, thus his personal data might be more vulnerable.

With the rapid changes of information technologies, the problem arises – how to facilitate favourable conditions for electronic business development and ensure also

the right to inviolability of one's private life. The means and ways to achieve such compatibility, to strengthen the confidence in data controllers by society, to create secure space of the Internet and tackle the threats, which appear due to the fast penetration of modern technologies into the operations of data processing were considered at the conference "E-commerce and data protection", which took the place on 14-15 November, 2005 in Vilnius. Other issues covered during the conference were: e-commerce and privacy policy, direct marketing and data protection, organization of data protection within the company, good practice of processing personal data within the international companies, identification on the Internet, fight against spam, cybercrime, e-banking and fraud.

Europol seminar. On 29 October 2004 the State Data Protection Inspectorate in an attempt to effectively implement the requirements set up by the Europol Convention and ensure that the personal data are processed legitimately, together with the Europol Joint Supervisory Authority organised a workshop on personal data processing supervision in compliance with the Europol Convention. The congratulatory speech was delivered by presiding at the workshop the Minister of Interior V. Bulovas. At the workshop the reports were presented by the leader of Europol Joint Supervisory Body on data protection secretariat, by Vice-president of Data Protection Body of the Netherlands, by Deputy President of Data Protection Body of Spain, by Deputy Commissioner for Information of the United Kingdom, by Supervisor of Europol Data Protection of Hungary, by the Chief of the Lithuanian National Department of Europol and by the Director of the State Data Protection Inspectorate. During the seminar the experiences were shared on fulfilling the duties of this highly responsible and not easy work. At the seminar the representatives of various law enforcement bodies were present.

PHARE project. The State Data Protection Inspectorate together with the Ludvig Boltzman Institute of Human Rights (Austria) from 29 March 2004 till the end of June 2005 carried out the PHARE program twinning project LT02/IB-JH-02/03 "Strengthening administrative and technical capacity of personal data protection" (hereinafter – Project).

On 30 June 2005 the PHARE project was accomplished. According to this project specialists from the Inspectorate had traineeships in Independent Centre for Privacy Protection in Schleswig-Holstein land and Data Protection Commissioner's Office in Bonn, in Germany, also Bureau of Data Protection Commission in Vienna, Austria. During the time of traineeships the specialists from the Inspectorate got to know about the procedures of executable inspections and of handling complaints, participated in the inspections on the spot. It is also worth mentioning that according to PHARE programme twinning project, Commentary to Law on Legal Protection of Personal Data of the Republic of Lithuania has been prepared, which will be very helpful in understanding the provisions of Law on Legal Protection of Personal Data of the Republic of Lithuania both to the data subject and to the data controller: state and municipal institutions and enterprises (for example, it will be helpful especially for judges in their activity in order to fairly interpret and apply the provisions of Law on Legal Protection of Personal Data of the Republic of Lithuania), for private institutions (enterprises).

Ochrona danych osobowych w Republice Litwy

I. USTAWODAWSTWO

Podstawy ochrony danych osobowych zostały ustanowione w Konstytucji Litwy w 1992 r. oraz w ustawie o ochronie danych osobowych z 1996 r. Artykuł 22 Konstytucji Republiki Litewskiej stanowi, co następuje:

„Życie prywatne jednostek powinno być nienaruszalne. Korespondencja osobista, rozmowy telefoniczne, wiadomości telegraficzne i inne sposoby porozumiewania się powinny być nietykalne. Informacje dotyczące życia prywatnego jednostek mogą być zbierane tylko po uzyskaniu uzasadnionego nakazu sądowego i zgodnie z prawem. Prawo i sądy chronią jednostki przed arbitralną i niezgodną z prawem ingerencją w ich życie prywatne lub rodzinne, jak również przed naruszeniem ich honoru i godności.”

W roku 2003 przyjęto nową wersję litewskiej ustawy o ochronie danych osobowych. Weszła ona w życie 1 lipca 2003 r. Ustawę przyjęto, aby dostosować litewskie rozwiązania prawne do *aquis communautaire* Unii Europejskiej. Oprócz tego nowa wersja ustawy wprowadza warunki przetwarzania danych osobowych dla celów oceny wypłacalności osób fizycznych oraz zarządzania ich długami, jak również definiuje sytuacje, w których Państwowy Inspektorat Danych Osobowych powinien przeprowadzić procedurę uprzedniej weryfikacji. Ustawa jest dostępna w języku angielskim na stronie www.ada.lt.

Niedawna nowelizacja ustawy (przyjętej przez Sejm 13 kwietnia 2004 r.) dotycząca uprzedniej weryfikacji weszła w życie 24 kwietnia 2004 r. Ustawa ogranicza konieczność uprzedniej weryfikacji do sytuacji, w których ma miejsce automatyczne przetwarzanie „wrażliwych” danych osobowych dla wewnętrznych celów administracyjnych lub w przypadkach określonych w artykule 10 i ustępach 2(6) i (7) artykułu 5 ustawy; kiedy administrator danych zamierza przetwarzać automatycznie pliki z danymi dostępnymi publicznie, chyba że regulacje prawne określają procedurę ujawniania tych danych.

Ustawa o komunikacji elektronicznej, dokonująca transpozycji Dyrektywy 2002/58/WE do prawa narodowego, została przyjęta 15 kwietnia 2004 r. i weszła w życie 1 maja 2004 r.

Uzupełnienia kodeksu administracyjnego przewidujące odpowiedzialność administracyjną za niezgodne z prawem przetwarzanie danych osobowych i naruszenie ochrony prywatności w ramach komunikacji elektronicznej, zostały przyjęte 22 kwietnia 2004 r. W kodeksie administracyjnym określa się wysokości kar pieniężnych za naruszenia ustawy o ochronie danych osobowych.

Nowa wersja kodeksu karnego, która weszła w życie 1 maja 2003 r., wprowadza odpowiedzialność karną za sprzeczne z prawem zbieranie informacji o życiu prywatnym osób fizycznych oraz ujawnianie i wykorzystywanie tego typu informacji. Przewidywane kary to: praca społeczna, grzywna, areszt bądź pozbawienie wolności do lat trzech. Odpowiedzialność karna obejmuje również osoby prawne.

W lutym 2000 r. Litwa podpisała, a w 2001 ratyfikowała „Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych” (ETS nr 108). Dnia 8

listopada 2001 r. Litwa podpisała, a 18 grudnia 2003 r. ratyfikowała Protokół Dodatkowy do „Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych”, dotyczący organów nadzorczych i transgranicznych przepływów danych.

Dnia 23 czerwca 2003 r. Litwa podpisała „Konwencję Rady Europy o przestępstwach elektronicznych”.

W dniu 8 marca 2004 r. parlament Republiki Litewskiej ratyfikował Konwencję przygotowaną na podstawie artykułu K.3 „Traktatu o Unii Europejskiej”, dotyczącą wykorzystywania technologii informatycznych dla potrzeb celnych. Dnia 15 lipca 2004 r. rząd Republiki Litewskiej wyznaczył Inspektorat jako instytucję odpowiedzialną za niezależny nadzór nad danymi osobowymi wprowadzanymi do Celnego Systemu Informatycznego i gwarantującą, że przetwarzanie i wykorzystywanie danych osobowych przechowywanych w Celnym Systemie Informatycznym nie narusza praw osób, których dane te dotyczą.

Dnia 22 kwietnia 2004 r. Parlament Republiki Litewskiej ratyfikował Konwencję przygotowaną na podstawie artykułu K.3 „Traktatu o Unii Europejskiej”, dotyczącą ustanowienia biura Europolu („Konwencja o Europolu”). W dniu 28 czerwca 2004 r. rząd Republiki Litewskiej wyznaczył Inspektoratowi zadanie niezależnej kontroli dopuszczalności wprowadzania i ekstrakcji danych osobowych oraz przekazywania ich do Europolu przez Republikę Litewską oraz wyjaśnienia czy takie działania nie naruszają praw osób, których dotyczą dane.

W dniu 20 maja 2003 r. Decyzją Rządu nr 624 Państwowemu Inspektoratowi Ochrony Danych Osobowych przydzielono zadanie niezależnej kontroli dopuszczalności przetwarzania danych osobowych w krajowym systemie informacyjnym Schengen.

II. PROBLEMY ZWIĄZANE Z OCHRONĄ DANYCH OSOBOWYCH

1) Sprzedaż alkoholu i tytoniu

Na początku maja 2004 r. doradca Prezydenta *ad interim* Republiki Litewskiej zwrócił się do Inspektoratu z prośbą o sprawdzenie, czy największe supermarkety nie naruszają ustawy o ochronie danych osobowych, kiedy żądają dokumentu tożsamości i wprowadzają do pamięci kas pierwsze siedem cyfr numeru identyfikacyjnego („PESEL”) klientów.

Zgodnie z ustawą o kontroli sprzedaży alkoholu, która weszła w życie 1 maja 2004 r., sprzedaż napojów alkoholowych osobom poniżej 18 roku życia jest zakazana. Osoby sprzedające napoje alkoholowe mają prawo, a jeśli istnieje podejrzenie, że nabywca ma mniej niż 18 lat, także obowiązek zażądać, aby osoba kupująca wyroby alkoholowe okazała dokument potwierdzający jej wiek. Jeśli nabywca nie okaże dokumentu potwierdzającego wiek, sprzedawca wyrobów alkoholowych musi odmówić sprzedaży. Ustawa o kontroli sprzedaży tytoniu zawiera takie same postanowienia dotyczące tytoniu.

Supermarkety chcąc zagwarantować, że produkty alkoholowe i tytoniowe nie będą sprzedawane nieletnim, zaczęły żądać dokumentów tożsamości od wszystkich obywateli.

W maju 2004 r. Inspektorat przeprowadził kontrolę, w zakresie wyjaśnienia czy podczas sprzedaży napojów alkoholowych i produktów tytoniowych nie zostały naruszo-

ne postanowienia ustawy o ochronie danych osobowych. Nie stwierdzono naruszeń, ponieważ supermarkety nie przetwarzały danych osobowych, a jeden z supermarketów używał pierwszych cyfr numeru identyfikacji osobistej tylko w jednym celu: aby ustalić wiek kupującego i na podstawie numerów niemożliwe było bezpośrednie ani pośrednie zidentyfikowanie danej osoby.

2) Sprawa Specjalnego Biura Śledczego

Na początku 2004 r. parlamentarna komisja bezpieczeństwa narodowego i obrony poinformowała Inspektorat o możliwych naruszeniach ustawy o ochronie danych osobowych w Specjalnym Biurze Śledczym.

Ustawa o zapobieganiu korupcji ustanawia ograniczenia dotyczące gromadzenia i wykorzystywania informacji o osobie ubiegającej się o stanowisko w administracji państwowej czy samorządowej lub piastującej takie stanowisko. Decyzja o wystąpieniu z wnioskiem do Specjalnego Biura Śledczego o dostarczenie informacji o takiej osobie należy do szefa danego organu lub polityka, który zamierza ją nominować lub właśnie nominował.

Podczas kontroli stwierdzono, że dane osobowe dostarczano osobom, które nie miały prawa otrzymywać tego typu informacji, stwierdzono również inne naruszenia zasad przetwarzania danych osobowych: Specjalne Biuro Śledcze przetwarzało „dane wrażliwe” bez przeprowadzenia uprzedniej weryfikacji, zbierało w sposób niezgodny z prawem informacje w niektórych instytucjach i nie informowało Inspektoratu o przypadkach automatycznego przetwarzania danych osobowych. Inspektorat polecił Specjalnemu Biuru Śledczemu zaprzestać ujawnionych praktyk w określonym terminie. Specjalne Biuro Śledcze odwołało się od decyzji Inspektoratu do sądu. Główna kwestia sporna wiązała się ze stosowaniem ustawy, szczególnie w kwestii przetwarzania uporządkowanych systemów kartotekowych metodami nieautomatycznymi. Specjalne Biuro Śledcze kwestionowało prawo Inspektoratu ustanowione w artykule 32 punkt 1 podpunkt 5 ustawy o ochronie danych osobowych do udzielania zaleceń i wydawania instrukcji administratorom danych w kwestii przetwarzania danych osobowych i ich ochrony, ponieważ Biuro nie jest administratorem danych. Sąd odrzucił ten argument, stwierdzając że administrator danych to osoba prawna bądź fizyczna, która samodzielnie lub wraz z innymi osobami decyduje o sposobie i celu przetwarzania danych osobowych. Jeżeli cele przetwarzania danych osobowych są ustalone ustawowo lub na mocy innych aktów prawnych, administratorzy danych i/lub procedury ich wyznaczania mogą być również definiowane ustawowo lub na mocy innych aktów prawnych. Przetwarzanie danych osobowych to każda operacja, której dokonuje się na danych osobowych, jak np. zbieranie, rejestrowanie, gromadzenie, przechowywanie, klasyfikowanie, grupowanie, łączenie, dokonywanie zmian (uzupełnianie lub korygowanie), ujawnianie, udostępnianie, wykorzystywanie, operacje logiczne i/lub arytmetyczne, przeszukiwanie, rozpowszechnianie, usuwanie i inne operacje lub zestawy operacji. Sąd orzekł, że Biuro wykonując swoje zadanie przeciwdziałania korupcji i przetwarzając dane osobowe stało się administratorem danych. Biuro argumentowało, że ustawa o ochronie danych osobowych nie ma zastosowania do działalności Biura, ponieważ artykuł 1 punkt 5 ustawy stanowi, że kiedy dane osobowe są przetwarzane w celach związanych z bezpieczeństwem lub obronnością państwa, ustawa będzie właściwa tylko wówczas, jeśli inna ustawa nie stanowi inaczej. Sąd odrzucił ten pogląd uzasadniając, że twierdzeniu o niestosowaniu się ustawy o ochronie danych osobowych brak jest podstaw. Jedyny

bezwzględny wyjątek wprowadzony w ustawie o ochronie danych osobowych to zapis, że Inspektorat nie będzie miał prawa monitorować przetwarzania danych osobowych w sądach.

3) Wykorzystywanie osobistych numerów identyfikacyjnych

Osobisty numer identyfikacyjny to unikalna sekwencja cyfr przypisana w celu identyfikacji osób fizycznych, zbierania o nich danych i zapewnienia kompatybilności rejestrów państwowych i systemów informatycznych. Przypisany osobisty numer identyfikacyjny jest unikalny i niezmienny. Administratorzy danych często zbierają osobiste numery identyfikacyjne osób nie w celu ich identyfikacji, ale żeby zachować te dane, chociaż nie są one wykorzystywane w żadnych innych celach, niż te dla których były zbierane.

Inspektorat otrzymuje coraz więcej zawiadomień od osób o zbieraniu ich osobistych numerów identyfikacyjnych na potrzeby kart zniżkowych i lojalnościowych sklepów i aptek. Po zbadaniu tych skarg Inspektorat ustalił, że administratorzy danych przetwarzają dane wykraczające poza konieczny zakres – chodziło o osobiste numery identyfikacyjne – i sporządził protokoły wykroczeń administracyjnych, które są obecnie badane przez sądy.

23 lipca 2004 r. Przewodniczący Parlamentu Republiki Litewskiej zorganizował dyskusję przy okrągłym stole o wykorzystywaniu osobistych numerów identyfikacyjnych, w której uczestniczył Dyrektor Państwowego Inspektoratu Ochrony Danych Osobowych. W trakcie obrad rozważano raport „*Przestrzeganie praw człowieka na Litwie*” przygotowany w 2004 r. przez Human Monitoring Institute, który zwracał uwagę na nadmierne wykorzystywanie osobistych numerów identyfikacyjnych na Litwie. Instytut stwierdził, że na Litwie obowiązuje około 560 aktów prawnych (wliczając w to nowelizacje i uzupełnienia) regulujących wykorzystanie osobistych numerów identyfikacyjnych. Uczestnicy debaty zgodzili się jednomyślnie, że należy poddać rewizji podstawy prawne wykorzystania numerów identyfikacyjnych, a także, że powinno się szerzej informować opinię publiczną, tak aby obywatele sami byli świadomi swojego prawa do udzielania zgody lub sprzeciwiania się przetwarzaniu swoich numerów identyfikacyjnych lub innych danych.

Także w roku 2004 Inspektorat przyjął skargę kwestionującą zgodność z prawem przetwarzania danych osobowych w pewnej spółce akcyjnej (zwanej dalej firmą X). Skarżący twierdził, że firma X domaga się podania osobistego numeru identyfikacyjnego od osób, którym oferuje kartę lojalnościową.

Podczas dochodzenia stwierdzono, że firma X dając do wypełnienia czysty formularz karty lojalnościowej (zwany dalej Formularzem) domagała się podania następujących danych: nazwiska, imienia, osobistego numeru identyfikacyjnego, płci, miejsca zamieszkania, numeru telefonicznego, adresu poczty elektronicznej. Firma X przetwarza osobiste numery identyfikacyjne klientów, mimo że numer ten nie jest wykorzystywany w żadnym konkretnym celu, nie jest niezbędny do dokonywania płatności podatków ani do innych celów. Ustalono, że celem przetwarzania danych wpisywanych w Formularzu było obliczenie ilości punktów, które mogą uzyskać osoby dokonujące płatności (przeprowadzające transakcje) za pomocą kart lojalnościowych w sieci sklepów zarządzanych przez firmę X oraz rozsyłanie właścicielom kart informacji o akcjach marketingowych i promocjach organizowanych w centrach handlowych. W punkcie 4.3 ogólnych zasad wykorzystania karty znajduje się jednak zapis, że właściciel karty firmy X używający karty po raz pierwszy i płacący za zakupy w sklepach firmy X, otrzyma

zniżkę w wysokości 10% całej wartości zakupu. Dlatego celem przetwarzania danych wpisywanych w Formularzu było nie tylko obliczanie ilości zdobytych punktów i wysyłanie do właściciela karty informacji związanych z promocjami, ale także przyznawanie nagród lojalnym klientom firmy X. Ustalono, że dane osobowe klientów firmy X były przetwarzane dla celów marketingu bezpośredniego i udzielania zniżek. Firma X przetwarza jeden typ danych osobowych wykraczający poza konieczny zakres i są to osobiste numery identyfikacyjne klientów.

Jeżeli chodzi o karty lojalnościowe klientów, zgodnie z zasadami przyjętymi przez firmę X i z ogólnymi zasadami wykorzystania kart (punkt 4.6), właściciel karty będzie za swoją zgodą informowany o nowościach, promocjach i specjalnych ofertach e-mailem, SMS-em i pocztą. Firma X nie informuje klienta o tym, że ma on prawo do sprzeciwienia się wykorzystaniu swoich danych osobowych do celów marketingu bezpośredniego.

W związku z powyższymi naruszeniami przygotowano protokół wykroczeń administracyjnych obciążający dyrektora firmy X. Sąd nałożył na niego karę 600 litów.

Ustawodawstwo Republiki Litewskiej o ochronie danych osobowych znajdujących się w państwowych rejestrach danych zostało przeanalizowane przez ekspertów projektu PHARE. W wyniku tego badania stwierdzono, że akty prawne dotyczące państwowych rejestrów są zgodne z *aquis communautaire* Unii Europejskiej w zakresie ochrony danych osobowych, jednak pozwolenia dla osób fizycznych wskazanych w artykule 7 punkt 3 podpunkt 4 ustawy o ochronie danych osobowych mają zbyt szeroki zakres. Jeżeli chodzi o liczbę osób prawnych, którym wolno wykorzystywać osobiste numery identyfikacyjne, zapis ten prowadzi nie tyle do ograniczenia, ile do rozszerzenia wykorzystywania osobistego numeru identyfikacyjnego. W chwili obecnej przygotowywany jest projekt ustawy o ochronie danych osobowych zmieniający artykuł 7, który został rozesłany do innych instytucji państwowych i organizacji pozarządowych w ramach procedury konsultacyjnej.

4) Ujawnianie danych osobowych wykraczających poza konieczny zakres

Państwowy Inspektorat Ochrony Danych Osobowych przeprowadził śledztwo dotyczące działalności komisji antykorupcyjnej Parlamentu Republiki Litewskiej badającej domniemane przypadki korupcji kilku członków Parlamentu. W trakcie tej sprawy media ujawniły numery telefonów i treść rozmów telefonicznych. W sierpniu 2004 r. Inspektorat otrzymał pięć skarg obywateli, których dane zostały upublicznione.

Po przebadaniu tych skarg Inspektorat stwierdził, że komisja antykorupcyjna Parlamentu Republiki Litewskiej, która działa niezależnie i bez jakiegokolwiek ingerencji Kancelarii Parlamentu, jest administratorem danych, ponieważ sprawa kryminalna (w tym akta zawierające dane osobowe) została jej przekazana bez pośrednictwa Kancelarii Parlamentu Republiki Litewskiej. Z tego względu sporządzono protokół wykroczenia administracyjnego obciążający Przewodniczącą Komisji Antykorupcyjnej, która przekazała mediom dane osobowe wykraczające poza konieczny zakres związany ze sprawą, dostarczając im informacji o podejrzanym oraz protokół przesłuchania świadka.

Sąd pierwszej instancji zdecydował o odrzuceniu sprawy administracyjnej przeciwko Przewodniczącej Komisji Antykorupcyjnej Parlamentu Republiki Litewskiej z powodu bezzasadności skargi o naruszenie prawa administracyjnego.

Po apelacji od decyzji sądu pierwszej instancji litewski Najwyższy Sąd Administracyjny podtrzymał decyzję sądu pierwszej instancji o bezzasadności zarzutów przeciwko pozwanej na podstawie protokołu wykroczeń administracyjnych. Zgodnie z litewską ustawą o ochronie danych osobowych „Administrator danych to osoba prawna lub fizyczna, która samodzielnie lub wraz z innymi osobami decyduje o sposobie i celu przetwarzania danych osobowych. Jeżeli cele przetwarzania danych osobowych są ustalone ustawowo lub na mocy innych aktów prawnych, administratorzy danych i/lub procedury ich wyznaczania mogą być również ustalane ustawowo lub na mocy innych aktów prawnych. Osoba przetwarzająca dane jest to osoba prawna lub fizyczna, ale nie pracownik administratora danych, przetwarzający dane osobowe w imieniu administratora danych. Osoba przetwarzająca dane i (lub) procedura jej wyznaczania mogą być ustalone ustawowo lub na mocy innych aktów prawnych.” Najwyższy Sąd Administracyjny, biorąc pod uwagę definicje zawartą w litewskiej ustawie o ochronie danych osobowych, orzekł, że Przewodnicząca Komisji Antykorupcyjnej Parlamentu Republiki Litewskiej nie może być uznana ani za osobę przetwarzającą dane, ani za administratora danych, ponieważ nie odpowiada przedstawionym powyżej cechom charakterystycznym osoby przetwarzającej dane ani administratora danych i dlatego też nie może być pociągnięta do odpowiedzialności za złamanie przepisów ustawy o ochronie danych osobowych zgodnie z zarzutami sformułowanymi w protokole wykroczeń administracyjnych. Ustawa o parlamentarnej komisji antykorupcyjnej nie określa bezpośrednio implikacji dotyczących przetwarzania danych osobowych w rozumieniu ustawy o ochronie danych osobowych, które wiążą się z obowiązkami powierzonymi członkom komisji antykorupcyjnej. Karę administracyjną można nałożyć jedynie za brak poszanowania jasno i jednoznacznie sformułowanych zakazów.

5) Otrzymywanie niezamawianych wiadomości

W okresie od sierpnia 2004 r. do grudnia 2005 r. Inspektorat przyjął 12 skarg dotyczących otrzymywania pocztą elektroniczną niezamawianych wiadomości (informacji handlowej). Badanie tego typu skarg przez Inspektorat nie jest łatwe, ze względu na trudność w zidentyfikowaniu nadawców. Wiadomości są zwykle rozsyłane z kafejek internetowych, które nie przechowują informacji, kto był nadawcą czy jakie dane innych osób zostały wykorzystane. W czterech przypadkach Inspektorat nie był w stanie dotrzeć do sprawcy wykroczenia, ponieważ niemożliwe było zidentyfikowanie nadawcy. W jednym przypadku nie wykryto naruszenia litewskiej ustawy o ochronie danych osobowych. Sporządzono 8 protokołów wykroczeń administracyjnych przeciwko przedsiębiorstwom, które rozsyłały wiadomości elektroniczne bez uzyskania wcześniejszej zgody odbiorców, jednemu przedsiębiorstwu udzielono pouczenia.

Inspektorat otrzymał skargę na otrzymywanie niezamawianych wiadomości wysłanych z 49 witryn internetowych i jednego adresu IP. W skardze zaznaczono, że właścicielem i administratorem tych 49 adresów witryn internetowych jest przedsiębiorstwo działające w Republice Litewskiej. Podczas kontroli tego przedsiębiorstwa stwierdzono, że otrzymało ono nowy numer IP, inny od wskazanego w skardze. W trakcie dochodzenia dyrektor przedsiębiorstwa zeznał, że witryny internetowe wymienione w skardze nie są zarejestrowane w imieniu przedsiębiorstwa. Na stronie internetowej firmy znajdują się jej dane, dlatego inne osoby mogły zarejestrować stronę internetową w jej imieniu. W publicznie dostępnej internetowej bazie danych www.ripe.net odkryto, że numer IP wymieniony w skardze należy do sieci RTCOMM Federacji Rosyjskiej. Z tego też powodu

Inspektorat nie mógł wykryć, kto jest providerem usług internetowych wskazanych stron internetowych i wirtualnego serwera poczty elektronicznej. Provider ten mógłby sprawdzić, czy to wspomniane wyżej przedsiębiorstwo zapłaciło za utworzenie stron internetowych i wykorzystanie serwera poczty elektronicznej, czyli potwierdzić, że wspomniane przedsiębiorstwo prowadziło działalność w zakresie marketingu bezpośredniego.

6) Problemy związane z przetwarzaniem danych osobowych do badań historycznych

Od dnia 1 stycznia 2005 r. weszła w życie ustawa o dokumentach i archiwach Republiki Litewskiej, w związku z którą osoby prowadzące badania historyczne stanęły wobec problemu dostępu do dokumentów. Zgodnie z ustawą o dokumentach i archiwach Republiki Litewskiej, dostęp do dokumentów Narodowego Funduszu Dokumentacyjnego zawierających informacje o życiu prywatnym osób fizycznych oraz do uporządkowanych zestawów danych osobowych przeniesionych do archiwów państwowych jest ograniczony przez okres 50 lat od śmierci danej osoby, a w przypadku niemożności ustalenia daty śmierci przez okres 100 lat od utworzenia rzeczonych dokumentów. W rezultacie pojawiły się trudności interpretacyjne dotyczące badań historycznych, ponieważ ustawa o ochronie danych osobowych nie zawiera żadnych szczegółowych przepisów w kwestii prowadzenia badań historycznych, chociaż wchodzi w jej skład regulacje dotyczące prowadzenia badań naukowych. Zgodnie z litewską ustawą o ochronie danych osobowych, dane osobowe mogą być przetwarzane, jeżeli osoby prowadzące badanie naukowe otrzymają zgodę osoby, której dotyczy badanie. Bez zgody podmiotu badań jego dane osobowe mogą być przetwarzane na potrzeby badań naukowych jedynie wówczas, gdy Państwowy Inspektorat Ochrony Danych Osobowych (który musi przeprowadzić uprzednią weryfikację) został o tym odpowiednio poinformowany. W związku z tym problemem organizowano spotkania przedstawicieli Departamentu Archiwów i historyków, podczas których rozwiązywano bieżące trudności. Obecnie przygotowywane są zalecenia w sprawie przetwarzania danych osobowych w ramach badań historycznych oraz zalecenia dotyczące wypełniania formularza zawiadomienia w sprawie uprzedniej weryfikacji, poprzedzającej przetwarzanie danych osobowych dla celów badań historycznych. Oprócz tego planuje się nowelizację ustawy o ochronie danych osobowych i jej uzupełnienie o przepisy dotyczące przetwarzania danych osobowych dla potrzeb badań historycznych.

7) Dochodzenie w sprawie Ministerstwa Spraw Wewnętrznych.

Dnia 11 kwietnia 2003 r. Przewodniczący Tymczasowej Komisji Śledczej Sejmu badającej zgodność z prawem publicznego ogłoszenia przez Ministra Spraw Wewnętrznych zarzutów wobec Głównego Komendanta Policji, jego zawieszenia w czynnościach i przeprowadzenia badania poczytalności, wystąpił do Inspektoratu z prośbą o zbadanie prawidłowości przetwarzania danych osobowych, wykorzystania haseł i bezpieczeństwa danych w bazach danych Ministerstwa Spraw Wewnętrznych (zwanego dalej MSW) i Departamentu Policji. W wyniku kontroli przeprowadzonej w MSW i jego departamencie informatyki i komunikacji stwierdzono, że w bazie danych „mieszkańcy” są przechowywane dane osobowe, bez uzasadnionego prawnie celu. Stworzono również wyszukiwarkę umożliwiającą łączenie i grupowanie danych osób, w powiązaniu z danymi ich krewnych, sąsiadów oraz ze środkami transportu. Do stworzenia takiej wyszukiwarki brakowało podstawy prawnej. Dane osobowe są udostępniane (poprzez zapewnienie

możliwości podłączenia się do baz danych) odbiorcom danych bez umów o udostępnianiu danych osobowych i bez określania celu ich wykorzystywania. Osoby, których dane znajdują się w tych bazach danych, nie są informowane o ich przetwarzaniu. Rozwiązania organizacyjne służące ochronie danych osobowych nie są wdrażane we właściwy sposób. MSW otrzymało polecenie przygotowania planu usunięcia stwierdzonych naruszeń, które zostały wskazane w raporcie z dochodzenia, w terminie jednego miesiąca i jego skoordynowania z Inspektorem. Plan ten został uzgodniony z Inspektorem i zatwierdzony, jednak jego wdrożenie opóźnia się.

W wyniku przeprowadzonej kontroli nie stwierdzono wykroczeń w Departamencie Policji. W podsumowaniu raportu z kontroli stwierdzono, że Departament Policji gromadzi, przechowuje i wykorzystuje informacje w ramach centralnych, wyspecjalizowanych systemów dla celów prowadzonej działalności operacyjnej. Departamentowi Policji nie są bezpośrednio przypisane zadania kontroli, jeśli oficerowie używają centralnej bazy danych MSW zgodnie z prawem i w określonym celu a zgodnie z rozporządzeniem Ministra ds. wewnętrznych nr 343 „w sprawie poleceń zalogowywania się i wylogowywania się użytkowników centralnej bazy danych Ministerstwa ds. wewnętrznych” z dnia 5 maja 1999 r. szefowie komisariatów policji oraz szefowie MSW i jego komórek organizacyjnych są odpowiedzialni za zgodność z prawem i celowość wykorzystywania centralnej bazy danych przez pracowników policji.

W tym samym roku Inspektorat przeprowadził bezpośrednią kontrolę zgodności z prawem przetwarzania danych osobowych w Radzie Funduszu Ubezpieczenia Społecznego (zwanej dalej instytucją). W wyniku przeprowadzonej kontroli stwierdzono, że instytucja ta codziennie przekazywała dane osobowe wszystkich obywateli Litwy posiadających ubezpieczenie społeczne (z wyjątkiem osób mających stopień wojskowy) policji i prokuraturze, które przeprowadzały działania operacyjne. Dane osobowe były przekazywane przy wykorzystaniu opcji „Oracle materialized view” lub „Oracle snapshot” przez przesyłanie częściowej kopii bazy danych. „Częściowa” kopia oznacza, że nie przesyłano wszystkich elementów danych osobowych przechowywanych w bazie danych. Prokuratura i policja otrzymują listę wszystkich osób (poza tymi, które mają stopień wojskowy), które są w bazie danych tej instytucji, nawet tych, które w danej chwili nie są przedmiotem działań operacyjnych – nie otrzymują jednak wszystkich elementów ich danych osobowych.

III. INICJATYWY PAŃSTWOWEGO INSPEKTORATU OCHRONY DANYCH OSOBOWYCH

Państwowy Inspektorat Ochrony Danych Osobowych powziął nowe inicjatywy, aby pomóc osobom fizycznym chronić swoją prywatność, czy też w inny sposób zarządzać swoimi danymi osobowymi.

Inspektorat inicjuje szereg działań mających na celu podniesienie poziomu wiedzy osób, których dane są przetwarzane, o przysługujących im prawach i sposobach ich egzekwowania, ponieważ powszechna świadomość w tym zakresie nie jest wystarczająca. Przedstawiciele Inspektoratu biorą udział w publicznych debatach radiowych i telewizyjnych poświęconych zagadnieniom związanym z ochroną danych osobowych, piszą też artykuły do dzienników i tygodników. Przygotowano także plakat informacyjny „Zainteresuj się”, który rozwieszono w 100 egzemplarzach w różnych

miastach na przystankach autobusowych. Miał on zaznajomić Litwinów z prawem do ochrony danych osobowych. W telewizji publicznej wyświetlono edukacyjny film dokumentalny o ochronie danych osobowych „Prawo do informacji”. Został on nakręcony, aby zaznajomić szerszą grupę ludzi z ochroną danych osobowych i prawami osób, których dotyczą dane. Zorganizowano także konkurs wśród uczniów na najlepsze wypracowanie o zagadnieniach związanych z ochroną danych osobowych, które były nadsyłane do Inspektoratu przez szkoły z różnych regionów Litwy. Najlepsze prace zostały nagrodzone.

Konferencja „E-handel a ochrona danych osobowych”. Obecnie w sferze zainteresowań zagadnieniami związanymi z rozwojem społeczeństwa informacyjnego na Litwie nabiera znaczenia ochrona danych osobowych. Internet i oferowane przez niego możliwości wkraczają do coraz liczniejszych dziedzin aktywności publicznej, zwiększając zakres danych osobowych zbieranych i przetwarzanych w Internecie. Osoby w przestrzeni elektronicznej wyjątkowo łatwo jest zauważyć, przez co ich dane osobowe mogą być bardziej narażone na niebezpieczeństwo.

Wraz z szybkimi zmianami w dziedzinie technologii informatycznej pojawia się problem, jak ułatwić tworzenie warunków korzystnych dla rozwoju biznesu elektronicznego, gwarantując jednocześnie prawo do nienaruszalności życia prywatnego ludzi. Środki i metody pozwalające osiągnąć zbieżność pomiędzy tymi celami – umacniające społeczne zaufanie do administratorów i sprzyjające tworzeniu bezpiecznej przestrzeni w Internecie oraz radzeniu sobie z zagrożeniami, które pojawiają się w związku z szybkim przenikaniem nowoczesnych technologii do operacji przetwarzania danych – były przedmiotem konferencji „E-handel i ochrona danych osobowych”, która odbyła się w dniach 14-15 listopada 2005 r. w Wilnie. Do pozostałych zagadnień poruszanych w trakcie konferencji należały e-handel i polityka prywatności, marketing bezpośredni i ochrona danych osobowych, organizacja ochrony danych osobowych w ramach przedsiębiorstwa, dobre praktyki przetwarzania danych osobowych w przedsiębiorstwach międzynarodowych, identyfikacja w Internecie, walka przeciwko spamowi, przestępstwa elektroniczne oraz oszustwa w bankowości elektronicznej.

Seminarium Europolu. W dniu 29 października 2004 r. Państwowy Inspektorat Ochrony Danych Osobowych, w ramach starań o skuteczne wdrażanie wymogów zawartych w „Konwencji o Europolu” oraz zagwarantowanie zgodnego z prawem przetwarzania danych osobowych, zorganizował razem ze Wspólnym Organem Kontrolnym Europolu warsztaty dotyczące nadzoru nad przetwarzaniem danych osobowych zgodnie z „Konwencją o Europolu”. Przemówienie powitalne wygłosił przewodniczący warsztatom Minister spraw wewnętrznych V. Bulovas. W trakcie warsztatów zaprezentowane zostały sprawozdania: Szefa Sekretariatu Wspólnego Organu Kontrolnego Europolu ds. ochrony danych osobowych, Wiceprzewodniczącego Holenderskiego Biura Ochrony Danych Osobowych, Wiceprzewodniczącego Hiszpańskiego Biura Ochrony Danych Osobowych, zastępcy Komisarza ds. Informacji Wielkiej Brytanii, Inspektora Europolu ds. ochrony danych osobowych z Węgier, Szefa Krajowego Departamentu Europolu na Litwie i Dyrektora Państwowego Inspektoratu Ochrony Danych Osobowych. W trakcie seminarium wymieniono poglądy na temat wypełniania obowiązków związanych z tą bardzo odpowiedzialną i niełatwą pracą. Na seminarium byli obecni przedstawiciele różnych organów policji.

Projekt PHARE. Od 29 marca 2004 r. do końca czerwca 2005 Państwowy Inspektorat Danych Osobowych we współpracy z Instytutem Praw Człowieka Ludwiga Boltzmanna (Austria) prowadził bliźniaczy projekt programu PHARE LT02/IB-JH-02/03 „Wzmacnianie kompetencji administracyjnych i technicznych instytucji ds. ochrony danych osobowych” (zwany dalej Projektem).

30 czerwca 2005 r. projekt PHARE został zakończony. W jego ramach specjaliści z Inspektoratu odbyli staże w Niezależnym Centrum Ochrony Sfery Prywatnej w landzie Szlezwik-Holsztyn oraz w Biurze Komisarza Ochrony Danych Osobowych w Bonn (Niemcy), jak również w Biurze Komisji Ochrony Danych Osobowych w Wiedniu (Austria). W trakcie stażów specjaliści z Inspektoratu poznali procedury kontrolne i rozpatrywania skarg oraz uczestniczyli w kontrolach. Warto także wspomnieć, że zgodnie z projektem bliźniaczym programu PHARE przygotowano komentarz do ustawy o ochronie danych osobowych Republiki Litewskiej, który będzie bardzo przydatny do zrozumienia zawartych w niej przepisów, zarówno dla osób, których dane dotyczą, jak i dla administratorów danych: instytucji państwowych i samorządowych (szczególnie w pracy sędziów, pomagając we właściwej interpretacji i stosowaniu przepisów ustawy o ochronie danych osobowych) oraz dla instytucji prywatnych (przedsiębiorstw).

Prof. dr hab. Czesław Martysz

Prezes Samorządowego Kolegium Odwoławczego w Katowicach, Polska
President of the Self-Government Board of Appeal in Katowice, Poland

Informacja publiczna czy chronione dane osobowe.

Już kilkuletni okres obowiązywania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych¹ wyraźnie wskazuje, jak bardzo było potrzebne jej uchwalenie. Świadczy o tym ilość i rodzaj spraw rozstrzyganych przez Generalnego Inspektora Ochrony Danych Osobowych, liczne orzecznictwo sądowe w tych sprawach, a także dość obszerna literatura przedmiotu. Ustawa w tym czasie była też kilkakrotnie nowelizowana, co może potwierdzać tezę, że swą regulacją wyprzedziła ona stan świadomości społecznej.² Jednocześnie nowelizacje te wskazują, że w niektórych jej obszarach ustawa nie zawierała regulacji odpowiadającej potrzebom tzw. społeczeństwa informacyjnego, w którym dobra osobiste podlegają szczególnej ochronie w związku z szerokim stosowaniem automatycznego przetwarzania danych. Stąd konieczność wprowadzania nowych standardów dotyczących warunków dopuszczalności pozyskiwania danych osobowych, zasad administrowania tymi danymi oraz uprawnień osób, których te dane dotyczą.³

Uchwalenie ustawy miało także ujemne konsekwencje. W szczególności poprzez rozszerzające interpretowanie pojęcia „dane osobowe”, utrudnione zostało w sposób znaczący pozyskiwanie niektórych informacji, zwłaszcza dotyczących organizacji i funkcjonowania administracji publicznej. Tak więc pod pozorem ochrony prywatności, czy ochrony danych osobowych ograniczane bywa jedno z podstawowych praw, czyli prawo do informacji o działalności tych organów, a także prawo do informacji o osobach pełniących funkcje publiczne.⁴ Problem ten został nieco złagodzony po wejściu w życie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej,⁵ niemniej praktyka stosowania tych ustaw w dalszym ciągu wskazuje na nieuzasadnione odmawianie dostępu do informacji, które nie podlegają szczególnej ochronie. Wręcz przeciwnie, informacje te stanowią często informację publiczną i podlegają bezwarunkowemu udostępnieniu każdemu, kto o taką informację wystąpi do podmiotu, który ją posiada. Wynika to wprost z treści ustawy o dostępie do informacji publicznej, wedle której prawo dostępu do informacji publicznej, przysługuje każdemu i nie musi on wykazywać w tym względzie swego interesu prawnego lub faktycznego. Ograniczenia tego prawa mogą wynikać wyłącznie z przepisów ustaw szczególnych. Nie ulega wątpliwości, że taką ustawą szczególną jest ustawa o ochronie danych osobowych, stąd bardzo często podmioty zobowiązane do udostępniania informacji publicznych odmawiają ich udostępniania, zasłaniając się niezasadnie potrzebą ochrony danych osobowych.

¹) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. 101, poz. 926 z późn. zm.).

²) I. Lipowicz, Zasady administracyjno-prawnej ochrony danych osobowych, [w:] Przetwarzanie danych osobowych. Red. G. Szpor, Katowice, 1998, s. 1.

³) Prawa osoby w świetle ustawy o ochronie danych osobowych, [w:] Prawne i finansowe aspekty funkcjonowania samorządu terytorialnego, t. I Prawo samorządowe i administracyjne. Red. T. Dolata. Opole 2000, s. 377-388.

⁴) Art. 61 ustawy z dnia 2 kwietnia 1997 r. – Konstytucja Rzeczypospolitej Polskiej, (Dz.U. z 1998r. Nr 78, poz. 483).

⁵) Dz.U. Nr 112, poz. 1198 z późn. zm.

Pojęcie „danych osobowych”, jakim posługuje się ustawa o ochronie danych osobowych, od samego początku jej obowiązywania budziło kontrowersje. Przypomnijmy, że w pierwotnej wersji art. 6 tej ustawy stanowił, że jest to każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby. W literaturze podkreślano, więc że ściśle językowa wykładnia tego przepisu prowadziłaby do absurdu, bowiem sama pojedyncza informacja w zasadzie nigdy (z wyjątkiem np. zdjęcia czy kodu genetycznego) nie pozwala na określenie tożsamości osoby, której dotyczy.⁶ Podobne stanowisko zajął A. Mednis wskazując, że definicja ta została błędnie sformułowana, bowiem „Jeśli ustawa dotyczy tylko takich informacji, które same w sobie pozwalają na identyfikację osoby, to takich informacji jest niewiele”.⁷ Z tego też powodu art. 6 ustawy został w 2001 r. uzupełniony⁸ m. in. o ust. 2 poprzez wskazanie, że „Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne”. Jednocześnie w celu ograniczenia nieuzasadnionego poszerzenia obszaru ochrony, ustawodawca w ust. 3 wprowadził regulację, że „Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań”.

Jak zaznaczyłem wyżej, w praktyce dochodzi niekiedy do swoistego konfliktu pomiędzy przedmiotowym zakresem ochrony, wynikającym z ustawy o ochronie danych osobowych, a przedmiotowym zakresem udostępniania danych stanowiących informację publiczną. Konflikt ten widać szczególnie w tym obszarze funkcjonowania administracji publicznej, który pozwala na dość swobodne i w pełni samodzielne kształtowanie sytuacji prawnej obywateli. Do takiej sfery należy niewątpliwie problematyka zaspokajania potrzeb mieszkaniowych przez organy samorządu gminnego, uregulowana ustawą z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie kodeksu cywilnego.⁹

Wedle art. 4 tej ustawy „1. Tworzenie warunków do zaspokajania potrzeb mieszkaniowych wspólnoty samorządowej należy do zadań własnych gminy. 2. Gmina, na zasadach i w wypadkach przewidzianych w ustawie, zapewnia lokale socjalne i lokale zamienne, a także zaspokaja potrzeby mieszkaniowe gospodarstw domowych o niskich dochodach. 3. Gmina wykonuje zadania, o których mowa w ust. 1 i 2, wykorzystując mieszkaniowy zasób gminy lub w inny sposób.” W celu realizacji tych zadań, gmina może tworzyć i posiadać zasób mieszkaniowy, a także może wynajmować lokale od innych właścicieli i podnajmować je osobom, których gospodarstwa domowe osiągają niski dochód (art. 20 ust. 1 i 2a ustawy). Wreszcie, zgodnie z art. 21 ust. 1 omawianej ustawy rada gminy jest zobowiązana do uchwalenia wieloletniego programu gospodarowania mieszkaniowym zasobem gminy oraz zasad wynajmowania lokali wchodzących w jego skład.

Należy podkreślić, że wieloletni program gospodarowania mieszkaniowym zasobem gminy powinien być opracowany na co najmniej pięć kolejnych lat, a jego treść szcze-

gółowo reguluje art. 21 ust. 2 ustawy. Z kolei wśród zasad wynajmowania lokali wchodzących w skład mieszkaniowego zasobu gminy winny się znaleźć informacje szczególnie ważne nie tylko dla mieszkańców danej wspólnoty samorządowej, ale także dla innych osób, pragnących zamieszkać w danej miejscowości. Zasady te winny zatem określać m.in. wysokość dochodu gospodarstwa domowego uzasadniającą oddanie w najem lub w podnajem lokalu na czas nieoznaczony i lokalu socjalnego, wysokość dochodu gospodarstwa domowego uzasadniającą zastosowanie obniżek czynszu, warunki zamieszkiwania kwalifikujące wnioskodawcę do ich poprawy, kryteria wyboru osób, którym przysługuje pierwszeństwo zawarcia umowy najmu lokalu, a także tryb rozpatrywania i załatwiania wniosków o najem tych lokali, oraz sposób poddania tych spraw kontroli społecznej (podkr. C.M), co wynika z art. 21 ust. 3 pkt 5 tej ustawy. Nie ulega zatem wątpliwości, że zasady wynajmowania lokali z gminnego zasobu mieszkaniowego są aktem prawa miejscowego.¹⁰ Należy także zgodzić się z poglądem, że określone w art. 21 zasady są „zawarte w katalogu otwartym (wyliczenie ma charakter przykładowy), co upoważnia gminy do rozwinięcia i wprowadzenia jeszcze innych dodatkowych warunków, które jednak (...) zawsze podlegają kontroli”.¹¹ Problematyka ta jak widać ma podstawowe znaczenie dla realizacji zasady przejrzystości i jawności działania organów publicznych w szczególności w tych obszarach, które mogą być ze swej istoty narażone na zarzut kumoterstwa, nepotyzmu, stronnictwa, czy wręcz działań noszących znamiona przestępstwa np. łapownictwa. Do takiej sfery niewątpliwie należał i należy nadal najem lokali mieszkalnych, stanowiących mieszkaniowy zasób gminy.

Na tle powyższej regulacji pojawić się zatem może pytanie, czy udostępnienie samego wykazu lokali stanowiących mieszkaniowy zasób gminy, które zostały wynajęte o określonym czasie stanowić będzie informację publiczną, czy też ujawnienie tych informacji doprowadzi do ujawnienia danych osób, którym te lokale zostały wynajęte. Pytanie to nie ma tylko teoretycznego charakteru, bowiem w praktyce często dochodzi do odmowy udostępnienia tych informacji, z powołaniem się na ochronę danych osobowych. W rozstrzygnięciach tych wskazuje się zawsze na możliwość łatwego ustalenia danych osób wynajmujących te lokale. Należy zatem wyrazić pogląd, że informacje te nie podlegają ochronie na podstawie ustawy o ochronie danych osobowych i jako podlegające udostępnieniu, stosuje się do nich ustawę o dostępie do informacji publicznej. W istocie rzeczy nie chodzi tutaj o udostępnienie danych osób, którym zostały te mieszkania wynajęte, ale o sam wykaz (adresy) lokali już wynajętych.

Należy jednak zwrócić uwagę także na inny aspekt tej sprawy. Gdyby bowiem nawet założyć, że spełnienie tak sformułowanego przedmiotu żądania doprowadziłoby do ujawnienia listy osób wynajmujących lokale komunalne, to działanie takie byłoby w pełni legalne, bowiem omawiana tutaj ustawa w art. 21 ust. 3 pkt 5 wyraźnie formułuje tezę, że najem tych lokali podlega kontroli społecznej. W tym stanie rzeczy nawet ujawnienie wykazu osób, z którymi zawarto umowę najmu, nie stanowi naruszenia zasad ochrony ich danych osobowych.

Stanowisko takie prezentuje także na swej stronie internetowej Generalny Inspektor Ochrony Danych Osobowych (GIODO). Jak podkreśla, przywołując stosowne przepisy

⁶) Barta, R. Markiewicz, Ochrona danych osobowych. Komentarz, Zakamycze, 2000, cyt. za LEX/el. 2006.

⁷) A. Mednis, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 1999, s. 21.

⁸) Zob. art. 1 pkt 1 ustawy z dnia 25 sierpnia 2001 r. (Dz.U. Nr 100, poz. 1087) zmieniającej tę ustawę z dniem 3 października 2001 r.

⁹) Dz.U. z 2005r. Nr 31, poz. 266 z późn. zm.

¹⁰) Wyrok NSA z dnia 20 marca 2002 r., II SA/Wr 177/02, (OSS 2002, nr 3, poz. 73).

¹¹) M. Olczyk, Komentarz do ustawy z dnia 17 grudnia 2004 r. o zmianie ustawy o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie kodeksu cywilnego oraz o zmianie niektórych ustaw, LEX/el. 2006.

ustawy o ochronie praw lokatorów, gmina na zasadach i w wypadkach przewidzianych w tej ustawie, „zapewnia lokale socjalne i lokale zamienne, a także zaspokaja potrzeby mieszkaniowe gospodarstw domowych o niskich dochodach (...). Stosownie natomiast do art. 21 ust. 1 pkt 2 powołanej ustawy, rada gminy uchwała zasady wynajmowania lokali wchodzących w skład mieszkaniowego zasobu gminy. Powinny one określać między innymi wysokość dochodu gospodarstwa domowego uzasadniającą oddanie w najem lokalu na czas nieoznaczony i lokalu socjalnego, kryteria wyboru osób, którym przysługuje pierwszeństwo zawarcia takiej umowy, a także tryb rozpatrywania i załatwiania wniosków o najem lokali oraz sposób poddania tych spraw kontroli społecznej (art. 21 ust. 3 pkt 1, 3 i 5 powołanej ustawy). Przepis ten nakłada na gminy obowiązek poddania kontroli społecznej zasad wynajmowania lokali wchodzących w skład mieszkaniowego zasobu gminy. Należy uznać, że formą takiej kontroli jest m.in. ujawnienie danych osobowych takich osób”¹² (podkr. C.M.).

Problem zdaje się więc nie budzić wątpliwości, niemniej można także postawić pytanie, czy udostępnienie wyłącznie danych o wynajętych lokalach, w prosty sposób prowadzić może do ujawnienia danych osób, którym te lokale wynajęto. Należy przypomnieć, że treść art. 6 ustawy o ochronie danych osobowych, nie daje jednoznacznej odpowiedzi na pytanie, czy do tych danych zaliczyć można tylko takie dane, przy których określenie tożsamości jest proste, względnie nie przysparza znacznych trudności, czy też jakiegokolwiek informacje pozwalające na określenie tożsamości osoby. Ale gdyby nawet przyjąć to drugie założenie, ujawnienie takich danych osobowych wiązałoby się z działaniami niewspółmiernymi do kosztów, czasu lub działań podjętych w celu ich uzyskania, o czym mówi art. 6 ust. 3 ustawy o ochronie danych osobowych. Innymi słowy wymagałoby to szczególnych nakładów, przygotowania, wiedzy, kompetencji, jakich nie posiada przeciętny człowiek. Należy zatem zgodzić się z wyrażonym w literaturze poglądem, że „sens wielu przewidzianych tą ustawą instytucji, wielu zawartych w niej przepisów posługujących się określeniem «dane osobowe», bazuje na założeniu, że chodzi tu o informacje, przy których tożsamość osoby zainteresowanej jest podana. Można wszakże twierdzić, iż także informacje, które bez nadzwyczajnego wysiłku, bez nieproporcjonalnie dużych nakładów dają się «powiązać» z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, również zasługują na zaliczenie ich do kategorii danych osobowych, o jakich traktuje analizowana ustawa (...). Natomiast, naszym zdaniem, nie zasługują z pewnością na taką kwalifikację te informacje, których «powiązanie» z oznaczoną osobą nie jest łatwo osiągalne, wymaga nakładów nadzwyczajnych. Pogląd, że nie mają charakteru danych osobowych informacje, przy których ustalenie tożsamości osoby wymaga nieproporcjonalnie dużego nakładu czasu, pracy czy kosztów, wyrażony został również w raporcie wyjaśniającym do Konwencji Strasburskiej oraz w rekomendacjach Komitetu Ministrów Rady Europy...”¹³ Jak z powyższego wynika, także i ta argumentacja pozwala w pełni na ujawnienie wykazu lokali podlegających wynajęciu, jak i wykazu lokali już wynajętych na omawianych tu zasadach.

Bez względu jednak na to, jaki przyjmiemy zakres pojęcia „dane osobowe”, rozstrzygające znaczenie ma tutaj wskazane wyżej, trafne stanowisko GODO, wedle którego nawet dane osób, którym wynajęto mieszkanie komunalne, nie podlegają ochronie na

podstawie ustawy o ochronie danych osobowych. Skoro tak, to tym bardziej nie można zaliczyć do danych osobowych podlegających ochronie informacji o adresach lokali należących do mieszkaniowego zasobu gminy. Zatem dane te jako niepodlegające ochronie stanowią informację publiczną i winny zostać udostępnione.

Na tle omawianej sprawy należy również rozważyć, czy do decyzji odmawiających udostępnienia informacji publicznej wydawanych przez organy I instancji, ma zastosowanie regulacja zawarta w art. 22 ustawy o dostępie do informacji publicznej. Wedle tego przepisu podmiotowi, któremu odmówiono prawa dostępu do informacji publicznej ze względu na wyłączenie jej jawności z powołaniem się m.in. na ochronę danych osobowych, przysługuje prawo wniesienia powództwa do sądu powszechnego o udostępnienie takiej informacji. Podmiot, którego dotyczy wyłączenie informacji publicznej, ma interes prawny w przystąpieniu w charakterze interwenienta ubocznego po stronie pozwanej, a sądem właściwym do orzekania w tych sprawach, jest sąd rejonowy właściwy ze względu na siedzibę podmiotu, który odmówił udostępnienia informacji publicznej. Innymi słowy powstaje pytanie, czy decyzja administracyjna odmawiająca udostępnienia informacji publicznej z powołaniem się na ochronę danych osobowych, winna zawierać pouczenie o przysługującym stronie odwołaniu do organu wyższego stopnia w administracyjnym toku instancji, czy też pouczenie, że w tym przypadku środek zaskarżenia należy skierować do właściwego sądu powszechnego.

Przypomnijmy zatem raz jeszcze, że zgodnie z art. 22 ustawy o dostępie do informacji publicznej, podmiotowi, któremu odmówiono prawa dostępu do informacji publicznej ze względu na wyłączenie jej jawności z powołaniem się m.in. na ochronę danych osobowych, przysługuje prawo wniesienia powództwa do sądu powszechnego o udostępnienie takiej informacji. Przepis ten stanowi uzupełnienie treści art. 21 tej ustawy, w której określona została kognicja sądu administracyjnego do kontroli decyzji administracyjnych w sprawach udostępnienia informacji publicznej. Ustawa wprowadza więc dwa tryby sądowej kontroli tych decyzji: kontrolę sądu administracyjnego i kontrolę sądu powszechnego.

W pierwszej kolejności należy zatem wyjaśnić, o jaką decyzję odmawiającą udostępnienia informacji tutaj chodzi: czy o decyzję organu I instancji, czy też o decyzję organu II instancji, a więc decyzję ostateczną. Gdyby przyjąć założenie, że chodzi o decyzję organu I instancji, to w każdym przypadku odmowy udostępnienia informacji z powołaniem się, na przykład, na ochronę danych osobowych, wyłączona byłaby możliwość kontroli instancyjnej tych decyzji w postępowaniu administracyjnym. Wydaje się, że przyjęcie takiej wykładni art. 22 ustawy, spowodowałoby całkowity paraliż instytucji udostępnienia informacji publicznej, bowiem w każdym takim przypadku dopiero sąd powszechny mógłby zagwarantować obywatelom prawo do uzyskania takich informacji. Można sobie wyobrazić sytuację, w której osoba zainteresowana żąda od organu administracji publicznej określonych informacji, co do których nie ma żadnej wątpliwości, że taką informację publiczną stanowią i spotyka się z nieuzasadnioną odmową ich udostępnienia z powołaniem się na ochronę danych osobowych. Może to być np. żądanie udostępnienia protokołu z sesji rady gminy, której obrady są jawne, a jawność tę gwarantuje zarówno art. 61 Konstytucji, jak i art. 11b ustawy z dnia 8 marca 1990r. o samorządzie gminnym.¹⁴ W przypadku zatem

¹²⁾ http://www.giodo.gov.pl/368/id_art/988/j/pl/

¹³⁾ J. Barta, R. Markiewicz, Ochrona danych osobowych, op.cit.

¹⁴⁾ Dz.U. z 2001 r. Nr 142, poz. 1591 z późn. zm.

odmowy udostępnienia takiej informacji z powołaniem się na ochronę danych osobowych (że np. podczas sesji rozpatrywano skargi konkretnych mieszkańców gminy, którzy nie życzyli sobie ujawniania ich nazwisk), organy odwoławcze nie mogłyby wykonywać kontroli tych decyzji w administracyjnym toku instancji i pozostawałaby wyłącznie droga ochrony przed sądem powszechnym, ze wszystkimi jej konsekwencjami, łącznie z nieznanym bliżej terminem rozstrzygającego wyroku w tej sprawie. Wydaje się zatem, że art. 22 ustawy o dostępie do informacji publicznej dotyczy sądowej kontroli decyzji ostatecznych, w których organ odwoławczy utrzymał w mocy decyzję organu I instancji w sprawie odmowy udostępnienia informacji, z przyczyn zawartych w tym przepisie, a więc np. związanych z ochroną danych osobowych. Należy dodać, że przyjęcie takiego stanowiska będzie rzutować także na właściwość sądu powszechnego w tej sprawie, będzie to bowiem sąd rejonowy właściwy dla siedziby organu odwoławczego, a nie siedziby organu I instancji.

W literaturze zagadnienie to nie doczekało się wyczerpującego wyjaśnienia. Autorzy albo pomijają te kwestie, albo skupiają się na zagadnieniach procesu sądowego.¹⁵ Jedyne S. Szuster podkreśla, że „Uprawnienie do wniesienia powództwa o udostępnienie informacji publicznej przez osobę, której podmiot zobowiązany nie udzielił żądanej informacji, nie będzie konkretyzować się w chwili wydania odmownej decyzji przez podmiot, do którego osoba ta zwróciła się o udostępnienie informacji, ale dopiero w momencie zastosowania przewidzianego w k.p.a. trybu odwoławczego (wniesienia odwołania lub wniosku o ponowne rozpatrzenie sprawy). Przyjęcie takiego stanowiska wynika przede wszystkim z przepisu art. 15 k.p.a., który wprowadza zasadę dwuinstancyjności jurysdykcyjnego postępowania administracyjnego. Rozwiązanie to umożliwia także podmiotowi zainteresowanemu uzyskanie szybszego rozstrzygnięcia ze strony organu (podmiotu) wyższego stopnia”.¹⁶

Pogląd ten należy w pełni podzielić. Oznacza to, że w przypadku wydania decyzji o odmowie udostępnienia informacji publicznej z powołaniem się na ochronę danych osobowych, prawo złożenia powództwa do sądu powszechnego przysługuje stronie wyłącznie wówczas, gdy taką decyzję wyda organ II instancji. Innymi słowy droga do sądu powszechnego jest otwarta dopiero po wydaniu ostatecznej decyzji odmawiającej. Nie tylko wynika to z zasady dwuinstancyjności, która nie została w tym przypadku wyraźnie wyłączona (a jako wyjątek od reguły konstytucyjnej takie wyłączenie musiałoby być jednoznaczne), ale także z łącznego zestawienia treści art. 22 ust. 1 ustawy z treścią art. 16 ustawy o informacji publicznej. Formuła zawarta w art. 22 ust. 1 o treści: „odmówiono prawa dostępu do informacji publicznej”, ze względu na brak jakichkolwiek zastrzeżeń czy wyłączeń, musi być rozumiana jako tożsama z „odmową udostępnienia informacji publicznej” w rozumieniu art. 16 ust. 1 tej ustawy, który zakłada decyzyjną formułę odmowy udostępnienia informacji. Tak więc skoro odmowa ta następuje w formie decyzji, a zgodnie z art. 16 ust. 2 omawianej ustawy, od takiej decyzji służy odwołanie do organu wyższego stopnia na ogólnych zasadach uregulowanych w k.p.a. Zmodyfikowane zostały jedynie terminy jego rozpatrzenia i wymogi procesowe uzasadnienia decyzji. Skoro tak, to wykluczony jest alternatywny sposób zaskarżania takich decyzji w drodze powództwa do sądu powszech-

nego. Droga ta będzie natomiast przysługiwać po wyczerpaniu toku instancji, jako inny (niż skarga do sądu administracyjnego) środek zaskarżenia takiej decyzji. Wskazuje na to także zestawienie treści art. 21 i 22 omawianej ustawy. W pierwszym z nich ustanowiona jest ogólna zasada, że w sprawach skarg na decyzje administracyjne wydawane w postępowaniu o udostępnienie informacji publicznej stosuje się przepisy ustawy z dnia 30 sierpnia 2002 r. – prawo o postępowaniu przed sądami administracyjnymi.¹⁷ Przepis ten stanowi zresztą nawiązanie do art. 3 § 2 pkt 1 tej ostatniej ustawy, która wprowadza generalną zasadę kontroli działalności administracji publicznej przez sądy administracyjne, obejmując orzekanie m. in. w sprawach skarg na decyzje administracyjne. W ustawie o dostępie do informacji publicznej zmieniono tylko termin udzielenia odpowiedzi na skargę i termin przekazania akt sądowi, a także ustanowiono sztywny termin rozpatrzenia takiej skargi przez sąd. Należy przypomnieć także, że – jako zasada – prawo skargi do sądu administracyjnego przysługuje po wyczerpaniu toku instancji, a więc po wyczerpaniu przysługujących stronie środków zaskarżenia.

Natomiast art. 22 ustawy o dostępie do informacji publicznej wprowadza wyjątek od tej zasady. W przypadku, gdy stronie odmówiono udostępnienia informacji publicznej z powołaniem się na ochronę danych osobowych nie przysługuje skarga do sądu administracyjnego, ale powództwo do sądu powszechnego. Jednak jak podniesiono wyżej, środek taki przysługiwałby wyłącznie wówczas, gdy organ II instancji utrzymałby w mocy decyzję odmawiającą udostępnienia informacji publicznej, wydaną przez organ I instancji. We wszystkich zatem przypadkach, w których organy administracji publicznej odmówią udostępnienia informacji publicznej, organem właściwym do rozpoznania środka prawnego od takiej decyzji jest organ administracji publicznej wyższego stopnia, a nie sąd powszechny.¹⁸

Public information or protected personal data

Just the few years of the operation of the Act of August 29, 1997 on the protection of personal data¹ has indicated how needed it was. The number and nature of cases reviewed by the Inspector General for Personal Data Protection, numerous court decisions with regard to that issue, as well as extensive literature on the subject prove the same. During that time the Act has been amended several times, which may support the opinion that the act went ahead of the social awareness.² At the same time, those amendments indicate that some areas of the act did not include provisions that were relevant to the needs of the information

¹⁷⁾ Dz.U. Nr 153, poz. 1270 z późn. zm.

¹⁸⁾ Odmienne: zob. postanowienie Samorządowego Kolegium Odwoławczego we Wrocławiu z dnia 5 lutego 2005 r. (SKO 4541/4/04, OSS 2004, nr 3, poz. 59), gdzie został wyrażony pogląd, że „Jeżeli odmowa udostępnienia informacji publicznej nastąpiła z powołaniem się na ochronę danych osobowych, prawo do prywatności oraz tajemnicę przedsiębiorcy, czyli tajemnicę inną niż państwowa, służbowa, skarbową lub statystyczna, to zostały spełnione przesłanki wniesienia powództwa do sądu powszechnego (...) co wyklucza jednoczesną drogę administracyjną.

¹⁵⁾ Zob. M. Jabłoński, K. Wygoda, Ustawa o dostępie do informacji publicznej. Komentarz, Wrocław 2002, s. 259 – 263, T. R. Aleksandrowicz, Komentarz do ustawy o dostępie do informacji publicznej, Warszawa 2002, s. 166-169, P. Sitniewski, Dostęp do informacji publicznej w jednostkach samorządu terytorialnego, Białystok 2005, s. 243.

¹⁶⁾ Komentarz do art. 22 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, LEX/el. 2003.

¹⁾ The Act of August 29, 1997 on the protection of personal data (Dz.U. (Journal of Laws) of 2002, No. 101, item 926, as amended)

²⁾ I. Lipowicz, Zasady administracyjnoprawnej ochrony danych osobowych (Rules on administrative and legal protection of personal data), [in]: Przetwarzanie danych osobowych (Personal data processing). Editor G. Szpor, Katowice, 1998, page 1.

society, where personal rights are subject to particular protection with regard to the extended application of automatic data processing. Hence the need to introduce new standards on obtaining and managing personal data, and the rights of persons the data pertain to.³

However, passing the act also had some negative effects. In particular, the very broad interpretation of the term "personal data" made it difficult to obtain some information, specifically information on organisation and operations of public administration. Thus under the pretence of protecting the privacy or personal data, one of the basic rights is being restricted, namely the right to information on activities of such institutions, as well as information concerning public officials.⁴ The problem has been mitigated to some extent after the Act of September 6, 2001 on access to public information⁵ came into force, but the practice of application of those acts still shows unjustified denials of access to information which is not covered by special protection. On the contrary, such information often constitutes public information and must be provided unconditionally to anyone requesting it from the entity holding such information. This follows directly from the contents of the Act on access to public information, which states that anyone has the right to access public information and no one needs to prove their legal or actual interest in this regard. Limitation of such right may only result from the provisions of specific legislative acts. There is no doubt that the Act on the protection of personal data constitutes such an act, therefore very often the entities obliged to provide public information refuse to disclose it, unduly declaring the need to protect personal data.

The term "personal data", as used by the Act on the protection of personal data, has been controversial from the very beginning of its operation. It needs to be mentioned that the original version of Article 6 of the said Act sets out that personal data is any information relating to a natural person that allows for identification of such a person. The literature is stressing the fact that strict linguistic interpretation of this provision would reduce it to absurdity, as in principle, a single piece of information (apart from i.e. a photo or genetic code) never allows for identification of a person it relates to.⁶ Mr A. Mednis presented a similar opinion indicating that the term was formulated wrongly, as "If the act relates only to information that in itself allows for identification of a person, then not much of such information exists".⁷ For that reason, in 2001, Article 6 of the Act was supplemented⁸ with, among others, paragraph 2 indicating that „Identifiable person is a person, identity of which may be established indirectly or directly, in particular by referring to an identity number or one or more specific features describing such person's physical, physiological, mental, economic, cultural or social characteristics". At the same time, in order to limit unjustified extension of the scope of protection, in paragraph 3 the lawmaker introduced provision that: "Information is not deemed information allowing identification if this would require significant cost, time or action".

³) Prawa osoby w świetle ustawy o ochronie danych osobowych (Personal rights and the act on protection of personal data), [in:] Prawne i finansowe aspekty funkcjonowania samorządu terytorialnego (Legal and financial aspects of local self-government operations), volume I: Prawo samorządowe i administracyjne (The self-government and administration law). Editor T. Dolata. Opole 2000, pages 377-388.

⁴) Article 61 of the Act of April 2, 1997 – the Constitution of the Republic of Poland (Dz.U. of 1998, No. 78, item 483).

⁵) Dz.U. No. 112, item 1198, as amended.

⁶) Barta, R. Markiewicz, Ochrona danych osobowych. Komentarz (Protection of personal data – Commentary), Zakamycze, 2000, quoted after LEX/el 2006.

⁷) A. Mednis, Ustawa o ochronie danych osobowych. Komentarz (The act on the protection of personal data – Commentary), Warszawa 1999, page 21.

⁸) See: Article 1 point 1 of the Act of August 25, 2001 (Dz.U. No. 100, item 1078) amending the Act of October 3, 2001.

As I mentioned above, in reality we sometimes observe a peculiar conflict between the scope of protection in question arising from the Act on the protection of personal data and the scope of availability in question of public information. The conflict is particularly evident in the area of public administration, which allows for rather free and individual shaping of the citizens' legal situation. Undoubtedly, this area includes problems of the communal self-government providing for housing needs, as regulated by the Act of June 21, 2001 on protection of residents' rights, the commune's housing stock and changes to the Civil Code.⁹

According to Article 4 of this Act "1. The commune's particular duties include providing conditions to fulfil the housing needs of the local community. 2. According to the rules of and in cases provided for in the law, the commune shall provide social housing and replacement housing, and shall address the housing needs of the low-income households. 3. The commune shall carry out the duties mentioned in point 1 and 2 using the local council housing stock or in another manner." In order to perform the duties the commune may establish and possess the housing stock, as well as lease dwellings from other owners and sublease such to the low-income households (Article 20, paragraph 1 and 2a of the Act). Finally, according to Article 21, paragraph 1 of the Act in question, the local council is obliged to develop a long-term management plan for the local housing stock and rules on renting dwellings listed as such.

It should be stressed that long-term management plan for the housing stock should be developed for at least five consecutive years, and the content of such plan is regulated in detail in Article 21, paragraph 2 of the Act in question. On the other hand, the rules on renting dwellings included in the housing stock should contain information of particular importance not only to the local community, but also to those willing to move into specific location. Those rules should therefore specify, among others, household income to qualify for leasing or subleasing of unspecified-period dwellings as well as social dwellings, household income to qualify for reduced rent, living conditions which require improvement, selection and priority criteria for lease agreements, as well as procedures for reviewing and handling applications for such types of dwellings, and procedures for community's control over such matters (underlined by C.M.), which arises from Article 21, paragraph 3, point 5 of the Act. Therefore, there is no doubt that rules on renting apartments from the housing stock constitute the acts of the local law.¹⁰ Also, we have to agree that rules, as specified in Article 21, are "included in an open catalogue (quoting is given as example only), which entitle the commune to expand and introduce additional terms and conditions, but (...) they are always subject to control".¹¹ It is evident that those issues are of key importance for execution of the rule of transparency and openness of public institutions' activities, in particular within those areas where, by their nature, there is a threat of alleged cronyism, nepotism, partiality, or even activities constituting unlawful acts, e.g. bribery. Undoubtedly, renting dwellings from the council's housing stock was, and still is, such an activity.

⁹) Dz.U. of 2005 No. 31, item 266, as amended.

¹⁰) The ruling of the Supreme Administrative Court of March 20, 2002, II SA/Wr 177/02, (OSS 2002, no. 3, item 73).

¹¹) M. Olczyk, Komentarz do ustawy z dnia 17 grudnia 2004 r. o zmianie ustawy o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego oraz o zmianie niektórych ustaw (Commentary to the Act of December 17, 2004 on amendments to the act on protection of tenants, the commune's housing stock, changes to the Civil Code and some other acts), LEX/el. 2006.

In light of the above-mentioned regulation, a question may arise whether publication of the list of dwellings of the local housing stock that were rented out within specific dates constitutes a public information or whether providing such information would bring about disclosure of personal data of those who leased them. This is more than just a theoretical question, as in reality it often happens that a denial of such information is based on personal data protection. Decisions always indicate possibility of easy identification of personal data of those leasing such dwellings. The opinion should be formulated that such information is not subject to protection under the Act on the protection of personal data, but is governed by the Act on access to public information. In fact, the issue is not about providing personal data of those who leased such dwellings, but it is about the very list of dwellings (addresses) which were rented.

Still, another aspect of this issue should be mentioned. Even if we assume that fulfilling the request formulated in that way would lead to disclosure of the list of people leasing the communal dwellings, such activity would be fully legitimate, as the Act, as discussed in this paper, in Article 21 paragraph 3, point 5 expressly sets out that renting such type of dwellings shall be controlled by the local community. In such case disclosure of list of people executing lease contracts will not constitute the breach of the rules on protection of their personal data.

The same opinion is also presented by the Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych, GIODO) on the official website. The GIODO emphasizes, by quoting relevant provisions of the Act on protection of the residents' rights, according to the rules of and in cases provided for in this Act, the commune "shall secure social housing and replacement housing, and shall address the housing needs of the low-income families (...). Then, according to Article 21 paragraph 1 point 2 of the above-mentioned Act, the local council sets out the rules on renting dwellings from the local housing stock. The rules should specify, among others, the household income to qualify for leasing of unspecified-period dwellings and social dwellings, selection and priority criteria for lease agreements, as well as procedures for reviewing and handling applications for such types of dwellings, and procedures for public control over such matters (Article 21, paragraph 3, points 1, 3 and 5 of the Act in question). This provision imposes on the local council the obligation of submitting rules on renting dwellings from the housing stock to the community's control. It should be acknowledged that disclosing personal data of such persons is one of the ways of such control"¹² (underlined by C.M.).

The problem seems to raise no doubt, still the question can be put forward whether providing just the information on space rented might lead directly to disclosure of personal data of the tenants. It should be reminded that the content of Article 6 of the Act on the protection of personal data does not provide explicit answer to whether this data include only such data, where the identification of a person is easy or at least not troublesome, or any information allowing for identification of a person. Even if the latter interpretation is adopted, disclosure of such personal data would require activities incommensurable to the costs, time or actions undertaken in order to obtain such data, as specified in Article 6 paragraph 3 of the Act on the protection of personal data.

In other words, this would require significant resources, preparation, knowledge, and competence not typical of an average person. Therefore, one can only agree with the opinion expressed in the literature that "the meaning of many terms provided for in this Act and of many regulations therein, which utilize the term <personal data>, is based on the assumption that we are talking about information where the identity of the person in question is provided. Nevertheless, one can claim that also the information that could be <associated with> a specific person without extraordinary effort, disproportionately significant resources, particularly by using easily accessible and commonly available sources, also deserve being included in the category of personal data, as regulated by the act under discussion (...). However, in our opinion, such qualification definitely should not be applied to information that cannot be easily <associated> with a given person or which requires extraordinary resources. The opinion that information where identification requires disproportionately significant time, effort or cost, is not of a personal data nature was also expressed in the explanatory report on the Strasbourg Convention and the recommendations of the Committee of Ministers of the Council of Europe...".¹³ As follows from the above, also this reasoning allows for full disclosure of the list of dwellings available for lease, as well as the list of dwellings already rented, on terms and conditions discussed herein.

However, no matter what scope of the "personal data" definition is adopted, the above-mentioned and correct opinion of Inspector General is decisive in this case, and according to this opinion even personal data of those who leased communal dwellings are not subject to protection under the Act on the protection of personal data. If this is the case, then the information on addresses of dwellings listed under the local housing stock is even less eligible as protected personal data. Therefore, such data which are not protected constitute public information and should be provided.

In light of the issue discussed herein, we should also consider whether regulation of Article 22 of the Act on access to public information should apply to decisions denying public information, as issued by the first instance bodies. According to this regulation, an entity that was deprived of the right of access to public information due to exclusion of its disclosure based on, among others, protection of personal data, has the right to submit an action to the courts of justice to demand disclosure of such information. The entity to which the exclusion of public information pertains, has legal interest in entering the case as a secondary intervener on the defendant's side, and the competent court for resolving the case shall be the district court relevant for the seat of the entity which denied the public information. In other words, the question is whether an administrative decision denying public information based on personal data protection should include information on the right to appeal to the institution of higher level in the administrative two-instance procedure or the information that for this matter the case should be submitted to the relevant court of justice.

Once again it should be reminded that according to Article 22 of the Act on access to public information, an entity which was denied access to public information due to exclusion of its disclosure based on, among other things, personal data protection, is entitled to submit the action to the court of justice for disclosure of such information.

This provision supplements the content of Article 21 of the said Act, which sets out the cognizance of the administrative court for control over administrative decisions on providing public information. Therefore, the Act introduces two ways of court control over such decisions: control of the administrative court and the court of justice.

First of all, it should be specified what decision on denial of information is the issue in this case: the decision of the first instance body or the decision of the second instance body, namely the final decision. Assuming that we are talking about the decision of the first instance body, then in each case of denial of the information based on personal data protection the possibility of control under the administrative two-instance proceedings for such decisions would be excluded. It seems that adopting such interpretation of Article 22 of the Act would overpower the bodies providing public information, as in each individual case only a court would be able to guarantee the citizens the right to obtain such information. Is it easy to imagine the situation when a person requires a public administration body to provide specific information, about which there is no doubt as to whether it constitutes public information and faces unjustified denial based on protection of personal data. It might be, for example, a request to disclose the minutes from the council's session; such meetings are open, and the disclosure is guaranteed by both Article 61 of the Constitution, and Article 11b of the Act of March 8, 1990 on the commune self-government.¹⁴ Therefore, in case of denial of the information based on personal data protection (e.g. during the session complaints of individual inhabitants of the commune have been examined, and such inhabitants do not wish their names to be disclosed), the appeal bodies would not be able to carry out control over such decisions under the administrative instance procedures, and the only way of protection would be the submission of the action to the court of justice with all consequences of such, including an indefinite date of the final judgment. Therefore, it seems that Article 22 of the Act on access to public information provides for the court control over final decisions, in which the appeal body sustained the decision of the first instance body to deny the information for reasons provided for in this regulation, including, for example, reasons relating to personal data protection. It should be added that adopting such a view will also influence the jurisdiction over such case, as it will be the district court relevant for the seat of the appeal body, not for the seat of the first instance body.

There is still no exhaustive explanation of this issue in the subject literature. The authors either do not comment on this matter or they focus on the issue of the court procedure.¹⁵ Only S. Szuster emphasizes that "Entitlement of a person that was denied requested information to submit the action on providing public information will not arise upon issuing the denial by an entity to which the person applied for information, but when the appeal procedure, as specified by the code of administrative proceedings, is deployed (submitting an appeal or a motion for reconsidering the matter). Adopting such stance is based mainly on the provision of Article 15 of the code of administrative proceedings, which introduces the rule of two-instance jurisdictional administrative proceedings. This solution also allows the entity in question to obtain prompter decision from the body (entity) of higher instance".¹⁶

¹⁴) Dz.U. of 2001 No. 142, item 1591, as amended.

¹⁵) See: M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji publicznej. Komentarz* (The act on access to the public information – Commentary), Wrocław 2002, pages 259 – 263, T. R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej* (Commentary to the Act on access to the public information), Warszawa 2002, pages 166-169, P. Sitniewski, *Dostęp do informacji publicznej w jednostkach samorządu terytorialnego* (Access to the public information in the local self-government units), Białystok 2005, page 243.

¹⁶) Commentary to Article 22 of the Act of September 6, 2001 on access to public information, LEX/el. 2003

One can only agree with this view. It means that in case the decision is issued denying public information based on personal data protection, the party shall have the right to submit the action to the court of justice only if such decision is issued by the body of second instance. In other words, one can take the legal action no earlier than upon issuance of the final decision on denial. This derives not only from the rule of two-instance proceedings, that was not explicitly excluded for that case (and, as an exception from the constitutional rule, such exclusion would have to be explicit), but also from the joint application of the content of Article 22 paragraph 1 of the Act and Article 16 of the Act on public information. The wording of Article 22 paragraph 1, namely "the right to access public information was denied", as there are no reservations or exceptions, must be understood as identical with "denial of public information" as provided for in article 16 paragraph 1 of this Act, and which assumes the decisive form of denial of public information. Therefore, as the denial is made in form of decision, and according to Article 16 paragraph 2 of the Act in question, such decision may be appealed against to the body of higher instance under general rules provided for in the code of administrative proceedings. Only the dates for examining the denial and procedural requirements for justifying the decisions were modified. In such case an alternative way to appeal against such decisions, in form of a court case in the court of justice, is excluded. This way can be taken after using the two-instance procedure, as the other mean (other than complaint filed with the administrative court) of appealing against such decision. The same is indicated by comparing the content of Article 21 and 22 of the Act in question. The first article sets out the general rule that for complaints against administrative decisions issued under proceedings for providing public information, the regulations of the Act of August 30, 2002 – the law on proceedings before administrative courts shall apply.¹⁷ Nevertheless, this regulation constitutes the reference to Article 3 § 2 point 1 of the latter Act that introduces the general rule of control over public administration carried out by the administrative courts, including, among others, decisions with regard to complaints on administrative decisions. In the Act on access to public information only the due date for reply to the complaint and dates for transferring the case to the court were modified, and the fixed date for resolving such complaint by the court was set out. It should also be reminded that, as a rule, the right of complaint to the administrative court is vested no earlier than after using the two-instance proceeding, therefore after utilizing the means of appeal, as applicable.

However, Article 22 of the Act on access to public information introduces an exemption to that rule. In case when the party was denied public information based on protection of personal data, such party is not entitled to appeal against the decision to the administrative court, but to the court of justice. But, as it was mentioned above, such remedy would be available only when the body of the second instance sustains the decision to deny public information, as issued by the body of the first instance. Therefore, in all cases where the public administrative bodies deny public information, the body competent to examine the legal remedy for such decision is the public administrative body of higher instance, and not the court of justice.¹⁸

¹⁷) Dz.U. No. 153, item 1270, as amended.

¹⁸) Different opinion: See: the decision of the self-government appeal court in Wrocław of February 5, 2005 (SKO 4541/14/04, OSS 2004, no. 3, item 59), where an opinion was stated that "If denial of public information was made based on protection of personal data, the right of privacy and entrepreneur's secret, namely the secret other than the state, official, tax or statistical secret, then the premises for the case being brought before the court of justice (...) have been fulfilled, and such excludes carrying out the administrative proceeding at the same time.

Uznanie nazwiska w świetle konwencji nr 31 Międzynarodowej Komisji Stanu Cywilnego z 2005 r.

Imię i nazwisko to podstawowe dane, za pomocą których dokonuje się identyfikacja osoby fizycznej. Jest ona dokonywana zarówno w sferze stosunków regulowanych prawem prywatnym, jak prawem publicznym. W tej ostatniej sferze coraz częściej konkurują z nazwiskiem innego rodzaju oznaczenia (np. za pomocą kombinacji cyfr). W sferze prawa prywatnego dopuszczalne jest posługiwanie się innym oznaczeniem niż nazwisko, które zgodnie z prawem przysługuje danej osobie (np. pseudonimem). Mimo to nazwisko nadal jeszcze pełni rolę najważniejszego instrumentu identyfikacji osoby. Dlatego problematyka ta, a w szczególności kwestia „kształtu” nazwiska, jest przedmiotem unormowań przewidzianych w przepisach prawa pozytywnego poszczególnych państw. Przepisy te regulują zarówno kwestię „kształtu” nazwiska,¹ jak jego ochrony jako jednego z dóbr osobistych,² a także jego wykorzystania w obrocie prawnym.³

Gdy chodzi o ustalenie, jakie nazwisko nosi osoba przedmiotem regulacji prawnej są dwa kompleksy zagadnień. Pierwszy związany jest z nazwiskiem nabywanym w chwili urodzenia. Unormowanie przewidujące zależność tego nazwiska od nazwiska rodziców (obojga lub jednego) zakłada uprzednie ustalenie stosunku rodzicielstwa. Drugi kompleks zagadnień związany z pytaniem o to, czy nazwisko uzyskane w chwili urodzenia może być następnie zmienione (czyli zastąpione lub uzupełnione innym). Ustawodawca dopuszczający taką możliwość powinien rozstrzygnąć nie tylko, czy zmiana polega na zastąpieniu dotychczasowego nazwiska nowym, czy na połączeniu obu nazwisk powodującym powstanie nazwiska wielocłonowego, ale przede wszystkim określić, w jakiej sytuacji i w jakim trybie zmiana nazwiska może nastąpić. Najczęstszym przykładem sytuacji powodującej zmianę nazwiska jest zmiana stanu cywilnego. Tradycyjne przekonanie, iż nazwisko służy nie tylko identyfikacji osoby, ale i wskazaniu jej przynależności do rodziny, uzasadniało postulat, aby wszyscy członkowie rodziny (małżonkowie i dzieci) nosili takie samo nazwisko. To przekonanie stopniowo przestaje być akceptowane, przede wszystkim gdy chodzi o małżonków. We współczesnych systemach prawnych widoczna jest także tendencja do przechodzenia od rozwiązań zakładających automatyzm zmiany nazwiska jako skutku zmiany stanu cywilnego do rozwiązań, według których czynnikiem decydującym jest wola bezpośrednio zainteresowanej osoby. Odstępuje się też od uregulowań przewidujących przymusową zmianę nazwiska w

drodze aktu władzy publicznej (np. na podstawie przepisów nakazujących eliminację nazwisk o brzmieniu „obcym”, albo upoważniających sąd orzekający rozwód do pozbowienia małżonka winnego nazwiska nabytego wskutek zawarcia małżeństwa).

Nazwisko jest wpisywane w rejestrach stanu cywilnego, a w ślad za nimi – w dokumentach, za pomocą których dokonuje się ustalenia tożsamości osoby. W związku z tym powstają pozornie drobne, ale w praktyce doniosłe i trudne do rozstrzygnięcia problemy związane np. z pisownią nazwiska; nie ograniczają się one tylko do transkrypcji nazwiska zapisanego innym alfabetem.

Dla należytego pełnienia przez nazwisko funkcji identyfikacyjnej jest konieczne, a przynajmniej pożądane, aby ta sama osoba była wszędzie oznaczana tym samym nazwiskiem. Ten idealny stan jest niełatwy do osiągnięcia. Przyczyną jest zarówno rozbieżność regulacji merytorycznych, jak niejednolitość zapatrywań co do wskazania prawa decydującego o nazwisku. Ten ostatni problem należy do dziedziny prawa prywatnego międzynarodowego. Rozwiązaniem, które współcześnie można uznać za dominujące, jest poddanie nazwiska prawu wskazanemu łącznikiem personalnym, w pierwszym rzędzie – prawu państwa, którego obywatelem jest dana osoba.⁴ Coraz mniej popularna jest lansowana niegdyś w doktrynie niemieckiej teza poddająca kształt nazwiska prawu właściwemu dla zdarzenia, z którym łączy się skutek w postaci nabycia (zmiany) nazwiska.⁵ Rzecz jasna – poddanie kwestii nazwiska prawu ojczystemu nie przekreśla wpływu takich zdarzeń na nazwisko, ale tylko poddaje go prawu ojczystemu osoby, o której nazwisko chodzi.⁶ O ile w dawnych kodyfikacjach kwestia prawa właściwego dla nazwiska była przeważnie pomijana,⁷ o tyle ostatnio jest ona przedmiotem coraz bardziej szczegółowych unormowań.⁸

Warto przyjrzeć się próbie uporządkowania tej skomplikowanej i trudnej materii, podjętej niedawno przez Międzynarodową Komisję Stanu Cywilnego (CIEC).⁹ Problematyka nazwiska jest przedmiotem kilku konwencji opracowanych już wcześniej przez tę organizację. Wymienić tu można: konwencję nr 4 dotyczącą zmiany nazwisk i imion, podpisaną w Stambule dnia 4 września 1958 r., konwencję nr 19 o prawie właściwym dla nazwisk i imion, podpisaną w Monachium dnia 5 września 1980 r., a także konwencję nr 14 dotyczącą wpisywania nazwisk i imion w rejestrach stanu cywilnego, podpisaną w Bernie dnia 13 września 1973 r. i konwencję nr 21 dotyczącą wydawania zaświadczenia o noszeniu różnych nazwisk rodowych, podpisaną w Hadze 8 września 1982 r.

⁴ P. Wypych, *Prawo właściwe dla nabycia i zmiany nazwiska*, w: *Prawo rodzinne w Polsce i Europie*, Lublin 2005, s. 563 i n., wcześniej tak samo co do wpływu rozvodu na nazwisko A. Mączyński, *Rozwód w prawie prywatnym międzynarodowym*, Warszawa 1983, s. 109 i n.

⁵ Za tezę tą opowiada się, nie podając uzasadnienia, M. Pazdan, *Prawo prywatne międzynarodowe*, Warszawa 2005, s. 105 (tak samo w wydaniach poprzednich).

⁶ Ocena prawna zdarzenia, które jest przyczyną zmiany nazwiska stanowi tzw. kwestię wstępną, która w tym przypadku powinna być rozstrzygana zgodnie z prawem właściwym na podstawie norm kolizyjnych obowiązujących w państwie ojczystym danej osoby (albo zgodnie z obowiązującymi tam normami regulującymi skuteczność orzeczeń zagranicznych).

⁷ Obowiązująca w Polsce ustawa z dnia 12.XI.1965 r. – Prawo prywatne międzynarodowe, Dz.U. nr 46, poz. 290 ze zm., nie zawiera przepisu mówiącego o nazwisku.

⁸ Zob. np. § 13 austriackiej ustawy o prawie prywatnym międzynarodowym, kilkakrotnie w ostatnich latach zmieniany art. 10 ustawy wprowadzającej niemiecki kodeks cywilny, art. 37-40 szwajcarskiej ustawy związanej o prawie prywatnym międzynarodowym, art. 14 rumuńskiej ustawy o uregulowaniu stosunków prawa prywatnego międzynarodowego, art. 36-39 belgijskiego kodeksu prawa prywatnego międzynarodowego.

⁹ E. Wojnicka, *Międzynarodowa Komisja Stanu Cywilnego. Historia, osiągnięcia oraz znaczenie jej konwencji dla prawa polskiego*, Kwartalnik Prawa Prywatnego 1998, z. 2, s. 269 i n. Polska jest członkiem CIEC od 1998 r., ale przystąpiła jedynie do trzech z przygotowanych przez tę organizację konwencji.

¹ W prawie polskim kwestie te regulowane są w przepisach kodeksu rodzinnego i opiekuńczego (k. r. o.), prawa o aktach stanu cywilnego (pr. a. s. c.), a także ustawy z dnia 15 XI 1956 r. o zmianie imion i nazwisk, Dz.U. z 2005 r. nr 233, poz. 1992.

² W prawie polskim art. 23 i 24 k. c.

³ Np. art. 43⁴, art. 43⁵ § 3 i art. 43⁸ k. c., dotyczące firmy zawierającej nazwisko.

Najnowszą konwencją opracowaną przez CIEC jest konwencja nr 31 o uznawaniu nazwisk, podpisana w tureckim mieście Antalya¹⁰ dnia 16 września 2005 r.¹¹ Autentyczny tekst konwencji został sporządzony w języku francuskim. Konwencja składa się z 17 artykułów,¹² przy czym zasadnicze unormowania wyrażone są w pierwszych ośmiu artykułach. Do konwencji dołączono trzy aneksy, określające wzór informacji o nadaniu nazwiska, sporządzanej na podstawie art. 4 ust. 2. Wraz z konwencją ogłoszono jej urzędowe uzasadnienie (*rapport explicatif*).

Konwencja nr 31 jest otwarta na podpisanie dla państw członkowskich CIEC (art. 11), mogą do niej przystąpić także państwa członkowskie Rady Europy, a za jednogłosem zgodą państw będących członkami CIEC – także inne państwa (art. 12).

Cel, którego realizacji służyć ma ta konwencja, został określony w preambule – jest nim ułatwienie uznania nazwiska nabytego przez urodzenie lub zmienionego w następstwie zawarcia małżeństwa, rozwodu lub z innych przyczyn. Trzeba tu zaznaczyć, że słowo „uznanie” występuje tu w znaczeniu specyficznym, odmiennym niż np. w przepisach o uznaniu orzeczeń zagranicznych. Założeniem regulacji konwencyjnej jest to, że dana osoba w jednym z umawiających się państw uzyskała nazwisko przez urodzenie lub z jakiejś przyczyny zmieniła dotychczasowe nazwisko.¹³ Wprowadzona przez konwencję regulacja zmierza do tego, aby to nabyte lub zmienione nazwisko we wszystkich umawiających się państwach służyło do identyfikacji osoby. Składa się na to ciążący na każdym z umawiających się państw obowiązek pozytywny – uznanie, że dana osoba nosi takie właśnie nazwisko, jakie nadano jej w innym umawiającym się państwie, oraz obowiązek negatywny – polegający na tym, że danej osobie nie przypisuje się innego nazwiska. Konwencja nie wprowadza jednolitej regulacji merytorycznej (nie określa jakie nazwisko uzyskuje się przez urodzenie ani jakie zdarzenia uzasadniają jego zmianę) ani jednolitej regulacji kolizyjnej (nie wskazuje prawa właściwego dla określenia nazwiska). Te kwestie, także po wejściu w życie konwencji, każde umawiające się państwo reguluje samo.

Konwencja określa natomiast przesłanki, od których zależy skuteczność nabycia lub zmiany nazwiska w innych umawiających się państwach. Przesłanki te – mówiąc najogólniej – oparte są na okolicznościach dotyczących osoby, o której nazwisko chodzi, lub zdarzenia, którego skutkiem jest nabycie nazwiska. Innymi słowy, konwencja uzależnia uznanie nazwiska od tego, czy jego nabycie nastąpiło w państwie, z którym dana osoba jest połączona odpowiednio intensywną więzią. Okoliczności świadczące o istnieniu takiej więzi są określone w poszczególnych przepisach konwencji w zróżnicowany sposób. Mają one charakter podmiotowy (obywatelstwo, zwykły pobyt) lub przedmiotowy (urodzenie, wydanie orzeczenia).

Regulacja konwencyjna ma ograniczony zakres, którym nie są objęte wszystkie sytuacje, w których w jednym z umawiających się państw nastąpiło zdarzenie powodujące

uzyskanie lub zmianę nazwiska, nawet gdy chodzi o nazwisko osoby będącej obywatelem innego umawiającego się państwa. Sytuacje nie objęte tym zakresem podlegają regulacji przyjętej w prawie wewnętrznym poszczególnych państw.

Wbrew kolejności, w jakiej ułożono postanowienia konwencji, ich przedstawienie zaczynam od regulacji dotyczącej nabycia nazwiska przez urodzenie. Przypomnieć warto, że art. 7 ust. 1 konwencji o prawach dziecka przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r.¹⁴ nakazuje, aby niezwłocznie po urodzeniu dziecka został sporządzony jego akt urodzenia. Akt taki sporządzany jest w państwie, w którym dziecko urodziło się, a jego istotnym elementem jest nazwisko dziecka.

Art. 4 konwencji nr 31 nakazuje uznanie nazwiska nadanego dziecku w państwie, w którym dziecko urodziło się, jeżeli ma ono obywatelstwo tego państwa. Postanowienie to odnosi się tylko do dzieci mających obywatelstwo dwóch lub więcej państw, a jego praktyczne znaczenie polega przede wszystkim na tym, że każde państwo, którego obywatelstwo ma dane dziecko, uznaje nazwisko nadane w innym państwie, którego to dziecko jest obywatelem, o ile z tym państwem jest ono związane także przez miejsce swego urodzenia. Łącznikiem uzasadniającym zastosowanie omawianej normy są więc dwie okoliczności wskazujące to samo umawiające się państwo, a mianowicie obywatelstwo i miejsce urodzenia, przy czym warunkiem dodatkowym jest posiadanie przez dziecko obywatelstwa kilku państw – niezależnie od tego, czy są nimi tylko umawiające się państwa. Konwencja nie wypowiada się na temat uznania nazwiska dziecka, które urodziło się w umawiającym się państwie ale nie ma ono jego obywatelstwa, ani nazwiska dziecka będącego obywatelem umawiającego się państwa, które urodziło się w innym państwie i nie nabyło jego obywatelstwa.

Wyjątek w stosunku do regulacji przewidzianej w art. 4 ust. 1 konwencji nr 31 wprowadza art. 4 ust. 2. Przewiduje on uznanie nazwiska nadanego dziecku w innym umawiającym się państwie, którego dziecko ma obywatelstwo, zgodnie z wolą jego rodziców (tekst francuski używa zwrotu: *la demande des parents*). Założeniem zastosowania tej normy jest obowiązywanie w tym państwie regulacji dopuszczającej wpływ rodziców na nazwisko ich dziecka.¹⁵ Nazwisko nadane dziecku zgodnie z wolą jego rodziców jest uznawane w innych umawiających się państwach, łącznie z tym, w którym dziecko urodziło się. Gwarancją realności tej normy jest postanowienie przewidujące dostarczenie urzędnikowi stanu cywilnego państwa, w którym dziecko urodziło się, dokumentu informującego o nadaniu nazwiska, sporządzonego według wzoru dołączonego do tekstu konwencji.

Art. 5 konwencji nr 31 dotyczy zmiany nazwiska osoby mającej obywatelstwo dwóch lub więcej państw. W przepisie tym mówi się ogólnie o zmianie bez nawiązania do przyczyny i trybu jej dokonania. Chodzi tu zatem zarówno o zmianę nazwiska spowodowaną zmianą ustaleń dotyczących pochodzenia dziecka lub jego przysposobieniem, jak o zmianę będącą skutkiem złożenia oświadczenia¹⁶ albo wydania decyzji admini-

¹⁰ W starożytności miasto to nosiło nazwę Attalia.

¹¹ Na temat konwencji nr 14, 19 i 21 oraz przyjętego w 2003 r. projektu konwencji nr 31 (różniącego się od wersji ostatecznej) zob. M. Scherer, *Le nom en droit international privé*, Paris 2004, s. 213 i n. Tekst konwencji nr 31 (*Convention sur la reconnaissance des noms*) jest dostępny na stronach internetowych www.ciec1.org.

¹² Niektóre z nich dzielą się na ustępy, oznaczone tylko cyframi, ale w tekście konwencji nazywane paragrafami.

¹³ W dalszym ciągu mowa będzie o nabyciu nazwiska w sensie obejmującym zarówno jego uzyskanie przez urodzenie jak zmianę (czyli uzyskanie nowego nazwiska) w następstwie jakiegoś późniejszego zdarzenia.

¹⁴ Dz.U. z 1991 r. nr 120, poz. 56, zm. 2000 nr 2, poz. 11.

¹⁵ Co do stanowiska prawa polskiego w tej kwestii zob. art. 88 i 89 § 1 k. r. o.

¹⁶ Art. 90 k. r. o. dopuszcza zmianę nazwiska dziecka w drodze oświadczenia złożonego przez matkę dziecka i jej męża. Niektóre państwa pozostawiają pełną swobodę zmiany nazwiska przez złożenie stosownego oświadczenia, natomiast w prawie polskim nawet uwzględnienie wniosku o wydanie decyzji administracyjnej o zmianie nazwiska może nastąpić tylko z określonych ustawowo przyczyn.

stracyjnej¹⁷ lub orzeczenia sądowego.¹⁸ W art. 5 ust. 2 wyłączono jednak z tego unormowania zmianę nazwiska spowodowaną zawarciem małżeństwa, jego ustaniem i unieważnieniem, bowiem te przypadki zmiany nazwiska są objęte postanowieniami art. 1 i 2 konwencji nr 31. Zgodnie z art. 5 ust. 1 zdanie 1 zmiana dokonana w umawiającym się państwie, którego obywatelstwo ma dana osoba, jest uznawana w innych umawiających się państwach. Jeżeli jednak zmiana nazwiska jest następstwem orzeczenia sądowego zmieniającego stan cywilny danej osoby, umawiające się państwo może nie uznać zmiany nazwiska, jeżeli nie uznaje ono tego orzeczenia (art. 5 ust. 1 zdanie 2).

Problematyka wpływu wywieranego na nazwisko przez zdarzenia z dziedziny prawa małżeńskiego unormowana została w dwóch pierwszych artykułach konwencji nr 31. Konfrontacja ich treści z treścią art. 5 nasuwa wniosek, że przewidziana w nich regulacja nie zakłada posiadania przez osobę, o której nazwisko chodzi, obywatelstwa kilku państw. Nie jest wszakże jasne, czy przepisy te można stosować także do osób mających obywatelstwo dwóch lub więcej państw. Udzielenie na to pytanie odpowiedzi twierdzącej wywołuje pytanie, czy zastosowanie tych przepisów jest uzasadnione zawsze wtedy, gdy jedno z posiadanych przez daną osobę obywatelstw jest obywatelstwem umawiającego się państwa, czy też przypadki wielorakiego obywatelstwa każde państwo rozstrzyga kierując się treścią unormowań przewidzianych w swym prawie wewnętrznym. Treść regulacji zawartej w art. 5 ust. 2 konwencji nr 31, wyłączającym stosowanie art. 5 ust. 1, który to przepis wyraźnie ogranicza zastosowanie przewidzianego w nim unormowania do osób o wielorakim obywatelstwie, przemawiać może przeciwko stosowaniu art. 1 i 2 konwencji w sytuacji, gdy zainteresowana osoba jest obywatelem dwóch lub więcej państw.

Nie we wszystkich państwach przyjęta jest regulacja, zgodnie z którą zawarcie małżeństwa pociąga za sobą skutek w postaci zmiany nazwiska małżonka. Współcześnie nawet te państwa, które akceptują taki skutek zawarcia małżeństwa, odrzucają automatyzm regulacji, uwzględniają natomiast odpowiednio wyrażoną wolę zainteresowanej osoby, a przy tym nie zawsze wymagają, aby małżonkowie nosili jednakowe nazwiska.¹⁹ Dobrym przykładem jest ewolucja stanowiska zajmowanego w tej materii przez prawo polskie. Punktem wyjścia był dekret o prawie małżeńskim z 1945 r., który zgodnie z tradycyjnie przyjętym zapatrywaniem stanowił, że żona przyjmuje nazwisko męża, pozwalając jednak na przybranie podwójnego nazwiska, którego pierwszym członem było dotychczasowe nazwisko. Późniejsze przepisy dopuściły zachowanie przez mężatkę dotychczasowego nazwiska, a potem także przyjęcie przez męża nazwiska żony. Ewolucję tych kolejno wprowadzanych unormowań zamknęła dokonana w 1998 r. nowelizacja kodeksu rodzinnego i opiekuńczego.²⁰

Art.1 konwencji nr 31 reguluje uznanie nazwiska zmienionego w związku z zawarciem małżeństwa.²¹ Przepis ten nie dotyczy zmiany nazwiska następującej *ex lege*, lecz

tylko zmiany dokonanej w drodze oświadczenia woli złożonego przez jednego lub oboje małżonków. Chodzi o oświadczenie złożone w związku z zawarciem małżeństwa (wynika to stąd, że przepis mówi o nazwisku noszonym podczas małżeństwa), ale nie koniecznie w czasie ceremonii zawarcia.²² Milczącym założeniem regulacji konwencyjnej jest to, że złożone oświadczenie wywołało skutek w postaci zmiany nazwiska (polegającej na przyjęciu nazwiska małżonka zamiast dotychczasowego nazwiska, albo na połączeniu obu nazwisk).

Wymieniony przepis konwencji przewiduje uznanie zmienionego nazwiska, jeżeli stosowne oświadczenie zostało złożone w tym umawiającym się państwie, którego jeden z małżonków jest obywatelem²³ albo, w którym w chwili złożenia oświadczenia oboje mają miejsce zwykłego pobytu. Chodzi tu o okoliczności istniejące w dniu złożenia oświadczenia. Łącznikiem, uzasadniającym zastosowanie tej normy konwencyjnej, a w konsekwencji uznanie zmiany nazwiska, jest więc obywatelstwo jednego z małżonków lub zwykły pobyt obojga małżonków. Określenia „zwykłego pobytu” konwencja nie podaje, nie różniąc się w tym punkcie od innych konwencji, w których występuje tak nazwany łącznik.²⁴ Omawiany przepis mówi o wspólnym zwykłym pobycie małżonków (*la residence habituelle commune des époux*), ale uzasadnienie wyjaśnia, że chodzi tu o pobyt obojga małżonków na obszarze tego samego państwa, ale nie koniecznie „pod jednym dachem”. Zgodnie z art. 14 ust. 1 konwencji nr 31 umawiające się państwo może złożyć zastrzeżenie, iż oświadczenie, o którym mowa w art. 1, złożone w państwie zwykłego pobytu małżonków, a dotyczące nazwiska swego obywatela, uzna tylko wtedy, gdy jeden z małżonków jest obywatelem tego państwa.

Prawo państwa, dopuszczającego zmianę w następstwie zawarcia małżeństwa, umożliwia anulowanie tej zmiany w razie, gdy małżeństwo „wygasa”. Ma to szczególne znaczenie w razie rozvodu (czyli wtedy, gdy małżeństwo ustaje w wyniku inicjatywy jednego lub obojga małżonków) albo unieważnienia małżeństwa (czyli w tych sytuacjach, w których doszło do naruszenia norm dotyczących jego zawarcia).

Regulacja przewidziana w art. 2 konwencji jest oparta na odróżnieniu sytuacji, w której były małżonek składa oświadczenie i takiej, w której zmiana nazwiska następuje z mocy prawa.

Tu zwraca uwagę zróżnicowanie zastosowanej w tym artykule terminologii. W ust. 1 użyta została nazwa *dissolution*, w ustępie 2 – nazwa *divorce*, a oprócz nich w obu ustępach – nazwa *annulation*. Polskim odpowiednikiem tej ostatniej nazwy powinna być

¹⁷ Nie rozstrzygnięto tu czy chodzi o zmianę nazwiska osoby pozostającej w związku małżeńskim (w szczególności żony), spowodowaną z mocy prawa dokonaną w trybie administracyjnym zmianą drugiego małżonka (w szczególności męża). W prawie polskim regulacja taka, przewidziana w ustawie z dnia 15.XI.1956 r. o zmianie imion i nazwisk, obowiązywała aż do dokonanej w 1998 r. nowelizacji tej ustawy.

¹⁸ Wydanie orzeczenia sądowego rozstrzygającego o nazwisku przewidziano w art. 88 § 2 i 3, art. 122 § 2 i 3 i art. 126 § 2 k. r. o.

¹⁹ Podobną ewolucję przeszła regulacja obywatelstwa kobiet zamężnych.

²⁰ Zob. art. 25 k. r. o. w brzmieniu nadanym mu ustawą z dnia 24.VII.1998 r., Dz.U. nr 117, poz. 757.

²¹ Konwencja w tym i w innych miejscach mówi o uznaniu oświadczenia, ale w istocie chodzi o uznanie jego skutku w postaci zmiany nazwiska.

²² U nas oświadczenie w sprawie nazwiska małżeńskiego składane jest zasadniczo w czasie zawierania małżeństwa (art. 7 § 2 k. r. o.), jednakże gdy małżeństwo ma być zawarte w tzw. formie konkordatowej – wcześniej (art. 25 § 1 k. r. o.), zaś w razie zawarcia małżeństwa za granicą – jednocześnie z wnioskiem o wpisanie małżeństwa do polskiej księgi małżeństw (art. 62 ust. 3 pr. a. s. c.).

²³ Przepis nie wymaga, aby był to małżonek składający oświadczenie.

²⁴ Na temat pojęcia zwykłego pobytu zob. A. Maczyński, *Zamieszkanie jako podstawa łącznika normy kolizyjnej*, Zesz. Nauk. UJ DX, Prace Prawnicze zesz. 81, Kraków 1976, s. 55, w literaturze obcej N. Siep, *Der gewöhnliche Aufenthalt im deutschen internationalen Privatrecht*, Köln 1981, D. Baetge, *Der gewöhnliche Aufenthalt im Internationalen Privatrecht*, Tübingen 1994. W urzędowych tłumaczeniach umów międzynarodowych francuska nazwa *residence habituelle* jest na ogół tłumaczona jako zwykły (rzadziej – stały) pobyt. Występującą czasem w doktrynie nazwę „zwyczajny pobyt” należy ocenić jako niepoprawną pod względem językowym, skoro chodzi tu o to, gdzie dana osoba zwykle (lub stale) przebywa, a nie, gdzie przebywa ona „zwyczajnie”.

nazwa „unieważnienie małżeństwa”. Natomiast gdy chodzi o dwie pierwsze nazwy, to nie jest uzasadnione ich traktowanie jako synonimów, trzeba raczej przyjąć, że w ust. 2 chodzi o rozwód (bez ograniczenia tylko do rozwodu orzeczonego przez sąd), a w ustępie 1 – zarówno o rozwód, jak inne sytuacje, w których dochodzi do ustania małżeństwa.²⁵ Potwierdza to uzasadnienie konwencji, w którym powiedziano, że art. 2 stosuje się we wszystkich przypadkach ustania małżeństwa, bez względu na to, czy chodzi o rozwód, unieważnienie małżeństwa, śmierć jednego z małżonków (tylko gdy chodzi o ust. 1), a nawet o separację – w takiej mierze, w jakiej ta wywiera skutki dotyczące nazwiska.²⁶

Oświadczenie, o którym mowa w art. 2 ust. 1 konwencji nr 31, może dotyczyć albo powrotu do nazwiska noszonego poprzednio (przed zmianą związaną z zawarciem małżeństwa) albo zachowania nazwiska noszonego podczas trwania małżeństwa. Spowodowana nim zmiana nazwiska jest skuteczna we wszystkich umawiających się państwach, jeżeli oświadczenie zostało złożone w umawiającym się państwie, którego obywatelem jest dany małżonek albo w którym ma on miejsce zwykłego pobytu – w dniu złożenia oświadczenia.²⁷

Art. 2 ust. 2 konwencji nr 31 dotyczy sytuacji, w której mimo rozwodu lub unieważnienia małżeństwa oświadczenie w sprawie nazwiska nie zostało złożone. Jeżeli w takiej sytuacji państwo, którego obywatelem jest dany małżonek, będące zarazem państwem, w którym orzeczono rozwód lub unieważnienie małżeństwa, przewiduje zmianę nazwiska polegającą na powrocie do poprzednio noszonego nazwiska, to zmiana ta jest uznana we wszystkich umawiających się państwach. Wydaje się, że chodzi tu tylko o zmianę następującą *ex lege*, a nie taką, która jest następstwem rozstrzygnięcia władzy publicznej.

Na podstawie art. 3 konwencji nr 31 umawiające się państwo może oświadczyć, że postanowienia art. 1 i 2 rozciąga na zarejestrowane partnerstwo.

W kolejnych postanowieniach konwencji nr 31 uregulowano kilka zagadnień o ogólnym charakterze. Najistotniejsze znaczenie ma art. 8, który przewiduje, że nazwisko uznane na podstawie konwencji jest wpisywane do urzędowych rejestrów bez jakiegokolwiek procedury. Podkreślić trzeba, że konwencja nr 31 dotyczy tylko nazwisk podlegających wpisowi do takich rejestrów, nie dotyczy zaś nazwiska, którego dana osoba może używać, ale które nie figuruje w dotyczących jej dokumentach. Zgodnie z art. 7 konwencji nr 31 odmowa uznania nazwiska (poza sytuacją określoną w omówionym już art. 5 ust. 1 zdanie 2) jest dopuszczalna tylko wtedy, gdy uznanie byłoby oczywiście sprzeczne (*manifestement contraire*) z podstawowymi zasadami porządku prawnego (*ordre public*)²⁸ państwa, w którym ma miejsce powołanie się na uznanie. Według art. 6 ust. 1 konwencji nr 31 oświadczenia, o których mowa w art. 1 i 2, złożone przed urzędnikiem konsularnym umawiającego się państwa, są uważane za składane w pań-

stwie wysyłającym tego urzędnika, zaś art. 6 ust. 2 przewiduje podobną regulację dotyczącą nadania lub zmiany nazwiska w sytuacjach, o których mowa w art. 4 i 5 (chodzi np. o sporządzenie aktu urodzenia przez urzędnika konsularnego).

Zakres czasowy norm konwencyjnych został uregulowany w art. 9. Obejmuje on nadanie lub zmianę nazwiska, które nastąpiły po wejściu w życie konwencji w stosunku do danego państwa, z tym, że w razie wcześniej dokonanego nadania lub zmiany nazwiska w warunkach odpowiadających wymaganiom określonym w konwencji można żądać wpisania tego nazwiska w rejestrach urzędowych prowadzonych w danym państwie.

Recognition of surnames in light of Convention No. 31 of the International Commission on Civil Status of 2005

The first name and surname of an individual are basic personal data by which one is able to determine the identity of a person. This is undertaken both in the sphere of regulations within private law as well as public law. In the latter, other forms of designation are becoming increasingly common, for example, combinations of numbers. The use of a different designation or surname is admissible for within private law relations, if an individual is legally entitled to use this designation, for example, a pseudonym. In spite of this, the surname still fulfils the most important role as a tool for the identification of the individual. Therefore, this issue, and in particular the form of the surname, is the subject of standards provided in the regulations of legal positivism for particular countries. The regulations determine both the form of the surname,¹ the protection² of it as one of the individual's personal rights, as well as its use in legal relations.³

Two complex issues can be posited in the recognition of a surname used by individuals in legal regulation. The first issue is related to the surname acquired at birth. The regulation determining the dependence of one's surname on the surname of one's parents (either one or both) assumes the previous recognition of parenthood. The second issue is related to the question of whether the surname acquired at birth can be later modified (that is, substituted by or supplemented with another name). Legislators allowing for this eventuality should firstly determine not only if such a modification consists in the substitution of the current surname with a new one or the combination of both the surnames of the parents to create a double-barrelled surname, but also and above all, in which situation and in what way a modification of surname can take place. The most common situation causing a modification in surname is a change in

²⁵ Nie byłoby uzasadnione tłumaczenie nazwy *dissolution du mariage* jako „rozwiązanie małżeństwa”, bo trudno objąć zakresem tej nazwy ustanie małżeństwa przez śmierć małżonka.

²⁶ W prawie polskim orzeczenie separacji wywołuje wprawdzie w zasadzie takie same skutki jak rozwiązanie małżeństwa przez rozwód, ale art. 61⁴ § 5 k. r. o. wyłącza złożenie przez osobę separowaną oświadczenia dotyczącego powrotu do nazwiska noszonego przed zawarciem małżeństwa.

²⁷ Wg art. 59 k. r. o. osoba rozwiedziona może w ciągu trzech miesięcy od uprawomocnienia orzeczenia rozwodu złożyć oświadczenie o powrocie do nazwiska noszonego przed zawarciem małżeństwa.

²⁸ Konwencja nr 31 posługuje się tu sformułowaniem przyjętym od kilkudziesięciu lat w Konwencjach Haskiej Konferencji Prawa Prywatnego Międzynarodowego. Merytorycznie nie różni się ono od unormowania przewidzianego w art. 6 polskiego prawa prywatnego międzynarodowego.

¹ In Polish Law, these issues are regulated in the Family and Guardianship Code, the Civil Status Act as well as the Act on the Change of First Names and Surnames of November 15th 1956, Law Gazette 2005 no. 233, 1992.

² In Polish Law, Article 23 and 24 of the Civil Code.

³ For example, Article 43⁴, Article 45⁵ § 3 and Article 43⁸ of the Civil Code concerning companies' names containing surnames.

one's marital status. The traditional belief that a surname serves not only to identify the individual but also indicate one's family membership has justified the assertion that all family members (husband, wife and children) have the same surname. This firm conviction is gradually being accepted less and less, especially when it concerns husbands and wives. In modern legal systems, there is a visible trend moving away from solutions that see the automatic modification of one's surname due to a change in marital status to solutions where the crucial and deciding factor are the personal wishes of the individual concerned. There is also a move away from regulations which force a modification in one's surname through public authority certificates (for example, on the basis of regulation requiring the removal of 'foreign' sounding names, or authorising a Divorce Registry to deprive the guilty husband or wife from using a name which has been acquired through marriage).

The surname is entered in the Register of Civil Status and it follows that this information can be found in documentation through which one can determine an individual's identity. Consequently, issues arise which may appear to be superficially trivial, but in practice are very significant and make it difficult to solve problems related, for example, to the spelling of surnames where the issue of transcribing a surname written in another orthographic system is but one of a whole host of complicated problems.

In order for a surname to fulfil its due function of identification, it is necessary, or at least desirable, for an individual to be designated with the same surname everywhere. This ideal state of being is not easy to achieve. This is due to the fact that there are both discrepancies in the content of regulations as well as a lack of uniformity in the standpoints taken in legal indications which determine one's surname. The former belongs to the domain of International Private Law. The solution that prevails nowadays is for the surname to be subject to law with an indication of a personal link, first and foremost subject to the law of the particular state of which the given individual is a citizen.⁴ The approach that was once promoted in Germany that saw the legally-binding form of a surname being taken from a particular event with the rights to its acquisition (that, is modification) also stemming from the same event, is becoming increasingly less popular.⁵ It is obvious that subjecting the issue of surnames to National Law does not invalidate the influence that such events can have on a surname, but only subjects the person concerned to the National Law.⁶ Insofar as the codification of legal issues relevant to surnames was usually passed over⁷, it is now the subject of increasingly detailed standards.⁸

⁴ P. Wypych, *Prawo właściwe dla nabycia i zmiany nazwiska*, In *Prawo rodzinne w Polsce i Europie*, Lublin 2005, p. 563 and the influence of divorce on surnames A. Maczyński, *Rozwód w prawie prywatnym międzynarodowym*, Warsaw 1983, p. 109.

⁵ In agreement with this thesis (without putting forward justification) is M. Pazdan, *Prawo prywatne międzynarodowe*, Warsaw 2005, p. 105.

⁶ A legal opinion of a situation which is the cause of a modification of a surname constitutes a so-called preliminary question which should be resolved according to the applicable law on the basis of norms regulating conflict of laws which are legally binding in the home state of the given individual (or according to norms in that country which regulated the effectiveness of international rulings).

⁷ In Poland, the Act of 12 November 1965 is legally binding – International Private Law, Law Gazette No. 46, 290, it does not contain regulation pertaining to surnames.

⁸ See § 13 of the Austrian Act of International Private Law, Article 10 introducing the German Civil Code has been amended several times in the last few years, Articles 37-40 of the Swiss Act on International Private Law, Article 14 of the Romanian Act on the regulation of Private International Law, Articles 36-39 of the Belgian Private International Law Code.

It is worth looking into an attempt to regulate this complicated and difficult matter undertaken by the International Commission on Civil Status (*Commission Internationale de l'état civil* – CIEC).⁹ The issue of surnames has been the subject of a variety of conventions previously prepared by this organisation. Several can be mentioned here: the Convention No. 4 on changes of surnames and forenames signed at Istanbul on September 4, 1958, the Convention No. 19 on the law applicable to surnames and forenames signed at Munich on September 5, 1980, as well as Convention No. 14 concerning the recording of surnames and forenames in Civil Status Registers signed at Berne on September 13, 1973 and Convention No. 21 on the issue of a certificate of differing surnames signed at the Hague on September 8, 1982. The newest convention prepared by the CIEC is Convention No. 31 on the recognition of surnames signed at the Turkish city of Antalya¹⁰ on September 16, 2005.¹¹ It is worth noting that only the French original is authentic. The Convention is made up of 17 articles,¹² of which the most important standards are expressed in the first eight articles. Three appendices have been attached to the Convention, which define the kind of information required for a surname to be attributed to an individual, based on Article 4 (2). Together with the Convention the explanatory report or *rapport explicatif* was announced.

Convention No. 31 is open to signature by the member states of the CIEC (Article 11). Any member state of the Council of Europe may also accede to this Convention as well as any other state pursuant to a unanimous decision of the member states of the CIEC (Article 12).

The goal that is to be achieved by the Convention is defined in the preamble. It is to facilitate the recognition of surnames attributed by birth or modified following a marriage or a divorce or for some other cause. It should be highlighted here that the word "recognition" has a specific meaning here, which is different from that used in, for example, regulations concerning the recognition of international rulings. The principles of the regulations in the Convention are that a particular individual from one of the Contracting States can bear a surname that is attributed at birth or later modified for some cause.¹³ The principles laid down in the Convention's regulations aim to have the surname attributed at birth or modified at a later stage serve to identify the individual in all Contracting States. There is thus a positive responsibility on all Contracting States to recognise that a given individual assumes the surname that has been conferred on them by another Contracting State as well as a negative responsibility which consists of the fact that a given individual does not go under another surname. The Convention does not introduce uniform regulation in this matter (it does not indicate which surname is assumed at birth or an event justifying a modification) or uniform conflict regulation (it does not indicate the applicable law for the definition of the surname). These issues as well as the ratification of the Convention is regulated individually by every Contracting State.

⁹ E. Wojnicka, *Międzynarodowa Komisja Stanu Cywilnego. Historia, osiągnięcia oraz znaczenie jej konwencji dla prawa polskiego*, Kwartalnik Prawa Prywatnego 1998, 2, p. 269. Poland is a member of the CIEC from 1998, but only acceded to one of the three Conventions prepared by the organisation.

¹⁰ Known as Attalia in ancient times.

¹¹ See M. Scherer, *Le nom en droit international privé*, Paris 2004, p. 213 on the subject of Conventions No. 14, 19 and 21 as well as the Convention No. 31 (different from the final version). The text of Convention No. 31 (Convention sur la reconnaissance des noms) can be downloaded from www.ciec1.org.

¹² Some are divided into paragraphs which are marked only by numerical figures, but are called paragraphs in the text of the Convention.

¹³ Later, there is mention of attribution of a surname in an all-encompassing sense whether this is at birth

The Convention defines the factors which determine the effectiveness of the attribution or modification of a surname in other Contracting States. Generally speaking, these factors are based on circumstances surrounding the individual whose surname is concerned or an event following which a surname is attributed. In other words, according to the Convention the recognition of a surname is dependent on its attribution in a state with which the given individual has an appropriate tie. The circumstances testifying to the existence of such a tie are defined in particular regulations in the Convention in a variety of ways. They can be either objective (nationality, habitual residence) or subjective (birth, issue of a ruling).

The regulations of the Convention have a limited extent whereby not all situations are covered where within one Contracted State there is an event that causes the attribution or modification of a surname even if the surname of the individual is a citizen of another Contracted State. The situations that do not come under this extent, are subject to regulations ratified under the internal law in the particular states.

Contrary to the sequence of the rulings in the Convention, their introduction begins with regulations concerning the attribution of a surname at birth. It is worth noting that Article 7 (1) of the Convention on the Rights of the Child as ratified by the General Assembly of the United Nations on November 20, 1989¹⁴ requires that the child be registered immediately after birth. The birth certificate is drawn up in the state in which the child was born and the fundamental element of every birth certificate is the surname of the child.

Article 4 of Convention No. 31 requires that the surname of the child is recognised in the state in which the child is born if it is a citizen of this state. This ruling only relates to children possessing nationalities in two or more states and in practice means that above all every state that the child is a citizen of must recognise the surname given to it in the other state of which it is also a citizen, insofar as the child is tied to this state by virtue of also being born there. The justifying principle in the implementation of the above-mentioned norms are two circumstances that indicate the same Contracting State, namely nationality and place of birth. Also, an additional condition is for the child to be a citizen of several countries irrespective of them being Contracting States or not. The Convention does not address the recognition of child's surname in the event of the child being born in a Contracting State, but not being a citizen of that state nor does it address the recognition of child's surname which is a citizen of a Contracting State, but was born in another state and has not obtained nationality there.

An exception to the regulations defined in Article 4 (1) of Convention No. 31 is introduced in Article 2 (1). It determines the recognition of a child's surname in another Contracting State of which the child is a citizen at the request of the parents (the French text uses the phrase: *la demande des parents*). The premise behind the application of this norm is that within the bounds of that state's regulations the parents of the child can have an influence on the name of their child.¹⁵ The name attributed to a child at the request of the parents is recognised in other Contracting States, including

the state in which the child was born. The guarantee of this norm is the ruling that stipulates that the Civil Registrar of the state where the child is born, be supplied with information concerning the child's surname according to the specimen as provided in text of the Convention.

Article 5 of Convention No. 31 concerns modifications to the name of a person possessing nationalities in two or more states. In this regulation, there is only mention of a modification without reference to its cause or way in which it is undertaken. However, this concerns a modification of surname caused by a change in the determination of the child's descent or the child's adoption, as well as a modification in consequence of a declaration,¹⁶ administrative decision¹⁷ or judicial decision.¹⁸ A modification of a surname through marriage, its dissolution or annulment is excluded from these norms in Article 5 (2), as the circumstances of these modifications are covered by rulings in Articles 1 and 2 of Convention No. 31. In accordance with Article 5 (1), a modification undertaken in a Contracting State in which an individual possesses the nationality should also be recognised in other Contracting States. However, if a surname modification is a consequence of a judicial decision modifying personal status, the Contracting State may refuse to recognise the modification in surname if it does not recognise that decision [Article 5 (1)].

The issue of the influence of certain events from Marital Law on surnames has been regulated in the first two articles on Convention No. 31. The juxtaposition of their subject matter with the subject matter of Article 5 allows one to conclude that the regulations defined therein do not require the individual whose surname is concerned to possess the nationalities of several states. It is not, however, clear whether the regulations can be applied to individuals possessing nationalities of two or more states. A positive answer to this question begs another question: is the application of these regulations always justified when one of the states in which the individual is a national of is a Contracting State, or in cases of multiple nationality, each state settles the issue defined through standards within its internal law. Article 5 (2) of Convention No. 31 excluding the application of Article 5 (1) which clearly limits its application for individuals possessing multiple nationalities can be an argument against the application of Article 1 and 2 of the Convention in situations where the individual concerned is a national of two or more states.

The regulation that sees the consequence of marriage as being the modification of a spouse's surname is not applicable in all states. Nowadays, even those states which accept such a consequence of marriage reject the automatic modification of surnames, instead taking into consideration the personal choice of the person considered, simul-

¹⁴) Law Gazette 1991 no. 120, 56, 2000 no. 2, 11.

¹⁵) The position of Polish Law with regards this point can be found in Article 88 and 89 § 1 of the Family and Guardianship Code.

¹⁶) Article 90 of the Family and Guardianship Code permits a modification in the child's surname in consequence of a declaration by the child's mother and her husband. Some states permit complete freedom in the modification of the surname through applicable declaration, however, in Polish law even consideration of a proposal of an administrative decision concerning a modification of surname can only take place in certain circumstances which are specified by law.

¹⁷) It is not clear and the matter has not been settled whether this point concerns a modification of surname of persons who are married (in particular the wife) caused by a modification of the spouse's surname (in particular, the husband) through administrative regulation *ipso iure*. In Polish Law this regulation is determined in the Act of 15th November 1956 on Modification of Forenames and Surnames, which was in force until its amendment in 1998.

¹⁸) Judicial declarations that decide surnames are defined in Articles 88 § 2 and 3, Article 122 § 2 and 3 and Article 126 § 2 of the Family and Guardianship Code.

taneously not requiring partners to possess the same surname.¹⁹ A good example is the development of the position taken in this matter by Polish Law. The starting point of this position was the issue of a decree on Marital Law of 1945, which in line with the traditionally established views specified that wife assumes the surname of her husband allowing her, however, to assume a double-barrelled surname, where the first part of the surname is her original surname. Later regulation allowed the woman to maintain her original surname and the man to assume his wife's surname. The development of these norms could be said to have reached an end in 1998 with the amendment to the Family and Care Code.²⁰

Article 1 of Convention No. 31 regulates the recognition of surnames modified in consequence of marriage.²¹ This regulation does not concern a modification of surname following *ex lege*, but only modifications undertaken through declaration of intent by one or both of the partners. This declaration is submitted in consequence of marriage (which is a result of the fact that the regulation mentions the surname assumed during marriage), but not necessarily during the marriage ceremony.²² The unwritten assumption of the regulations of the Convention is that the submission of a declaration causes a modification of surname (consisting of the adoption of the surname of the spouse rather than keeping the original surname or joining the two surnames together).

The above-mentioned regulation of the Convention stipulates the recognition of a modified surname if an appropriate declaration is submitted in a given Contracting State, in which one of the spouse's is a national,²³ or at the moment of submitting the declaration both spouses have habitual residence. The circumstances on the day in which the declaration was submitted are important here. The connecting links that justify the application of the norms of the Convention (in consequence, the recognition of a modification of surname) are the nationality of one of the spouses or the habitual residence of both the spouses. The Convention does not give the definition of "habitual residence", not differing from other Conventions in this matter, in which such connecting links are mentioned.²⁴ The regulation that is under discussion mentions common habitual residence of the spouses (*la residence habituelle commune des époux*), but the explanatory notes explain that this relates to the residence of both spouses in the same state and not necessarily "under the same roof". According to Article 14 (1) of Convention No. 31 Contracting States reserve the right to recognise a declaration of common habitual residence of the spouses (mentioned in Article 1) concerning the surname of its nationals only when one of the spouses is a national of the state.

¹⁹ The regulation concerning the nationality of married women has undergone similar development.

²⁰ See Article 25 of the Family and Guardianship Code.

²¹ In this and other points, the Convention mentions the recognition of declarations, but in essence it concerns their consequence which is a modification of surname.

²² In Poland, a declaration on the marital surname is submitted during the marriage itself in principle (Article 7 § 2 of the Family and Guardianship Code), however, when a marriage is entered into through concordat this proceeds earlier (Article 25 § 1 of the Family and Guardianship Code), whereas when a marriage is entered into abroad, it is submitted simultaneously with an application to have the marriage registered in the Polish Marriage Register (Article 6 (3) of the Civil Status Act).

²³ The regulation does not require that it is a spouse submitting the declaration.

²⁴ With regards common habitual residence please see A. Mączyński, *Zamieszkanie jako podstawa łącznika normy kolizyjnej*, Zesz. Nauk. UJ DX, , Kraków 1976, p. 55. In other languages see N. Siep, *Der gewöhnliche Aufenthalt in deutschen internationalem Privatrecht*, Köln 1981; D. Baegte, *Der gewöhnliche Aufenthalt im Internationalen Privatrecht*, Tübingen 1994.

The state law allowing for a modification of surname in consequence of entering into marriage allows the annulment of this modification if the marriage is "expires". This is of particular significance when a divorce takes place (that is, when the marriage ends due to the initiative of one or both the spouses) or the marriage is annulled (that is, in situations where the terms of the agreement are broken).

The regulation stipulated in Article 2 of the Convention is based on the differentiation of a situation where the spouse submits a declaration and a situation where the modification of a surname occurs in consequence by operation of law.

The terminology used in the Article concerning this differentiation needs to be mentioned at this point. The French *dissolution* is used in paragraph 1, whereas *divorce* in paragraph 2 as well as *annulation* in both. The Polish equivalent of the former should read an "annulment of marriage". However, there is no justification for treating the first two words as synonyms, but one must assume that in paragraph 2 the term applies to divorce (through a judicial ruling), whereas in paragraph 1 the term applies to divorce or other situations in which the marriage comes to an end.²⁵ This is confirmed in the explanatory notes of the Convention in which it is given that Article 2 is applied in all cases of a dissolution of marriage, irrespective of this being a divorce, annulment, through the death of one of the spouses (only in respect to paragraph 1) or even separation in situations where this relates to changes in the surnames.²⁶

The declaration mentioned in Article 2 (1) of Convention No. 31 can apply to either a return to the surname used earlier (before the modification in consequence of entering into marriage) or keeping the surname that was assumed during the marriage. The modification is effective in all Contracting States if the declaration was submitted in one of the Contracting States, of which the given spouse is a national or a habitual resident on the day of submitting the declaration.²⁷

Article 2 (2) of Convention No. 31 applies to a situation in which (irrespective of it being a divorce or annulment of marriage) the declaration regarding a modification of surname was not submitted. If, in this situation, a state of which a given individual is a national and in which the divorce or annulment is ruled, stipulates a modification of a surname consisting in a return to the former surname, then this modification is deemed valid in all Contracting States. It seems that this applies to modifications taking place *ex lege* rather than those taking place in consequence of a settlement by the public authorities.

According to Article 3 of Convention No. 31 Contracting States can declare that the regulations of Articles 1 and 2 are extended to registered partnerships.

In successive rulings of Convention No. 31, several general issues are also regulated. Of fundamental import is Article 8, which determines that a surname recognised on

²⁵ There is no justification for translating *dissolution du mariage* as "dissolution of marriage" as this would not include the end of a marriage through the death of one of the spouses.

²⁶ In Polish Law, a ruling of separation, in truth, has the same consequences as an annulment of marriage through divorce, but Article 61⁴ § 5 of the Family and Guardianship Code does not allow the separated individual to submit a declaration for a return to the surname assumed prior to entering into marriage.

²⁷ In Article 59 of the Family and Guardianship Code divorcees can submit a declaration on the reversion to their former surname within three months of the divorce ruling.

the basis of the Convention is entered in the Register of Civil Status without any kind of procedure being needed. It should be highlighted that Convention No. 31 concerns only surnames that are entered in such Registers, but does not concern surnames which an individual can use but do not figure in the appropriate documentation. According to Article 7 of Convention No. 31 the refusal to recognise a surname [other than in the above-mentioned situation referred to in Article 5 (1)] is admissible only when the recognition of a surname is incompatible (*manifestement contraire*) with the basic rules of public policy (*ordre public*)²⁸ of the state in which the recognition of the surname is attributed. According to Article 6 (1) of Convention No. 31, the declaration mentioned in Articles 1 and 2 made by a consular authority with the Contracting State shall be deemed as being made in that state, whereas Article 6 (2) determines similar regulation concerning the attribution or modification of a surname in situations mentioned in Articles 4 and 5 (that is drawing up a Birth Certificate by a consular authority).

The time scale of the norms of the Convention is regulated in Article 9. This includes the attribution and modification of surnames that have taken place after the Convention has entered into force in a given state, however, when attribution or a modification has been undertaken earlier in situations that fulfil the conditions laid down in the Convention, one can demand the recording of this surname in the official Registers of that particular state.

²⁸⁾ Convention No. 31 uses an expression that has been in use in the conventions of the Hague Conference on Private International Law for a lengthy period of time. Its subject matter does not differ from the regulations set down in Article 6 of Polish Private International Law.

Peter Michael

Data Protection Secretary, Joint Supervisory Authorities
Sekretarz Ochrony Danych, Wspólne Organy Nadzorcze

Law enforcement and data protection in the European Union, the need for a common approach

Criminal activities are probably as old as mankind. However, their impact on global society has never been so prominent as in the last 20 years. And in the past five years it has become painfully clear that criminal activities are also used for political purposes.

The impact of these activities, and certainly when they have an organized structure and international dimension, forces Member States of the European Union to invest jointly in the fight against crime. Cooperation between law enforcement authorities and other forms of common action is seen as the effective countermeasure dealing with the increasing impact of organized crime and terrorism in the European society.

This aim was embedded in Title VI of the Treaty on the European Union¹ describing the Union's objective in the Third Pillar area as *to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia*.

This objective should be achieved by developing common action among the Member States in the field of police and judicial cooperation.

Title VI of the Treaty of the European Union basically creates a common approach as an answer to the EU-wide operating criminal or criminal structures. They can only be combated effectively in a joint effort including the dismantling of any existing obstacles for effective joint police actions.

The Treaty of the European Union is not the sole legal instrument for developing common actions. Cooperation was already established using various legal instruments and forms of cooperation. Cooperation via Interpol and the Schengen agreements² are only two examples of increasing flux in developing cooperation. The establishment of Euro-pol and Eurojust furthermore reflects a policy whereby cooperation within the European Union should (also) be stimulated and enhanced on the European level.

¹⁾ Treaty of Maastricht of 7 February 1992.

²⁾ Agreement between the Benelux, France and Germany on the gradual abolition of checks at their common borders (14 June 1985) and the Convention implementing the Schengen Agreement (19 June 1990).

To achieve the objective of the European Union, crime should be prevented and combated through closer cooperation between police forces, customs authorities and other competent authorities as well as through closer cooperation between judicial authorities. The common actions are diverse in nature although some of these common actions focus on the collection, storage, processing, analysis and exchange of information. From a data protection point of view the most important one.

It would be interesting to explore the link between these common actions and the obligation to respect fundamental rights, such as the general data protection principles.

Cooperation on the EU level

Many initiatives have been developed in the past to achieve the objective of Title VI. These initiatives can be divided in three mainstream activities: the creation of EU information systems (the Schengen Information System, Europol and Eurojust); the creation of communication networks or systems to be used for exchanging information on a bi- or multilateral basis (Ante Fraud Information System, Bureau De Liaison (BDL) and the Europol Secure Communication network); and harmonizing national legislation or policies in the police and justice area (EU Drugs Action Plan 2005-2008³ and the EU plan on best practices, standards and procedures for combating and preventing trafficking in human beings⁴).

The harmonization initiatives are interesting to explore for their impact on data protection. The apparent need for harmonizing national legislation in a wide area such as freedom, security and justice, is clearly visible in the number and variety of subjects that are dealt with at the European level.

A common strategy for customs cooperation under the Third Pillar, a directive relating to compensation for crime victims, a directive dealing with the issue of residence permits to third-country nationals who are victims of trafficking in human beings, a resolution on a model protocol for the establishment of partnerships between the public and private sectors to reduce the harm caused by organized crime, the development of an European Criminal record are just mere examples of initiatives aiming to achieve the objective of Title VI.

The Council recently adopted a multi-annual programme to strengthen freedom, security and justice in the European Union.⁵ Ranging from immigration to actions enhancing police cooperation, this programme introduces a variety of measures to achieve the objectives of the European Union.

Another and also recent example is the approval by the European Parliament of a Directive of the European Parliament and Council on the retention of communication data, obliging providers of public electronic communication services to retain certain traffic data for law enforcement purposes.

All these initiatives have one aspect in common: Member States can apparently not sufficiently achieve a satisfactory result in dealing with these subjects on their own. The Council, applying the subsidiarity principle, clearly promotes the European initiative that will better attain the objectives sought by specific proposals.

All these initiatives furthermore promote common and horizontal standards for the use of law enforcement data which will result in an information policy harmonizing procedures followed by law enforcement authorities of the Member States.⁶ This will indirectly influence law enforcement competences and practices in all Member States.

For a better understanding of the impact of these proposals in the law enforcement area and especially in the area of cooperation and exchange of personal data, it is necessary to explore first the relation between law enforcement, the processing of personal data and data protection laws on a national level.

A national perspective

Important data protection principles applying to law enforcement are laid down in the Convention of the Council of Europe of 28 January 1981 (Convention 108). All 25 EU Member States have ratified this convention. Another instrument – albeit not binding – is Recommendation No. R(87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987. Although this Recommendation was adopted some 17 years ago, the third evaluation of this instrument in 2002 concluded that the principles laid down in this Recommendation are still relevant.

All 25 Member States have data protection laws that apply to police and judicial files. 22 of these Member States apply general data protection laws implementing the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Three Member States have specific data protection laws for police files (Finland, Holland and Sweden).

The competence for collecting data by law enforcement authorities is regulated in specific national laws regulating law enforcement competence. It is difficult to produce a total overview of all the different laws in the Member States regulating this competence. However, the existing investigation methods including the interception of communication, the use of informants and infiltrators and the possibility to require information demonstrate that police and judicial authorities have a great variety of instruments to collect information at their disposal.

Where these laws create the right to collect data, and when these data are actually collected, national data protection laws apply to the collected data. National data protection laws regulating the processing of data by law enforcement authorities may thus be regarded as connected to national laws regulating the competence to collect data.

Depending on the kind of law enforcement action, different categories of data and sources of information may be distinguished. It is also necessary to differentiate data collection when trying to solve or prevent crime.

³) OJ C. 168, 8.7.2005, p. 1.

⁴) OJ C. 311, 9.12.2005, p.1.

⁵) The Hague Programme, European Council, 4-5 November 2004.

⁶) See also: Joint Position Paper of the European data protection authorities, Krakow, 25-26 April 2005.

The first source of information is often the crime itself. Investigation on the scene of the crime, statements from victims or witnesses, or other available law enforcement information, these are all important sources of information. Depending on the kind of crime or the findings of the investigation, different other sources of information such as private or public sector information are needed. Financial information, travel movements and information on the use of telecommunication facilities, these are sometimes necessary to effectively fight crime and are of special interest in crime prevention.

These data are generally collected by organizations in the private or public sector. National data protection laws implementing the Directive 95/46 apply. The basic principle for the processing of personal data is that these data may only be processed (collected) fairly and lawfully, and only used for the purpose of processing. Member States may adopt legislative measures to restrict this principle when such restriction is necessary for the purpose of preventing, investigating, detecting and prosecuting criminal offences.⁷

The collection by law enforcement authorities of these data from the private and public sector must thus be in compliance with specific laws regulating the competence of police and judicial authorities. These specific laws are the exception to the principle of purpose limitation.

Since Member States increasingly introduce new laws, providing law enforcement authorities with more possibilities to require personal data, this increased use of the exception to the purpose limitation will slowly undermine this basic data protection principle.

What is the experience gained from national laws and law enforcement cooperation? Caution is advised as no in-depth evaluation has been made on this subject. However, on the basis of publications, the three evaluations on the Recommendation R(87) 15 and of the explanatory memoranda of many European Union initiatives, the following aspects are of interest:

As already stated, data protection laws in the Member States are based on Convention 108 or the Directive 95/46. According to these instruments, the exchange of information within the EU may not be prohibited for the sole purpose of data protection. Cooperation and exchange of data between the Member States are thus allowed in principle.

However, owing to the differences in national laws on police and judicial activities, and more specific the differences in competence and investigation methods and information gathering, it is difficult to compare the impact of data protection law on data processing by law enforcement authorities and the exchange of personal data. For example, do specific provisions under Finnish, Swedish and Dutch law governing criminal intelligence have the same impact as do the general data protection laws? Are we, in fact, talking about the same category of data when referring to the criminal intelligence? And what is the impact of the different national data protection legislation on

this type of data? This subject becomes extremely important where intelligence-led policing becomes the general policy in the European Union.

All data protection laws encompass the principle that data should be lawfully obtained. However, what is the impact of this principle on the exchange of personal data between law enforcement authorities of the Member States? For example, are all the methods of investigation in the EU the same? Is provoking an individual to commit a crime an accepted method of investigation in all the Member States? And if not, does this not mean that, according to the principle that personal data should be lawfully obtained, the result of such a method may be processed in the Member State which accepts this method as a legal method of investigation but not in the Member State where that method is not accepted? This just underlines that it is sometimes difficult to exchange information between law enforcement authorities within the EU and to process such data further in view of the differences between sectorial laws on law enforcement competence.

To summarize, one could say in general that national data protection laws do not present an obstacle to data processing, including the exchange of data within the European Union. Differences between the national sectorial laws, and sometimes as a result of data protection legislation, are the most important reasons that the cooperation between the law enforcement authorities of the Member States including the exchange of data cannot take place.

However, at the Conference in Krakow on 24-25 April 2005, the European Data Protection Authorities adopted a Position paper on Law Enforcement & Information Exchange in the EU opinion in which they stated that *EU initiatives requiring the collection, retention or exchange of personal data for law enforcement purposes are bound to highlight differences in the law on data protection throughout the EU. Such discrepancies might have unacceptable consequences from a data protection point of view, and possibly for those trying to tackle crime.*

A European data protection perspective

This opinion of the European data protection authorities does not go against the conclusion that national data protection laws as such are no obstacle to processing, including the exchange of data. It does, however, emphasize that the European Union initiatives in the field of law enforcement and the national impact of such initiatives, should be linked to the attainment of an adequate level of data protection.

An effective common information policy in the area of law enforcement will only be possible when combined with a harmonized approach to data protection safeguards.

On 4 October 2005, the Commission submitted a proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.⁸

This important initiative for a harmonized approach of data protection under the Third Pillar was welcomed by the Conference of European Data Protection Authorities and

⁷ Article 13(1) Directive 95/46/EC.

⁸ COM(2005) 475

the European Data Protection Supervisor. It creates a necessary tailor-made law enforcement data protection regime. If this Framework Decision is adopted, it will no doubt mark an important step towards creating better and more adequate data protection safeguards in the area of freedom, security and justice.

However, it should be also mentioned that this Framework Decision does not prevent the increasing use of the exception from the fundamental data protection rule on the purpose limitation. This should form the subject of discussion between all European data protection authorities. Any new legislation leading to exceptions should be assessed whether or not the proposal is proportionate. However, is this principle of proportionality still the only and effective way of assessing new legislative measures? And if so, should the still increasing use of the exception from the purpose limitation principle not be accompanied by extra safeguards?

If the scale tips in favour of law enforcement, a standard data protection reaction is trying to remove the weight that favours law enforcement. It might be also interesting to invest in extra data protection checks so as to restore the balance. Developing extra data protection safeguards may be one way of contributing to that goal.

This will be a real challenge for the future.

Ściganie przestępstw oraz ochrona danych w Unii Europejskiej, potrzeba wspólnego podejścia

Przestępstwa towarzyszyły ludzkości od zawsze. Niemniej jednak ich wpływ na globalne społeczeństwo nigdy jeszcze nie był tak znaczący jak w ostatnich 20 latach. Zaś w ciągu ostatnich pięciu lat stało się aż nadto jasne, że działania przestępcze stosuje się również dla celów politycznych.

Wpływ powyższych działań, szczególnie w sytuacji, gdy posiadają one zorganizowaną strukturę i międzynarodowy wymiar, wymusza na Państwach Członkowskich Unii Europejskiej wspólne zaangażowanie w walkę z przestępczością. Współpraca między organami ścigania oraz inne formy wspólnych działań postrzegane są jako skuteczny środek mogący zapobiec wzrastającym oddziaływaniom przestępczości zorganizowanej i terroryzmu na społeczność europejską.

Temat ten poruszono w tytule VI „Traktatu o Unii Europejskiej”¹, opisując cel Unii w trzecim filarze jako *zapewnienie obywatelom wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości przez rozwijanie wśród Państw Członkowskich wspólnych działań w dziedzinie współpracy policyjnej i sądowej w sprawach karnych oraz przez zapobieganie rasizmowi i ksenofobii oraz zwalczanie ich*.

Cel ten powinien zostać osiągnięty poprzez rozwijanie wśród Państw Członkowskich wspólnych działań na polu współpracy policyjnej i sądowej.

Tytuł VI „Traktatu Unii Europejskiej” kreuje wspólne podejście zasadniczo jako odpowiedź na przestępczość i struktury przestępcze działające w skali całej UE. Ich skuteczne zwalczanie możliwe jest tylko przy wspólnie podjętych wysiłkach, obejmujących usuwanie wszelkich istniejących przeszkód w prowadzeniu skutecznych wspólnych działań policyjnych.

„Traktat Unii Europejskiej” nie jest jedynym instrumentem prawnym służącym rozwojowi wspólnych działań. Współpraca została już zainicjowana z wykorzystaniem różnych instrumentów prawnych i różnych form współdziałania. Współpraca za pośrednictwem Interpolu oraz porozumienia z Schengen² stanowi tylko dwa przykłady nieustannie narastających zmian w rozwijającej się współpracy. Stworzenie Europolu i Eurojustu stanowi dalsze odzwierciedlenie polityki, dzięki której współpraca w obrębie Unii Europejskiej powinna być stymulowana i ulepszana (także) na poziomie europejskim.

Aby osiągnąć ten cel, konieczne jest zapobieganie i zwalczanie przestępczości poprzez bliższą współpracę między siłami policyjnymi, administracją celną i innymi właściwymi organami, a także przez bliższą współpracę między władzami sądowymi. Natura wspólnie podejmowanych działań bywa różnorodna, jednak niektóre z nich koncentrują się na zbieraniu, przechowywaniu, przetwarzaniu, analizowaniu oraz wymianie informacji. Z punktu widzenia ochrony danych właśnie ten aspekt jest najważniejszy.

Interesująca będzie analiza zależności między owymi wspólnymi działaniami a zobowiązaniem do przestrzegania praw podstawowych, takich jak ogólne zasady ochrony danych.

Współpraca na poziomie UE

W celu osiągnięcia celów tytułu VI w przeszłości podejmowanych było wiele inicjatyw. Inicjatywy te podzielić można na trzy główne rodzaje aktywności: tworzenie systemów informacyjnych UE (system informacyjny Schengen, Europol i Eurojust); tworzenie sieci lub systemów komunikacji służących dwu- lub wielostronnej wymianie informacji (system informacyjny ds. zwalczania nadużyć finansowych, Bureau De Liaison (BDL) oraz bezpieczna sieć komunikacyjna Europolu); oraz harmonizacja krajowego ustawodawstwa lub polityki w dziedzinie policji i sądownictwa (plan działania UE w zakresie narkotyków na lata 2005-2008³ oraz plan UE dotyczący najlepszych praktyk, standardów i procedur zwalczania handlu ludźmi i zapobiegania mu⁴).

Badanie inicjatyw harmonizacyjnych jest interesujące z uwagi na ich wpływ na ochronę danych. Oczywista potrzeba harmonizacji ustawodawstwa krajowego w szerokim za-

¹) Traktat z Maastricht z dnia 7 lutego 1992 r.

²) Porozumienie między krajami Beneluksu, Francją i Niemcami o stopniowym znoszeniu kontroli na wspólnych granicach (14 czerwca 1985 r.) oraz „Konwencja wykonawcza do układu z Schengen” (19 czerwca 1990 r.).

³) Dz. U. C 168, 8.7.2005, s. 1

⁴) Dz. U. C 311, 9.12.2005, s. 1

kresie, na przykład, w dziedzinie wolności, bezpieczeństwa i sprawiedliwości, jest wyraźnie widoczna w wielu różnych, poruszanych na poziomie europejskim zagadnieniach.

Wspólna strategia współpracy celnej na mocy trzeciego filaru, dyrektywa związana z odszkodowaniami dla ofiar przestępstw, dyrektywa zajmująca się kwestią zezwoleń na pobyt dla obywateli krajów trzecich będących ofiarami handlu ludźmi, rezolucja na temat modelowego protokołu w sprawie ustanowienia partnerstwa między sektorem państwowym i prywatnym, w celu ograniczenia szkód powodowanych przez przestępczość zorganizowaną, stworzenie europejskiego rejestru skazanych – oto zaledwie kilka przykładów inicjatyw zmierzających do osiągnięcia celów tytułu VI.

Niedawno Rada przyjęła wieloletni program służący wzmocnieniu wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej.⁵ Obejmując kwestie od imigracji do działań usprawniających współpracę policyjną, program ten wprowadza różnorodne środki służące osiągnięciu celów Unii Europejskiej.

Innym, również niedawnym, przykładem jest zatwierdzenie przez Parlament Europejski Dyrektywy Parlamentu Europejskiego i Rady w sprawie zachowywania danych w zakresie łączności, zobowiązującej dostawców publicznych usług łączności elektronicznej do zachowywania niektórych danych dotyczących ruchu dla celów ścigania przestępstw.

Wszystkie te inicjatywy posiadają jeden wspólny aspekt: Państwom Członkowskim, jeśli zajmują się tymi zagadnieniami w pojedynkę, najwyraźniej nie udaje się w wystarczającym stopniu osiągać satysfakcjonującego rezultatu. Rada, stosując zasadę pomocy, wyraźnie promuje inicjatywę europejską, która w większym stopniu umożliwi osiągnięcie zakładanych celów.

Ponadto wszystkie te inicjatywy promują wspólne i horyzontalne standardy w sprawie wykorzystywania danych związanych ze ściganiem przestępczości, co będzie skutkowało polityką w dziedzinie informacji harmonizującą procedury przestrzegane przez organy ścigania Państw Członkowskich.⁶ Pośrednio wpłynie to na kompetencje organów ścigania oraz stosowane przez nie praktyki we wszystkich Państwach Członkowskich.

W celu lepszego zrozumienia wpływu tych propozycji w obszarze ścigania przestępczości, zaś szczególnie w dziedzinie współpracy i wymiany w zakresie danych osobowych, konieczne jest najpierw zbadanie zależności między ściganiem przestępstw, przetwarzaniem danych osobowych i przepisami o ochronie danych na poziomie krajowym.

Perspektywa krajowa

W „Konwencji Rady Europy z dnia 28 stycznia 1981 r.” („Konwencja 108”) określone zostały istotne zasady ochrony danych, mające zastosowanie do ścigania przestępstw.

Konwencję tę ratyfikowało wszystkich 25 Państw Członkowskich UE. Innym instrumentem – choć niewiążącym – jest rekomendacja nr R(87) 15 Komitetu Ministrów Rady Europy z dnia 17 września 1987 r. Chociaż zalecenie to przyjęto około 17 lat temu, w ramach trzeciej oceny tego instrumentu, dokonanej w 2002 r., stwierdzono, że określone w zaleceniu zasady wciąż są istotne.

Wszystkich 25 Państw Członkowskich posiada prawo ochrony danych mające zastosowanie do kartotek policyjnych i sądowych. 22 spośród Państw Członkowskich stosuje ogólne przepisy o ochronie danych, wprowadzające w życie Dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Trzy Państwa Członkowskie posiadają odrębne przepisy o ochronie danych, dotyczące kartotek policyjnych (Finlandia, Holandia i Szwecja).

Kompetencje w zakresie zbierania danych przez organy ścigania określone są w konkretnych przepisach krajowych regulujących kwestie kompetencji odnośnie ścigania przestępstw. Trudno byłoby przedstawić pełen przegląd wszystkich różnorodnych ustaw regulujących te kompetencje w Krajach Członkowskich. Jednakże istniejące metody śledcze, w tym przechwytywanie wiadomości, posługiwanie się informatorami, stosowanie infiltracji i możliwość żądania przekazania informacji pokazują, że organy policyjne i władze sądowe dysponują szerokim wachlarzem instrumentów służących zbieraniu informacji.

O ile przepisy te dają prawo zbierania danych i o ile dane te faktycznie są zbierane, o tyle do zebranych danych stosują się krajowe przepisy o ich ochronie. Krajowe przepisy o ochronie danych, regulujące przetwarzanie danych przez organy ścigania, mogą więc być postrzegane jako wiążące się z przepisami krajowymi, regulującymi kompetencje w zakresie zbierania danych.

W zależności od rodzaju działania mającego na celu egzekwowanie prawa, wyróżnić można różne kategorie danych oraz źródeł informacji. Konieczne jest także odrębne traktowanie zbierania danych w przypadku próby wyjaśnienia przestępstwa lub zapobieżenia mu.

Pierwszym źródłem informacji jest często samo przestępstwo. Dochodzenie na miejscu przestępstwa, zeznania poszkodowanych i świadków, bądź inne dostępne informacje śledcze, wszystkie one są istotnymi źródłami informacji. Zależnie od rodzaju przestępstwa i wyników dochodzenia, potrzebne są różne inne źródła informacji, takie jak informacje z sektora prywatnego lub publicznego. Informacje finansowe, dane dotyczące przemieszczania się i podróży oraz informacje o wykorzystywaniu urządzeń telekomunikacyjnych często bywają niezbędne do skutecznego zwalczania przestępstw, są również szczególnie interesujące, gdy chodzi o zapobieganie im.

Dane te zbierane są na ogół przez organizacje w sektorze prywatnym lub państwowym. Znajdują tutaj zastosowanie krajowe przepisy o ochronie danych wdrażające Dyrektywę 95/46/WE. Podstawowa zasada przetwarzania danych osobowych mówi, że mogą one być przetwarzane (zbierane) tylko w sposób rzetelny i zgodny z prawem oraz mogą być wykorzystywane tylko do celów, dla których się je przetwarza. Państwa Członkowskie mogą przyjąć środki prawne w celu ograniczenia tej zasady wtedy, gdy

⁵⁾ Program Haski, Rada Europy, 4-5 listopada 2004 r.

⁶⁾ Patrz też, dokument określający wspólne stanowisko europejskich organów ochrony danych, Kraków, 25-26 kwietnia 2005 r.

takie ograniczenie jest konieczne dla prowadzenia śledztwa oraz zapobiegania, wykrywania i ścigania wykroczeń kryminalnych.⁷

Zbieranie przez organy ścigania danych z sektora prywatnego i publicznego musi się zatem odbywać w zgodzie z konkretnymi przepisami regulującymi kompetencje organów policyjnych i sądowych. Przepisy te stanowią wyjątek od zasady ograniczenia celu.

Ponieważ Państwa Członkowskie w coraz większym stopniu wprowadzają nowe przepisy nadające organom ścigania większe możliwości występowania z żądaniem udostępnienia danych osobowych, owa intensyfikacja posługiwania się zasadą wyjątku od ograniczenia celu powoli podważa tę podstawową zasadę ochrony danych.

Jakie zebrano doświadczenia na podstawie przepisów krajowych oraz współpracy w ściganiu przestępstw? Zaleca się ostrożność, ponieważ nie zostały przeprowadzone żadne wnikliwe oceny tego zagadnienia. Jednakże, na podstawie publikacji, na podstawie trzech ocen rekomendacji R(87) 15 oraz uzasadnień wielu inicjatyw Unii Europejskiej, interesujące okazują się następujące aspekty:

Jak już stwierdzono, przepisy o ochronie danych w Państwach Członkowskich opierają się na Konwencji 108 lub Dyrektywie 95/46/WE. Zgodnie z tymi instrumentami nie jest możliwy zakaz wymiany informacji w obrębie UE wyłącznie w celu ochrony danych. Współpraca i wymiana informacji między Państwami Członkowskimi są więc w zasadzie dozwolone.

Niemniej jednak, z powodu różnic w przepisach krajowych dotyczących działań policyjnych i sądowych, a w szczególności różnic co do zakresu kompetencji, metod śledczych i gromadzenia informacji, trudno jest porównywać wpływ prawa o ochronie danych na przetwarzanie danych przez organy ścigania oraz na wymianę danych osobowych. Jako przykład rozważmy specjalne postanowienia w prawie fińskim, szwedzkim i holenderskim regulujące działalność wywiadu kryminalnego; czy mają one taki sam wpływ, jak ogólne przepisy o ochronie danych? Czy odnosząc się do wywiadu kryminalnego mówimy w gruncie rzeczy o tej samej kategorii danych? A jaki jest wpływ na tego typu dane różnego rodzaju ustawodawstwa krajowego związanego z ochroną danych? Kwestia staje się niezwykle istotna tam, gdzie działania policyjne kierowane przez wywiad stają się w Unii Europejskiej powszechnie przyjętą zasadą.

Wszystkie przepisy o ochronie danych obejmują zasadę, że dane powinny być pozyskiwane w sposób zgodny z prawem. Jednakże jaki ma ta zasada wpływ na wymianę danych osobowych pomiędzy organami ścigania Państw Członkowskich? Na przykład, czy wszystkie metody prowadzenia śledztw w UE są takie same? Czy prowokacja osoby fizycznej do popełnienia przestępstwa jest akceptowaną metodą śledczą we wszystkich Państwach Członkowskich? Jeśli zaś nie, to czy oznacza to, zgodnie z zasadą pozyskiwania danych osobowych w sposób zgodny z prawem, że informacje pozyskane w wyniku zastosowania tej metody mogą być wykorzystywane przez Państwa Członkowskie, które uznają tę metodę prowadzenia śledztwa za legalną, ale nie w tych

Państwach Członkowskich, w których metoda ta nie jest akceptowana? Uzmysławia to tylko, że czasem wymiana informacji między organami ścigania w obrębie UE oraz ich dalsze przetwarzanie są trudne z uwagi na różnice w ustawodawstwie sektorowym dotyczącym kompetencji organów ścigania.

Podsumowując, można by ogólnie stwierdzić, że krajowe przepisy o ochronie danych nie stoją na przeszkodzie przetwarzaniu danych, w tym także wymianie danych w obrębie Unii Europejskiej. Różnice między krajowymi przepisami sektorowymi, a czasem także ustawodawstwem dotyczące ochrony danych, są najpoważniejszymi przyczynami, z powodu których współpraca pomiędzy organami ścigania Państw Członkowskich, wliczając w to wymianę danych, nie może mieć miejsca.

Niemniej jednak, podczas konferencji w Krakowie w dniach 24-25 kwietnia 2005 r., europejskie organy ochrony danych przyjęły dokument określający stanowisko w sprawie ścigania przestępstw i wymiany informacji w UE, w którym stwierdzają, że *inicjatywy UE wymagające zbierania, zachowywania lub wymiany danych osobowych dla celów ścigania przestępstw muszą nieuchronnie podkreślić różnice w prawodawstwie dotyczącym ochrony danych w obrębie UE. Rozbieżności te mogłyby prowadzić do konsekwencji niemożliwych do przyjęcia z punktu widzenia ochrony danych, a być może niemożliwych do zaakceptowania także dla tych, którzy starają się zwalczać przestępczość.*

Ochrona danych – perspektywa europejska

Powyższa opinia europejskich organów ochrony danych nie stoi w sprzeczności z konkluzją, że krajowe przepisy o ochronie danych jako takie nie stanowią przeszkody w przetwarzaniu, a w tym również w wymianie danych. Podkreśla ona jednak, że inicjatywy Unii Europejskiej na polu ścigania przestępczości oraz wpływ takich inicjatyw na poziomie krajowym powinny być połączone z osiągnięciem odpowiedniego poziomu ochrony danych.

Wspólna, skuteczna polityka informacyjna w dziedzinie ścigania przestępstw możliwa jest do osiągnięcia tylko w połączeniu ze zharmonizowanym podejściem do kwestii zabezpieczeń ochrony danych.

W dniu 4 października 2005 r. Komisja złożyła wniosek dotyczący Decyzji Ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.⁸

Konferencja europejskich organów ochrony danych oraz Europejski Inspektor Ochrony Danych z zadowoleniem przyjęli tę ważną inicjatywę zharmonizowania podejścia do kwestii ochrony danych w ramach trzeciego filaru. Tworzy ona niezbędny i skrojony na miarę system ochrony danych w kwestiach ścigania przestępstw. Jeśli decyzja ramowa zostanie przyjęta, z pewnością oznaczać to będzie ważny krok w kierunku budowania lepszych i bardziej odpowiednich zabezpieczeń ochrony danych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Niemniej jednak, powinno się także wspomnieć o tym, że powyższa decyzja ramowa nie zapobiega wzrostowi stosowania wyjątku od podstawowej reguły ochrony danych dotyczącej ograniczenia celu. Kwestia ta powinna stać się tematem rozmów między wszystkimi europejskimi organami ochrony danych. Wszelkie nowe ustawodawstwo prowadzące do wyjątków powinno być oceniane pod kątem tego, czy propozycja jest czy też nie jest proporcjonalna. Czy jednak zasada proporcjonalności nadal jest jedynym skutecznym sposobem oceny nowych środków legislacyjnych? Jeśli tak, to czy wciąż narastającemu posługiwaniu się wyjątkiem od zasady ograniczenia celu nie powinny towarzyszyć dodatkowe zabezpieczenia?

Jeśli szale przechylają się na korzyść organów ścigania, standardową reakcją organów ochrony danych jest dążenie do tego, by usunąć argument, który stawia organy ścigania na uprzywilejowanej pozycji. Interesująca mogłaby być inwestycja w dodatkową kontrolę ochrony danych, tak aby przywrócić równowagę. Rozwinięcie dodatkowych zabezpieczeń ochrony danych jest być może jednym ze sposobów przyczynienia się do osiągnięcia tego celu.

Będzie to prawdziwe wyzwanie na przyszłość.

Philippos Mitleton¹

Hellenic data Protection Authority
Organ Ochrony Danych, Grecja

Public Security and Personal Data Protection²

INTRODUCTION

The conflict between the right to the protection of personal data and the "*right to security*" is particularly interesting, not only because it touches upon the core of the protection of personal rights but also because it affects the everyday life of anyone who has to choose between technology, which offers increasingly more sophisticated means for achieving an indefinable form of security, and a private life which is constantly shrinking.

The concept of public security, to which we refer in the current paper, concerns the political initiatives and the measures taken at the governmental level (national as well as international), mainly for the protection against terrorist activities and in the framework of transnational cooperation for the fight against terrorism.

It is evident that it all goes back to 11 September. The attacks that took place on that day led to a series of initiatives, which conduce, in the name of security, to a "*controlled shrinking of rights*".

Nobody denies having feelings of fear in view of unknown possibilities and of course nobody could take on the responsibility for an inadequate policy in the area of security. Still, we cannot but observe that the "open society" is no longer what it used to be and that all the initiatives that are taken for the transition to a "secure society" are "overwhelming" and leave no room for the opposite view to be heard.

At an international level, we refer indicatively to:

1. the initiatives taken by the USA for access to passengers' personal data (PNR) when flying to the USA as well as the new legislative regulations for the incorporation of biometric data in visas.

¹⁾ Attorney at Law, Athens. DEA in Public International Law (Paris I). Auditor at the Data Protection Authority.

²⁾ The current paper is a contribution to the one-day conference "Problems and Special Regulations for the Protection of Categories of Personal Data" which took place on 24.01.2005 at the Society for Judicial Studies and organised jointly by the Italian Cultural Institute in Athens, the Garante per la Protezione dei Dati Personali and the Greek Data Protection Authority. The paper echoes the writer's personal views. Translation from Greek by Vilemini Sosoni.

2. the EU initiatives for the incorporation of biometric data in the new uniform EU citizens' passports³ and visas and for the creation of an electronic Visa Information System (VIS)⁴.
3. the European "Hague Programme"⁵ for the free exchange of information among police services and the maximal use of information systems such as SCHENGEN, EUROPOL, EURODAC, EUROJUST, etc.

The issue, however, is not straightforward. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁶ does not apply to the area of police cooperation and, in general, to the Third Pillar.

As a result, the protection of personal data in these areas is regulated by the national legislation of the Member States or it constitutes the object of specific international agreements, like the Schengen Agreement and the Convention for its implementation, the EUROPOL Convention and the decisions for the set-up of EURODAC⁷ and EUROJUST⁸, where there are special provisions for the protection of data.

In Greece, Law 2472/97 *on the Protection of Individuals with regard to the Processing of Personal Data*⁹ also applies to the records of the Third Pillar.

The present paper sets out to present the "jurisprudence" of Hellenic Data Protection Authority in the area of public security, by focusing on three representative cases which have different characteristics but deal with topics of an international character.¹⁰

I. The case of the biometric data processing pilot project by the International Athens Airport "ELEFThERIOS VENIZELOS"

A. At the "time of security", new technologies are required to play an increasingly important role. Among them, the science of biometrics seems to have taken the lion's share.

The collection, storage and processing of biometric data is particularly useful at the time of security, because it allows for the most accurate verification of the identity of the holder of papers or user of high risk services.

It is, therefore, clear why security services opt for biometric technologies. We have already referred to the relevant initiatives undertaken by the EU and the USA.

Nevertheless, the processing of biometric data involves significant compatibility problems in relation to fundamental principles which permeate the protection of the personality of individuals who undergo such processing. This is due to the fact that the processing of biometric data, besides the inevitable psychological associations that it evokes (until recently fingerprint taking was mainly linked to criminal activities, thus the term "*branded*"), can lead to situations that may easily get out of hand and divert from the stated aim of the scientific verification of identity to different forms of scientific testing of the personality or the behaviour of social groups.

Research centres, especially in the USA, have already started to carry out research, still in its infancy or based on pilot projects, which involves the additional processing of biometric data, aiming at extracting data which can lead to information regarding the health or psychological state of individuals. There are also different types of research which aim at designing monitoring devices for the collection of the biometric characteristics of randomly selected individuals in public areas, which, in turn, can lead to their identification through central databases of biometric information.

All the above explain why the processing of biometric data should be approached cautiously and why the examination of such issues should not be just technical, even in cases where the right at stake is minor.¹¹

B. In the case under attention, the Data Protection Authority was asked to issue a decision regarding the lawfulness of the pilot project, financed by the EU, which was going to be put into practice by the airports of Athens and Milan and was aiming at faster customer screening during check-in and boarding.

More specifically, the International Athens Airport "ELEFThERIOS VENIZELOS" submitted, as was its duty, notification no. 2055/29.08.03 concerning the implementation of a pilot European-level project in collaboration with the International Airport at Milan, ALITALIA Airlines and International Air Transport Association (IATA). The basic aim of the project is the establishment of a biometric model for identity verification of registered passengers during departure from the airport.

The system presents the following characteristics:

- a) It is based on the processing of finger and iris biometric characteristics.
- b) Participation is voluntary, i.e. the condition for the data subject's consent is fulfilled.
- c) The passengers' data, including the selected biometric data, are stored in smart cards which they carry with them.
- d) The data are not stored in a central database.

The process envisaged by the project is the following: the finger and iris biometric characteristics of the passengers who have agreed to take part in the project are stored in a smart card. During the two stages of the process, i.e. during check-in and boarding, the passenger is asked to insert the smart card in the special card reader and at the same time place his/her finger on the fingerprint taking device and look into

³⁾ European Commission, *Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports* [COM (2004) 116 final – 2004/0039 (CNS) / 18.02.2004].

⁴⁾ *Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC)* [L 213 of 15 June 2004, p. 5]. See also *Opinion 7/2004 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data which was set up with Article 29 of the Directive 95/46/EC (Article 29 Working Party)*. Access to the Article 29 Working Party's decisions is through the webpage www.europa.eu.int/Commission/InternalMarket/DataProtection/Art.29.

⁵⁾ See Council of European Union, *Presidency Conclusions 4 & 5 November 2004, Annex I* (14292/04 – CONCL 3 / 5.11.2004 p. 11).

⁶⁾ L281of 23.11.1995, p.31.

⁷⁾ *Council Regulation 2725/2000 of 11.12.2000* [L 316 of 15.12.2000 p. 1].

⁸⁾ *Council Decision of 28.02.2002 (2002/187/JHA)* [L 63 of 6.03.2002 p. 1].

⁹⁾ Government Gazette A50.

¹⁰⁾ The decisions of Hellenic Data Protection Authority can be retrieved from the website www.dpa.gr.

¹¹⁾ For the processing of biometric data, see Working Document by the Article 29 Working Party on Biometrics of 1.08.2003.

the special iris reading camera. The system automatically compares the characteristics it reads with the ones already stored in the card and identifies the passenger.

It is a rather "mild" form of biometric data processing, since there is no central database of the data involved.

C. With decision no. 52/2003, the Data Protection Authority initially invoked the principle of necessity (Article 4, paragraph 1, point b, Law 2472/97) and then found that the suggested processing was not lawful, because the purpose sought with the above-mentioned method could be achieved in a milder way *"with the passenger showing the identity card along with the ticket and the boarding card"*.

The particularity of the decision in question lies in the fact that the Authority used the principle of proportionality in order to prohibit the project, simply because the purpose could be achieved with milder traditional means. In other words, the Authority foresaw a particular danger in the idea of biometric data processing and took a negative stance towards it, despite the fact that the undertaking did not aim at the protection of security nor did it include the creation of a central database. Therefore, there was no danger of further illegal processing. What is more, the participation in the project was on a voluntary basis and the consent of the participating passengers was a prerequisite.

One could ask whether the Authority would have decided differently in case it was stated that the purpose of the processing was the security of the passengers or flights. Could it be possible then to invoke the principle of necessity or even the principle of proportionality, in order to find the processing unlawful? Or would the Authority have to find the processing lawful in the name of legal realism in combination with the system's mild technical specifications?

The question comes to reveal the importance of the purpose of processing in the legal system of personal data protection, since a decision on the lawfulness or not of a certain processing is always closely related to the stated or presumed purpose.

Still, in the case under attention, under the light of the initial thoughts set out in relation to the processing of biometric data, we deem that the Authority's decision was right. This is due to the fact that since the Authority is by nature an independent intermediary institution of the civil society and has an educational role, it chose, in the case under attention, to use this institutional particularity.

II. Olympic Games Security

A. As it might be clear to everybody, the organisation and delivery of the Athens 2004 Olympic Games led the government to implement an organised security scheme, which included, among others, measures which affected directly the citizens' personal data.

The Data Protection Authority followed the matter closely right from the beginning and had the chance to intervene in many cases for the sake of the citizens. We indicatively refer to the set-up of a record of accreditations by the Olympic Games Security Division (OGSD) of Hellenic Police, the operation of a zeppelin and two helicopters equip-

ped with TV circuit, the installation of CCTV on Olympic venues and the installation of CCTV on the Athens (Attica) road network.

In the present paper, we will focus on the last case, which received more attention than any other case due to its special character which is not linked just to the delivery of the Olympic Games, since it does not only involve the Olympic venues, but is extended to the entire road network of Athens.

B. In conformity with Article 6 of Law 2472/97, the Olympic Games Security Division (OGSD) notified the Authority of the installation of the relevant system. In the initial notification, the OGSD noted that the purpose of processing was not only the regulation of traffic circulation, but also the *"direct intervention of public authority in cases of unlawful acts against individuals and goods"*, stressing the necessity for taking measures in view of the Olympic Games. The notification referred to 293 cameras installed on the entire road network of Athens.

The Authority, based on the principles of necessity and proportionality, issued Decision no. 28/2004. It explicitly referred to Article 1 of the 1122/2000 Directive for CCTV, which stipulates that *"recording and processing of personal data by a closed circuit television operating on a regular, continuous or permanent basis is prohibited, because it may infringe on individuals' right to privacy"*. In addition, it accepted that the secure delivery of the Olympic Games justifies taking of special measures, under strict conditions. In particular, it points out that *"given the need for the secure and successful delivery of the Olympic Games, as well as the large numbers of visitors, the need for smooth traffic circulation and the protection of individuals during the 2004 Olympic and Paralympic Games constitute a priority"*. Consequently, it is deemed that the above-mentioned criteria of lawfulness [proportionality – necessity] are met during the period that is considered to be the Operational Stage of the Olympic Games (...).

The conditions set by the Authority for the lawful operation of the system are the following:

- It must operate in such a way that taking and recording pictures of the entrance or the interior of houses is not possible.
- It must operate in such a way that taking and listening to the conversations of neighbours or passers-by is not possible.
- For every one of the cameras, before the person enters its range, he/she must be informed through an adequate number of discernible signs in conspicuous positions, that he/she enters an area that is monitored, and also of the purpose of monitoring.
- The technical security measures must be kept unswervingly.
- The data are kept for a maximum of 7 days.

Finally, the system's lawful operation is set to be from 1 July 2004 to 4 October 2004, i.e. until the end of the Paralympic Games.

C. Still, the most interesting aspect of this case involves the operation of cameras after 4 October 2004.

The State has recurrently expressed, directly or indirectly, through the competent authorities, its wish to continue the operation of the system. When OGSD submitted on 4 October 2004 an application to continue the operation of the system, it stated as the exclusive purpose of the processing the regulation of traffic circulation, without making any reference to security issues.

In that case, Decision no. 63/2004 of the Authority is characterised by a strict examination of the legal basis of data processing through the use of CCTV.

First of all, it expressly refers to Opinion no. 4/2004 of the Article 29 Working Party,¹² according to which *"the over-proliferation of image acquisition systems in public and private areas should not result in placing unjustified restrictions on citizens' rights and fundamental freedoms; otherwise, citizens might be actually compelled to undergo disproportionate data collection procedures which would make them massively identifiable in a number of public and private places"*. It also stresses that *"the rapid development of technology brings us before situations which may constitute a particularly severe personality insult and unjustifiably shrink citizens' rights. There are, for example, technical systems capable of combining image recording with studying and the predictability of human behavior, so as to move from the known form of "static" surveillance to "dynamic-precautionary" surveillance forms"*.

It also states that the legal basis for examining the issue consists, among others, of the following:

- Article 8 of the European Convention on Human Rights for the Protection of private life.
- Convention 108/1981 of the Council of Europe for the protection of Individuals with regard to Automatic Processing of Personal Data.
- Articles 7 (protection of private life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union.
- Articles 9 and 9^A of Hellenic Constitution.

Based on the above, the Authority reaches the decision that *"the purpose for which the operation license of the closed circuit of TV system on the road network of the Prefecture of Attica is being asked, that is regulating the circulation of vehicles, is lawful only under specific conditions, under which it will be insured that the system is not used for other purpose and no other departments of the Hellenic Police is using it than the ones legally assigned the regulation of the circulation of vehicles"* and sets strict conditions for the temporary use of the system (for a 6-month period).

We consider that the most important condition is the removal of specific cameras (32 of them are expressly referred to in the decision) which are installed on areas that were not justifiable by the purpose that was invoked (like pedestrian zones, small junctions around universities, squares and parks, etc.).

The rest of the conditions are following:

- The system should operate exclusively for the purpose of regulating the traffic of vehicles. Using the system and utilizing the data, collected through the system and recorded on it, for any other reason is forbidden, including discovering offences, other than those related to the regulation of circulation.
- Taking and recording pictures of the entrance or the interior of houses is prohibited.
- Taking and recording sound is prohibited. Therefore, microphones must be taken off the poles, on which they are set.
- The operation of cameras is prohibited when the traffic of vehicles is interrupted, i.e. during manifestations, demonstrations etc.
- The system must be supervised and controlled only by the Operations Room for the Monitoring and Control of Circulation of the Traffic Police Headquarters and no other Department will have access to it, than the Traffic Police Headquarters.
- Transmitting data to third parties is prohibited.
- The data will be kept for seven days at the most, after the passage of which, the data will have to be deleted.
- For every camera, before the person enters its range, he/she must be informed, with an adequate number of discernible signs in conspicuous positions, that he/she enters an area that is monitored, and also of the purpose of monitoring.

We believe that with the above decision, the Authority fulfilled its role, as described earlier, since it followed a meaningful approach to this particularly sensitive issue, an approach which respects and protects the citizens' rights to the greatest possible extent.

III. PNR

A. The least understood of all of the Authority's decisions which has also been severely criticised is the one involving the transfer of passengers' data to the USA customs authorities.

Olympic Airways submitted an application to the Authority, asking it to grant a permit for the transfer of passengers' data to the USA, in accordance with Article 9 of Law 2472/97.

In particular, after the 2001 Aviation & Transportation Act came into force in the USA, the Department of Homeland Security – Bureau of Customs and Border Protection "CBP" requires that all airline companies which operate flights to and from the USA or pass through them grant it the access to the Passenger Manifests, known as PNR (Passenger Name Record)¹³, before each flight's arrival to USA airports, in order to facilitate prior passenger control with a view to guaranteeing the safety of flights and preventing terrorist activities. American authorities gain access to PNRs through the electronic system APIS (Advanced Passenger Information System) by using an online pull system of data.

¹²⁾ The Article 29 Working Party has a consultative character and consists of one representative from the Data Protection Authority of each Member State of the EU. For access to the Working Party's Decision see Footnote 4.

¹³⁾ There are 34 data included in PNRs and these appear in tabular form in Annexe A of the European Commission's Decision of 14.05.2004 (See Footnote 17).

According to Article 9 of Law 2472/97, the transfer of personal data to a non-EU country shall be permitted only following a permit granted by the Authority. The Authority may grant such a permit only if it deems that the country in question ensures an adequate level of personal data protection.

This provision is, in fact, the incorporation into Greek law of the corresponding Article 25 of Directive 95/46/EC which stipulates that:

"1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. (...)

3. (...)

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

The Member States shall take the measures necessary to comply with the Commission's decision."

The particularity of Greek law lies in the fact that the transfer of personal data to non-EU countries requires a permit granted by the Authority.

B. The issue has already been dealt with by the European Commission and the EU's Data Protection Authorities in the framework of the Article 29 Working Party.

Within the framework of its competence and in compliance with Directive 95/46/EC, Article 25, paragraph 6, the Commission, following the procedure of the EC Treaty, Article 300, has negotiated with the USA competent authorities (DHS) in order to come up with a commonly accepted solution.

For that reason, following the Olympic Airways request, the Authority has issued a temporary decision (Decision no. 4/2004), which took into account the financial, commercial and political position in which OA is found as well as the forthcoming developments at an international level, and granted a temporary three-month permit, on the condition that passengers are previously informed and give their consent.

In May 2004, the picture was no longer blurred. The negotiations led to a bilateral agreement, approved by the Council.¹⁴ Subsequently, the Commission with its Decision of 14 May 2004¹⁵ decided that:

"For the purposes of Article 25(2) of Directive 95/46/EC, the United States' Bureau of Customs and Border Protection (CBP) is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States (...)".

Consequently and in compliance with Directive 95/46/EC, Article 25, paragraph 6, the Authority had to follow the Commission's decision.

To that end, the Authority issued Decision no. 67/2004 which grants the Olympic Airways a three-year¹⁶ permit, on the condition that passengers are informed according to the suggestions made by the Article 29 Working Party in its Opinion of 8/2004.¹⁷

The Authority had no longer the discretion to examine whether or not there was an adequate level of protection. It followed circumscribed powers, since as it is expressly stipulated in the law, the Authority can decide on the level of protection only if the predominantly competent institution, i.e. the European Commission, has not done so yet. If the level of protection is considered to be adequate, the Authority is simply required to issue the grant. The only ability that it has is to set additional conditions with a view to strengthening protection in the Greek territory, to the measure that each case is different and as long as they do not run contrary to the European law.

C. It is interesting to look at the criticism that this decision received.

It is also interesting that the Authority's Decision in fact includes this criticism, since the most important arguments have been posed during the discussion of the case, as it emerges from the minutes of the meeting.

a) The first argument is of a constitutional nature and focuses on the constitutionally established right for the protection of personal data. Does the Constitution have supremacy over Community law? Although the issue has been dealt with on many occasions by the European Court of Justice,¹⁸ which ruled in favour of Community law, it is lawful to raise objections, especially when dealing with the very sensitive area of personal rights. When a civil case or a commercial right is violated, the undermining of the supremacy of Community law would not stand many chances of becoming acceptable both legally and socially. But when civil rights are at stake, every opinion that tends to defend their primacy – even if it is *contra legem* – is acceptable, respected and should

¹⁴ See Council Decision of 17.05.2004 (2004/496/EC) [L 183 of 20.05.2004, p. 83] where the full text of the Agreement can be found in the Annexe.

¹⁵ Commission Decision of 14.05.2004 (2004/535/EC) [L235 of 6.07.2004, p. 11].

¹⁶ Article 7 of the Commission's Decision stipulates that it ceases to be valid 3 years and six months after its notification date.

¹⁷ For PNR issues, the Article 29 Working Party has issued during the whole time of the negotiations Opinions nos 6/2002, 4/2003, 2/2004 and 6/2004.

¹⁸ See: *Stauder* 29/69, Coll. 1970, 419, *Internationale Handelsgesellschaft* 11/70, Coll. 1970, 1135, *Simmenthal II* 106/77, Coll. 1978, 629, *Hauer* 44/79, Coll. 1979, 3727, *Verholen* C-87,88,89/90, Coll. 1991, I-3757 etc.

be set at the table for discussion. And when deciding for or against the acceptability of a given opinion, strong legal arguments should always be used.

As an answer to that argument, the Authority points out that it does not solely act as a public authority, but as an authority the competence of which is based on the Constitution. The constitutional right of personal data protection is guaranteed, as is expressly stated in Article 9^A, through the competence of the Authority which was set up and operates in accordance with Law 2472/97 for the protection of personal rights. In turn, Law 2472/97 incorporated the European law into the Greek law.

b) The second argument focuses on the legal nature of the applicable European law act. According to this argument, the direct or indirect application of the European law should be decided in relation to the nature and scope of the applicable act, i.e. to the particular case of the bilateral agreement. In that sense, if an agreement, drawn in accordance with Article 300 of the EC Treaty, goes against the Treaty and its fundamental rights, among which is the respect for human rights and fundamental freedoms, the institutions and Member States should not implement it.

Still, it is difficult to understand how an act which derives from the procedures provided for by the Treaty and Directive on the protection of a fundamental right can go against the Treaty and the principle of respect for human rights and fundamental freedoms. The Directive sets the scope and the conditions for the protection. It provides for ways of remedy, at the European level, in cases where these conditions are not met. It also provides for the competent authority at the European level to decide whether the conditions are met and what procedure should be followed. The final act does not only regulate a situation protected differently by the Treaty and the Directive; it owes its legal grounding to that particular Directive and that particular Treaty.

CONCLUSION

The Authority's role is hard. By nature, it stands between the Citizen on the one hand, and the State (or the private sector) on the other, and it is often the recipient of attacks from both sides.

The last two cases, as referred to in this paper, are typical examples of this attack. On the one hand, some citizens believed that the Authority did not adequately protect their rights. On the other hand, controllers thought that the Data Protection Authority, with the conditions that it set, significantly restricted their effectiveness.

What should be made clear, however, is the fact that the Data Protection Authority is an independent administrative authority. And independent administrative authorities are the institutional fruit of the civil society. Independent Administrative Authorities were developed historically (since the time of the first ever Ombudsman) in order to meet the needs of the civil society in parallel with the State and opposite the State, in the same way that the civil society was born, gained momentum and was legalized in parallel with the State and opposite the State. Independent Administrative Authorities met the needs that the State could not and was not legalized to meet, and which they were required to meet by using alternative ways of thought and action.

The role of independent authorities is in fact mediatory and it takes shape depending on the powers (consultative, ruling, auditory, regulatory) assigned to them by law.

The Data Protection Authority was formed to defend citizens against the State or against the private sector from the illegal or disproportionate processing of data which violate their privacy. It's not, however, an activist organisation. It is the fruit of the civil society, but it is not a non-governmental organisation. It acts and takes action within the framework of the law; its *raison d'être* lies in the law and it is held accountable depending on the lawfulness of its actions.

It is in that light that the Authority's work should be viewed. And it should always be borne in mind that in this "time of security" its role is crucial and of utmost importance, if the words of the famous Greek poet Odysseas Elytis (Nobel Prize 1979) "*When you hear «order» human flesh smells*"¹⁹ are to be avoided.

Philippos Mitleton¹

Bezpieczeństwo publiczne a ochrona danych osobowych²

WSTĘP

Konflikt między prawem do ochrony danych osobowych a „prawem do bezpieczeństwa” jest kwestią szczególnie zajmującą, nie tylko dlatego, że dotyczy samego sedna problemu ochrony praw osobistych, lecz także dlatego, że wpływa na codzienne życie każdego, kto musi wybierać między technologią – oferującą coraz bardziej zaawansowane sposoby osiągania niedefiniowalnej formy bezpieczeństwa, a życiem prywatnym – którego przestrzeń nieustannie ulega zawężeniu.

Koncepcja bezpieczeństwa publicznego, do której odwołujemy się w niniejszym artykule, dotyczy inicjatyw politycznych oraz środków podjętych na poziomie rządowym (zarówno krajowym, jak i międzynarodowym) głównie w celu ochrony przed działalnością terrorystyczną oraz w ramach ponadpaństwowej współpracy w walce z terroryzmem.

Oczywiste jest, że wszystkie te działania odwołują się niejako do daty 11 września. Dokonane w tym dniu ataki doprowadziły do serii inicjatyw prowadzących, w imię bezpieczeństwa, do „kontrolowanego ograniczenia praw”.

¹⁹⁾ Odysseas Elytis "Maria Nefeli", 1978.

¹⁾ Adwokat, Ateny. Dyplom DEA Międzynarodowe prawo publiczne (Paryż I). Biegły rewident w Urzędzie ochrony danych.

²⁾ Niniejszy artykuł stanowi wkład autora w jednodniową konferencję „Problemy i przepisy szczególne doty-

Wobec nieznanych ewentualności nikt nie zaprzecza odczuwanym przez siebie obawom i oczywiście nikt też nie może brać na siebie odpowiedzialności za niewłaściwą politykę w dziedzinie bezpieczeństwa. A jednak nie pozostaje nam nic innego, jak tylko zauważyć, że „społeczeństwo otwarte” nie jest już tym, czym było niegdyś oraz że wszystkie inicjatywy podejmowane z myślą o transformacji ku „społeczeństwu bezpiecznemu” są tak „nieodparte”, że nie zostawiają przestrzeni dla wysłuchania przeciwnych im poglądów.

Na poziomie międzynarodowym w sposób poglądowy chcielibyśmy odwołać się tu do następujących elementów:

1. Inicjatywy podjęte przez USA w celu dostępu do danych osobowych pasażerów (PNR), podczas przelotów do USA, jak również nowe przepisy ustawodawcze w sprawie włączania danych biometrycznych do wiz.
2. Inicjatywa UE w sprawie włączenia danych biometrycznych do nowych, zuniформizowanych paszportów³ obywateli UE i wiz oraz w sprawie utworzenia elektronicznego systemu informacji wizowej (VIS).⁴
3. Europejski „Program haski”⁵ w sprawie swobodnej wymiany informacji wśród służb policyjnych oraz maksymalnego wykorzystania systemów informacyjnych, takich jak Schengen, Europol, Eurodac, Eurojust itp.

Kwestia nie jest jednak tak prosta. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób prywatnych w zakresie przetwarzania danych osobowych oraz w sprawie swobodnego obiegu tychże danych⁶ nie ma zastosowania do obszaru współpracy policyjnej ani w ogóle do Trzeciego Filaru.

W rezultacie ochronę danych osobowych w tych obszarach reguluje ustawodawstwo krajowe Państw Członkowskich lub też stanowi ona przedmiot stosownych porozumień międzynarodowych, takich jak Układ z Schengen i Konwencja wykonawcza do tego układu, Konwencja o Europolu oraz decyzje powołujące EURODAC⁷ i EUROJUST⁸, w których zawarte są szczególne postanowienia dotyczące ochrony danych.

W Grecji ustawa 2472/97 o ochronie osób fizycznych w zakresie przetwarzania danych osobowych⁹ ma również zastosowanie do akt w obrębie trzeciego filaru.

Niniejszy artykuł, koncentrując się na trzech reprezentatywnych przypadkach o różnych cechach, z których jednak każdy dotyczy kwestii o charakterze międzynarodowym,¹⁰ ma na celu przedstawienie linii orzecznictwa greckiego Urzędu ochrony danych w obszarze bezpieczeństwa publicznego.

³) Komisja Europejska, projekt rozporządzenia Rady w sprawie norm dla funkcji bezpieczeństwa i biometrii w paszportach obywateli UE [COM (2004) 116 wersja ostateczna - 2004/0039 (CNS)/18 luty 2004 r.].

⁴) Decyzja Rady z dnia 8 czerwca 2004 r. ustanawiająca System Informacji Wizowej (VIS) (2004/512/WE) [L 213 z dnia 15 czerwca 2004, str. 5]. Zobacz także: opinia 7/2004 Grupy Roboczej w sprawie ochrony osób prywatnych w zakresie przetwarzania danych osobowych wydana na podstawie art. 29 Dyrektywy 95/46/WE (Grupa Robocza Art. 29). Dostęp do decyzji Grupy Roboczej Art. 29 pod adresem www.europa.eu.int/Commission/InternalMarket/DataProtection/Art.29.

⁵) Patrz Rada Unii Europejskiej, Wnioski z Prezydencji 4 i 5 października 2004 r., załącznik I (14292/04 - CONCL 3 / 5 listopad 2004 r., str. 11).

⁶) L281 z dnia 23 listopada 1995 r., str. 31.

⁷) Rozporządzenie Rady 2725/2000 z dnia 11 grudnia 2000 r. [L 316 z dnia 15 grudnia 2000 r., str. 1].

⁸) Decyzja Rady z dnia 28 lutego 2002 r. (2002/187/JHA) [L 63 z dnia 6 marca 2002 r., str. 1].

⁹) Dz.U. A50.

¹⁰) Decyzje Greckiego Urzędu Ochrony Danych znaleźć można na stronie internetowej www.dpa.gr.

I. Sprawa projektu pilotażowego przetwarzania danych biometrycznych przez międzynarodowy port lotniczy w Atenach „ELEFTHERIOS VENIZELOS”.

A. Oczekuje się, że w „okresie bezpieczeństwa” nowe technologie odgrywać będą coraz większą rolę. Wydaje się, że znaczącą rolę odgrywa tu biometria.

Zbieranie, przechowywanie i przetwarzanie danych biometrycznych jest szczególnie użyteczne w „okresie bezpieczeństwa”, pozwala bowiem na najdokładniejszą weryfikację tożsamości posiadacza dokumentów lub użytkownika usług wysokiego ryzyka.

Jest zatem jasne, dlaczego służby bezpieczeństwa optują za technologiami biometrycznymi. Przytoczyliśmy już odpowiednie inicjatywy UE i USA.

Niemniej jednak przetwarzanie danych biometrycznych łączy się ze znacznymi problemami zgodności w związku z podstawowymi zasadami leżącymi u podstaw ochrony osób fizycznych, których dane są przetwarzane. Wynika to z faktu, że przetwarzanie danych biometrycznych, oprócz nieuchronnych skojarzeń psychologicznych, jakie wywołuje (jeszcze do niedawna odciski palców pobierano głównie w związku z działalnością przestępczą, stąd też termin „napiętnowany”), może prowadzić do sytuacji, które łatwo mogą się wymknąć spod kontroli i zamiast – zgodnie z deklarowanym celem – zmierzać w kierunku naukowej weryfikacji tożsamości, zboczyć w stronę różnego rodzaju form naukowego testowania osobowości lub badania zachowań grup społecznych.

W ośrodkach badawczych, głównie w USA, badania takie już się rozpoczęły, choć znajdują się jeszcze na etapie wstępnym lub opierają się na projektach pilotażowych, obejmujących dodatkowe przetwarzanie danych biometrycznych, mające na celu wyekstrahowanie danych, które mogłyby prowadzić do informacji związanych ze zdrowiem i stanem psychicznym osób fizycznych. Prowadzi się także różnego rodzaju badania, których celem jest zaprojektowanie urządzeń monitorujących, zbierających cechy biometryczne losowo wybranych osób fizycznych w miejscach publicznych, co z kolei może prowadzić do ich identyfikacji przez centralne bazy danych z informacjami biometrycznymi.

Powyższe rozważania tłumaczą, dlaczego do kwestii przetwarzania danych biometrycznych należy podchodzić ostrożnie oraz dlaczego ich analiza nie powinna być czynnością wyłącznie techniczną, nawet w sprawach dotyczących praw o niewielkim znaczeniu.¹¹

B. W rozpatrywanej sprawie Urząd ochrony danych został poproszony o wydanie decyzji w sprawie legalności projektu pilotażowego finansowanego ze środków UE, przewidzianego do wprowadzenia w życie w portach lotniczych w Atenach i Mediolanie oraz mającego na celu szybszą kontrolę podróżnych w czasie odprawy i wchodzenia na pokład.

W szczególności międzynarodowy port lotniczy w Atenach „ELEFTHERIOS VENIZELOS”, zgodnie ze swoim obowiązkiem, złożył powiadomienie nr 2055/29.08.03 w sprawie

¹¹) Odnośnie do przetwarzania danych biometrycznych, patrz dokument roboczy Grupy Roboczej Art. 29 w sprawie biometrii z dnia 1 sierpnia 2003 r.

wdrażania europejskiego projektu pilotażowego realizowanego we współpracy z międzynarodowym portem lotniczym w Mediolanie, liniami lotniczymi ALITALIA oraz Zrzeszeniem Międzynarodowego Transportu Lotniczego (IATA). Głównym celem projektu jest stworzenie biometrycznego modelu weryfikacji tożsamości zgłoszonych pasażerów podczas odlotu z lotniska.

System posiada następujące cechy:

- a) opiera się na przetwarzaniu cech biometrycznych palców i tęczy;
- b) uczestnictwo w programie jest dobrowolne, tzn. spełniony jest warunek mówiący o zgodzie posiadacza danych;
- c) dane pasażerów, w tym wybrane dane biometryczne, przechowywane są w noszonych przez nich kartach chipowych;
- d) danych nie przechowuje się w centralnej bazie danych.

Projekt zmierza do realizacji następującego procesu: cechy biometryczne palców i tęczy pasażerów, którzy wyrazili swoją zgodę na udział w projekcie, zapisywane są w karcie chipowej. W trakcie dwóch etapów projektu, tj. podczas odprawy i wchodzenia na pokład, pasażer proszony jest o włożenie karty chipowej do specjalnego czytnika kart oraz o jednoczesne ułożenie palca na czytniku odcisków palców i spojrzenie w specjalną kamerę rejestrującą obraz tęczy. System automatycznie porównuje odczytane cechy z danymi zapisanymi na karcie i identyfikuje pasażera.

Ponieważ nie ma tu centralnej bazy analizowanych danych, projekt należy uznać za dość „łagodną” formę przetwarzania danych biometrycznych.

C. W decyzji nr 52/2003 Urząd ochrony danych odwołał się na wstępie do zasady konieczności (art. 4, par. 1, lit. b ustawy 2472/97) i następnie uznał, że proponowane przetwarzanie nie jest zgodne z prawem, ponieważ cel, który próbuje się osiągnąć wspomnianą wyżej metodą, mógłby być osiągnięty w łagodniejszy sposób „przez okazywanie przez pasażerów, razem z biletem i kartą pokładową, dokumentów potwierdzających tożsamość”.

Osobliwość rozpatrywanej decyzji leży w tym, że w celu zakazania realizacji projektu, wydający ją Urząd posłużył się zasadą proporcjonalności po prostu dlatego, że cel daje się osiągnąć przez zastosowanie tradycyjnych, łagodniejszych środków. Innymi słowy Urząd przewidział szczególne niebezpieczeństwo tkwiące w idei przetwarzania danych biometrycznych i zajął w jej kwestii negatywne stanowisko, pomimo że przedsięwzięcie nie miało na celu zapewniania bezpieczeństwa ani też nie zawierało propozycji stworzenia centralnej bazy danych. Z tego powodu nie istniało zatem niebezpieczeństwo dalszego niezgodnego z prawem przetwarzania. Co więcej, uczestnictwo w projekcie było dobrowolne, a zgoda pasażerów stanowiła warunek wstępny.

Można zapytać, czy decyzja Urzędu byłaby inna w przypadku, gdyby oświadczone, że celem przetwarzania jest bezpieczeństwo pasażerów i lotów. Czy byłoby wówczas możliwe przywołanie zasady konieczności lub nawet zasady proporcjonalności w celu wykazania nielegalności przetwarzania danych? Czy też Urząd musiałby uznać przetwarzanie za zgodne z prawem w imię prawnego realizmu i w połączeniu z łagodnością stosowanych w systemie rozwiązań technicznych?

Pytanie to ujawnia znaczenie, jakie w systemie prawnej ochrony danych osobowych ma kwestia celu ich przetwarzania, ponieważ decyzja o zgodności lub niezgodności z prawem jakiegokolwiek przypadku przetwarzania zawsze ściśle wiąże się z deklarowanym lub przewidywanym celem.

Mimo to, w świetle wstępnych przemyśleń przedstawionych w związku z wykorzystywaniem danych biometrycznych, w rozpatrywanym przypadku jesteśmy skłonni uznać, że decyzja Urzędu była słuszna. Wynika to z faktu, że ponieważ Urząd [ochrony danych] z natury jest niezależną instytucją pośredniczącą społeczeństwa obywatelskiego i ponieważ posiada rolę edukacyjną, w rozpatrywanej sprawie zdecydował się skorzystać z tej szczególnej pozycji instytucjonalnej.

II. Bezpieczeństwo igrzysk olimpijskich

A. Jest faktem być może dla wszystkich oczywistym, że organizacja i przeprowadzenie olimpiady w Atenach w 2004 r. doprowadziły rząd do wdrożenia zorganizowanego systemu bezpieczeństwa obejmującego między innymi środki mające bezpośrednio wpływ na dane osobowe obywateli.

Od samego początku sprawie skrupulatnie przyglądał się Urząd ochrony danych, w wielu przypadkach mając okazję interweniować na korzyść obywateli. Dla przykładu odwołajmy się tu do powstania rejestru akredytacji prowadzonego przez jednostkę policji greckiej ds. bezpieczeństwa igrzysk olimpijskich (OGSD), do działania sterowca i dwóch helikopterów wyposażonych w system TV, a także do instalacji CCTV na terenie olimpijskim oraz w obrębie ateńskiej sieci drogowej (Attica).

W niniejszym artykule skoncentrujemy się na tym ostatnim przypadku, wzbudzającym większe niż pozostałe zainteresowanie z powodu swojego szczególnego charakteru, niezwiązanego wyłącznie z organizacją olimpiady. Nie dotyczy on bowiem tylko terenów olimpijskich, ale rozciąga się także na całą sieć drogową Aten.

B. Zgodnie z art. 6 ustawy 2472/97 jednostka ds. bezpieczeństwa igrzysk olimpijskich (OGSD) poinformowała Urząd o instalacji odpowiedniego systemu. We wstępnym powiadomieniu OGSD odnotowała, że celem przetwarzania danych jest nie tylko regulacja ruchu drogowego, ale także „bezpośrednie interweniowanie władz publicznych w przypadkach niezgodnych z prawem czynów przeciw osobom fizycznym i dobrom materialnym”, przy czym nacisk położony został na konieczność podjęcia takich środków z uwagi na igrzyska olimpijskie. Powiadomienie mówiło o 293 kamerach zainstalowanych w obrębie całej sieci drogowej Aten.

Urząd [ochrony danych], opierając się na zasadach konieczności i proporcjonalności, wydał decyzję nr 28/2004. Odwołuje się ona bezpośrednio do art. 1 Dyrektywy 1122/2000 w sprawie CCTV, zastrzegającego, że „nagrywanie i przetwarzanie danych osobowych przez systemy telewizyjnego zamkniętego obwodu działające regularnie, w sposób ciągły lub przez czas nieokreślony, jest zabronione, ponieważ może naruszać prawo osób fizycznych do prywatności”. Ponadto zgodził się on, że bezpieczne przeprowadzenie igrzysk olimpijskich uzasadnia, pod ścisłymi warunkami, podjęcie nadzwyczajnych środków. W szczególności Urząd wskazał, że „biorąc pod uwagę potrzebę bezpiecznego i pomyślnego przeprowadzenia igrzysk olimpijskich, a także dużą liczbę gości, ko-

nieczność zapewnienia płynności ruchu drogowego oraz ochrony osób fizycznych w czasie igrzysk olimpijskich i paraolimpijskich 2004 stanowi priorytet. W konsekwencji przyjmuje się, że wyżej wymienione kryteria legalności [proporcjonalność – konieczność] są spełnione w okresie uznawanym za fazę operacyjną igrzysk olimpijskich (...)”.

Wyznaczone przez władze warunki legalności funkcjonowania systemu są następujące:

- Musi on funkcjonować w taki sposób, aby nie było możliwe wykonywanie ani zapisywanie zdjęć wejść do budynków lub zdjęć ich wnętrza.
- Musi on funkcjonować w taki sposób, aby nie było możliwe rejestrowanie ani podsłuchiwanie rozmów sąsiadów lub przechodniów.
- Zanim osoba znajdzie się w zasięgu którejkolwiek z kamer, musi zostać o tym poinformowana odpowiednią liczbą łatwo zauważalnych, umieszczonych w widocznych miejscach znaków, informujących o wejściu na teren monitorowany oraz wskazujących także celu monitoringu.
- Techniczne środki bezpieczeństwa muszą być niezawodne.
- Dane przechowywane są przez okres nie dłuższy niż 7 dni.

Na koniec ustalono czas legalnego funkcjonowania systemu na okres od 1 lipca 2004 r. do 4 października 2004 r., tj. aż do zakończenia paraolimpiady.

C. Mimo to najbardziej interesujące aspekty tego przypadku dotyczą działania kamer po 4 października 2004 r.

Pośrednio lub bezpośrednio, poprzez właściwe organy, państwo wielokrotnie wyrażało swoje życzenie utrzymania funkcjonowania systemu. Gdy w dniu 4 października 2004 r. OGSD złożyła podanie o przedłużenie działania systemu, jako jedyny cel przetwarzania podała regulację ruchu drogowego, nie czyniąc jakichkolwiek odniesień do kwestii bezpieczeństwa.

W sprawie tej podjętą przez Urząd decyzję nr 63/2004 charakteryzuje ścisła analiza podstaw prawnych kwestii przetwarzania danych z wykorzystaniem CCTV.

Przede wszystkim decyzja odwołuje się bezpośrednio do opinii nr 4/2004 Grupy Roboczej Art. 29,¹² zgodnie z którą „nadmierne rozprzestrzenianie się systemów pozyskiwania obrazu w miejscach publicznych i prywatnych nie powinno skutkować nieuzasadnionym ograniczaniem praw i podstawowych wolności obywateli; w przeciwnym przypadku obywatele ci mogą być zmuszeni do przechodzenia przez nieproporcjonalne procedury pozyskiwania danych, co masowo uczyniłoby ich rozpoznawalnymi w wielu publicznych i prywatnych miejscach”. Podkreśla też, że „szybki rozwój technologii stawia nas w obliczu sytuacji mogących stanowić szczególnie ostre naruszenie praw jako osoby i w sposób nieuzasadniony ograniczać prawa obywatelskie. Istnieją, na przykład, systemy techniczne zdolne do kojarzenia nagrania obrazu z analizą i prognozowaniem ludzkich zachowań, tak by od znanych «statycznych» form nadzoru przejść do ich form «dynamicznie-zapobiegawczych»”.

¹²⁾ Grupa Robocza Art. 29 ma charakter konsultacyjny, w jej skład wchodzi po jednym przedstawicielu organów ochrony danych każdego z Państw Członkowskich UE. Na temat dostępu do decyzji Grupy Roboczej patrz przypis 4.

Decyzja stwierdza też, że podstawę prawną do badania sprawy stanowią m.in. następujące dokumenty:

- Art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka, w sprawie ochrony życia prywatnego.
- „Konwencja Rady Europy” nr 108/1981 o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych.
- Art. 7 (poszanowanie życia prywatnego) i 8 (ochrona danych osobowych) „Karty praw podstawowych Unii Europejskiej”.
- Art. 9 i 9^A Konstytucji Grecji.

W oparciu o powyższe Urząd podejmuje decyzję, że „cel, dla którego wystąpiono o zgodę na działanie systemu telewizji zamkniętego obwodu w sieci drogowej prefektury Attica, to jest regulacja ruchu pojazdów, jest zgodny z prawem tylko pod szczególnymi warunkami, na mocy których zapewnione będzie, że system nie jest wykorzystywany do innych celów oraz że nie korzystają z niego żadne inne wydziały policji greckiej oprócz tych, które prawnie powołane są do regulowania ruchu pojazdów” oraz wyznacza surowe warunki tymczasowego korzystania z systemu (na okres 6 miesięcy).

W naszej opinii najistotniejszym warunkiem jest usunięcie części kamer (z których 32 zostały wyraźnie wymienione w decyzji), które zainstalowane są w obszarach niepodlegających przywołanemu uzasadnieniu (np. strefy ruchu pieszego, niewielkie skrzyżowania wokół uniwersytetów, place, parki itp.).

Pozostałe warunki są następujące:

- System powinien działać wyłącznie dla celów regulacji ruchu pojazdów. Używanie systemu i wykorzystywanie zbieranych oraz rejestrowanych przez system danych dla jakichkolwiek innych celów jest zabronione, co obejmuje również wykrywanie przestępstw innych niż związane z regulacją ruchu.
- Zabrania się wykonywania i rejestrowania zdjęć wejść do budynków lub zdjęć ich wnętrza.
- Zabrania się nagrywania i rejestrowania dźwięku. Z tego powodu należy zdemonstrować mikrofony ze słupów, na których je umieszczono.
- W przypadku przerwy w ruchu pojazdów, np. w czasie manifestacji, demonstracji itp., działanie kamer jest zabronione.
- System musi być nadzorowany i kontrolowany wyłącznie przez centralę monitoringu oraz kontroli ruchu komendy głównej policji drogowej; za wyjątkiem komendy głównej policji drogowej nie może mieć do niego dostępu żaden inny wydział.
- Zabrania się przekazywania danych osobom trzecim.
- Dane należy przechowywać przez okres co najwyżej 7 dni, po upływie których dane należy skasować.
- Zanim osoba znajdzie się w zasięgu którejkolwiek z kamer, musi zostać o tym poinformowana odpowiednią liczbą łatwo zauważalnych, umieszczonych w widocznych miejscach znaków, informujących o wejściu na teren monitorowany oraz wskazujących celu monitoringu.

Ponieważ w tej szczególnie drażliwej kwestii Urząd zajął wiele mówiące stanowisko, prezentując podejście, które w największym możliwym stopniu respektuje i zabezpie-

cza prawa obywateli, w naszej opinii, podejmując powyższą decyzję, władze spełniły swoją rolę tak samo jak to już wcześniej opisano.

III. PNR

A. Spośród wszystkich decyzji Urzędu [ochrony danych] najmniej zrozumiałą i będącą również przedmiotem ostrej krytyki jest decyzja dotycząca przekazywania amerykańskim organom celnym danych pasażerów.

Linie lotnicze Olympic przedłożyły Urzędowi podanie, w którym zwracają się z prośbą o przyznanie pozwolenia na przekazywanie danych pasażerów do USA zgodnie z art. 9 ustawy 2472/97.

W szczególności w USA, od czasu wejścia w życie, w roku 2001, ustawy o lotnictwie i transporcie, Departament Bezpieczeństwa Wewnętrznego – Biuro Cel i Ochrony Granic wymaga, aby wszyscy przewoźnicy lotniczy, obsługujący loty do oraz z USA, lub takie, które odbywają się przez terytorium Stanów Zjednoczonych, przed każdym przylotem do portu lotniczego położonego na terenie USA zagwarantowali mu dostęp do listy pasażerów znanej jako PNR (Imienny Rejestr Pasażerów)¹³ w celu ułatwienia wcześniejszej kontroli pasażerów i mając na uwadze zapewnienie bezpieczeństwa lotów oraz zapobieganie działalności terrorystycznej. Organy amerykańskie uzyskują dostęp do PNR poprzez system elektroniczny APIS (zaawansowany system informacji o pasażerach), korzystając z internetowej bazy danych w systemie „pull”.

Zgodnie z art. 9 ustawy 2472/97, przekazywanie danych osobowych państwu spoza UE dozwolone jest tylko po uzyskaniu wydanego przez Urząd [ochrony danych] zezwolenia. Urząd może wydać takie zezwolenie tylko wtedy, gdy uzna, że rozpatrywane państwo zapewnia odpowiedni poziom ochrony danych osobowych.

Postanowienie to stanowi w gruncie rzeczy włączenie do prawodawstwa greckiego stosownego art. 25 Dyrektywy 95/46/WE, przewidującego, co następuje:

„1. Państwa Członkowskie zapewniają, że przekazywanie do państwa trzeciego danych osobowych, podlegających przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu, nastąpi tylko wówczas, gdy niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów niniejszej Dyrektywy, dane państwo trzecie zapewni odpowiedni stopień ochrony.

2. (...)

3. (...)

4. Jeżeli Komisja stwierdzi, na podstawie procedury przewidzianej w art. 31 ust. 2, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony w rozumieniu ust. 2 niniejszego artykułu, Państwa Członkowskie podejmą konieczne środki, aby nie dopuścić do przekazania jakichkolwiek danych tego samego rodzaju do wspomnianego państwa trzeciego.

5. We właściwym czasie Komisja przystąpi do negocjacji w celu rozwiązania sytuacji problemowej stwierdzonej na podstawie ust. 4.

6. Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia prawidłowy stopień ochrony w rozumieniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji określonych w ust. 5, w zakresie ochrony życia prywatnego i podstawowych praw oraz wolności osób fizycznych.

Państwa Członkowskie podejmują środki niezbędne w celu wykonania decyzji Komisji.”

Osobliwość prawa greckiego charakteryzuje się tym, że przekazywanie danych osobowych do państw poza UE wymaga zgody wydanej przez Urząd.

B. W ramach Grupy Roboczej Art. 29 kwestią zajmowała się już Komisja Europejska i organy ochrony danych UE.

W obrębie swoich kompetencji i zgodnie z Dyrektywą 95/46/WE, art. 25, par. 6, Komisja, opierając się na procedurach „Traktatu UE”, art. 300, podjęła negocjacje z właściwymi organami amerykańskimi (DHS) w celu osiągnięcia wspólnie akceptowanego rozwiązania.

Z tego też powodu, w odpowiedzi na żądanie linii lotniczych Olympic, Urząd wydał decyzję tymczasową (decyzja nr 4/2004), która uwzględniając finansową, handlową i polityczną sytuację, w jakiej znajduje się OA oraz zbliżające się wydarzenia międzynarodowe, przyznała tymczasowe – trzymiesięczne pozwolenie, stawiając jako warunek wcześniejsze poinformowanie pasażerów o procedurze oraz wyrażenie przez nich zgody.

W maju 2004 r. sytuacja przestała być niejasna. Negocjacje doprowadziły do dwustronnego, zatwierdzonego przez Radę¹⁴ porozumienia. Następnie, decyzją¹⁵ z dnia 14 maja 2004 r., Komisja zdecydowała, że:

„Dla potrzeb art. 25 ust. 2 Dyrektywy 95/46/WE, uznaje się, że amerykańskie Biuro Cel i Ochrony Granic (CBP) zapewnia odpowiedni poziom ochrony przekazywanych ze Wspólnoty danych PNR dotyczących lotów do oraz ze Stanów Zjednoczonych (...).”

W konsekwencji oraz zgodnie z Dyrektywą 95/46/WE, art. 25, par. 6, Urząd musiał zastosować się do decyzji Komisji.

W tym celu Urząd wydał decyzję nr 67/2004, która przyznaje liniom lotniczym Olympic trzyletnie¹⁶ zezwolenie pod warunkiem stosownego informowania pasażerów zgodnie z sugestiami wyrażonymi przez Grupę Roboczą Art. 29 w jej opinii 8/2004.¹⁷

Urząd nie miał już swobody rozstrzygania w kwestii istnienia lub nieistnienia odpowiedniego poziomu ochrony. Wykonał jedynie swe ograniczone kompetencje, gdyż –

¹⁴) Patrz decyzja Rady z dnia 17 maja 2004 r. (2004/496/WE) [L 183 z dnia 20 maja 2004 r., str. 83], w załączniku do której znajduje się pełen tekst porozumienia.

¹⁵) Decyzja Komisji z dnia 14 maja 2004 r. (2004/535/WE) [L235 z dnia 6 lipca 2004 r., str. 11].

¹⁶) Art. 7 decyzji Komisji przewiduje, że zezwolenie traci swą ważność po trzech latach i sześciu miesiącach od daty jej ogłoszenia.

¹⁷) W okresie trwania negocjacji w kwestii PNR, Grupa Robocza Art. 29 wydała opinie nr 6/2002, 4/2003, 2/2004 i 6/2004.

¹³) PNR zawiera 34 rekordy podane w formie tabeli w załączniku A do decyzji Komisji Europejskiej z dnia 14 maja 2004 r. (patrz przypis 17).

tak jak wyraźnie przewiduje to prawo – Urząd może decydować o poziomie ochrony tylko wówczas, gdy główna instytucja właściwa, tj. Komisja Europejska, jeszcze tego nie uczyniła. Jeśli poziom ochrony uznaje się za odpowiedni, Urząd musi tylko wystawić zezwolenie. Jedyne, co może uczynić, to nałożenie dodatkowych warunków z myślą o wzmocnieniu ochrony na terytorium Grecji, z uwzględnieniem odrębności każdego przypadku oraz dopóki warunki te nie naruszają prawa europejskiego.

C. Interesująca będzie analiza krytyki, z jaką spotkała się powyższa decyzja.

Interesujące jest również to, że w rzeczywistości już sama decyzja Urzędu obejmuje ową krytykę, ponieważ, jak wynika z protokołów z zebrań, najważniejsze argumenty zostały przedstawione już w trakcie dyskusji nad sprawą.

a) Pierwszy argument jest natury konstytucyjnej i koncentruje się na konstytucyjnie ustanowionym prawie do ochrony danych osobowych. Czy Konstytucja posiada zwierzchność nad prawem wspólnotowym? Choć przy wielu okazjach kwestię tę rozpatrywał Europejski Trybunał Sprawiedliwości,¹⁸ orzekając na korzyść prawa wspólnotowego, przedstawianie w tej sprawie wątpliwości jest dopuszczalne, zwłaszcza w przypadku tak drażliwego obszaru, jakim są prawa osobiste. W sprawach cywilnych lub gdy złamane zostaje prawo handlowe, podważanie zwierzchności prawa wspólnotowego nie miałoby wielkich szans na przyjęcie, ani prawne ani społeczne. Jednak w kwestiach dotyczących praw cywilnych każda opinia skłaniająca się ku obronie ich nadrzędności – nawet *contra legem* – jest akceptowana, respektowana i powinna być rozwiązywana przy stole rozmów. Zaś podczas rozstrzygania o „za” i „przeciw” akceptowalności danej opinii, zawsze należy korzystać z silnych argumentów prawnych.

Jako odpowiedź na ten argument Urząd wskazuje, że nie działa on wyłącznie jako organ publiczny, ale jako organ, którego kompetencje opierają się na Konstytucji. Jak wyraźnie stwierdza to art. 9^A, konstytucyjne prawo do ochrony danych osobowych gwarantowane jest przez kompetencje Urzędu, który został powołany i działa zgodnie z ustawą 2472/97 w sprawie ochrony praw osobistych. Z kolei ustawa 2472/97 włączyła do prawodawstwa greckiego prawo europejskie.

b) Drugi argument koncentruje się na naturze prawnej mającego zastosowanie europejskiego aktu prawnego. Zgodnie z tym argumentem, o bezpośredniej lub pośredniej stosowalności prawa europejskiego powinno się decydować w połączeniu z naturą i zakresem mającego zastosowanie aktu, tzn. w połączeniu ze szczególnym przypadkiem porozumienia dwustronnego. W tym sensie, jeśli porozumienie, zawarte zgodnie z art. 300 „Traktatu UE”, stoi w sprzeczności z „Traktatem” i jego podstawowymi prawami, wśród których znajduje się poszanowanie praw człowieka oraz wolności podstawowych, wówczas instytucje i Państwa Członkowskie nie powinny go wprowadzać w życie.

Mimo to trudno jest zrozumieć, w jaki sposób akt, który wywodzi się z procedur przewidzianych Traktatem i Dyrektywą w sprawie ochrony praw podstawowych może stać w sprzeczności z Traktatem i z zasadą poszanowania praw człowieka oraz wolności

podstawowych. Dyrektywa wytycza zakres i warunki ochrony. W sprawach, w których warunki te nie są spełnione, przewiduje ona środki zapobiegawcze na poziomie europejskim. Przewiduje też, na poziomie europejskim, organ właściwy do podejmowania decyzji o tym, czy warunki są spełnione oraz jaką należy stosować procedurę. Ostateczny akt nie tylko reguluje sytuację, którą w różny sposób chronią Traktat i Dyrektywa, ale wręcz zawdzięcza on swoje prawne podstawy tej właśnie konkretnej Dyrektywie i temu właśnie Traktatowi.

ZAKOŃCZENIE

Rola Urzędu nie jest łatwa. Z natury stoi on między obywatelem z jednej a państwem (lub sektorem prywatnym) z drugiej strony; często jest obiektem ataków z obu stron.

Ostatnie dwa przypadki omówione w artykule stanowią typowy przykład takiego właśnie ataku. Z jednej strony część obywateli jest zdania, że Urząd strzegł ich praw w niewystarczającym stopniu. Z drugiej natomiast, w opinii administratorów, poprzez stawiane przez siebie warunki Urząd ochrony danych w znacznym stopniu ograniczył ich skuteczność.

Należy jednak jasno stwierdzić, że Urząd ochrony danych jest niezależnym organem administracyjnym. A niezależne organy administracyjne są instytucjonalnym owocem społeczeństwa obywatelskiego. Niezależne organy administracyjne rozwijały się historycznie (od czasów pierwszego rzecznika praw obywatelskich) w celu sprostania potrzebom społeczeństwa obywatelskiego – równoległe z państwem, ale także przeciw państwu; w taki sam sposób, w jaki zrodziło się, nabrało impetu i zostało zalegalizowane społeczeństwo obywatelskie – równoległe z państwem, ale również *wbrew* niemu. Niezależne organy administracyjne sprostają wymogom, którym nie mogło podołać państwo, do których państwo nie było uprawnione. Oczekiwano też od nich, że wypełnią je przy pomocy alternatywnych metod myślenia i działania.

W rzeczywistości rola niezależnych organów polega na mediacji i przybiera określony kształt w zależności od przyznanych im przez prawo uprawnień (doradczych, orzeczniczych, kontrolnych lub regulacyjnych).

Organy ochrony danych zostały powołane w celu obrony obywateli przed państwem lub przed sektorem prywatnym w kwestii niezgodnego z prawem lub nieproporcjonalnego przetwarzania danych w sposób naruszający prywatność obywateli. Nie są one jednak organizacją aktywistów. Są owocem społeczeństwa obywatelskiego, nie są jednak organizacją pozarządową. Działają i podejmują czynności w ramach określonych przepisami prawa, ich *raison d'être* stanowi prawo i również ponoszą one odpowiedzialność w zależności od legalności swojego postępowania.

W takim to świetle należy postrzegać pracę Urzędu. Nie należy też nigdy zapominać o tym, że w obecnym „okresie bezpieczeństwa” pełni on kluczową rolę i ma zasadnicze znaczenie, jeśli tylko mamy uniknąć tego, co wyraża aforyzm słynnego poety greckiego Odysseasa Elytisa (Nobel 1979): „Czuć ludzkim mięsem, gdy słyszysz słowo «rozkaz»”¹⁹ [tłumaczenie dosłowne – przypis tłumacza].

¹⁸⁾ Patrz Stauder 29/69, Coll. 1970, 419, Internationale Handelsgesellschaft 11/70, Coll. 1970, 1135, Simmenthal II 106/77, Coll. 1978, 629, Hauer 44/79, Coll. 1979, 3727, Verholen C-87,88,89/90, Coll. 1991, I-3757 etc.

¹⁹⁾ Odysseas Elytis „Maria Nefeli”, 1978.

Personal Data Protection in Public and Private Sectors

(experience of the Czech Republic)

From historical view, the problems of personal data and their protection have specific features in each of the sectors. In a number of countries, the legal rules for data protection were initially different for the public and private sectors, or the regulatory legislation first applied only to the public sector and only later was extended to the private sector. The main reason for certain hesitation in taking measures towards the private sector was admittedly the conviction of the need to avoid as much as possible the State interventions into the freedom of business. Furthermore, there was possibly also belief that the danger of the Big Brother phenomenon and the most erosive and mass impacts on the privacy of individuals could be expected from the public sector.

Legislation for both sectors has gradually become equal, as it became apparent that "the weaker on the market", this usually being an individual in the position of an employee or consumer (or potential employee or potential consumer), also cannot be left, at the time of globalization and monopolies, without any protection whatsoever in the area of privacy, including management of his/her personal data. This is true almost absolutely in households and family life, where the fundamental right to privacy and data protection is a dominant democratic value, but also, with a certain reasonable limitation, for areas, such as workplaces or supermarkets, where this right can collide with other basic democratic values, such as the right to pursue business and to freely manage one's own property, including its protection.

It is typical for the Czech Republic, where the legislative regulation of personal data protection is being introduced with a certain delay compared to the countries of Western Europe, where the democratic development was not interrupted, or was interrupted to a lesser degree in the 20th century, that the legal regulation of personal data protection has been uniform for both sectors from the beginning. Indeed, the first comprehensive Czech legal regulation of 1992 was already relatively very strongly based on Convention of the Council of Europe No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), which was the driving force in the area of personal data protection for a quarter of a century, at least in Europe. Nevertheless, I believe that the distinctive features of the two sectors and the related risks and dangers for the life of individuals cannot be absolutely neglected in the practice, in spite of existence of a uniform legislation and common principles of protection. It is not without reason that the fundamental EU legislation concerning personal data protection (Directive 95/46/EC) contains provisions supporting free flow of data and a balanced approach, also with respect to the legitimate interests of the controller, which is motivated by an effort to ensure fluent operation of the EU internal market, and thus, primarily related to the private sector. A case where data of obliga-

torily registered citizens are leaking from a central register kept by a ministry should probably be assessed differently, with a different level of strictness or tolerance, compared to a case where an entrepreneur forgets to lock his computer in his everyday haste. Similarly, in spite of the generally valid principle that ignorance of law is not an excuse, mistakes caused by ignorance of government officials and their agencies should not be assessed under the same criteria as insufficient knowledge of a small owner who is not served by a similar team of lawyers.

From the viewpoint of the recent practical supervisory activities of the Office for Personal Data Protection (hereinafter only "the Office"), we can identify a number of highly problematic or potentially dangerous features that are typical for one sector or the other.

Public sector

In the public sector, it is necessary to avoid an imbalanced approach to increasing public safety and State security on the one hand, and to the fundamental rights of individuals, including the right to privacy on the other hand. This includes especially certain ongoing, planned or discussed security measures, which are usually justified by the fight against terrorism and which tend to be gradually extended to other forms of crime, with an extensive impact on privacy of a great many persons. It must be emphasized that these are mostly innocent people who have never had and will never have anything in common with any criminal activities whatsoever. The duty of business entities to retain, over and above the framework of their usual activities and needs, personal data of their clients, such as operational data of providers of telecommunication and Internet services, or identification data of air passengers, and submit them to the authorities is an example of this phenomenon. Appropriateness of processing such a vast quantity of data, which can undoubtedly be misused and are also partly sensitive (e.g. location data which can constitute sensitive information under certain circumstances), with respect to the anticipated security effects, has never been credibly documented. The introduction of biometric elements to travel and other documents, as another example, results in addition to the potential misuse, in a danger of traumatizing the data subjects due to mistakes caused by imperfectness of the newly introduced equipment or technology. It must be noted that, as far as the adopted and contemplated measures are concerned, the Czech Republic does not differ from other European countries. However, there is a lot of sympathy and understanding in this respect from many representatives of Czech law enforcement bodies.

It is clear that the roots of a majority of the aforementioned tendencies to introduce extensive security measures can be found in the United States and this is also comprehensible after the events of September 2001. Undoubtedly, this has an impact on key democratic rights whose modern forms usually also have their roots in that country. It is gratifying that even in the United States there are increasing calls for the need of a balanced approach, of awareness of certain limits which should not be exceeded without sacrificing those values of the democratic world that must be defended against terrorism, and of assessing the efficacy of adopted measures from the viewpoint of the security effects, on the one hand, and the expended material and moral costs, on the other hand. The pending investigations pursued by the American Congress, which examines activities of the Government in its pursuit of terrorists in the area of telephone communications and the Internet, is an act worthy of following in Europe, including the Czech Republic.

To illustrate the situation in the Czech Republic from the viewpoint of practical experience of the Office, I should also note that a number of findings on breach of law have been made during the Office's control activities concerned with law enforcement authorities. The taking of biometric samples of fingerprints is an example where a relatively high fine has been imposed. In particular, contrary to the special laws regulating this procedure, data on fingerprints stored in information systems were also utilized for purposes other than those stipulated by the applicable laws. It is very likely that this is a very common, if not general, practice. We have also found other shortcomings, such as routine obtaining of data on fingerprints from persons where this was not based on the statutory provisions providing for this type of identification, common processing of data for various tasks, contrary to the statutory requirement for their separate processing, and non-compliance with the duty to verify, at least once every three years, whether the processed data are further needed, which is related to the duty stipulated by the Personal Data Protection Act to destroy personal data after expiry of the period required for their processing. On the basis of complaints, the Office also dealt with some relatively unique phenomena, such as communication of excessive data of a person suspected of committing a crime to his employer, inappropriate combination of data on different criminal offences against property within a common dossier, requesting sensitive data on nationality (not in the sense of citizenship) without statutory grounds and without the consent of the data subjects, etc.

With respect to the public sector, the Office believes that high risks are also related to extensive databases and central registers, from the Commercial Register, through health-care and demographic registers, to, e.g., the Land Registry, and also particularly the current tendencies to interconnect such registers and make them accessible to an increasingly large group of entities. The growing danger of misuse, including the so-called "identity theft", is self-evident.

During the legislative process, the Office lodged its objections against excessive disclosure on the Internet of personal data from the Land Registry, concerning the property of owners of real estate, and it also vigorously discusses the manner of application of the adopted special law. Similarly, transferring of the Commercial Register to the Internet without a certain limitation of access to particular data (e.g. the home addresses of company representatives) or complete prevention of public access (birth identification number) is, in our opinion, unacceptable. The Commercial Register has thus become a readily accessible source of information, e.g., for the purposes of sending unsolicited commercial communications and, which is worse, for more aggressive forms of infringing on privacy and the safety of individuals.

Thus, the issue of the nature of existing registers is now aggravated by the danger of their further augmentation. A register of all employees of the State administration is now imminent in the framework of the State Administration Act. Adoption of a measure, which is being enforced by the Government and which would lead to establishment of a register of debtors of the State (in addition to a number of registers of debtors in the private sector, which will be discussed below), seems very realistic. This register should contain, for example, information on outstanding taxes and premiums for social insurance and public health insurance. In the longer term, it should also include other debts to the State, such as outstanding electronic toll, court fees, etc. Proposals for establishment of three widely accessible central registers, namely the Central Register of Citizens, the Register of Territorial Identification and Addresses of Real Estate and the Central Economic Register, are being prepared.

Private sector

With respect to the private sector, I would like to mention three high-risk areas. These unambiguously include banking and the entire sphere of provision of financial services, including leasing. The typically weaker position of the client – natural person – on the financial market, which follows from the nature of business activities and business entities, and partially also from specific legislation, is further weakened by a certain information monopoly related to super-registers of information on debts of clients and other information on clients. Excessive application of the principle of due diligence ("Know your client"), not only in relation to registers, in combination with the aforementioned weaker position of the client, results in inappropriate requests for data. This also raises doubts with respect to the free nature of granting the data subject's consent in cases where data processing is conditional on such consent.

Of course, the main role in "closing in on" individuals by the information monopoly of banks and other financial institutions is played by the above-mentioned super-registers. The Bank Register of Information on Clients has been functional in the Czech Republic since 2002 and the number of member banks is constantly increasing. A much newer register, established in the middle of 2005, is the Non-Bank Register of Information on Clients, which contains information of leasing and credit companies without a banking license. In both cases, the registers comprise information, not only on the debts of the clients, but also on other aspects, including positive data related to the solvency of clients. The client is assigned an entry in the register from the beginning of the credit relationship. In both cases, the entry is deleted only 4 years after termination of the contract. Both registers are being mutually connected at the beginning of 2006, covering through their member companies already 95 % of the banking market, over 90% of the leasing market and approximately 50% of the market of sales on instalments. The SOLUS association, whose members are companies offering instalments, certain banks and mobile operators, keeps another important register. It comprises information only on the negative history of clients, i.e. data on failures to repay or substantial delays in the repayment of loans. An entry is deleted only 3 years after the loan is repaid by the client. While the Bank Register is based on the provisions of a special law (Act on Banks) and the consent of the data subjects to their inclusion in the register is not necessary, the Non-Bank Register and SOLUS operate on the basis of a consent. In the context of external instigations, the Office is currently also dealing with certain circumstances of accession of mobile operators to the SOLUS association, which need careful assessment from the viewpoint of personal data protection.

The Office is permanently concerned not only with registers, but also with other activities related to personal data processing by banks and other financial institutions. For example, the Office has dealt with the matter of acquisition (and recording) of personal data by certain banks within the provision of information on annual percentage rate of costs by telephone. This information can be ascertained from a majority of banks via a special information line established by the respective bank. Although the person using the line requires only information on the offered product, rather than the product itself (he/she is not becoming the client of the bank), prior to providing the information, the bank requests personal data within an inappropriate scope. The birth identification number, place of birth, address, telephone number, highest obtained education, name of the employer and a number of other pieces of information are frequently

requested, while only some of them have any relation to the subject of the matter. The banks record the thus-obtained data and store them for a certain period of time.

One of the highest fines in the history of the Office was imposed on a newly established bank which exerted inappropriate pressure on its employees to provide personal data of their relatives and friends who could become potential clients of the bank, usually without their consent. The Office also currently deals with the general terms and conditions of certain banks into which the data subject's consent as well as the mandatory information of the bank are incorporated in an inappropriate manner. It is likely that, in the future, Czech personal data protectors will continue to be concerned and pay attention mainly to the quality of consent granted in the specific environment of this specific area of business.

Outside the sphere of banking and other financial services, increased risks as regards personal data protection are also related to major supranational corporations, given their tendencies to transfer data of their employees and/or clients abroad and carry out their centralized processing, usually at the seat of the parent company, and often with the possibility of sharing centralized databases by subsidiaries, branches, etc. This can become a serious problem if the center of processing or the connected branches are located in countries with insufficient legislation on personal data protection. The usually imperfect or poorly enforceable internal regulations of the corporations, even though these are sometimes designated as the Binding Corporate Rules, mostly do not provide adequate guarantees of satisfactory management of personal data. Although the subject of BCRs has been dealt with, in the long term, by an independent advisory body of the European Commission – the Article 29 Working Party (WP 29), not even this body has been able to find any unambiguous and generally applicable criteria for assessing BCRs as an adequate guarantee. Only the attempt of WP 29 to create a mechanism of cooperation and mutual recognition of decisions in cases where some of the companies constituting a supranational corporation are active in several member countries of the EU was more successful. Nevertheless, the relevant approved document of WP 29 does not impair in any way the sovereignty and responsibilities of national data protection authorities in their decision-making on data processing within their jurisdiction and, therefore, it does not provide a very effective instrument and an unequivocal guidance for assessing all the facts of individual cases.

In any case, in dealing with central processing of personal data of employees or clients connected with the transfer of these data to "third countries" without an adequate legislation or with access to these data from such countries, to date, the Office has always requested that one of the conditions, which the EU legislation, as well as the national legislation of the Czech Republic, stipulates as an adequate guarantee for data processing, be met. A contractual arrangement, which is usually concluded in the form of a "standard contractual clause" approved by a decision of the European Commission, is increasingly being applied as an acceptable guarantee for the transfer of data to entities in third countries. Of course, supranational companies continue to use, in most cases, the consent provided by data subjects which, however, similar to financial institutions, raises concerns related to the quality of the consent from the viewpoint of free choice and awareness of the person providing the consent.

A third area entailing increased risk is the area of collecting and processing of personal data for marketing purposes. Bad experience of the Office and a number of complaints

are not concerned only with specialized marketing companies, but also with a wide range of business entities, including primarily major retail chains, supermarkets, etc. At the present time, technology enables very sophisticated procedures leading from collection and sorting of the obtained data, including information on even the most private purchases, to modeling of the conduct of an individual for the needs of very purposefully targeted offers of goods and services. The rapid development of information and communication technologies will lead to new dangers of an increasingly aggressive infringement on privacy.

During our control work, we have encountered a great many abuses, some of which could be described as curiosities. For example, several commercial companies agreed, without the consent and knowledge of customers, on sharing their customer databases. And they exchanged the data in an open Internet network, without any organizational and technical provisions whatsoever. An even more absurd was a case where a commercial company rented out part of its premises to a detective agency with which it also concluded a contract for the provision of detective services. On the basis of a complaint against unauthorized management of personal data by the detective agency, which proved to be justified, the Office ascertained that the agency provided the commercial company with personal data obtained in connection with protection of property of that company, which further processed and stored those data.

Particularly in relation to major retail chains, the Office has encountered cases where a number of negative features were combined. In addition to dubious procedures in obtaining personal data for marketing purposes and breach of law in their subsequent processing, this also includes the totally unacceptable practices of certain security agencies contracted by those companies, inappropriate scope and manners of camera surveillance and the subsequent processing of camera recordings, etc.

When describing the negative experience of the Office, a mention must also be made of the closely related area of unsolicited commercial communications sent by electronic means, i.e. "commercial spam". However, this is a very extensive and specific subject (in which the Office obtained additional competence for supervision and imposing of sanctions at the end of 2004) which would require a special chapter. I would only like to note that, from the originally absolutely strictly and consistently applied "opt-in" concept, we are now adopting a "soft opt-in" concept, i.e. an approach permitting that the companies may address their own customers without their prior consent, but with the possibility of simple rejection of single or repeated offers of goods and services.

Finally, it should also be stated that, in spite of the specific features and different nature of the public and private sectors from the viewpoint of risks and abuses in the area of protection of personal data and privacy of individuals – and the related supervisory practice – there are also a great many problematic features occurring **across the sectors**. Data protectors will continue to be concerned with certain aspects of development of *new information technologies*, including the Internet and the related services. Let us mention, e.g., the increasing possibilities of mutual connection of information systems both inside sectors (e-Government, interactive networks of supranational monopolies in the globalized world) and amongst them (tendencies to commercially reuse public information). The increasingly extensive and sophisticated application of *biometric data* – for the present primarily for identification purposes – which are employed both in investiga-

tion of crime and in tourism, as well as at entrances to buildings of major commercial companies, is also a serious general and intersectoral phenomenon. The possibilities of abusing *mobile technology* of the RFID type or other means of processing location data, from search for persons in providing for public safety to the related services with an added value offered by the private sector, are also increasing. The issue of excessive use of camera systems has already become an evergreen, etc.

However, in the future, it will not only be necessary that the supervisory bodies warn against such trends or, where appropriate, entirely reject them. A much more effective and realistic option is to take an active part in them and consistently promote a balanced approach that would attempt, while avoiding dogmatic or fundamentalist approach, to prevent fundamental infringement on democratic values, such as the right to privacy generally and the protection of personal data specifically.

Ochrona danych osobowych w sektorze publicznym i prywatnym (doświadczenia Republiki Czeskiej)

Z historycznego punktu widzenia oceniając, w każdym z sektorów można wskazać specyficzne problemy związane z danymi osobowymi i ich ochroną. W kilku krajach początkowo obowiązywały inne przepisy prawne w sektorze prywatnym i w sektorze państwowym bądź też regulacje prawne najpierw odnosiły się tylko do sektora publicznego, a następnie został nimi objęty także sektor prywatny. Główną przyczyną pewnych obaw w podejmowaniu działań w sferze ochrony danych w sektorze prywatnym było, trzeba to przyznać, przekonanie o konieczności unikania, na ile to możliwe, interwencji państwa w swobodne prowadzenie interesów. Ponadto, istniało być może przekonanie, że z sektora publicznego można się spodziewać najbardziej niszczącego i masowego wpływu zjawiska „Big Brother” na prywatność jednostek.

Stopniowo ustawodawstwo dotyczące obu sektorów zostało ujednolicone. Oczywiście bowiem okazało się, że nie można w czasach globalizacji i monopolizacji pozostawić „słabszego na rynku”, czyli zazwyczaj jednostki w postaci pracownika bądź konsumenta (lub potencjalnego pracownika lub potencjalnego konsumenta), bez jakiegokolwiek ochrony w sferze prywatności, w tym zarządzania jej danymi osobowymi. Sprawdza się to w dużym stopniu w gospodarstwach domowych i życiu rodzinnym, gdzie fundamentalne prawo do prywatności i ochrona danych to dominująca, demokratyczna wartość, ale też z pewnymi ograniczeniami w takich sferach, jak miejsce pracy czy supermarket, gdzie prawo to może kolidować z innymi podstawowymi wartościami demokracji, takimi jak prawo do prowadzenia interesów i swobodnego zarządzania własnym mieniem, łącznie z jego ochroną.

Typową sytuacją dla Republiki Czeskiej, gdzie regulacje prawne dotyczące danych osobowych są wprowadzane z pewnym opóźnieniem w porównaniu z innymi państwami Zachodniej Europy, w których to rozwój demokracji trwał nieprzerwanie bądź był zakłócany – choć w mniejszym stopniu – tylko w XX wieku, jest jednolitość regulacji prawnych dotyczących ochrony danych osobowych w obu sektorach od samego początku. W rzeczywistości pierwsza pełna regulacja prawna w tej dziedzinie z 1992 roku w stosunkowo

dużym stopniu opierała się na „Konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych” (ETS 108), która była podstawą działań, przynajmniej w Europie, w dziedzinie ochrony danych osobowych przez ćwierć wieku. Niemniej jednak, uważam, że nie można lekceważyć w praktyce cech odróżniających oba sektory i związanych z tym niebezpieczeństw oraz zagrożeń dla jednostek, mimo obowiązywania jednolitego ustawodawstwa i wspólnych zasad ochrony. Nie bez powodu podstawowe unormowanie UE w dziedzinie ochrony danych osobowych (Dyrektywa 95/46/WE) zawiera klauzule popierające swobodny przepływ danych, a także wyważone stanowisko odnośnie usankcjonowanych prawnie interesów administratora w celu zapewnienia płynnego działania rynku wewnętrznego UE. Dlatego też dotyczy głównie sektora prywatnego. Zagadnienie przedostania się danych obywateli, obowiązkowo zarejestrowanych, z centralnego rejestru znajdującego się w ministerstwie prawdopodobnie powinno zostać inaczej potraktowane – w sensie stopnia rygorystyczności czy tolerancji – w porównaniu z przypadkiem, kiedy to przedsiębiorca zapomni w codziennym pośpiechu zamknąć komputer. Podobnie, mimo powszechnie obowiązującej zasady, że nieznanostwo prawa nie jest usprawiedliwieniem, błędy spowodowane niewiedzą urzędników instytucji rządowych i ich biur nie powinny być oceniane według tych samych kryteriów, co błędy właściciela małego przedsiębiorstwa wynikające z niewystarczającej wiedzy, ponieważ nie ma on w otoczeniu całej grupy prawników.

Na podstawie podjętych niedawno przez Biuro Ochrony Danych Osobowych (zwane dalej „Biurem”) działań nadzorczych możemy określić kilka problematycznych bądź potencjalnie niebezpiecznych charakterystycznych cech typowych dla jednego bądź drugiego sektora.

Sektor publiczny

W sektorze publicznym należy unikać braku równowagi między zwiększaniem bezpieczeństwa publicznego i bezpieczeństwa państwa z jednej strony a fundamentalnymi prawami jednostek, w tym prawem do prywatności, z drugiej. Dotyczy to przede wszystkim stosowanych, planowanych bądź omawianych środków bezpieczeństwa, których wprowadzenie jest uzasadniane zazwyczaj walką z terroryzmem, a którymi są stopniowo obejmowane inne formy przestępczości i przy tym mają one duży wpływ na prywatność wielu osób. Należy podkreślić, że są to zazwyczaj osoby niewinne, które nigdy nie miały i nie będą miały nic wspólnego z jakąkolwiek działalnością przestępczą. Przykładem może być obowiązek podmiotów gospodarczych dotyczący przechowywania – poza ramami wynikającymi ze zwykłych działań i potrzeb – danych osobowych ich klientów, takich jak dane operacyjne dostawców usług telekomunikacyjnych i internetowych, dane tożsamości pasażerów linii lotniczych oraz przekazywanie ich odpowiednim władzom. Nigdy nie została wiarygodnie udokumentowana potrzeba przetwarzania tak olbrzymiej ilości danych w odniesieniu do oczekiwanych efektów bezpieczeństwa, które bez wątpienia mogą być użyte niewłaściwie i częściowo należą do kategorii danych wrażliwych (np. dane dotyczące lokalizacji, które mogą być danymi wrażliwymi w pewnych okolicznościach). Wprowadzenie elementów biometrycznych do dokumentów podróży i innych to kolejny przykład na to, że podmiot, którego dane dotyczą, może być narażony na niewłaściwe ich wykorzystanie, a dodatkowo na błędy wynikające z niedoskonałości nowo wprowadzanego sprzętu i technologii. Należy zauważyć, że jeśli chodzi o przyjęte i rozpatrywane środki, Republika Czeska nie odbiega od innych państw europejskich. Jednak przedstawiciele czeskich organów prawnych wykazują wiele zrozumienia w tej dziedzinie.

Oczywiście tendencja do wprowadzania rozbudowanych środków bezpieczeństwa ma swoje źródło w Stanach Zjednoczonych. Stało się to zrozumiałe po wydarzeniach 11 września 2001 roku. Bez wątpienia wpływa to na podstawowe prawa demokratyczne, których współczesna forma ma także zwykle swe korzenie w tym kraju. Zadowolające jest to, że nawet w Stanach Zjednoczonych zwiększa się liczba osób dostrzegających konieczność przyjęcia wyważonego stanowiska w tej sprawie, świadomych pewnych ograniczeń, których nie należy przekraczać bez poświęcenia tych wartości demokratycznego świata, których trzeba bronić w walce z terroryzmem, oraz wskazujących na potrzebę oceny skuteczności przyjętych środków z punktu widzenia rezultatów związanych z bezpieczeństwem z jednej strony a kosztami materialnymi i moralnymi z drugiej. Toczące się postępowanie Amerykańskiego Kongresu w sprawie działań rządu związanych ze ściganiem przestępców w obszarze łączności telefonicznej i Internetu jest działaniem, które warto podjąć w Europie, w tym w Republice Czeskiej.

By zilustrować sytuację w Republice Czeskiej z punktu widzenia praktycznych doświadczeń Biura, warto odnotować, że w wyniku czynności kontrolnych dotyczących działania organów egzekwujących prawo, odkryto kilka przypadków naruszenia przepisów. Stosunkowo wysoką grzywnę nałożono za pobieranie próbek biometrycznych odcisków palców. Wbrew szczegółowym przepisom regulującym tę procedurę, dane o liniach papilarnych przechowywane w systemie informacyjnym były wykorzystywane również do innych celów niż ustalone przez odpowiednie regulacje. Prawdopodobnie jest to bardzo częsta, jeśli nie powszechna praktyka. Odkryliśmy również inne uchybienia, takie jak: rutynowe pobieranie odcisków palców w przypadku, gdy tego typu identyfikacja nie była ustawowo uregulowana, powszechne przetwarzanie danych do różnych celów wbrew wymogom ustawowym o ich oddzielnym przetwarzaniu, nieprzestrzeganie obowiązku weryfikowania co najmniej raz na trzy lata, czy przetwarzane dane są wciąż potrzebne, co odnosi się do obowiązku zawartego w ustawie o ochronie danych osobowych niszczenia danych osobowych po wygaśnięciu terminu wymaganego do ich przetwarzania. W wyniku napływających skarg Biuro zajęło się kilkoma dość wyjątkowymi sprawami, takimi jak przekazanie nadmiernej ilości danych o osobie podejrzanej o popełnienie przestępstwa jego pracodawcy, niewłaściwe łączenie danych dotyczących różnych wykroczeń przeciwko mieniu w jednych aktach, pytanie o narodowość (nie w kontekście obywatelstwa) bez ustawowych podstaw i bez zgody podmiotu, którego dane dotyczą itd.

Jeśli chodzi o sektor publiczny, Biuro jest zdania, że wysoki poziom ryzyka odnosi się również do obszernych baz danych i centralnych rejestrów: od rejestru handlowego, przez służby zdrowia i rejestry demograficzne, do na przykład rejestru nieruchomości, a zwłaszcza do obecnych tendencji łączenia tych rejestrów i udostępniania ich coraz większej liczbie podmiotów. Wzrastające niebezpieczeństwo nadużyć, w tym tzw. kradzież tożsamości, jest sprawą oczywistą.

Podczas procesu legislacyjnego Biuro zgłosiło zastrzeżenia, co do nadmiernego ujawniania w Internecie danych z rejestru nieruchomości dotyczących posiadanego mienia. Podjęto dyskusję na temat sposobu stosowania przyjętych szczególnych regulacji. Naszym zdaniem, umieszczenie danych z rejestru handlowego w Internecie bez wprowadzenia pewnych ograniczeń w dostępie do szczególnych danych (np. domowych adresów przedstawicieli firmy) bądź bez zabezpieczenia przed publicznym dostępem do danych (numer identyfikacyjny nadany po urodzeniu) jest nie do przyjęcia. Rejestr

handlowy zatem stał się łatwo dostępnym źródłem informacji, np. do celów przesyłania niezamawianych informacji komercyjnych, a co gorsza – do bardziej agresywnych form naruszania prywatności i bezpieczeństwa jednostek.

Zatem problem obecnego kształtu istniejących rejestrów pogłębia jeszcze niebezpieczeństwo ich dalszego pomnażania. W ramach ustawy o administracji państwowej nieuchronne jest bowiem powstanie rejestru pracowników tej administracji. Możliwe wydaje się zastosowanie środków, które są obecnie wprowadzane przez rząd, a które doprowadzą do ustanowienia rejestru dłużników państwa (oprócz kilku rejestrów dłużników w sektorze prywatnym, które omówię później). Rejestr ten powinien zawierać, na przykład, informacje o zaległych podatkach i składkach ubezpieczeniowych oraz o składkach na ubezpieczenie zdrowotne. Patrząc z innej perspektywy, powinien on zawierać również inne informacje o długach wobec państwa, takich jak: zaległe opłaty drogowe, opłaty sądowe itd. Przygotowywane są wnioski o utworzenie trzech centralnych, powszechnie dostępnych rejestrów, a mianowicie: centralnego rejestru obywateli, rejestru identyfikacji terytorialnej i adresów nieruchomości oraz centralnego rejestru ekonomicznego.

Sektor prywatny

W odniesieniu do sektora prywatnego chciałbym wspomnieć o trzech obszarach dużego ryzyka. Jednym z nich będzie bezsprzecznie bankowość i cała sfera świadczenia usług finansowych, w tym leasingu. Typową słabszą pozycję klienta – osoby fizycznej – na rynku finansowym, wynikającą z istoty działań biznesowych i podmiotów gospodarczych, a częściowo z określonego ustawodawstwa, osłabia jeszcze monopol informacyjny związany z „super-rejestrami” zawierającymi informacje o zadłużeniu klientów oraz inne. Nadmierne stosowanie zasady „należytej pilności” („poznaj swojego klienta”), nie tylko w odniesieniu do rejestrów, w połączeniu ze wspomnianą wcześniej słabszą pozycją klienta, prowadzi do stosowania niewłaściwych wymagań dotyczących danych. Rodzi to również wątpliwości, co do swobodnego wyrażania zgody przez podmiot, którego dane dotyczą, w przypadkach, kiedy przetwarzanie danych jest uwarunkowane wyrażeniem takowej zgody.

Oczywiście, główną rolę w „otaczaniu” jednostek monopolem informacyjnym przez banki i inne instytucje finansowe odgrywają wspomniane wcześniej „super-rejestry”. Od 2002 roku funkcjonuje rejestr bankowy informacji o klientach i ciągle zwiększa się liczba banków przyłączających się do tego rejestru. Nowszym rejestrem, założonym w połowie 2005 roku, jest nie-bankowy rejestr informacji o klientach, zawierający informacje o firmach leasingowych i kredytowych niemających koncesji bankowej. W obu przypadkach rejestry te zawierają informacje dotyczące nie tylko zadłużenia klientów, ale również innych aspektów, wliczając dane o wypłacalności klientów. Dane są wpisywane do rejestru od początku trwania umowy kredytowej. W obu przypadkach wpis ten jest usuwany 4 lata po wygaśnięciu umowy. Oba rejestry od początku 2006 roku są ze sobą łączone, obejmują 95% rynku bankowego, ponad 90% rynku leasingu i około 50% rynku sprzedaży ratalnej. Stowarzyszenie SOLUS, skupiające członków z przedsiębiorstw sprzedaży ratalnej, niektórych banków i operatorów telefonów komórkowych, ma kolejny ważny rejestr zawierający wyłącznie negatywne informacje o klientach, tj. dane dotyczące niespłacenia bądź znacznych opóźnień w spłacie pożyczek. Zapisy te są usuwane po 3 latach od spłaty kredytu przez klienta. Rejestr bankowy działa według szczegółowych przepisów (ustawy o bankach),

nie jest wymagana zgoda podmiotu na włączenie danych jego dotyczących do rejestru, natomiast rejestr nie-bankowy i SOLUS działają na zasadzie wyrażenia zgody przez podmiot. W wyniku nacisków zewnętrznych Biuro zajmuje się okolicznościami przystąpienia operatorów telefonii komórkowej do stowarzyszenia SOLUS, które należy ocenić z punktu widzenia ochrony danych.

Do stałych zadań Biura należy nie tylko zajmowanie się rejestrami, ale również innymi działaniami banków i instytucji finansowych, związanymi z przetwarzaniem danych osobowych. Biuro analizowało, na przykład, sprawę uzyskiwania (i rejestrowania) danych osobowych przez pewne banki w ramach telefonicznego udzielania informacji o rocznej stopie procentowej. Informacje te można otrzymać od większości banków przez specjalną linię utworzoną przez dany bank. Mimo że osoba korzystająca z tej linii chce uzyskać tylko informacje o oferowanym produkcie, a nie ten produkt (nie staje się klientem banku), bank przed udzieleniem informacji pyta o dane osobowe w nieodpowiednim zakresie, a mianowicie często są zadawane pytania o numer identyfikacyjny nadany po narodzeniu, miejsce urodzenia, adres, numer telefonu, wykształcenie, nazwę pracodawcy i wiele innych, podczas gdy tylko niektóre z tych danych mają jakikolwiek związek z konkretną sprawą. Banki zapisują informacje uzyskane w ten sposób i przechowują je przez pewien czas.

Jedna z największych kar pieniężnych w historii działalności Biura została nałożona na nowo powstały bank, który wywierał nacisk na pracowników w celu uzyskania danych o ich krewnych, którzy mogli zostać potencjalnymi jego klientami, zazwyczaj bez ich zgody. Obecnie Biuro zajmuje się ogólnymi warunkami narzucanymi przez niektóre banki, w których określają one nieprawidłowo sytuacje wymagające wyrażenia zgody przez podmiot na pozyskanie jego danych, jak też sytuacje dotyczące uzyskiwania obowiązkowych informacji. Prawdopodobnie czeskie organy ochrony danych zwrócą w przyszłości uwagę głównie na „jakość” wyrażonej zgody w tym szczególnym kontekście tej specyficznej sfery działalności.

Poza sferą bankowości i innych usług finansowych zwiększone ryzyko w dziedzinie ochrony danych osobowych występuje w znaczących korporacjach ponadnarodowych, które mają tendencję do przekazywania danych pracowników i (lub) klientów za granicę. Dokonują zcentralizowanego ich przetwarzania, zazwyczaj w firmie macierzystej, zapewniając często możliwość dostępu do zcentralizowanych baz danych filiom, oddziałom itd. Może stać się to poważnym problemem w przypadku, gdy firma przetwarzająca dane bądź jej filie znajdują się w państwach, w których nie ma odpowiedniego ustawodawstwa dotyczącego ochrony danych. Zazwyczaj słabo egzekwowane regulacje wewnętrzne korporacji, mimo że niekiedy odgrywają rolę wiążących przepisów korporacyjnych („Binding Corporate Rules – BCR”), najczęściej nie gwarantują właściwego zarządzania danymi osobowymi. Chociaż przepisami tymi zajmował się przez długi czas niezależny organ doradczy Komisji Europejskiej – Grupa Robocza Art. 29, nawet ten organ nie był w stanie opracować jednoznacznych, mających powszechne zastosowanie kryteriów w ocenie BCR jako wystarczających gwarancji ochrony danych. Większym sukcesem zakończyła się próba Grupy Roboczej Art. 29 stworzenia mechanizmu współpracy i wzajemnego uznawania decyzji w przypadkach, kiedy przedsiębiorstwa ponadnarodowe prowadzą działalność w kilku Państwach Członkowskich UE. Niemniej jednak zatwierdzony dokument tej Grupy nie ogranicza w żaden sposób suwerenności i obowiązków krajowych organów ochrony danych w podejmowaniu

decyzji dotyczących przetwarzania danych w obrębie własnej jurysdykcji, dlatego też nie jest skutecznym instrumentem i jednoznacznym poradnikiem przy rozpatrywaniu wszelkich aspektów poszczególnych spraw.

W każdym razie w przypadku centralnego przetwarzania danych osobowych pracowników bądź klientów związanego z transferem tych danych do „państw trzecich” niemających odpowiedniego ustawodawstwa w tej dziedzinie bądź, gdy dostęp do danych nastąpił w tych państwach, Biuro domagało się, aby zostały spełnione warunki zgodne z unormowaniami UE oraz krajowego ustawodawstwa Republiki Czeskiej, zapewniając w ten sposób dostateczną gwarancję ochrony danych. Coraz częściej są stosowane umowne ustalenia, które zazwyczaj są zawarte w „standardowej klauzuli umownej” zatwierdzonej decyzją Komisji Europejskiej jako akceptowanej gwarancji w przypadku transferu danych do podmiotów w „państwach trzecich”. Oczywiście, przedsiębiorstwa ponadnarodowe najczęściej stosują zgodę podmiotu, którego dane dotyczą, jednak – podobnie jak w odniesieniu do instytucji finansowych – pojawia się pytanie dotyczące jakości tej zgody z punktu widzenia wolności wyboru oraz świadomości osoby wyrażającej zgodę.

Trzeci obszar zwiększonego ryzyka wiąże się ze zbieraniem i przetwarzaniem danych osobowych dla celów marketingowych. Złe doświadczenia Biura w tej dziedzinie oraz wiele skarg nie dotyczyło wyłącznie specjalistycznych firm marketingowych, ale również dużego kręgu podmiotów gospodarczych, w tym głównie znaczących sieci handlu detalicznego, supermarketów itd. Dzisiejsza technologia umożliwia przeprowadzanie bardzo skomplikowanych procedur, począwszy od zbierania i sortowania uzyskanych danych, w tym informacji dotyczących nawet bardzo osobistych zakupów, aż do profilowania zachowania się jednostki dla potrzeb ukierunkowanych ofert towarów i usług. Szybki rozwój technologii informacyjnej i komunikacji doprowadzi przy tym do pojawienia się nowych zagrożeń związanych z naruszaniem prywatności.

Podczas naszej pracy polegającej na kontrolowaniu znaczących podmiotów sieci sprzedaży detalicznej odkryliśmy wiele nadużyć. Niektóre z nich można potraktować jako ciekawostki. Na przykład kilka spółek handlowych porozumiało się bez zgody i wiedzy konsumentów, co do podzielenia się bazami danych swoich klientów. Wymieniły się danymi przez otwartą sieć internetową, bez jakichkolwiek organizacyjnych bądź technicznych zabezpieczeń. Jeszcze bardziej absurdalna była sprawa, kiedy to przedsiębiorstwo handlowe wynajęło część swojej siedziby agencji detektywistycznej, z którą zawarło umowę na świadczenie usług. Rozpatrując skargę złożoną przez agencję, a dotyczącą bezprawnego zarządzania danymi osobowymi, która zresztą okazała się zasadna, Biuro ustaliło, że agencja dostarczyła przedsiębiorstwu dane osobowe w związku z ochroną mienia firmy, która następnie je wykorzystwała i zachowała.

W przypadku głównych sieci sprzedaży detalicznej Biuro zetknęło się z sytuacją nałożenia się kilku negatywnych aspektów. Oprócz wątpliwych procedur uzyskiwania danych dla celów marketingowych i w następstwie naruszania prawa w wyniku ich przetwarzania, miały też miejsce niedopuszczalne praktyki pewnych agencji ochrony, m.in. związane z niewłaściwym zakresem i sposobem stosowania nadzoru z użyciem kamer, a w następstwie z przetwarzaniem zarejestrowanych kamerą danych itd.

Opisując negatywne doświadczenia Biura, należy także wspomnieć o łączącym się z tym zagadnieniem, a mianowicie niezamawianych informacji komercyjnych przesyła-

nych drogą elektroniczną, tzw. commercial spam. Jest to bardzo obszerny i specyficzny temat (pod koniec 2004 roku Biuro uzyskało dodatkowe kompetencje w tym zakresie, dotyczące nadzorowania i nakładania sankcji), któremu trzeba by poświęcić kolejny rozdział. Chciałbym zauważyć, że przeszliśmy od wprowadzanej początkowo konsekwentnie koncepcji „opt-in” do koncepcji „soft opt-in”, tj. do stanowiska zezwalającego na zwracanie się do klientów bez ich wcześniejszej zgody, jednakże należy się liczyć ze zwykłym odrzuceniem jednej bądź wielu ofert towarów czy usług.

Podsumowując, należy również podkreślić, że mimo specyficznych cech i różnic między sektorem publicznym i prywatnym z punktu widzenia ryzyka oraz naruszania prawa ochrony danych osobowych oraz prawa jednostek do prywatności, a także praktyki organów nadzorczych w tej dziedzinie, jest wiele problematycznych działań, które występują **w obu obszarach**. Organy zajmujące się ochroną danych w dalszym ciągu będą zajmować się pewnymi aspektami rozwoju *nowej technologii informacyjnej*, w tym Internetu i związanymi z nim usługami. Wymieńmy, na przykład, coraz większe możliwości łączenia systemów informacyjnych zarówno wewnątrz sektorów (e-rząd, interaktywne sieci ponadnarodowych firm monopolowych w zglobalizowanym świecie), jak i między nimi (tendencje do komercyjnego, powtórnego wykorzystania informacji publicznych). Coraz powszechniejsze i skomplikowane zastosowanie *danych biometrycznych* – obecnie głównie do celów identyfikacji – zarówno w postępowaniach dochodzeniowych, jak i w turystyce, a także przy wejściach do budynków dużych firm handlowych – to również ważne, powszechne zjawisko „międzysektorowe”. Coraz większe są, ponadto, możliwości nadużywania *telefonii komórkowej* opartej na technologii RFID bądź innych sposobów przetwarzania danych dotyczących lokalizacji, począwszy od poszukiwania osób w celu zapewnienia bezpieczeństwa publicznego do pokrewnych usług, a także w sektorze prywatnym. Kwestia zbyt częstego używania kamer również stała się obecnie aktualnym tematem itd.

W przyszłości będzie jednak niezbędne nie tylko ostrzeganie przez organy nadzorcze przed takimi trendami lub, gdy będzie to konieczne, całkowite ich wyeliminowanie. Dużo skuteczniejszym i realnym rozwiązaniem będą aktywne działania oraz nieustanne promowanie „zrównoważonego stanowiska”, polegającego na unikaniu dogmatycznego i fundamentalistycznego stanowiska w celu zapobiegania naruszaniu podstawowych wartości demokratycznych, takich jak – ogólnie rzecz biorąc – prawo do prywatności, a ściślej – prawo do ochrony danych osobowych.

Karel Neuwirt

Former President of the Office for Personal Data Protection, Czech Republic
Były Przewodniczący Urzędu Ochrony Danych Osobowych, Republika Czeska

Data protection and smart cards

It is almost half a century when the first plastic credit card was issued. It was done by the Bank of America in 1960. But a milestone in the card technology was then the card equipped with the memory elements which enabled the card to carry some information. Farther development of this technology increased capacity of the card memory, which enabled to store the large amount of data, and to create modern and secure technology which is used in many areas of daily life of citizens.

Among traditional use of the smart card as a payment instrument, they are also used in health, transport, telecommunication, market and many other fields. The use of smart card as an identity document increased. From the privacy and data protection point of view we will talk about “smart cards” as a plastic card with an embedded integrated circuit (chip).

Smart card can provide easy access to information held in the card’s memory with high secure policy at the same time. It is a portable data carrier where the use of information stored in the chip is under control of the card holder. Current smart cards are uniquely capable of complying with strong privacy principles and guidelines. They enforce the privacy and security policies set up by national and international bodies.

In general, smart cards are divided by different characteristics. For example, by the type of access (connection) to information (data is read by reader with direct physical contact or with a remote contactless electromagnetic interface – contact card, contactless card), the type of memory (with magnetic strip – magnetic card, with a serial memory integrated circuit (IC) – memory card, with more secure microprocessor (MCU – smart card), security module (data is crypted by cryptographic module – cryptocard) and also by method of use – single application, multiapplication, multipurpose, and so on.

Basic requirements imposed for storage of and access to information in the chip fulfil major principles of information protection which are as follows:

- availability: data is accessible and usable upon demand by authorized persons,
- confidentiality: data is protected against access by unauthorized (non-legitimate) persons,
- integrity: data is protected against unauthorized change, alteration or destruction.

The smart card industry is growing progressively. The largest sector of the smart card industry is telecommunication which is still on top. In 2005 1.3 billion identity module cards for mobile phones were expected. In 2006 the growth will continue – mainly because of new subscribers in Asia, China and India. For example, only China’s SIM cards market in 2005 expected about 300 million. According to the analysis issued by Eurosmart, sales of SIM cards will grow by 25% this year. Significant expectations in

the smart card applications are from the government (national ID documents, driver's license), healthcare (about 60 million by the end of 2005) and banking (about 330 million) sectors.

Another important issue, mainly from security and privacy point of view, is the growth of the applications with high-end SIM cards, with at least 64 kilobytes of rewriteable memory (supported 3G networks).

In 2006 a roll-out of contactless card payment will be continued. More tests of contactless payment applications, both on cards and mobile phones are expected. That year will continue the migration to cards and terminals complying with the EMV standard which reduce certain types of cards fraud (EMV is the international standard for credit and debit smart cards).

Important growth in the government applications is thanks to issuing electronic passports and other electronic travel and identity documents. The year 2006 is a deadline when EU Member States shall add contactless smart card chips and tiny antennas to their passports that carry a digital image of a face, fingerprint and, perhaps, other biometric data of passport holder. Tiny antenna, as part of the chip, enables to transmit data through the air to the passport readers. This card is called RFID card (radiofrequency identification). E-passport was driven by the United States, which in reaction to terrorist attacks on Sept. 11, 2001, passed a law in spring 2002 requiring friendly nations to introduce electronic passports carrying biometric data by October 2004. Some 40 countries are announced to work on electronic passport programme. The reason of implementing the chip in the passports is primarily to store biometric data. This data will be used to verify that the person presenting the passport is the same person whom the passport was issued to. For example, putting that digital photo on the chip reduces the counterfeiting of passports by criminals who replace a photo on the data page. When an electronic passport is used, the border inspector would also see the photo written on the chip when the passport was issued. It is very difficult, almost impossible, to replace the photo on data page and on the chip identically. Second security aspect is that at issuance the chip will be locked against rewriting, so that no new data or modification of data can be added. Technical parameters of the chip in combination with the feature of biometric data provide high accuracy in verification of passport holder. According to an Australia's test with facial recognition (conducted with Qantas airlines crew members in year 2002), recognition was proved accurate in 98%, compared to 60% accuracy when recognition was made by human inspectors by matching a photo to live person (according to Bob Nash, head of passports in the Department of Foreign Affairs and Trade). The combination of biometrics and contactless chip will make the new electronic passport far more secure than today's passports, says Barry Kefauver, a consultant and former U.S. State Department official, who chairs a committee of the International Standards Organization that advises ICAO on e-passports. It is no doubt that biometrics, like fingerprint or face, is a valuable identification tool. But very bad and dangerous is a view of many people that biometric data processing has zero-error rate against misuse or serious attack. The interception is a serious threat in any systems with contactless cards. It is necessary to give greater scrutiny to this kind of personal data processing. Many privacy advocates criticize the concept of electronic passports with biometric personal data, saying that they will lead to the creation of a global database of biometrics from millions of individuals, and hand travellers' personal data to regimes that violate human rights. "Privacy will

remain a big issue as advanced technology is increasingly used to verify identity", said Don Davis, editor and associated publisher of the Card Technology Magazine. Experts in contactless technology argue that it would be difficult to skim data in real-world settings. But pressure from privacy experts and groups has forced governments to take a close look at how contactless card works, and to adopt additional security measures.

But description and analysis of risks of biometric personal data processing is not the aim of this article.

About 4 million passports are expected to be produced annually. Some countries (e.g. the United Kingdom) plan to issue a different kind of electronic identification documents. The European Union has set August 28, 2006 as a deadline of the first step in introducing e-passports for the EU citizens. Electronic passport creates new issues concerning security and privacy protection. Many people worry criminals will be able to read illegally the data from the passport chip. The aim of e-passports is to increase border security, but the focus may be on such issues as the privacy of personal data. If one of most important expectation is that e-passports are the instrument in the fight against terrorism, it is necessary to say that the most sensational threat is that terrorists could read data off of passport's chip from afar and then target citizens of particular nations. "In effect, these passports would be painting giant bulls eyes on the back of all who carry them", the influential American Civil Liberties Union wrote this spring in a letter to the U.S. State Department. For the e-passport applications in the travel sector it is a very problematic issue to achieve interoperability between contactless chips and readers produced by different producers and suppliers. This issue will be (probably) solved by the International Civil Aviation Organization (ICAO) that sets standards for travel documents and settled on contactless chips as the standard way of carrying data about the passport holder (standard 9303 for Machine Readable Travel Documents). ICAO standard has the endorsement of the International Organisation for Standards (ISO) and has achieved the status of worldwide standard.

The Council of Europe pays attention to risks to privacy raised by modern technology, including smart cards. Since 1996, the Project Group on Data Protection (CJ-PD) has been engaged in issues and problems of protection of personal data and privacy in smart cards technology. The first document of the Council of Europe concerning smart cards problem was issued in 1985 (Legal Problems Resulting from Official Machine-Readable Identification Documents. Council of Europe, CJ-PD(85)3, 1985). In 2003, the Council of Europe Project Group on Data Protection (CJ-PD) has elaborated and adopted an important document on protection of personal data when smart cards are used - DRAFT GUIDING PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA WITH REGARD TO SMART CARDS (adopted by the CDCJ in May 2004). The point of this document was doubt on privacy by increasingly using various smart cards applications. The Council of Europe's data protection experts expressed an opinion that modern technology brought a number of advantages to the daily lives of citizens, as well as risks due to the possibility of interfering in the privacy of individuals. The nature and capability of smart cards create many data protection issues and these new problems need to be addressed; for example, who controls the personal data used in the system? Who is responsible for the accuracy and security of the data when the system is accessible to a number of other entities? How can the multiplication of risks of the possible invasion of the citizens' privacy due to the use of smart card technology be

countered? Who has access to the data subject's personal data and under what conditions? And more. It is not, therefore, the objective of this Council of Europe document to describe the advantages of using smart cards, but to specify the approach that should be followed in order to improve personal data protection when smart card technology is used. A smart card is always used as part of a wider information system and the overall effective protection of personal data of such a system depends on many different factors and circumstances. The security of a system also greatly depends on the behaviour of the people who come into contact with it. Information systems which use smart cards entailing the processing of personal data fall within the scope of application of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No.108). Collecting and processing of personal data in such systems should also respect all the principles of personal data protection established by national data protection legislation.

The document on data protection with regard to smart cards established some basic principles to avoid risks to private life of individuals. Even though the Council of Europe guiding principles are not intended to be an exhaustive solution to all the data protection issues arising with respect to the use of smart cards, it is useful and interesting to take them into account when this technology is used. The guiding principles are intended to set out the basic principles that will not significantly change with innovations in the technology. Nevertheless, it will be appropriate to supplement these principles with the continuing developments in this field.

The Council of Europe GUIDING PRINCIPLES

1. The collection and processing of personal data by means of smart cards should be fair and lawful. Only the personal data necessary for the fulfilment of the purposes for which the card is used should be collected and stored on the card. Systems using smart cards should be transparent to the data subjects whose personal data are processed.
2. Personal data should only be collected and stored on a smart card for legitimate, specific and explicit purposes. They should not be used subsequently in a way which is incompatible with these purposes.
3. The obligations with regard to the protection of personal data fall upon the person who determines the purpose of the system and the means that are used to fulfil this purpose. This implies, in the case of a multipurpose card, that different controllers are each responsible for their part.
4. If a smart card is used for different purposes, the processing should be organised in such a way that the data are not used for purposes other than those for which they were collected. When the same data are used for several purposes they should be limited to what is strictly necessary.
5. Sensitive personal data to be recorded in the card's memory should only be collected if provided for by law or if the data subject has given his/her explicit consent. These data should only be processed in accordance with appropriate safeguards laid down by law. If the collection and processing of such data are based on explicit consent, the data subject should have the right to withdraw consent at any time. Refusal or withdrawal of consent should not be sanctioned with any negative consequences for the data subject.

6. Data recorded on a card should be protected against any unauthorised or accidental access, alteration and/or erasure. The card should offer an appropriate level of security given the state of technology, the sensitive or non-sensitive nature of the data recorded, the number and type of applications and the evaluation of possible risks. The conditions under which third parties may have access to data recorded on the card should be established beforehand for each of the separate purposes for which the card is used.
7. Where personal data are collected and stored on a smart card, the data subject should be informed of the purposes of processing, the identity of the controller, the categories of data concerned and the recipients or categories of recipients of the data that are stored. Other information should be provided to the data subject, where this is necessary to guarantee fair processing of personal data.
8. When a card is issued, the holder should be properly informed about how to use his/her card and what to do in case of fraud or unauthorised disclosure.
9. Whenever personal data are exchanged between a smart card and the system, the data subject should be alerted, unless he/she already has this information. This is particularly important in the case of contactless cards, that is to say if the data subject does not insert or present the card to the system him-/herself.
10. Data subjects should have the right of access to personal data relating to them contained on the card and should have the right to have them corrected or, where necessary, updated.
11. Data resulting from the use of a smart card should be deleted if they are no longer necessary for the specific purpose for which the card was used.
(Full text of the T-PD document is published in the Council of Europe website: www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection)

In the context of security and personal data protection in the electronic passport, it is interesting to mention here also smart card applications as electronic ID card. It is expected that electronic ID cards will reduce illegal immigration, fight terrorism and reduce counterfeiting, ID theft and abuse. There are some different ID card projects in Europe but not fully harmonized – both technology and data content. France is planning to issue ID smart cards in 2007. Besides digital fingerprint, photo and certificate, it is planned to store in chip also some data about cardholder, such as name, address and date of birth. As a technology base it is planned to use dual-interface chip with at least 32 kilobytes memory. The card would have contactless interface what raises some privacy problems (but it is questioned if dual-interface chip has the same level of protection as RFID chip has). Memory capacity of the chip is enough to store biometrics, digital credentials and possibly more personal information. But it is not planned to combine e-ID card with health card (currently Sezam Vital smart health card is used).

Germany is planning to roll out electronic health card as first and e-ID card until around 2009 as the second. There are some activities of cooperation between France and Germany focused on interoperability of ID smart cards in both countries and possibly within more European countries. Four European countries already start a roll-out of chip based ID cards with storing digital certificates – Belgium, Estonia, Finland and Italy and accordingly force cardholders to use electronic signature. A well-known project, published frequently, is ID card in the U.K. It is clear that some European standard on ID cards harmonization will be necessary. Regardless of many interesting pilot and roll-out applications of smart card technology, issuing of RFID passports is in centre.

Applications of RFID technology opened debates between both technology and privacy experts. How much this technology will influence privacy of individuals is a matter of a couple of future years. In 2005 many privacy experts were warning of very specific risks to private life. For example, Mr Bruce Schneier, top U.S. technology expert, cautioned against the possible misuse of RFID chip in passports. "RFID chip can be read by any reader, not just the ones at passport control. It means that passport holders are continuously broadcasting their name, nationality, age, address and whatever else is on the RFID chip. Anyone with a reader can learn that information, without the passport holder knowledge or consent", he said (International Herald Tribune, October 4, 2004).

At the beginning of 2005 the Article 29 Working Party adopted and issued first document related to RFID technology. The WP 29 experts pointed out their concerns about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights. The WP 29 interesting "working document" on data protection issues related to RFID technology contributes to better understanding of influence of this technology to privacy of citizens (WP 105, January 19, 2005). The document is published on the web: http://europa.eu.int/comm/justice_home/fsj/privacy.

Also the Council of Europe will pay its attention to privacy issues related to RFID as was stated in the Draft Work Programme for future work of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS 108) (T-PD). On this issue the Council of Europe will cooperate with the WP 29.

We may expect that experts' works of both important data protection committees will set up sufficient documents to avoid most of risks when RFID is used.

Ochrona danych i karty elektroniczne

Pierwsza plastikowa karta elektroniczna została wydana prawie pół wieku temu, w 1960 r., przez Bank of America. Jednak krokiem milowym tej technologii było wyposażenie karty w elementy pamięci umożliwiające przenoszenie informacji. Kolejny etap rozwoju zaowocował zwiększeniem pojemności pamięci karty, co umożliwiło przechowywanie dużych ilości danych oraz tworzenie nowoczesnego i bezpiecznego narzędzia wykorzystywanego w wielu dziedzinach życia codziennego obywateli.

Tradycyjnie karty elektroniczne są stosowane do dokonywania płatności. Stosuje się je także w sektorze medycznym, transportowym, telekomunikacyjnym, rynkowym i wielu innych. Częstsze jest również używanie kart elektronicznych jako dokumentów tożsamości. Z punktu widzenia ochrony prywatności i danych będziemy mówić o „karcie elektronicznej” jako plastikowej karcie z mikroprocesorem (chipem).

Karta elektroniczna umożliwia łatwy dostęp do informacji przechowywanych w jej pamięci, zapewniając przy tym duży stopień bezpieczeństwa. Jest przenośnym nośnikiem danych, a informacje zawarte w chipie są wykorzystywane pod kontrolą posiadacza karty. Wyjątkową cechą obecnych kart elektronicznych jest możliwość dostosowania ich do obowiązujących zasad i wytycznych dotyczących ochrony prywatności – zgodnie z polityką organów krajowych i międzynarodowych w sprawie ochrony prywatności i bezpieczeństwa.

Ogólnie rzecz biorąc, karty elektroniczne można podzielić według różnych ich właściwości. Na przykład według: typu dostępu (połączenia) do informacji (dane są odczytywane przez czytnik za pomocą bezpośredniego kontaktu fizycznego lub bezkontaktowego interfejsu – karta kontaktowa, bezkontaktowa), rodzaju pamięci (z paskiem magnetycznym – karta magnetyczna, z mikroprocesorem – karta pamięci, z bezpieczniejszym mikroprocesorem karta MCU), modułu bezpieczeństwa (dane są szyfrowane za pomocą modułu kryptograficznego – kryptokarta), a także sposobu użycia: jednoaplikacyjne, wieloaplikacyjne, wielofunkcyjne itd.

Podstawowe wymagania dotyczące przechowywania oraz dostępu do informacji zawartych w chipie to zgodność z podstawowymi zasadami ochrony informacji, a mianowicie:

- dostępności – do danych ma dostęp i może z nich korzystać na żądanie upoważniona osoba,
- poufności – dane są chronione przed dostępem osób nieupoważnionych,
- integralności – dane są chronione przed bezprawnymi zmianami, przeróbkami bądź zniszczeniem.

Przemysł kart elektronicznych stopniowo się rozwija. Sektorem, w którym są one wykorzystywane w największym stopniu, jest telekomunikacja, która ciągle zajmuje czołowe miejsce. W 2005 r. przewidywano użycie 1,3 biliona kart SIM w telefonach komórkowych. W 2006 r. liczba ta zwiększyła się – głównie dzięki nowym abonentom w Azji, Chinach i Indiach. Na przykład tylko w Chinach rynek kart SIM w 2005 r. oceniano na 300 milionów. Według analizy dokonanej przez Eurosmart w roku 2006 zwiększył się sprzedaż kart SIM o 25%. Przewiduje się, że wzrośnie ich liczba w związku ze stosowaniem ich przez instytucje rządowe (krajowe dokumenty tożsamości, prawo jazdy), służbę zdrowia (około 60 milionów do końca 2005 r.) i sektor bankowy (około 330 milionów).

Kolejną istotną kwestią, przede wszystkim z punktu widzenia bezpieczeństwa i ochrony prywatności, jest wzrost stosowania technologii high-end SIM – kart SIM do wielokrotnego zapisu o pojemności co najmniej 64 kilobajtów (wspierającej technologię 3G).

W roku 2006 w dalszym ciągu będą wprowadzane na rynek bezkontaktowe karty płatności. Planuje się przeprowadzenie wielu testów bezkontaktowych form płatności. Dotyczy to zarówno kart, jak i telefonów komórkowych. W roku 2006 w dalszym ciągu będą rozwijane karty i terminale zgodne ze standardami EMV, ograniczającymi pewne typy oszustw dokonywanych za pomocą kart (EMV jest międzynarodowym standardem dotyczącym elektronicznych kart kredytowych i debetowych).

Znaczące zwiększenie zastosowania kart przez instytucje rządowe będzie miało związek z wydawaniem elektronicznych paszportów oraz innych elektronicznych dokumentów podróży i dokumentów tożsamości. Rok 2006 to ostateczny termin, do którego kraje członkowskie Unii Europejskiej mają wprowadzić bezkontaktowe chipy i małe anteny w paszportach. Będą one zawierać cyfrowe zdjęcie twarzy, linie papilarne i być może inne dane biometryczne posiadacza paszportu. Mała antena, będąca częścią chipa, umożliwia przesyłanie danych do czytników. Karta ta nazywana jest kartą RFID (identyfikacji częstotliwości radiowych). Stany Zjednoczone są siłą napędową we wprowadzaniu e-paszportów w reakcji na ataki terrorystyczne 11 września 2001 r. Wiosną 2002 r. uchwalono ustawę wymagającą od sojusznicznych państw wprowadzenie do października 2004 r. elektronicznych paszportów zawierających dane biometryczne. Prace nad wprowadzeniem programu

elektronicznych paszportów trwają w około 40 państwach. Głównym zastosowaniem chipa w paszportach jest przechowywanie w nim danych biometrycznych. Będą one wykorzystywane do weryfikowania, czy osoba legitymująca się paszportem jest tą samą osobą, której paszport został wydany. Na przykład umieszczenie cyfrowego zdjęcia na chipie ogranicza fałszowanie paszportów przez przestępców, którzy zamieniają zdjęcia na stronie zawierającej dane personalne. W przypadku paszportów elektronicznych kontroler służby granicznej miałby również możliwość zobaczenia zdjęcia zapisanego w chipie. Bardzo trudne, wręcz niemożliwe jest dokonanie zamiany zdjęcia na stronie z danymi osobowymi oraz w chipie w identyczny sposób. Kolejnym aspektem bezpieczeństwa jest to, że chip będzie chroniony przed ponownym zapisem. Nie będzie więc możliwe dodawanie nowych danych, czy też ich modyfikacja. Parametry techniczne chipa w połączeniu z danymi biometrycznymi zapewnią dużą dokładność w weryfikowaniu tożsamości posiadacza paszportu. Testy rozpoznawania twarzy przeprowadzone w Australii (przez pracowników linii lotniczych Qantas w 2002 r.) wykazały, że w 98% przypadków dokonano pozytywnego rozpoznania, natomiast w sytuacji rozpoznawania dokonywanego przez inspektora na podstawie porównywania zdjęcia do osoby wskaźnik ten wyniósł 60% (według Boba Nasha, dyrektora działu paszportów w Departamencie Spraw Zagranicznych i Handlu). Barry Kefauver, specjalista i były urzędnik Departamentu Stanu USA, przewodniczący Komisji Międzynarodowej Organizacji Standaryzacyjnej (ISO), który jest doradcą Międzynarodowej Organizacji Lotnictwa Cywilnego (ICAO) w sprawach e-paszportów, stwierdził, że połączenie danych biometrycznych i bezkontaktowego chipa spowoduje, że nowe elektroniczne paszporty będą dużo bezpieczniejsze od obecnych. Bez wątpienia dane biometryczne, takie jak linie papilarne bądź rysy twarzy, są cennym narzędziem służącym identyfikacji. Przy tym bardzo złe i niebezpieczne jest stanowisko wielu osób twierdzących, że przetwarzanie danych biometrycznych zawiera zerowy współczynnik błędów związany z niewłaściwym użytkowaniem bądź poważnym atakiem. Przechwycenie danych stanowi poważne zagrożenie we wszystkich systemach wykorzystujących karty bezkontaktowe. Dlatego ten rodzaj przetwarzania danych osobowych należy poddać dokładnej analizie. Wielu zwolenników prywatności krytykuje koncepcję elektronicznych paszportów zawierających dane biometryczne, twierdząc, że doprowadzi to do powstania globalnej bazy danych biometrycznych milionów osób, a dane osób podróżujących dostaną się w ręce tych, którzy nie przestrzegają praw człowieka. Don Davis, redaktor naczelny i wydawca „Card Technology Magazine” stwierdził, że „prywatność pozostanie wielką sprawą, gdy wzrasta zastosowanie zaawansowanej technologii do weryfikowania tożsamości”. Eksperti od spraw technologii bezkontaktowej uważają natomiast, że trudno byłoby w realnych warunkach zebrać te dane. Jednakże naciski ze strony ekspertów i grup do spraw ochrony prywatności wymusiły na rządzie USA zainteresowanie się działaniem kart bezkontaktowych oraz przedsięwzięcie dodatkowych środków bezpieczeństwa.

Opis i analiza ryzyka związanego z przetwarzaniem osobowych danych biometrycznych nie jest jednakże tematem tego artykułu.

Przewidywane jest wydawanie około 4 milionów paszportów rocznie. Niektóre państwa (np. Zjednoczone Królestwo) mają zamiar opracować inny rodzaj elektronicznych dowodów tożsamości. Unia Europejska wyznaczyła datę 28 sierpnia 2006 r. jako termin pierwszego etapu wprowadzania e-paszportów dla obywateli UE. Z wprowadzeniem elektronicznych paszportów wiążą się nowe obawy, co do zagrożenia bezpieczeństwa i ochrony prywatności. Wiele osób obawia się, że przestępcy będą umieli odczytywać nielegalnie dane z chipa umieszczonego w paszporcie. Celem wprowadzenia e-paszportów jest zabezpieczenie granic, jednakże trzeba skupić uwagę także na takich sprawach, jak pry-

watność danych osobowych. Jeśli jedno z głównych założeń dotyczyło utworzenia skutecznego narzędzia w walce z terroryzmem, czyli e-paszportów, należy zwrócić uwagę, że najbardziej sensacyjne zagrożenie stanowi sytuacja, w której terroryści odczytywali by dane z chipów w paszporcie na odległość, a następnie kierowali swe działania przeciwko obywatelom poszczególnych państw. W liście wpływowej Amerykańskiej Unii Swobód Obywatelskich (ACLU) skierowanym wnioskiem do Departamentu Stanu USA jest stwierdzenie, że „w efekcie paszporty te byłyby jak środek tarczy na plecach osób, które by je nosiły”. W przypadku zastosowania e-paszportów w branży turystycznej problematyczną kwestią jest osiągnięcie interoperacyjności między bezkontaktowymi chipami i czytnikami produkowanymi przez różnych producentów i dostawców. Kwestia ta będzie (prawdopodobnie) rozwiązana przez Międzynarodową Organizację Lotnictwa Cywilnego (International Civil Aviation Organization – ICAO), która ustanawia standardy dla dokumentów podróży. Zadecydowała ona o stosowaniu bezkontaktowych chipów jako standardowych nośników danych o posiadaczu paszportu (standard 9303 for Machine Readable Travel Documents). Standard ICAO zyskał poparcie Międzynarodowej Organizacji Standaryzacyjnej (ISO) i osiągnął status standardu światowego.

Rada Europy zwróciła uwagę na zwiększające się zagrożenie w dziedzinie ochrony prywatności wynikające z rozwoju nowoczesnej technologii, w tym kart elektronicznych. Od 1996 r. Grupa ds. Ochrony Danych (Project Group on Data Protection – CJ-PD) jest zaangażowana w sprawy ochrony danych osobowych i prywatności w odniesieniu do technologii kart elektronicznych. Pierwszy dokument dotyczący tych kart został wydany przez Radę Europy w 1985 r. [„Legal Problems Resulting from Official Machine-Readable Identification Documents”, CJ-PD (85)3, 1985 r.]. W 2003 r. CJ-PD opracowała i przyjęła ważny dokument w sprawie ochrony danych osobowych w przypadku używania kart elektronicznych – „Projekt wytycznych dotyczących ochrony danych osobowych w związku z używaniem kart elektronicznych” („Draft guiding principles for the protection of personal data with regard to smart cards”), przyjęty przez CDCJ * w maju 2004 r. Dokument ten poddał w wątpliwość skuteczność przestrzegania zasad ochrony prywatności na skutek coraz większego i bardziej zróżnicowanego zastosowania kart elektronicznych. Eksperti do spraw ochrony danych Rady Europy zauważyli, że nowoczesna technologia przynosi wiele korzyści obywatelom w życiu codziennym, niesie jednak ze sobą także zagrożenie ingerencją w sferę prywatności jednostek. Z właściwości i różnorodności zastosowań kart elektronicznych wynika wiele kwestii odnoszących się do ochrony danych. Tymi nowymi problemami należy się zająć. Dotyczą one, na przykład, osób kontrolujących dane osobowe stosowane w systemie. Kto jest zatem odpowiedzialny za dokładność i bezpieczeństwo danych, kiedy do systemu mają dostęp inne jednostki? Jak można przeciwdziałać zagrożeniu możliwą ingerencją w prywatność obywateli na skutek stosowania technologii kart elektronicznych? Kto ma dostęp do danych osobowych podmiotu i w jakich okolicznościach? I wiele innych, podobnych kwestii. Nie było celem dokumentu Rady Europy opisywanie zalet użytkowania kart elektronicznych, ale określenie stanowiska, które należy zająć dla zwiększenia ochrony danych osobowych przy stosowaniu technologii kart elektronicznych. Karta elektroniczna jest zawsze częścią większego systemu informacyjnego, a całkowita skuteczna ochrona danych osobowych tego systemu jest uwarunkowana wieloma różnymi czynnikami i okolicznościami. Bezpieczeństwo systemu zależy w dużym stopniu także od postępowania osób, które mają z nim kontakt. Systemy informacyjne wykorzystujące technologię kart

* Europejski Komitet Współpracy Prawnej, przyp. tłum.

elektronicznych i przetwarzające dane osobowe podlegają regulacjom „Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych” (ETS nr 108). Zbieranie i przetwarzanie danych w takich systemach powinno odbywać się z respektowaniem wszystkich zasad ochrony danych osobowych ustanowionych przez krajową legislację w dziedzinie ochrony tych danych.

W dokumencie dotyczącym ochrony danych w związku ze stosowaniem kart elektronicznych przyjęto kilka podstawowych zasad uniknięcia niebezpieczeństwa ingerencji w prywatne życie jednostki. Mimo że celem ich opracowania nie było zapewnienie ostatecznych rozwiązań w sprawie ochrony danych we wszystkich dziedzinach związanych z używaniem kart elektronicznych, jednakże w przypadku stosowania tej technologii należy je wziąć pod uwagę, gdyż są przydatne i interesujące. W dokumencie tym są przedstawione podstawowe zasady, które nie zmieniają się w istotnym stopniu w obliczu rozwoju technologii. Jednak stosowne byłoby uzupełnianie ich w miarę rozwoju tej technologii.

Wytyczne Rady Europy

1. Gromadzenie i przetwarzanie danych osobowych za pomocą kart elektronicznych powinno być uczciwe i zgodne z prawem. Na karcie powinny być gromadzone i przechowywane tylko te dane osobowe, które są niezbędne do osiągnięcia celów, dla których karta została wydana. Systemy korzystające z kart elektronicznych powinny być przejrzyste dla podmiotów, których dane osobowe są przetwarzane.
2. Dane osobowe powinny być gromadzone i przechowywane na karcie magnetycznej wyłącznie dla legalnych, określonych i jasnych celów. Nie powinny być wykorzystywane w sposób niezgodny z tymi celami.
3. Do przestrzegania przepisów związanych z ochroną danych osobowych są zobowiązane osoby, które określiły cel danego systemu oraz środki stosowane dla osiągnięcia tego celu. Oznacza to, że w przypadku kart wielofunkcyjnych za każdą część jest odpowiedzialny inny kontroler.
4. W przypadku stosowania karty do różnych celów, przetwarzanie danych powinno być zorganizowane w taki sposób, aby dane nie były wykorzystywane do celów innych niż te, dla których zostały zgromadzone. Jeśli te same dane są wykorzystywane do kilku celów, należy je ograniczyć do tych, które są konieczne.
5. Dane należące do szczególnej kategorii danych, które mają być zapisane w pamięci karty, mogą być gromadzone tylko w przypadkach usankcjonowanych prawnie bądź jeśli podmiot jasno wyraził na to zgodę. Dane te powinno się przetwarzać tylko przy zastosowaniu odpowiednich zabezpieczeń ustanowionych przez prawo. Jeśli gromadzenie i przechowywanie danych ma miejsce za wyraźną zgodą podmiotu, którego dane dotyczą, powinien on mieć prawo do wycofania zgody w dowolnym momencie. Odmowa bądź wycofanie zgody nie powinno być sankcjonowane żadnymi negatywnymi konsekwencjami dla podmiotu.
6. Dane zapisane na karcie powinny być zabezpieczone przed nieupoważnionym bądź przypadkowym dostępem innych osób, przed dokonywaniem w nich zmian i (lub) usuwaniem danych. Karta powinna zapewniać odpowiedni poziom ochrony z uwzględnieniem zastosowanej technologii, kategorii rejestrowanych danych, liczby i rodzaju aplikacji oraz oceny potencjalnego ryzyka. Warunki, na jakich osoby trzecie mogą mieć dostęp do danych zapisanych na karcie, powinny być ustalone wcześniej dla każdego z celów, do których karta jest używana.

7. Kiedy dane personalne są gromadzone i przechowywane na karcie elektronicznej, podmiot, którego dane dotyczą, powinien zostać poinformowany o celach przetwarzania tych danych, tożsamości kontrolera, kategoriach danych i odbiorcach bądź kategoriach odbiorców przechowywanych danych. Jeśli zaistnieje taka konieczność, podmiotowi należy udzielić innych informacji, by zagwarantować mu uczciwe przetwarzanie danych osobowych.
8. Z chwilą wydania karty właściciel powinien zostać odpowiednio poinformowany, jak ma z niej korzystać i co należy zrobić w przypadku oszustwa bądź bezprawnego ujawnienia danych.
9. Ilekroć dojdzie do wymiany danych osobowych między kartą elektroniczną a systemem, należy poinformować o tym podmiot, którego dane dotyczą, o ile nie ma on już tej informacji. Jest to szczególnie ważne w przypadku kart bezkontaktowych, tzn. jeśli podmiot nie posługuje się kartą osobiście.
10. Podmioty powinny mieć prawo dostępu do danych osobowych, które ich dotyczą, a które są umieszczone na karcie. Powinny też mieć prawo do tego, aby te dane poprawiano bądź – gdy zajdzie taka potrzeba – uaktualniano.
11. Dane stosowane przy użyciu kart elektronicznych powinny być usuwane, jeśli nie są już konieczne dla określonego celu, dla którego były wykorzystywane.
Pełny tekst dokumentu jest opublikowany na stronie internetowej Rady Europy:
www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/.

W kontekście bezpieczeństwa i ochrony danych osobowych w paszporcie elektronicznym interesującą kwestią jest stosowanie kart elektronicznych jako elektronicznych dowodów tożsamości. Przewiduje się, że dowody te przyczynią się do ograniczenia nielegalnej imigracji, do zwalczania terroryzmu, fałszerstw, kradzieży dowodów tożsamości i innych nadużyć. W Europie opracowano kilka różnych projektów dotyczących elektronicznych dowodów tożsamości, jednak nie są one w pełni zharmonizowane – zarówno pod względem technologii, jak i zawartości danych. Francja ma w planach wydanie dowodów w postaci elektronicznej w 2007 r. Oprócz cyfrowych linii papilarnych, zdjęcia i certyfikatu, jest planowane zamieszczenie w chipie danych dotyczących właściciela paszportu, takich jak nazwisko, adres i data urodzenia. Jeśli chodzi o technologię, planuje się zastosowanie chipa z podwójnym interfejsem mającym co najmniej 32 kilobajtów pamięci. Karta będzie wyposażona w bezkontaktowy interfejs, co rodzi problemy w dziedzinie ochrony prywatności (powstaje pytanie, czy chip z podwójnym interfejsem ma ten sam poziom zabezpieczeń co chip RFID). Pamięć chipa będzie miała wystarczającą pojemność, by przechowywać dane biometryczne, cyfrowe dokumenty uwierzytelniające i być może więcej danych personalnych. Nie planuje się jednak łączenia elektronicznych dowodów tożsamości z kartami zdrowia (obecnie używa się karty Sezam Vital).

Niemcy planują najpierw wydanie elektronicznej karty zdrowia, a następnie elektronicznych dowodów tożsamości do około 2009 r. Podjęto pewne kroki w celu nawiązania współpracy między Francją i Niemcami dla osiągnięcia interoperacyjności między elektronicznymi dokumentami tożsamości w obu krajach i być może w kilku innych krajach europejskich. Cztery państwa europejskie: Belgia, Estonia, Finlandia i Włochy rozpoczęły już wydawanie dokumentów tożsamości z chipami zawierającymi cyfrowe certyfikaty, co jest związane tym samym ze stosowaniem podpisu elektronicznego przez posiadaczy. Często publikowanym, bardzo znanym rozwiązaniem jest projekt dowodu tożsamości opracowany w Zjednoczonym Królestwie. Konieczne będzie przy tym wprowadzanie europejskich standardów w celu ujednolicenia dokumentów

tożsamości. Niezależnie od wielu interesujących pilotażowych zastosowań technologii kart elektronicznych, wydawanie paszportów z technologią RFID znajduje się wciąż w centrum uwagi. Aplikacje tej technologii zapoczątkowały debaty ekspertów do spraw technologii i ochrony prywatności. Kwestią najbliższych kilku lat jest określenie wpływu, jaki technologia ta będzie miała na prywatność jednostek. W 2005 r. wielu ekspertów do spraw ochrony prywatności ostrzegało przed ryzykiem wprowadzenia technologii RFID w życie prywatne. Na przykład Bruce Shneier, główny ekspert USA do spraw technologii, ostrzegał przed możliwym niewłaściwym użyciem chipa RFID w paszportach. Stwierdził, że „każdy czytnik może czytać chip RFID, nie tylko ten podczas kontroli paszportowej. Oznacza to, że posiadacze paszportów nieustannie ujawniają swoje nazwisko, narodowość, wiek, adres i inne informacje zawarte w chipie RFID. Każdy, kto posiada czytnik, może uzyskać te informacje bez wiedzy i zgody właściciela paszportu” („International Herald Tribune”, 4 października 2004 r.).

Na początku 2005 r. Grupa Robocza Art. 29 przyjęła i wydała pierwszy dokument dotyczący technologii RFID. Eksperci wyrazili wówczas swoje obawy co do możliwości stosowania tej technologii w celu naruszenia ludzkiej godności i prawa do ochrony danych. Ten interesujący „dokument roboczy” Grupy Roboczej Art. 29 odnoszący się do kwestii ochrony danych związanych ze stosowaniem technologii RFID przyczynił się do lepszego zrozumienia wpływu tej technologii na życie prywatne obywateli (WP 105, 19 stycznia 2005 r.). Dokument ten został opublikowany na stronie internetowej: http://europa.eu.int/comm/justice_home/fsj/privacy/.

Rada Europy również przywiązuje dużą wagę do spraw ochrony prywatności w związku z technologią RFID, co zostało ujęte w „Projekcie programu działania Grupy Koordynacyjnej ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych” („Draft Work Programme for future work of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”) (ETS 108) (T-PD). W kwestii tej Rada Europy będzie współpracować z Grupą Roboczą Art. 29. Można oczekiwać, że wynikiem prac ekspertów z obu ważnych organów będzie wystarczająca liczba dokumentów, aby uniknąć większości zagrożeń wynikających ze stosowania omawianej technologii.

Michel Parisse

Chairman of the Belgian Data Protection Authority
Przewodniczący Belgijskiego Organu Ochrony Danych

Spring conference in Krakow and data protection in the third pillar: one year later

Emergence of the need to increase European exchange of data

The terrorist attacks of September 2001 in New York resulted in a period of extensive counter-terrorism activities. The Madrid bombing in March 2004 (and later in July 2005 in London) further accelerated this process and a number of proposals designed to strengthen EU counter-terrorism activities arose. In particular, these proposals intend to develop closer cooperation, to increase data sharing and data exchange between Member States' law enforcement agencies and attempt to highlight the links between combating terrorism and tackling other forms of serious crime.

The fight against terrorism or other serious crime is not an isolated activity of one or two law enforcement agencies; it involves a huge number of agencies throughout the European Union and therefore can only be dealt with effectively through European and international cooperation. It is the reason why the Hague Programme strengthening freedom, security and justice in the European Union emphasizes the necessity of an innovative approach to the cross-border exchange of law enforcement information and introduces the principle of availability which means that “throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State.”

However, cooperation which involves such an exchange of personal data could only be allowed if strictly regulated with regard to data protection principles. In this respect, the Hague Programme stresses that the introduction of the principle of availability is dependent on the key conditions in the area of data protection.

Moreover, a harmonized standard of data protection is necessary insofar as personal data are communicated between States which may have different levels of data protection. For example, it would be unacceptable if a country, having received personal data from another Member State, was to retain those data for longer than they would have been retained in the originating Member State.

The pillar structure of the European Union

According to its current structure, the European Union takes decisions in three separate “domains” (policy areas), also known as the three “pillars” of the EU. While in

the First Pillar – which is covering most of the common policies – decisions are taken by the “Community method”, the two others are intergovernmental and decisions are taken by the Council, the powers of the European Parliament, the Commission and European Court of Justice being significantly limited. Until 1997, issues like asylum and immigration, external border checks (visas) and judicial cooperation in civil and commercial matters were the matters for direct cooperation between the EU governments. But the Treaty of Amsterdam transferred these issues from the intergovernmental to the “Community” domain, so they all now come under the First Pillar and are governed by the Community method with some specific arrangements. One field remains exclusively intergovernmental: the field of police and judicial cooperation in criminal matters which comes under the “Third Pillar”.

Due to the own rules and organs of each pillar, the legislative process may become particularly complicated when different pillars are concerned. This has been illustrated recently during the setting-up of the second general SIS (“SIS II”). Although the SIS II has to be considered as a single information system, separate instruments are necessary for governing the SIS II as it depends on two different legal bases. This leads to a rather complex regime, in particular concerning data protection rules.

This should be solved with the adoption of the European Constitution that suppresses the pillars and puts an end to the intergovernmental method governing the Third Pillar by making the legislative process, the representation, the judicial control and the enforcement of the legislative acts at the Union level subject to the rules, procedures and instruments of the Community method. In fact, the Constitution aligns the adoption of the acts with the Community method.

Data protection in the Third Pillar

Background

The Community has developed a detailed data protection framework for the First Pillar based on the 1995 Data Protection Directive, which contains detailed rules on, among other things, the principles governing data exchange, supervision, and the transfer of data to third countries while there is no general framework for data protection in the Third Pillar.

Specific rules on data protection and the supervision of data exchange are, on the other hand, contained in the legislation governing the functions of the individual Third Pillar bodies such as Europol and Eurojust. Another set of data protection rules also governs the operation of the Customs Information System and the Schengen Information System. The rules are tailor-made to the functions of each of these systems. Each body and system has its own supervision arrangements and the absence of general rules in the Third Pillar remains a problem.

Moreover, contrary to the First Pillar where the data protection commissioners have a suitable organizational framework dealing with data protection issues through the Article 29 Working Party; the Third Pillar does not have such a forum, the joint supervisory bodies in the Third Pillar (e.g. Europol, Schengen, Eurojust) having a specific mandate. Because of the lack of such a forum, data protection commissioners cannot ensure that their advice to the bodies involved in legislative measures on data protection issues is given at an early stage, after Europe-wide consultation and with the

requisite level of quality. This is why the European Conference of Data Protection Commissioners adopted a resolution in Wroclaw in September 2004 to set up a joint forum, the Working Party on Police, dealing with data protection in the Third Pillar.

Further to different European proposals involving the collection and the exchange of personal data, the Working Party on Police elaborated documents about the data protection in the Third Pillar that were presented at the Spring Conference of European Data Protection Commissioners which was held in April 2005 in Krakow.

Proposed argumentation

At the occasion of this conference, it seemed important to the author of this contribution to bring to the conference the following idea: the necessity of the specific – but not autonomous – Third Pillar regulation.

If the data protection legal framework in the Third Pillar cannot at the time be legally reached through an extension of the scope of application of Directive 95/46, a distinct legal instrument is therefore needed. It seems, nevertheless, that the principles of the Directive must be complied with, while still taking into account the fair Third Pillar specificity. In the long range, that is, after the adoption of the European constitution, an integrated data protection regime covering all pillars should emerge, that would guarantee a high level of protection.

As to the content of a draft framework decision on data protection in the Third Pillar and the legal technique used, one of the solutions analyzed by the services of the Commission was the reference, in the framework decision, to the provisions of the Directive – derogations and exceptions would be, of course, foreseen, as needed considering the Third Pillar specificity.

From a legal perspective, such « reference » technique should not pose any problem. It has been acknowledged that the Directive cannot at the moment be extended (and thus amended) to the Third Pillar, but this should not preclude from having a Third Pillar decision (adopted pursuant to the Third Pillar institutional rules) « borrowing » First Pillar legislation. These rules would thus get the statute of the Third Pillar rules as well. We would then have a sort of “functional division” and the Directive would be applicable *in se* in the First Pillar, and through reference in the Third Pillar.

The benefit of such a solution would be important as a symbol: from now on, Europe would clearly show how decisive it considers that the integrated regime we call for is effectively based on the level of protection guaranteed by the Directive. The merging of regulations (Directive/framework decision) would be facilitated, but even more, it would appear as a natural and logical follow-up of the legal technique used.

A second issue is the question of the advisory body that would be foreseen/designated/created within the Third Pillar.

It is advisable, and data protection commissioners have called for it at the occasion of the Wroclaw conference (see above), that an advisory body should be competent for the Third Pillar issues. This should not, however, lead to additional splitting of the consultative competences already existing. One could wonder whether there is no such risk in establishing in the Third Pillar a body distinct from the Article 29 Working Party.

The risk does not seem to be excessive, considering that for a large part, the same persons would participate in the two bodies. If this solution was to be adopted, symmetry and a composition as similar as possible should be ensured in the two bodies: this would be essential to avoid that data protection rules – presumed identical or comparable – be interpreted in divergent ways (precision of purpose, proportionality, security measures, etc.), depending on the body in which they are discussed.

In the perspective of the merging of the pillars, the most adequate solution should be the Article 29 Working Party be referred to as well, and that it would thus be explicitly given a second competence, so that it would formally be established/sanctioned as an “interpillar” body. What could be foreseen is the setting within the Art. 29 Working Party of a more specific cenacle. Beyond the advantage to prevent divergences of jurisprudence, once again the First and Third Pillars merging might be facilitated with regard to data protection, if we could avoid, at that time, the handling of the tasks of two advisory bodies that might, meanwhile, have developed their own lives.

However, if the solution of a unique body appears impracticable, for a number of reasons, at least in the short term, an autonomous body, «copied» on the Article 29 Working Party (or created within the Working Party) could constitute an adequate solution.

In order to avoid as much as possible the risk of diverging jurisprudence from that of the Article 29 Working Party, it seems important that representatives of the data protection authorities in this group should be, as much as possible and at least part of them, the same as those in the Article 29 Working Party. The high level of representation in the Article 29 Working Party is another argument in order to grant this new body the similar legitimacy to that of the Working Party – this being said without underestimating the role of technicians in the quality of the work performed and the concrete knowledge of the Third Pillar issues. Organizing the meetings of this new authority before or after the meetings of the Article 29 Working Party would certainly contribute to reaching these objectives.

The European Data Protection Supervisor and the presidents of the Joint Supervisory Bodies should be represented in this authority. It does not seem advisable to extend further the specific composition of this body with regard to that of the Art. 29 WP, especially considering the risks mentioned above.

Finally, it is essential that the supervisory body has sufficient means and resources (such as a secretariat, a budget, etc.) to be able to achieve effectively and efficiently its tasks.

Recent developments

During the Spring Conference of 2005 in Krakow, the European Data Protection Authorities have adopted three documents about data protection in the Third Pillar: the Krakow Declaration, the Position paper on Law Enforcement & Information Exchange in the EU constituting an addendum to the Krakow Declaration and the Opinion on the draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts.

In these documents, the Conference insists on the necessity to develop a harmonized data protection approach in the Union and the creation of a comprehensive European law on data protection covering all areas of processing personal data. In particular, the Conference stresses that: “In order to avoid a divergence between the First and the Third Pillar which would have a negative impact on enforcement and transparency and in view of the Charter of Fundamental Rights and the forthcoming Constitution for Europe which will abolish the Pillars, the Conference calls to preserve – and where necessary to regain – the coherence, the consistency and the unity of data protection. The principles of Directive 95/46 should form the common core of a comprehensive European data protection law”. The Conference also indicates that “stress must be put on the need for a EU Working Party composed of representatives of the national and the EU data protection supervisory authorities acting independently, entrusted with cooperation, monitoring and advisory missions”.

In the same perspective, the European Parliament has recommended to “harmonize existing rules on the protection of personal data in the instruments of the current Third Pillar, bringing them together in a single instrument that guarantees the same level of data protection as provided for under the First Pillar”.¹

In October 2005, the European Commission adopted a proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This proposal follows the principles laid down in the Directive 95/46/EC and takes into account many points of the position paper of the Krakow conference. Moreover, it creates an autonomous supervisory body based on the model used for the Article 29 Working Party.

Shortly after the meeting held in January 2006, the European Conference adopted an opinion on this proposal. In its opinion, the Conference welcomes the proposed introduction of specific data protection principles in the Third Pillar to safeguard citizens considering that the introduction of new, systematic, well-balanced safeguards will contribute to effectively enhancing the prevention of and fight against crime, but it also requested to clarify, supplement or amend some provisions in the text in order to prevent interpretive issues and excessively divergent applications.

Conclusion

The need for and the importance of the legal framework on data protection in the Third Pillar as well as the consistency of the data protection within the European Union have been emphasized on several occasions. The proposal of the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters proposed by the European Commission may be considered as an important step towards harmonization of the data protection rules in the Third Pillar.

Moreover, considering it as an intermediary step in order to facilitate, in due time, the adoption of a single instrument for the First-Third Pillar, the approach of the Commis-

¹) European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences [2005/2046(INI)].

sion taking into account the recommendation of the data protection authorities to follow principles laid down in the Directive 95/46 is very much welcome.

.....

Finally, I take the opportunity of this contribution to thank Mrs Kulesza as president of the Polish Data Protection Authority who has been hosting and organizing the two conferences where decisive steps were made by data protection authorities in their work on data protection in police and security issues.

She has enabled the data protection commissioners to bring their work to successful achievement in the data protection area and to give a consistent input in decision making on this matter.

On behalf of the Belgian DPA, I wish her every success and my best wishes in the pursuit of her career.

Wiosenna konferencja w Krakowie a ochrona danych w trzecim filarze: rok później

Powstanie potrzeby rozszerzenia europejskiej wymiany danych

W wyniku ataków terrorystycznych na Nowy Jork we wrześniu 2001 r., rozpoczął się okres intensywnych działań w dziedzinie zapobiegania terroryzmowi. Zamachy bombowe w Madrycie w marcu 2004 (a następnie zamach w Londynie w lipcu 2005) jeszcze bardziej przyspieszyły ten proces i przyczyniły się do powstania licznych projektów mających na celu wzmocnienie działalności antyterrorystycznej w Unii Europejskiej. Projekty te były w szczególności nastawione na zacieśnianie współpracy, zwiększenie przepływu danych i wymiany danych pomiędzy organami ścigania Państw Członkowskich. Miały one także na celu próbę podkreślenia podobieństw pomiędzy zwalczaniem terroryzmu a zwalczaniem innych form poważnej przestępczości.

Zwalczanie terroryzmu i innych form przestępczości zorganizowanej nie jest przedmiotem działania tylko organów ścigania. Wymaga bowiem współdziałania wielu służb w całej Unii Europejskiej i jako takie może być skutecznie prowadzone wyłącznie dzięki współpracy europejskiej oraz międzynarodowej. Z tego powodu „Program Haski”, którego celem jest wzmocnienie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, zwraca uwagę na konieczność nowatorskiego podejścia do przepływu przez granice informacji odnoszących się do przestępczości i wprowadza zasadę dostępności, zgodnie z którą „na obszarze całej Unii urzędnik organu ścigania w jednym Państwie Członkowskim, któremu niezbędne są informacje w związku z wykonaniem jego obowiązków, może je uzyskać od drugiego Państwa Członkowskiego oraz że organ ścigania w tym drugim Państwie Członkowskim, który posiada owe informacje, udostępni je we wskazanym celu, uwzględniając wymagania toczących się dochodzeń w danym państwie.”

Jednakże współpraca, która wymaga takiego przepływu danych osobowych może być dozwolona wyłącznie pod warunkiem istnienia ścisłych regulacji zgodnych z za-

sadami ochrony danych osobowych. W tym zakresie „Program Haski” podkreśla, że wprowadzenie zasady dostępności zależy od spełnienia zasadniczych warunków odnoszących się do ochrony danych.

Co więcej, zapewnienie spójności standardów ochrony danych osobowych jest konieczne ze względu na fakt, że dane przekazywane są pomiędzy państwami, które przyjęły różne poziomy ochrony danych osobowych. Byłoby na przykład nie do przyjęcia, gdyby państwo, po otrzymaniu danych osobowych od innego Państwa Członkowskiego, miało przechowywać je dłużej niż byłyby one przechowywane w państwie ich pochodzenia.

Struktura filarów Unii Europejskiej

Zgodnie ze swoją obecną strukturą Unia Europejska podejmuje decyzje w trzech oddzielnych „domenach” (obszarach polityki) znanych także pod nazwą „trzech filarów” Unii. O ile w pierwszym filarze, który jest domeną wspólnej polityki, decyzje podejmowane są „procedurą współdecydowania”, o tyle dwa pozostałe filary są międzyrządowe, a ich decyzje podejmowane są przez Radę, natomiast władza Parlamentu Europejskiego, Komisji Europejskiej oraz Europejskiego Trybunału Sprawiedliwości jest w znaczący sposób ograniczona. Do roku 1997 problemy, takie jak azyl polityczny, imigracja, zewnętrzna kontrola graniczna (wizy) i współpraca sądowa w sprawach cywilnych i handlowych były przedmiotem bezpośredniej współpracy pomiędzy rządami Państw Członkowskich Unii Europejskiej. Jednak „Traktat Amsterdamski” przeniósł te kwestie z obszaru międzyrządowego na obszar Wspólnoty, tak że obecnie wszystkie one wchodzą w zakres pierwszego filaru i rozstrzygane są według procedur współdecydowania z pewnymi szczególnymi ustaleniami. Jedyna dziedzina, która pozostała wyłącznie w gestii międzyrządowej, to współpraca policyjna i sądowa w sprawach karnych, która wchodzi w zakres trzeciego filaru.

Ponieważ w każdym z filarów istnieją odrębne przepisy i organy, proces legislacyjny staje się bardzo skomplikowany, gdy dotyczy różnych filarów. Dobrą ilustracją tego stwierdzenia było niedawne wprowadzenie drugiego ogólnego systemu SIS (SIS II). Mimo że SIS II był uznawany za system opierający się na jednym systemie informacyjnym, do zarządzania nim konieczne są zatem oddzielne instrumenty, ponieważ SIS II działa według dwóch niezależnych podstaw prawnych. Prowadzi to do powstania dość skomplikowanego reżimu, szczególnie w części dotyczącej ochrony danych.

Problem ten powinien zostać rozwiązany po przyjęciu konstytucji europejskiej, która będzie nadrzędna w stosunku do filarów i położy kres procedurze międzyrządowej obowiązującej w trzecim filarze, sprawiając, że proces legislacyjny, reprezentacji, kontrola sądowa, i wdrażanie aktów prawnych na poziomie Unii będą podlegać zasadom, procedurom i instrumentom metody współdecydowania. W rzeczywistości konstytucja sprawi, że procedura współdecydowania stanie się zwykłą procedurą ustawodawczą.

Ochrona danych osobowych w trzecim filarze

Kontekst

Wspólnota wprowadziła szczegółowy plan ramowy ochrony danych dla pierwszego filaru w oparciu o Dyrektywę o ochronie danych z roku 1995, która zawiera szczegółowe przepisy dotyczące, między innymi, zasad rządzących przepływem danych, nadzo-

rem, i przekazywaniem danych do państw trzecich, podczas gdy w trzecim filarze nie istnieje ogólny plan ramowy ochrony danych.

Z drugiej strony, szczegółowe zarządzenia dotyczące ochrony danych i nadzorowania przepływu danych zawarte są w przepisach regulujących funkcjonowanie poszczególnych organów trzeciego filaru, takich jak Europol czy Eurojust. Inny zbiór przepisów dotyczących ochrony danych osobowych reguluje działania Systemu Informacji Celnej i Systemu Informacji Schengen. Przepisy te zostały „skrojone na miarę” dla potrzeb funkcjonowania każdego z tych systemów. Każdy organ i system ma swoje własne ustalenia dotyczące nadzoru, a brak przepisów ogólnych w trzecim filarze wciąż pozostaje problemem.

Ponadto, przeciwnie niż w pierwszym filarze, gdzie inspektorowie ochrony danych pracują w ramach odpowiedniego ramowego planu organizacyjnego dotyczącego kwestii związanych z ochroną danych, w ramach Grupy Roboczej Art. 29, trzeci filar nie dysponuje takim forum, ponieważ połączone organy nadzoru w trzecim filarze (np. Europol, Schengen, Eurojust) działają na podstawie szczególnych uprawnień. Z powodu braku takiej grupy, członkowie komisji ds. ochrony danych nie mogą zapewnić odpowiednio wczesnego doradztwa dla organów uczestniczących w procesie legislacyjnym w kwestiach ochrony danych, po ogólnoeuropejskiej konsultacji i na odpowiednim poziomie jakościowym. Z tego powodu Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych, która odbyła się we Wrocławiu we wrześniu 2004 r., podjęła uchwałę o utworzeniu wspólnego forum, Grupy Roboczej ds. Policji, zajmującej się ochroną danych w ramach trzeciego filaru.

W konsekwencji różnych wniosków europejskich, dotyczących zbierania i przepływu danych osobowych, Grupa Robocza ds. Policji wypracowała dokumenty dotyczące ochrony danych w ramach trzeciego filaru, które zostały przedstawione na Wiosennej Konferencji Europejskich Organów Ochrony Danych, w Krakowie w kwietniu 2005 r.

Proponowana argumentacja

Przy okazji tejże konferencji, autor niniejszego referatu uznał za stosowne przekazanie jej uczestnikom następującego pomysłu: utworzenia odrębnej – lecz nie autonomicznej – regulacji dla trzeciego filaru.

Skoro w chwili obecnej ustalenie prawnego planu ramowego ochrony danych osobowych w ramach trzeciego filaru nie jest prawnie możliwe poprzez rozszerzenie zakresu stosowania Dyrektywy 95/46/WE, zachodzi potrzeba użycia innego instrumentu prawnego. Tym niemniej wydaje się, że należy działać zgodnie z przepisami Dyrektywy, nie zapominając przy tym o specyfice trzeciego filaru. W dalszej perspektywie, wynika z tego, że po przyjęciu konstytucji europejskiej, powinien powstać zintegrowany system ochrony danych obejmujący wszystkie filary, co zapewni wysoki poziom ochrony.

Jeśli chodzi o projekt ramowego planu ochrony danych w obrębie trzeciego filaru i zastosowanej techniki prawnej, jednym z rozwiązań analizowanych przez służby Komisji było odniesienie się w decyzji do ustaleń Dyrektywy – przewidując jednocześnie odstępstwa i wyjątki wymagane ze względu na specyfikę trzeciego filaru.

Z perspektywy prawnej taka technika „odniesienia” nie powinna stwarzać żadnych problemów. Przyznano, że w chwili obecnej Dyrektywa nie może ulec rozszerzeniu (ani

uzupełnieniu) dla celów trzeciego filaru, lecz to nie powinno przeszkodzić w podjęciu decyzji dotyczącej trzeciego filaru (uchwalonej zgodnie z zasadami instytucjonalnymi trzeciego filaru) „zapożyczającej” ustawodawstwo filaru pierwszego. W ten sposób przepisy te uzyskałyby status przepisów odnoszących się także do trzeciego filaru. Powstałby w ten sposób „podział funkcjonalny”, tak że Dyrektywa byłaby stosowana, jako taka, w filarze pierwszym, a poprzez odniesienie także w filarze trzecim.

Tego rodzaju rozwiązanie przyniosłoby ważne korzyści w postaci symbolicznej: od tej chwili Europa pokazałaby wyraźnie, jak wielką wagę przywiązuje do tego, aby zintegrowany system, którego się domagamy, powstał zgodnie z poziomem ochrony gwarantowanym Dyrektywą. Połączenie przepisów (Dyrektywy i ramowego planu prawnego) byłoby ułatwione, a co więcej, wydawałoby się naturalną i logiczną konsekwencją użytej techniki prawnej.

Druga kwestia dotyczy ciała doradczego, które zostałyby przewidziane/wyznaczone/ utworzone w obrębie trzeciego filaru.

Wskazane jest, aby – jak domagały się tego inspektoraty ochrony danych podczas wrocławskiej konferencji (patrz wyżej) – organ doradczy posiadał kompetencje odnośnie kwestii wchodzących w zakres trzeciego filaru. Nie powinno to jednak prowadzić do dodatkowego rozszczepienia już istniejących kompetencji konsultacyjnych. Powstaje pytanie czy istnieje takie ryzyko w przypadku ustanowienia w ramach trzeciego filaru organu różnego od Grupy Roboczej Art. 29.

Ryzyko z tym związane nie wydaje się nadmierne, zważywszy, że w dużej mierze w obu organach uczestniczyłyby te same osoby. Gdyby rozwiązanie takie zostało przyjęte, należałoby w obu organach zapewnić symetrię i tak podobny skład jak tylko to możliwe. W ten sposób uniknie się niebezpieczeństwa, że przepisy dotyczące ochrony danych – w założeniu identyczne lub porównywalne – zostaną interpretowane na rozbieżne sposoby (precyzja celów, proporcjonalność, środki ostrożności itd.), zależnie od stosującego je organu.

Mając w perspektywie połączenie filarów należałoby wybrać najodpowiedniejsze rozwiązanie, które polegałoby na uwzględnieniu również Grupy Roboczej Art. 29 oraz – co się z tym wiąże – nadanie jej w sposób jednoznaczny kolejnych uprawnień, tak by została formalnie usankcjonowana jako organ istniejący „pomiędzy filarami”. Należałoby przewidzieć powołanie wewnątrz Grupy Roboczej Art. 29 wyspecjalizowanej podgrupy. Poza korzyścią płynącą z zapobiegania rozbieżnym interpretacjom prawa, ułatwione będzie połączenie pierwszego i trzeciego filaru w dziedzinie ochrony danych, jeśli przy tym zapobiegnie się powstaniu dwóch odrębnych organów doradczych.

Jednakże, jeśli rozwiązanie polegające na ustanowieniu jednego organu z jakichś przyczyn wydawałoby się niepraktyczne, odpowiednim rozwiązaniem na krótką metę mogłoby być utworzenie autonomicznego organu „skopiowanego” z Grupy Roboczej Art. 29 (lub utworzonego wewnątrz tej Grupy Roboczej).

W celu jak największej minimalizacji ryzyka związanego z tworzeniem ustawodawstwa odbiegającego od ustaleń Grupy Roboczej Art. 29, ważne jest, aby reprezentanci organów ochrony danych w tej grupie byli, w największym możliwym zakresie, przynajmniej częściowo tymi samymi osobami, które należą do Grupy Roboczej Art. 29. Wysoki poziom reprezentacji w obrębie Grupy Roboczej Art. 29 stanowi kolejny argument za

przyznaniem nowo utworzonemu organowi podobnej legitymacji do tej, jaką nadano Grupie Roboczej – co nie oznacza, że nie zostałyby doceniony wkład techników w jakość wykonanej pracy i konkretną wiedzę o kwestiach z obszaru trzeciego filaru. Organizowanie spotkań nowo utworzonego organu bezpośrednio przed lub po posiedzeniach Grupy Roboczej Art. 29 z pewnością przyczyniłoby się do osiągnięcia ww. celów.

Europejski Inspektor Ochrony Danych oraz przewodniczący połączonych organów nadzorczych powinni mieć swoich reprezentantów w tym organie. Wydaje się, że nie należy dalej rozszerzać szczegółowego składu tego organu w stosunku do składu Grupy Roboczej Art. 29, zwłaszcza biorąc pod uwagę wyżej wymienione ryzyko.

Jest wreszcie konieczne, aby organ nadzorczy dysponował wystarczającymi środkami i zasobami (takimi jak sekretariat, budżet itp.), które umożliwią mu wykonywanie swoich zadań w sposób efektywny i wydajny.

Ostatnie osiągnięcia

W trakcie wiosennej konferencji w Krakowie w roku 2005 europejskie organy ochrony danych przyjęły trzy dokumenty dotyczące ochrony danych w trzecim filarze: „Deklarację Krakowską”, „Stanowisko w sprawie ochrony porządku publicznego i wymiany informacji w Unii Europejskiej”, będące uzupełnieniem „Deklaracji”, oraz opinię dotyczącą projektu decyzji ramowej w sprawie uproszczenia wymiany informacji oraz wywiadu pomiędzy organami ochrony porządku publicznego Państw Członkowskich Unii Europejskiej, w szczególności w odniesieniu do ciężkich przestępstw w tym aktów terroru.

W dokumentach tych Konferencja podkreśla konieczność rozwinięcia spójnego stanowiska w kwestii ochrony danych oraz ustanowienia zbiorczego aktu prawa europejskiego dotyczącego ochrony danych i obejmującego wszystkie obszary przetwarzania danych osobowych. W szczególności podkreślono, że: „W celu uniknięcia rozbieżności pomiędzy pierwszym a trzecim filarem, które wpływałyby negatywnie na ochronę porządku publicznego i przejrzystość, z punktu widzenia „Karty praw podstawowych” oraz przyszłej konstytucji europejskiej, która zniesie istniejące filary, Konferencja wzywa do zachowania – a w razie konieczności do odzyskania – spójności i jedności ochrony danych. Zasady zawarte w Dyrektywie 95/46/WE powinny stanowić rdzeń wspólnego europejskiego prawa o ochronie danych”. Konferencja wskazała także, iż „należy położyć nacisk na potrzebę utworzenia grupy roboczej Unii Europejskiej, złożonej z przedstawicieli narodowych i unijnych inspektoratów ochrony danych, działającej niezależnie, której zostanie powierzona misja współpracy, monitorowania i doradztwa.”

Z tej samej perspektywy Parlament Europejski zalecił „zapewnienie spójności istniejących przepisów o ochronie danych poprzez instrumenty właściwe dla obecnego trzeciego Filaru i połączenie ich w pojedynczy instrument gwarantujący taki sam poziom ochrony danych, jaki zapewniony jest w pierwszym filarze”.¹

W październiku 2005 r. Komisja Europejska przyjęła wniosek o podjęcie ramowej decyzji o ochronie danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Wniosek ten wynika z zasad wyłożonych w Dyrektywie 95/46/WE oraz uwzględnia wiele punktów zawartych w „Stanowisku” Konferencji krakowskiej. Ponadto ustanawia on autonomiczny organ nadzorczy w oparciu o model wykorzystany przy utworzeniu Grupy Roboczej Art. 29.

Wkrótce po posiedzeniu, które odbyło się w styczniu 2006 r., Konferencja Europejska przyjęła opinię na temat ww. wniosku. W opinii tej Konferencja popiera propozycję wprowadzenia szczególnych zasad ochrony danych w trzecim filarze, mających na celu ochronę obywateli, jednocześnie biorąc pod uwagę fakt, że wprowadzenie nowych, usystematyzowanych i zrównoważonych środków ochrony przyczyni się do efektywnej poprawy w obszarach zapobiegania i zwalczania przestępczości. Jednocześnie jednak Komisja domaga się wyjaśnienia, uzupełnienia lub poprawienia pewnych postanowień zawartych w tekście, celem zapobiegania problemom interpretacyjnym i nadmiernym rozbieżnościom w zastosowaniu przepisów.

Wniosek

Wielokrotnie wskazywano na konieczność i wagę ustanowienia ramowej decyzji prawnej o ochronie danych w trzecim filarze, jak również spójności ochrony danych w Unii Europejskiej. Wniosek dotyczący decyzji ramowej o ochronie danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, przedstawiony przez Komisję Europejską, może być uznany za ważny krok w kierunku zapewnienia spójności przepisów o ochronie danych w trzecim filarze.

Co więcej, można uznać go za krok na drodze do ułatwienia, w odpowiednim czasie, przyjęcia jednego instrumentu dla pierwszego i trzeciego filaru, a zatem stanowisko Komisji uwzględniające zalecenia inspektoratów ochrony danych w zakresie przestrzegania zasad wyłożonych w Dyrektywie 95/46/WE jest bardzo mile widziane.

.....

Na koniec chciałbym skorzystać z okazji, aby wyrazić podziękowania dla pani Ewy Kuleszy, polskiego Generalnego Inspektora Ochrony Danych Osobowych, która pełniła rolę gospodarza i organizatora dwóch konferencji, które zaowocowały podjęciem przez inspektorów ochrony danych istotnych decyzji w procesie ich pracy w kwestiach związanych z policją i bezpieczeństwem.

Pani Kulesza umożliwiła inspektorom ochrony danych uwieńczenie ich wysiłków w dziedzinie ochrony danych sukcesem oraz dodanie stałego wkładu w proces decyzyjny na tym polu.

W imieniu belgijskiego Inspektoratu Ochrony Danych życzę Pani Kuleszy dalszych sukcesów w karierze zawodowej.

¹⁾ Zalecenie Parlamentu Europejskiego dla Rady dotyczące planu działania Unii Europejskiej w zakresie wymiany informacji i współpracy w dziedzinie zwalczania terroryzmu [2005/2046(INI)].

**Boundary between data protection
and freedom of information,
with particular respect to data of public interest**

The fundamental right of freedom of information was established in Hungary in a completely different way than in many Western European countries. The comprehensive amendment of Hungary's Constitution in the wake of what is called the roundtable political negotiations of 1989 in Hungary allowed us to enshrine the right to freedom of information, in Hungary often referred to as the right to access data of public interest. Three years later, in 1992, Parliament passed Act LXIII on the Protection of Personal Data and Public Access of Data of Public Interest, adopting the model of Quebec, Canada, in using a single Act of Parliament to provide for both of these rights. Known also as the Data Protection and Freedom of Information Act (hereinafter referred to as: DP&FOIA) the law provided for the institution of a Commissioner, to be elected by a two-third majority of Parliament. The country's first such Commissioner was inaugurated after some delay, in the summer of 1995.

In Hungary, those assisting in the overhaul of the political system decided to take care of this issue by, as it were, a single master stroke. The brief work of preparation and debate lasted just a couple of months before Parliament, with a landslide ratio of for and against, passed what may be one of the most radical and libertarian acts on freedom of information anywhere. This headlong process left precious little time for future practitioners to prepare themselves, and also left a few minor incongruities and contradictions in the language of the hastily adopted law. The interpretation and resolution of these ambiguities have formed some of the most fascinating aspects of the Commissioner's work to date.

One of the distinctive features of the Hungarian law is its radical approach. It thrusts the gates wide open for publicity by declaring that all information handled by the agencies of the national and local governments shall be regarded as of public interest, except for personal data. The other interesting motive worth underlining is that the relevant Hungarian regulations – the DP&FOIA and the Secrecy Act – make an effort to strictly determine, almost with taxonomical rigor, those types of data of public interest that may be provisionally kept from publicity. They also strive to minimize the data controllers' discretion in making such decisions. Discovering where the boundaries of publicity lie is one of the most exciting fields in the Commissioner's work.

The boundaries of publicity and the secrets of the state

The fundamental principle underpinning the idea of freedom of information is the transparency of the government – especially with regard to public affairs and public funds. The adoption of the DP&FOIA and, in 1995, the Act on State Secrets and Office

Secrets (the "Secrecy Act") amounted to a smooth revolution for publicity in Hungary which abolished the government's occasional indulgence of disclosure as a special form of grace. The rule of thumb became publicity, with the burden invariably lying on the government to prove that withholding the information is inevitable for its own basic interests of operation. The fundamental content of the Secrecy Act was established by a resolution of the Constitutional Court in 1994. Freedom of information in Hungary is regarded as a constitutional right. The Constitution also declares that a fundamental right cannot be regulated except by Acts of Parliament, moreover that the essential content of a fundamental right may not be restricted by law.

In this way, Hungary's Secrecy Act stipulates rather severe conditions for the state to keep information undisclosed. In order for the classification to be lawful, the data must be of one of the categories specifically listed in an Appendix to the same Act. Furthermore, the classification must be entered by a person exercising a public function and properly authorized by law to do so, it must be for a specified period of time, and is subject to a set of strict formal and procedural rules. The significance of these stringent criteria was driven home to everyone in a high profile case involving certain allegedly top secret documents published by a Hungarian weekly paper. The Data Protection Commissioner held an investigation and found that the editor was within the law in printing the documents in question. Remarkably, the Commissioner reached this conclusion not with regard to the content or nature of the documents, but simply on the basis that the formal procedural rules of classification had been violated by the classifier.

However, it is not just the government that can have its secrets. The publicity of a specific range of data controlled by governmental bodies must be restricted in the interest of the private sphere. Without protecting business secrets, the market economy could not work, and reliable economic statistics would be unfeasible. The question is where to draw the limits. To put it in a different way: how transparency of public spending (and thereby combating corruption) can be ensured and reasonable protection to the players of the market be simultaneously extended.

Open secrets: business data and freedom of information

The right to protect business and commercial data is recognized by freedom of information legislation around the world. Most of these laws attempt to solve the conflict by delegating to the data controllers the responsibility to deliberate when "appreciable public interest" can justify the disclosure of business information controlled by governmental bodies.

The Hungarian solution departs from this approach when it considers that all information that is not personal in nature constitutes data of public interest. By definition, this should include business secrets – a group of data that legislators obviously overlooked in 1992. Although other statutory instruments in Hungary, in particular the Civil Code and the Fair Competition Act, do speak of the protection of business secrets, the Commissioner has found it a very demanding task to draw the boundaries of public access in this field.

From the outset, the Commissioner has identified two cases where a company has no appreciable interest in keeping business data secret. One is when a supervisory authority, such as an environmental or consumer protection agency, determines a violation and imposes a fine. In such cases, the institution of the business secret may not be

used to shelter the company in violation. The other type involves public bodies with discretion over public funds, for instance in conducting privatization, concession, and public procurement procedures – essentially one where contracts are awarded. The Commissioner has held that companies dealing with the government must suffer the disclosure of their business data to the extent relevant to the transaction at hand, as a means of enabling the public to ascertain that the government has made a well-founded and lawful decision. Prompted by the Commissioner's recommendations, the Parliament amended the rules of privatization and concession procedures, and imposed restrictions on bank secrets for transactions involving public funds.

Until now, however, Hungary has had no general provision of law in place that could have extended more effective guarantees than the Commissioner's not binding legally statements of position. The Parliament then adopted the so-called "Glass Pocket Act." Incorporating the proposals of the Commissioner, this legislative package amended about twenty acts in an effort to reinforce the system of assurances safeguarding the lawful and reasonable use, management, and monitoring of public funds. One of the acts modified, the DP&FOIA itself was supplemented by a provision prohibiting recourse to business secrets in an attempt to thwart access to or disclosure of data of public interest, whenever the information sought is connected with the use of the national or local budget, benefits and subsidies paid from such budget, as well as with the management, use, alienation, or encumbrance of assets and property owned by the national or local government, or the acquisition of any right in respect of such assets or property. The Act extends the principle of disclosure to apply to European Union funds as well.

The conflict of two rights and data of public figures

The enactment of a single Act to provide for the two informational rights of data protection and freedom of information, and the investiture of the same Commissioner to protect them, hopefully yielded the benefit of avoiding a narrow-minded and biased legal vision. At the same time – and partly due to the same reason – the DP&FOIA falls short of providing unambiguous guidelines to go by in cases when the two rights come into conflict. All that the law says on this count is that the name and position of a person acting on behalf of a body of public power constitute data of public interest. The Data Protection Commissioner was confronted by a set of new inquiries because of this simple rule, e.g.: should the financial statements filed by officials and Members of Parliament on a mandatory basis be disclosed to the public? What type of financial information should these forms be allowed to seek? What was the amount of severance pay disbursed to an undersecretary of state? What is the amount and legal grounds of benefits paid to each Member of Parliament? Does the State Audit Office's report condemning a mayor's decision as unlawful constitute data of public interest subject to disclosure?

In addition to the field of business secrets, the most challenging dilemma facing the Commissioner is, therefore, how to draw the limits of disclosure in those public affairs where the data pertaining to the operation of government also happen to be personal information. It is all about the transparency of individuals in public office – or "public figures" as widely accepted international usage will now have it. The question is not so much how far freedom of the press should be allowed to go, as precisely which of a public figure's data should be made available, on a mandatory basis, to anyone requ-

esting that disclosure. In other words, the question is better asked like this: What is the point beyond which privacy deserves protection under all circumstances?

In the absence of clear-cut provisions, the Hungarian Commissioner has in recent years relied on the perception of the Constitutional Court, which has argued that *"The values of democratic government and transparency of public affairs assign narrower limits to the constitutional protection of privacy for government officials and politicians appearing in public, who must accept to expose themselves to scrutiny more deeply than the ordinary citizen. This may entail access to their personal data, to the extent that these data are relevant to their function or public appearance. In relation to those in office or appearing in public as politicians, the right of the people, most notably of the voting citizen, to access data of public interest must enjoy precedence over the right of the former to protecting personal information that may be of relevance for assessing their civic pursuits. Access to such personal data is vital not only for an informed discourse on governance and public affairs, but also for the correct assessment of bodies of government and for shoring up the confidence to be vested in them."*

It was suggested by both the former and the present Data Protection Commissioner that the DP&FOIA should be amended by the declaration that the personal data of public figures in connection with their public duties constitute data of public interest accessible for anyone, unless appreciable private interests should dictate otherwise.

The issue which the present Data Protection Commissioner has been struggling with since the beginning of his work is that the DP&FOIA and other legal regulations in effect do not give unambiguous solutions for undoing the conflict of the two informational rights. The Data Protection Commissioner received thirty petitions seeking the specification of the boundary between the private and public sphere. In 2004 the main characteristic questions were: whether information about the education of a grammar school teacher belongs to the data of public interest; whether the declaration of wealth of a local authority representative is to be disclosed in a newspaper; whether the opinion of students of their professor is to be disclosed on the Internet; whether the list of political advisers employed by governmental bodies is accessible; whether the registry of health employees is data of public interest or is to be treated as personal data. The Data Protection Commissioner made efforts to answer all the questions by taking into consideration all the sectoral laws.

He represented the view that the legislator has to fill in the gap in the legislation and regulate that data related to the scope of duties of the person performing public functions – unless otherwise regulated by law – is public.

Publicity of personal data of public figures, persons performing public functions after the amendment of the DP&FOIA

One of the most important areas of the amendment to the DP&FOIA adopted in 2005 was the change regarding rules related to data public on grounds of public interest that is specified by the DP&FOIA itself. The modification concerning public personal data of "persons performing public functions" is to be highlighted here. The new regulation loosens strict provisions of the DP&FOIA regarding protection of personal data. By this the principle laid down in the Constitutional Court's Decision 60/1994

may take effect: „in case of those persons who exercise public authority or practice politics in the state, the right of people especially voting citizens – to public access to data of public interest prevails over the right of the formerly mentioned persons to protection of such personal data that may be relevant in consideration of their public activities and the valuation thereof.” The interpretation of the new rules of the DP&FOIA will probably raise many questions which can be seen in the following cases.

The position of the Data Protection Commissioner was requested by the chief clerk of a county on whether the discussion over the payment, income, premiums of the mayor should be held in an open meeting or not. With reference to Subsection (4) of Article 19 of the DP&FOIA, the Data Protection Commissioner stated: “*Personal data related to the scope of duties of the person performing public functions may be excluded from the principle of publicity only by law, the concerned person performing public functions “lost” his right to dispose over his personal data connected to the public function performed by him...*” According to Subsection (3) of Article 17 of the Act on Local Governments “*access to data of public interest and data public on grounds of public interest has to be provided even in cases involving camera meetings. Since in the cases arisen (establishing the income, premium, other payments of the mayor) data public on grounds of public interest were used by the body by the judgement, these data have to be made public even if the body holds a camera meeting...*”

The concept of “data related to the scope of duties” had to be construed by the Commissioner when a local authority representative asked whether the body of local authority representatives was entitled to observe personal data that are not related to the work. The Data Protection Commissioner stated that data related to the scope of duties of the person performing public functions had to be set apart from the data not related thereto.

Opinions already presented by the Commissioner in the subject of declaration of wealth had to be repeated in the year 2005, as a response either to a judge of the Constitutional Court, summarising previous statements: “*the constitutionality of legal regulations in effect prescribing the duty to make declaration of wealth is strongly disputable, because it is, considering both the aim, and the means chosen to achieve it, objectionable and it leads to the disproportionate limitation of the right of data subjects to informational self-determination.*”

One of the fields that was paid much attention is the past of agents. During the year, several well-known public officials were revealed to have served as agents and informants. These developments may explain the increased public curiosity about the issue. Apparently drafted without the adequately deliberated purpose and the requisite prudence that such matters require, the law in its present form jeopardizes the triumph of fundamental informational rights. The Data Protection Commissioner regularly insists on the need to make a distinction between access by specifically concerned individuals on the one hand and full public disclosure on the other. There can be no constitutional justification for, or any appreciable public interest in restricting the right to informational self-determination of those who were victimized by communist-era surveillance. In addition, the concept of ‘public personage’ is not clear in Hungarian legal regulations, it is not adequately defined, and therefore it leads to many disputes. It will be the task for the legislators to give satisfying definition thereto in the future.

Granica pomiędzy ochroną danych osobowych a wolnością informacji, ze szczególnym uwzględnieniem danych istotnych ze względu na interes publiczny

Fundamentalne prawo wolności informacji zostało ustanowione na Węgrzech w zupełnie inny sposób niż w krajach zachodnioeuropejskich. Całościowa zmiana Konstytucji Węgier w ramach tak zwanych negocjacji politycznych węgierskiego okrągłego stołu w 1989 r. pozwoliła nam objąć ochroną prawo do wolności informacji, nazywane często na Węgrzech prawem dostępu do danych istotnych ze względu na interes publiczny. Trzy lata później, w 1992 r., parlament przyjął LXIII „Ustawę o ochronie danych osobowych i o publicznym dostępie do danych istotnych ze względu na interes publiczny”, przyjmując model obowiązujący w kanadyjskiej prowincji Quebec, która zagwarantowała przestrzeganie obu tych praw na mocy jednej ustawy parlamentarnej. Wspomniana ustawa, znana także jako „Ustawa o ochronie danych osobowych i wolności informacji” (zwana dalej UODOiWO), stworzyła instytucję Komisarza ds. ochrony danych osobowych, wybieranego większością dwóch trzecich głosów przez parlament. Pierwszy węgierski Komisarz objął stanowisko z pewnym opóźnieniem, latem 1995 r.

Uczestnicy przebudowy systemu politycznego na Węgrzech zdecydowali się rozwiązać ten problem za pomocą jednego zdecydowanego posunięcia. Krótkie prace przygotowawcze i debata trwały tylko kilka miesięcy, po czym parlament, zdecydowaną większością głosów, przyjął prawdopodobnie jedną z najbardziej radykalnych i libertarianiskich ustaw o wolności informacji na świecie. Ta gorączkowa procedura pozostawiła niewiele czasu na przygotowania osobom, które miały stosować ustawę, a język tego pośpiesznie przyjętego aktu prawnego zawierał kilka drobnych niespójności i sprzeczności. Interpretacja i rozstrzyganie tych niejasności stanowiły jedne z najbardziej fascynujących aspektów dotychczasowej pracy Komisarza.

Jedną z cech charakterystycznych węgierskiej ustawy jest jej radykalne podejście. Otwiera ona szeroko wrota publicznemu dostępowi do danych, stwierdzając, że wszystkie informacje przetwarzane przez agendy rządowe i samorządowe będą traktowane jako dane istotne ze względu na interes publiczny, z wyłączeniem danych osobowych. Warto jest również podkreślić inną charakterystyczną cechę węgierskich przepisów: w UODOiWO oraz w „Ustawie o tajemnicy państwowej” podjęto próbę ścisłego, niemal z taksonomicznym rygorem, określenia typów danych istotnych ze względu na interes publiczny, do których można tymczasowo zablokować dostęp opinii publicznej. Próbowano także zminimalizować dowolność administratorów danych przy podejmowaniu takich decyzji. Odkrywanie gdzie leżą granice publicznego dostępu do danych jest jednym z najbardziej fascynujących obszarów pracy Komisarza.

Granice publicznego dostępu do danych a tajemnica państwowa

Fundamentalna zasada, która leży u podstaw koncepcji wolności informacji, to transparentność władzy – szczególnie jeśli chodzi o sprawy i fundusze publiczne. Przyjęcie UODOiWO oraz, w 1995 r., „Ustawy o tajemnicy państwowej i tajemnicy urzędowej” (nazywanej w skrócie „Ustawą o tajemnicy państwowej”) było łagodną rewolucją w kwestii zasad regulujących publiczny dostęp do danych na Węgrzech i zakończyło sy-

tuację, kiedy sporadyczne zezwalanie na ujawnienie danych było specjalną formą łaski ze strony rządu. Generalną zasadą rządzącą publicznym dostępem stała się jawność danych, przy czym ciężar dowodu, że nieupublicznienie informacji jest niezbędne dla podstaw funkcjonowania rządu, zawsze spoczywa na rządzie. Fundamentalna treść „Ustawy o tajemnicy państwowej” została wprowadzona w życie na mocy decyzji Sądu Konstytucyjnego w 1994 r. Wolność informacji jest uznawana na Węgrzech za prawo gwarantowane przez Konstytucję. Konstytucja stanowi także, że żadne fundamentalne prawo obywatelskie nie może być uregulowane inaczej, niż w drodze ustawy parlamentarnej, przy czym ustawa nie może ograniczać istoty tego prawa.

Węgierska „Ustawa o tajemnicy państwowej” nakłada w ten sposób na władze wymóg przestrzegania stosunkowo surowych zasad w zakresie blokowania publicznego dostępu do informacji. Aby utajnienie było zgodne z prawem, dane muszą należeć do jednej z kategorii szczegółowo wymienionych w załączniku do tej ustawy. Co więcej, decyzję o utajnieniu musi podjąć osoba sprawująca funkcję publiczną i odpowiednio umocowana ustawowo, utajnienie musi być ograniczone czasowo i podlega serii ścisłych wymogów formalnych i proceduralnych. Znaczenie tych rygorystycznych kryteriów unaocznili głośny proces związany z publikacją przez jeden z węgierskich tygodników pewnych rzekomo ściśle tajnych dokumentów. Komisarz ds. ochrony danych osobowych przeprowadził dochodzenie i ustalił, że wydawca miał prawo opublikować rzeczne dokumenty. Co istotne, Komisarz doszedł do tego wniosku nie na podstawie analizy treści czy charakteru tych dokumentów, ale po prostu na tej podstawie, że osoba klasyfikująca dane dopuściła się naruszenia obowiązujących w tym zakresie formalnych wymogów proceduralnych.

Jednakże nie tylko władze mogą mieć swoje tajemnice. Publiczne udostępnianie określonych zestawów danych znajdujących się pod kontrolą instytucji rządowych musi być ograniczone ze względu na interesy sektora prywatnego. Bez ochrony tajemnic biznesowych nie mogłaby funkcjonować gospodarka rynkowa i niemożliwe byłoby sporządzanie wiarygodnych statystyk gospodarczych. Pytanie brzmi, gdzie wyznaczyć granice. Mówiąc innymi słowami: jak zagwarantować transparentność wydatków publicznych (i dzięki temu zwalczać korupcję), zapewniając jednocześnie rozsądną ochronę podmiotów rynkowych.

Jawne tajemnice: dane biznesowe a wolność informacji

Wszędzie na świecie uregulowania prawne dotyczące wolności informacji uwzględniają również prawo do ochrony danych biznesowych i handlowych. Większość z tych ustaw stara się rozwiązać ten konflikt przekazując kontrolerom danych prawo do rozstrzygania, kiedy „istotny interes publiczny” może uzasadniać ujawnienie informacji biznesowych znajdujących się pod kontrolą instytucji rządowych.

Rozwiązania węgierskie różnią się od tego podejścia, ponieważ stwierdza się w nich, że wszystkie informacje, które nie mają charakteru danych osobowych należą do danych istotnych ze względu na interes publiczny. Zgodnie z tą definicją powinny one obejmować tajemnice przedsiębiorstw – grupę danych, którą prawodawca w sposób oczywisty przeoczył w 1992 r. Pomimo że inne uregulowania ustawowe na Węgrzech, w szczególności kodeks cywilny oraz ustawa o uczciwej konkurencji, mówią o ochronie tajemnic przedsiębiorstw, wytyczenie granic publicznego dostępu do tych danych było dla Komisarza bardzo trudnym zadaniem.

Już na samym początku Komisarz zidentyfikował dwa przypadki, w których nie istnieje ważny interes przedsiębiorstwa uniemożliwiający ujawnienie jego danych biznesowych. Jeden z nich to sytuacja, gdy instytucja nadzorująca, jak na przykład urząd ochrony środowiska albo ochrony konsumenta, stwierdza naruszenie przepisów i nakłada na przedsiębiorstwo karę. W takich przypadkach nie można powoływać się na instytucję tajemnicy przedsiębiorstwa w celu ochrony firmy, która dopuściła się naruszenia. W drugim przypadku mamy do czynienia z instytucjami publicznymi, które zarządzają funduszami publicznymi, na przykład podczas prywatyzacji, udzielania koncesji bądź prowadzenia procedury zamówień publicznych, w szczególności procedur decydujących o przyznaniu kontraktów. Komisarz uznał, że przedsiębiorstwa, które w swojej działalności współpracują z administracją rządową, muszą pogodzić się z ujawnieniem swoich danych biznesowych w zakresie stosownym do danej transakcji. W ten sposób opinia publiczna może ocenić, czy rząd podjął uzasadnioną i zgodną z prawem decyzję. Na podstawie rekomendacji Komisarza parlament przyjął poprawki do zasad prywatyzacji i procedur udzielania koncesji, oraz ograniczył tajemnicę bankową przy transakcjach z udziałem funduszy publicznych.

Do niedawna Węgry nie miały generalnych zasad prawnych, które mogłyby zapewnić skuteczniejsze gwarancje niż niewiążące prawnie opinie Komisarza. Ostatnio parlament przyjął tzw. „Ustawę o przezroczystych kieszeniach”. Wcielając w życie propozycje Komisarza, ten pakiet zmian prawnych wprowadził poprawki do około dwudziestu ustaw. Celem tych zmian było wzmocnienie systemu zabezpieczeń gwarantujących zgodne z prawem i racjonalne wydatkowanie funduszy publicznych, zarządzanie nimi oraz ich monitorowanie. Jedną ze zmienionych ustaw była właśnie UODOiWO, którą uzupełniono o przepis zabraniający powoływania się na tajemnicę służbową w celu zablokowania dostępu do danych istotnych ze względu na interes publiczny albo ich ujawnienia, w przypadku gdy informacje te są związane z wykonaniem budżetu państwowego bądź samorządowego, wypłatą pomocy i subsydiów z tych budżetów, czy też z zarządzaniem, wykorzystaniem, przeniesieniem prawa własności lub obciążeniem aktywów i majątku będącego własnością władz państwowych lub samorządowych, lub też nabyciem jakichkolwiek praw w stosunku do takich aktywów lub majątku. Ustawa rozciąga zasadę publicznego dostępu do danych także na fundusze Unii Europejskiej.

Konflikt dwóch praw dotyczących informacji i dane osób publicznych

Wprowadzenie w życie jednej ustawy gwarantującej dwa prawa dotyczące informacji, tj. ochronę danych i wolność informacji, oraz powołanie jednego Komisarza do ich ochrony pozwoliło, miejmy nadzieję, uniknąć ciasnego i ograniczonego podejścia do tych problemów. Jednocześnie – i częściowo z tych samych przyczyn – UODOiWO nie jest w stanie sformułować jednoznacznych wytycznych, które można by stosować w sytuacji, gdy oba wspomniane prawa stoją ze sobą w sprzeczności. Prawo stanowi w tej kwestii jedynie, że nazwisko i stanowisko osoby działającej w imieniu instytucji władzy publicznej stanowi dane istotne ze względu na interes publiczny. Komisarz ds. ochrony danych osobowych z powodu tej prostej zasady musiał zmierzyć się z szeregiem nowych zapytań, jak na przykład, czy oświadczenia majątkowe składane obowiązkowo przez urzędników i członków parlamentu powinny być udostępniane opinii publicznej; o jakie informacje finansowe można pytać w tych formularzach; jaka była wysokość odprawy wypłaconej podsekretarzowi stanu; w jakiej wysokości i na jakiej podstawie prawnej wypłaca się świadczenia członkom parlamentu; czy raport Pań-

stwowej Izby Kontroli uznający decyzję burmistrza za niezgodną z prawem stanowi dane istotne ze względu na interes publiczny i tym samym podlegające ujawnieniu.

Obok kwestii związanych z tajemnicą biznesową, najtrudniejszym zagadnieniem w pracy Komisarza jest problem wyznaczenia granic publicznego dostępu do danych w sprawach publicznych, gdzie dane związane z działalnością władz państwowych są także danymi osobowymi. Chodzi tu o transparentność osób zajmujących funkcje publiczne – bądź też „osób publicznych”, jak określa się je używając przyjętego powszechnie na świecie terminu. Największym problemem nie jest tutaj nawet jak daleko powinna sięgać wolność prasy, ale raczej, które z danych osób publicznych powinny być udostępniane każdemu, kto poprosi o ich upublicznienie. Innymi słowy, pytanie to lepiej sformułować następująco: gdzie jest granica, za którą prywatność powinna być chroniona w każdych okolicznościach?

Wobec braku jednoznacznych przepisów węgierski Komisarz opierał się w ostatnich latach na interpretacji Sądu Konstytucyjnego, który stwierdził, że *„Wartości takie jak demokratyczny rząd oraz transparentność spraw publicznych zawężają konstytucyjną ochronę prywatności urzędników rządowych i polityków występujących publicznie; muszą oni zaakceptować, że zostaną poddani bardziej dogłębnej kontroli niż zwykli obywatele. Może to się wiązać z dostępem do ich danych osobowych, w stopniu, w jakim dane te są istotne dla ich funkcji bądź aktywności publicznej. W stosunku do osób sprawujących urzędy bądź też uczestniczących w życiu publicznym w charakterze polityków, prawo ludzi, a szczególnie głoszących obywateli, do dostępu do danych o znaczeniu publicznym musi mieć pierwszeństwo nad prawem osób publicznych do ochrony informacji osobowych, które mogą mieć znaczenie przy ocenie ich działalności publicznej. Publiczny dostęp do tego typu danych jest niezbędny nie tylko po to, aby umożliwić rzeczowy dyskurs na temat sposobu sprawowania władzy i spraw publicznych, ale także do prawidłowej oceny instytucji rządowych i umocnienia zaufania, jakie się w nich pokłada.”*

Zarówno były, jak i obecny Komisarz ds. ochrony danych osobowych sugerowali, że UODOiWO powinna zostać zmieniona poprzez deklarację, że dane osobowe osób publicznych pozostające w związku z ich publicznymi obowiązkami należą do danych istotnych ze względu na interes publiczny i są dostępne dla każdego, chyba że ważny interes prywatny dyktowałby inne postępowanie.

Od początku pełnienia swojej funkcji obecny Komisarz ds. ochrony danych osobowych zmagał się z problemem braku w UODOiWO i innych obowiązujących aktach prawnych jednoznacznych rozstrzygnięć, co do konfliktu obu praw dotyczących informacji. Komisarz ds. ochrony danych osobowych otrzymał trzydzieści wniosków o ustalenie dokładnej granicy pomiędzy sferą publiczną i prywatną. Do głównych, najbardziej charakterystycznych zapytań, które przedłożono w 2004 r., należały: czy informacje o wykształceniu nauczyciela liceum należą do danych istotnych ze względu na interes publiczny; czy deklaracja majątkowa przedstawiciela samorządowego może być opublikowana w gazecie; czy opinia studentów o ich profesorze może być opublikowana w Internecie; czy istnieje dostęp do listy doradców politycznych zatrudnionych w instytucjach rządowych; czy rejestr pracowników służby zdrowia stanowi dane istotne ze względu na interes publiczny, czy też powinien być traktowany jako dane osobowe. Komisarz ds. ochrony danych osobowych starał się udzielić odpowiedzi na te pytania, biorąc pod uwagę wszystkie stosowne ustawy.

Komisarz stoi na stanowisku, że ustawodawca powinien uzupełnić luki w prawodawstwie i wprowadzić przepis, zgodnie z którym dane związane z zakresem obowiązków osoby sprawującej funkcję publiczną są jawne, o ile prawo nie stanowi inaczej.

Publiczny dostęp do danych osobowych osób publicznych i osób wykonujących funkcje publiczne po zmianie UODOiWO

Jedną z najważniejszych zmian w UODOiWO przyjętych w 2005 r. była modyfikacja zasad związanych z danymi jawnymi ze względu na interes publiczny, który jest określony w UODOiWO. Należy tutaj zaakcentować wprowadzenie zmiany dotyczącej jawnych danych osobowych „osób sprawujących funkcje publiczne”. Nowe przepisy łagodzą surowe postanowienia UODOiWO dotyczące ochrony danych prywatnych. Dzięki nim może zacząć obowiązywać zasada wyłożona w decyzji 60/1994 Sądu Konstytucyjnego: *„w przypadku osób, które sprawują funkcje publiczne lub uczestniczą w życiu politycznym na Węgrzech, prawo ludzi, a szczególnie głoszących obywateli, do publicznego dostępu do danych istotnych ze względu na interes publiczny przeważa nad prawem tych pierwszych do ochrony tych danych prywatnych, które mogą mieć znaczenie w związku z ich działalnością publiczną i jej oceną.”* Ta interpretacja nowych zasad zawartych w UODOiWO prawdopodobnie sprowokuje wiele pytań, które pojawią się w kolejnych sprawach.

Główny urzędnik jednego z węgierskich powiatów poprosił Komisarza ds. ochrony danych osobowych o stanowisko w kwestii, czy dyskusja o płacy, dochodach czy premiach burmistrza powinna mieć miejsce w trakcie otwartego zebrania czy też nie. W oparciu o podpunkt (4) artykułu 19 UODOiWO, Komisarz ds. ochrony danych osobowych stwierdził: *„Dane osobowe związane z zakresem obowiązków osoby sprawującej funkcje publiczne mogą być wyłączone spod działania zasady publicznego dostępu do danych tylko na podstawie ustawy; osoba sprawująca funkcje publiczne, o której mowa, „straciła” prawo do dysponowania swoimi danymi osobowymi związanymi z wykonywanymi przez nią funkcjami publicznymi...”* Zgodnie z podpunktem (3) artykułu 17 „Ustawy o Samorządzie Lokalnym” *„dostęp do danych istotnych dla interesu i danych publicznych ze względu na interes publiczny musi być zagwarantowany nawet w przypadku posiedzeń zamkniętych. Ponieważ w rzeczonej sprawie (ustalenie dochodu, premii i innych świadczeń, z których korzysta burmistrz) dane jawne ze względu na interes publiczny zostały wykorzystane przez organ przy podejmowaniu oceny, dane te muszą zostać udostępnione publicznie, nawet jeżeli posiedzenie organu miało charakter zamknięty.”*

Komisarz musiał dokonać interpretacji koncepcji „danych związanych z zakresem obowiązków”, gdy przedstawiciel władz lokalnych złożył zapytanie, czy przedstawiciele samorządu mają prawo brać pod uwagę prywatne dane, które nie są związane z pracą. Komisarz ds. ochrony danych osobowych stwierdził, że dane związane z zakresem obowiązków osoby sprawującej funkcje publiczne muszą być oddzielone od danych z nim niezwiązanych.

Opinie już sformułowane przez Komisarza w kwestii deklaracji majątkowych musiały zostać powtórzone w roku 2005, jako odpowiedź na zapytanie jednego z sędziów Sądu Konstytucyjnego. Podsumowywały one dotychczasowe stanowiska: *„konstytucyjność obowiązujących uregulowań prawnych nakładających obowiązek składania deklaracji majątkowej jest mocno dyskusyjna, ponieważ, jeśli weźmie się pod uwagę zarówno jej cel, jak i środki wybrane do jego realizacji, budzi sprzeciw i prowadzi do nieproporcjo-*

nalnego ograniczenia prawa osób, o których są zbierane dane, do określenia losu informacji ich dotyczących."

Jednym z zagadnień, któremu poświęcono dużo uwagi jest przeszłość współpracowników węgierskiej służby bezpieczeństwa. W ciągu tego roku ujawniono, że kilku znanych urzędników publicznych było agentami i informatorami. Sytuacja ta może tłumaczyć wzmożone zainteresowanie opinii publicznej tym problemem. Najwyraźniej ustawa w swojej obecnej formie, przygotowana bez wystarczającego przemyślenia celu, jakiemu miałaby służyć, i niezbędnej w takich kwestiach rozwagi, zagraża fundamentalnym prawom dotyczącym informacji. Komisarz ds. ochrony danych osobowych regularnie podkreśla potrzebę dokonania rozróżnienia z jednej strony pomiędzy dostępem do danych osób, których konkretnie dotyczy dany problem, a z drugiej strony pełnym publicznym dostępem do danych. Nie może być konstytucyjnego uzasadnienia ani nie ma też żadnego istotnego publicznego interesu w ograniczaniu prawa jednostek dotkniętych przez inwigilację w epoce komunistycznej do decydowania o losie informacji, które ich dotyczą. Co więcej, koncepcja „osoby publicznej” nie jest jasna w węgierskich uregulowaniach prawnych, nie jest odpowiednio zdefiniowana i dlatego prowadzi do wielu sporów. Zadaniem prawodawców będzie stworzenie zadowalającej definicji tego terminu w przyszłości.

Dr José Luis Piñar Mañas

Director, Spanish Data Protection Authority
Dyrektor Agencji Ochrony Danych, Hiszpania

The fundamental right to personal data protection, essential content and current challenges

I. THE ORIGIN OF DATA PROTECTION AS A FUNDAMENTAL RIGHT

1. Origin. "The right to be let alone"

The fundamental right to personal data protection is one of the most important rights existing in today's society. As previously discussed,¹ the European Treaty establishing a Constitution for Europe expressly sets out the fundamental right to personal data protection in two sections. Firstly, this concept appears in Article I-51 of Title VI ("The Democratic Life of the Union") in Part One;² and subsequently, in Article II-68, Title II ("Freedoms") of Part Two, the "Charter of Fundamental Rights of the Union".³ Despite the fact that changes in the European Constitution may still have some surprises in store for us, it is clear that not only the Constitution, but also the Charter of Fundamental Rights of the European Union approved in Nice in 2000 already heralded a significant change in the consideration given to the fundamental right of personal data protection. This, then, is the basic premise that must unquestionably be borne in mind.

Thomas COOLEY had already discussed "the right to be let alone"⁴ as far back as in 1888. In 1890, the *Harvard Law Review*⁵ published the now-famous article written by Samuel WARREN and Louis BRANDEIS entitled "The Right to Privacy"⁶. At that time WARREN and BRANDEIS discussed a new right: "Political, social, and economic changes entail the

¹ I have already referred to this point in "ECJ Case-Law on the Right to Protection of Personal Data", *BNA International. World Data Protection Report*. Part 1 and Part 2, January and February 2006, respectively, as well as in "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas" ("The right to personal data protection in European Court of Justice case law"), in *Cuadernos de Derecho Público*, no. 19-20, monograph on *Protección de Datos* ("Data Protection"), pages 45 and subsequent.

² Article I-51: *Protection of Personal Data*
1. Everyone has the right to the protection of personal data concerning him or her.
2. European laws or framework laws shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

³ Article II-68: *Protection of Personal Data*
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

⁴ *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, Callaghan 2nd ed., Chicago, 1888, p. 29.

⁵ Vol IV, 15 December 1890, no. 5.

⁶ To which Stefano Rodotà recently referred in *Intervista su Privacy e Libertà*, by Paolo CONTI, Editori Laterza, Roma-Bari, 2005, p. 7 and subsequent. The office of the *Garante per la protezione dei dati personali* recently re-published a bilingual version – Italian and English – of the article by WARREN and BRANDEIS, Rome, December 2005.

recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society... Now the right to life has come to mean the right to enjoy life, ...the right to be let alone". Society's society since that time has been unending. The fight for privacy has undoubtedly been a key factor in the development of democratic societies. Avoidance of all possibility of "Big Brother", of intolerable control over personal lives by the public or private sector was a compelling challenge to be faced. Within this framework, the appearance of automated personal data processing heralded a new turning point, which has affected the entire process from that time on. In the sixties and the seventies of the last century, the use of new technologies gradually came to the forefront – technologies that not only enable the collection and storage of an enormous amount of data, but also, and more importantly, the subjection of such data to processing. The possibilities for invasion of privacy burgeoned spectacularly, and legislators could no longer remain aloof from the new reality that was unceasingly emerging.

2. The conflict between privacy and computing the economic value of personal data and the independent fundamental right to data protection

In 1967⁷ a Consultative Committee was established within the European Council to study information technologies and their potential threat to personal rights, particularly the freedom from arbitrary interference in the personal lives of individuals (a right set out in the Universal Declaration of Human Rights⁸ and the International Covenant on Civil and Political Rights of 1966⁹). This Consultative Committee was the origin of Resolution 509 of the Assembly of the European Council on "*Human rights and the new scientific and technical achievements*", in response to growing concern all over Europe. It has been said, and not mistakenly, that the source of the legislative data protection movement that swept Europe from that time on was, in effect, based on this Resolution.

Frequent references are also made to the well-known Hessen Act, a pioneer in the issue, as well as to the German Federal Act of 1977. Also commonly mentioned is the 1978 French Act on Computing, Files and Freedoms, which after substantial amendments to adapt it to Directive 95/46/EEC, was replaced by Act no. 2004-801, of 6 August 2004, on the protection of individuals with respect to the processing of personal data.¹⁰ On 8 May 1979, the European Parliament approved a Resolution on "*The protection of individual rights with respect to the growing technical progress in the information sector*". In June 1978, two laws were approved in Denmark – one on private and the other on public registries. In 1978, Austria approved its Data Protection Act, which established the fundamental right of all citizens to demand confidentialia-

lity in the processing and communication of their personal data, and in 1979 Luxembourg passed a law on the use of data in computer processing.

In the eighties, the European Council would give its definitive support to the protection of privacy as regards information systems in Covenant 108 on the Protection of Individuals in automated personal data processing (1981). This Covenant establishes the principles and rights to be envisaged by all legislation addressed at the protection of personal data.

Covenant 108 attempts to reconcile the right to privacy with freedom of information, facilitating international cooperation in the sphere of data protection and limiting the risks of any deviations in national legislation. Chapter II of the Covenant establishes the basic principles of quality of the data, special protection and guaranteed security of data. Likewise, its Article 8 recognises the right to knowledge of the existence of automated personal data files, the main purposes of the same and the identity and address or main establishment of the authority controlling such data.

The OECD also published two important guidelines on this issue: the guideline on "*Protection of Privacy and Transborder Flows of Personal Data*" and the guideline on "*Security in Information Systems*".

The point of view set out in the regulations, international charters and documents listed above is clear: they all attempt to resolve the conflict between the increasingly common use of information systems and the risks these entail for the privacy of individuals. Information versus privacy: this was the great dilemma. This was also reflected in Article 18.4 of the Spanish Constitution of 1978.

In the nineties, still another element was added to the debate. The construction of a unified Europe, which undeniably calls for the creation of an internal market, requires the guarantee of free circulation of personal data, given the economic value of such data in commercial transactions, particularly in the framework of an ever more globalized and transborder economy. This was the scenario behind Directive 95/46/EC of the European Parliament of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The first three Recitals in this Directive are of capital importance and clearly set the tone of the entire regulation.¹¹

A new concept was added in the clash of privacy – information: the economic value of personal data – respect for rights and especially the right to privacy. The construc-

⁷) The following reflections are already set out in "ECJ-Case Law on the Right...", part 1, op. cit. pages 3 and subsequent, as well as in "El derecho a la protección de datos de carácter personal en la jurisprudencia..." ("The right to Personal Data Protection in Case Law"), op. cit., pages 47 and subsequent.

⁸) Article 12 establishes that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

⁹) In practically the same terms, Article 17 of the Covenant establishes:
"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks".

¹⁰) Regarding this law, see Alex TÜRK, "La Ley francesa de protección de datos de carácter personal" ("The French Data Protection Law"), at www.agpd.es. The full text of the Law is available at www.cnll.fr, and www.agpd.es.

¹¹) (1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;
(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;
(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured, require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.

tion of a unified Europe naturally involves the creation of an internal market that upholds the fundamental rights, and within this framework, the free movement of data versus the right to privacy is deemed to be of the utmost importance. Directive 95/46/EC responds to this new concept and lays the foundation for data protection legislation throughout the European countries, and in particular, for Act 15/1999, of 13 December.¹²

In the year 2000, the situation underwent a radical change both in the European Union and in Spain. It was the beginning of a new era, in which personal data protection was considered as a true fundamental right, autonomous and independent of the right to privacy. Such a radical innovation arose primarily from the Charter of Fundamental Rights of the European Union, proclaimed at the Nice Summit on 7 December 2000, which states briefly but clearly in its Article 8, within the Chapter on Freedoms, that *"Everyone has the right to the protection of personal data concerning him or her"*. There is no reference to privacy or intimacy, and none whatsoever to information systems. It does, however, place great emphasis on the fact that *"Compliance with these rules [on personal data protection] shall be subject to control by an independent authority"*. Moreover, separately in Article 7, it establishes the right to privacy and family life. There is then a clear differentiation between the two rights, the right to privacy and the right to data protection, which therefore require two different precepts.

In Spain, this move toward envisaging the right to data protection as a true autonomous and independent right arose from two highly significant judgments of the Constitutional Court: numbers 290 and 292 in 2000, both on 30 November. The first of these ratifies the existence of the Spanish Data Protection Agency, with authority throughout the entire country, to ensure that such fundamental right is homogenous for all persons (individuals).¹³ The second of these judgments consolidates a trend in constitutional case law that had been followed by data protection law since recognition of the right to privacy, which encompasses what is known as computing or informational self-determination.¹⁴ Constitutional Judgments 110/84, 254/93, 143/94, 94/98, 11/98, 144/

99 and 202/99¹⁵ are also noteworthy in this respect. In particular, STC 254/1993¹⁶ establishes that the Constitution of 1978 incorporated the "Right to protection against potential attacks on personal dignity and freedom arising from the illegal use of automated data processing". Furthermore, it finds unacceptable the concept that "the content of the fundamental right to privacy is expressed only in purely negative, exclusive powers. The powers necessary to know of the existence, purposes and controllers of automated files... are absolutely essential in ensuring that the interests protected by Article 18 of the Constitution, and which give rise to the fundamental right to privacy, are genuinely and effectively protected".

But it was STC 292/2000, of 30 November, which definitively recognised that the fundamental right to personal data protection arises directly from the Constitution and should be viewed as an autonomous, independent right. Legal Grounds Seven is unquestionably a key element in this recognition, and is transcribed below:

7. From the foregoing, it is clear that the content of the fundamental right to data protection comprises the power to control and dispose of personal data empowering the individual to decide which of such data will be provided to third parties, regardless of whether such third party is the State or a private individual, which data can be collected by the aforesaid third parties, and enables the individual to know who possesses his/her personal data and to oppose such possession or use. These powers of disposition and control of personal data, which comprise part of the content of the fundamental right to data protection, are legally expressed as the power to consent to the collection, obtaining and access to personal data, their subsequent storage and processing, and their use or possible uses by a third party, whether by the State or an individual. And this right to consent to knowledge and processing, whether automated or not, of personal data, requires certain indispensable supplementary elements; on the one hand the power to know at all times who holds such personal data and what use is being made of the same, as well as the power to object to such possession and uses. In summary, these are all elements that characterise the constitutional definition of

¹² In addition to the aforementioned Directive 95/46, data protection is also taken into consideration in other regulations, such as Directive 2002/58/EC of the European Parliament and Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector, also known as the "Directive on privacy and electronic communications", which replaced Directive 97/66/EC, concerning the processing of personal data and the protection of privacy in the telecommunications sector. In addition to the regulations on data protection, two further Directives supplement those mentioned above in the field of e-commerce, i.e. Directive 2000/31/EC, concerning electronic commerce and Directive 1999/93/EC, concerning electronic signatures, although neither replaces the first two Directives mentioned vis-à-vis personal data protection.

¹³ Spain is a decentralised state based on the model of what are known as Autonomous Communities, an intermediate step between a regional and a federal state. It is perhaps wise to remember the doctrine followed by the Constitutional Court concerning the division of authority between the State and the Autonomous Communities with regard to data protection. In the aforementioned Judgment 290/2000, the Court focuses its analysis on the study of the regulations relating to the existence or non-existence of a violation to the division of authority established in our Constitution. Legal Grounds 7 in this analysis states *"that the examination of the present dispute regarding competencies must be undertaken with a view to two issues: the content of the fundamental right to personal data protection and, secondly, the general features of the Data Protection Agency, given that the duty of this body is to ensure compliance with data protection legislation and to control its application"*, as set out in the first comment of Section a) of Art. 36 LORTAD. With respect to the second of the questions, I will refer to it later in the text.

¹⁴ Recently, a complete study of the Constitutional Court Case Law on this topic was undertaken by E. GUICHOT, in *Datos personales y Administración Pública* ("Personal Data and Public Administration"), Thomson-Civitas, Madrid, 2005, pages 68 and subsequent.

¹⁵ The judgments basically apply to appeals for legal protection against illegitimate processing that violate the principle of "informational self-determination", which is expressed as the right to control the data concerning the individual or, what is the same, the right of the data subject to control the use of his/her data. Hence, Judgments 144/99 and 202/1999, issued against the use by RENFE (the Spanish railway network) of employees' data with respect to labour-union affiliation (The Judgments related to the use of data by RENFE are numerous. See GUICHOT, *Datos personales...*, op. cit., page 71). Earlier Resolutions related the right to personal data protection to the right to privacy (STC 143/1944, 254/1993 and 110/1984), and generally declared *"the global recognition of the right to privacy or to private life, which encompasses its defence against any type of interference in that private sphere of life"*.

¹⁶ On this Judgment, see E. GUICHOT, *Datos personales y Administración Pública*, op.cit., pages 69 and subsequent; ARROYO YANES, L.M., *"El derecho de autodeterminación informativa frente a las Administraciones Públicas (Comentario a la STC 254/93, de 20 de julio)"* ("The right to informational self-determination before the Public Administration – Comments on STS 254/93/ of 20 July"), in *Revista Andaluza de Administración Pública*, 1993; ASPAS ASPAS, *"La libertad informática, un nuevo derecho fundamental desvelado por el Tribunal Constitucional (STC 254/1993, de 20 de julio)"* ("Freedom in information systems, a new fundamental right revealed by the Constitutional Court – STC 254/1993 of 20 July"), in *Revista Aragonesa de Administración Pública*, no. 4, 1994; GONZALEZ MURUA, *"Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales"* ("Comments on STC 254/1993 of 20 July. Reflections on article 18.4 of the Constitution and the protection of personal data"), in *Revista Vasca de Administración Pública*, no. 37, 1993; LUCAS MURILLO DE LA CUEVA, *"La construcción del derecho a la autodeterminación informativa"* ("The creation of the right to informational self-determination"), *Revista de Estudios Políticos*, no. 104, 1999.

the fundamental right to data protection, the rights of the data subject to consent to their collection and the use of his/her personal data and to be aware of such actions. And essential in making such right effective is the recognition of the right to information on the data controller and the purposes of the same, the right to object to such possession and use requiring the processor party to cease the said possession and use of the data, i.e., requiring the data controller to inform the subject if the personal data in its possession, accessing the relevant registries and entries, and to what purpose such data has been used, which also encompasses possible recipients of the same, and, if appropriate to require the data controller to rectify or erase the data.

No further emphasis need be placed on this Judgment, as its importance is clearly evident. It recognises the right to data protection as autonomous and independent of the right to privacy; it determines the essential content, relating it not only to Article 18.4 of the Constitution, but also to Article 10.2. Moreover, Legal Grounds 8 expressly mentions various international instruments, in particular and despite the fact that it was not yet in force (it had just been adopted), the Charter of Fundamental Rights of the European Union.

Thus, the concept of the right to data protection was consolidated, pioneering the concept of informational self-determination in law, which owes much to the well-known Judgment of 15 December 1983 by the German Constitutional Court on the Census Act.

The radical change brought about by Judgments 290 and 292/2000 was mirrored at the European level in the oft-mentioned Charter of Fundamental Rights of the European Union and the European Constitution, the essential data protection precepts of which are transcribed at the beginning of this article. Thus, the evolution of the data protection cycle finally reached its culmination with consideration of the right to data protection as an autonomous fundamental right.

II. CONTENT OF THE FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION

1. Principles that shape the essential content of the fundamental right to data protection

The key, then, lies in determining the essential content of the aforesaid right; the principles and characteristics that define it and which cannot be ignored without violating the right itself. The 27th International Conference on Data Protection and Privacy Commissioners held in Montreux, Switzerland on 13 – 15 September 2005 approved a Final Declaration on “The protection of personal data and privacy in a globalised world: a universal right respecting diversities”, which made express reference to the principles of the right to data protection:

16. Recognising that the principles of data protection derive from international legal binding and non binding instruments such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the United Nations Guidelines concerning Computerized Personal Data Files, the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the Asia Pacific Economic Cooperation Privacy Framework,

17. Recalling that these principles are in particular following:

- principle of lawful and fair data collection and processing;*
- principle of accuracy;*
- principle of purpose-specification and –limitation;*
- principle of proportionality;*
- principle of transparency;*
- principle of individual participation and in particular the guarantee of the right of access of the person concerned;*
- principle of non-discrimination;*
- principle of data security;*
- principle of responsibility;*
- principle of independent supervision and legal sanction;*
- principle of adequate level of protection in case of transborder flows of personal data.*

However, I believe that such principles may be summarised in those that lie at the heart of this right: consent, information, purpose, data quality, with special emphasis on proportionality and security. All these principles are expressed in the Spanish Data Protection Act, in Articles 4 and subsequent, to which the following may be added: fair use of the data and minimisation of their use (the latter, I also believe, falls within the principle of proportionality). To be effective, these principles require the recognition, guarantee and protection of the rights of access, rectification, erasure and objection (governed, in our case, by Articles 15 and subsequent of the LOPD – Spanish Data Protection Act).

It is important to note that the aforementioned principles reach their full significance when the recognition of the fundamental right to data protection is based on the data subject’s power to dispose of his/her data, and that such data are subject to processing. What the foregoing really means is that personal data processors are processing other people’s personal data, not their own, and thus, the rights of the data subject must be strictly upheld. And this brings us back to respect for the dignity of the individual, the fundamental basis of data protection, and clearly underlines the principles mentioned above.

In effect, if the data subject to processing belong to others and their use must occur within the framework of respect for the dignity of the individual and his/her power to dispose of such data, it is only logical that: the data subject be informed when the data are collected (Articles 10 and 11 of Directive 95/46/EC); that the processing be effected for legitimate purposes that envisage their use, with the consent of the data subject (Article 7 of the Directive and Article 8 of the Charter of Fundamental Rights of the European Union); that the data may only be used for the legitimate purpose(s) for which they were collected (Article 6.1. of the Directive); that the principle of proportionality and minimum interference in their processing must be respected, as well as the concept of fair and legitimate use (Article 6 of the Directive); and that personal data processing must involve security measures (Articles 16 and 17 of the Directive). All of which, as mentioned previously, are guaranteed, in turn, by recognition of the data subjects’ right to access, rectification, erasure and objection (Articles 12 and subsequent of the Directive), which are essential in ensuring that crucial right to dispose of one’s own personal data, which is the very foundation of the system.

2. The principle of independent control

Furthermore, the European Charter of Human Rights, in keeping with the previously mentioned texts, takes a vital step forward toward another of the inherent principles in data protection: the principle of independent control. In effect, when it declares that "*Compliance with these rules [on data protection] shall be subject to control by an independent authority*", it is establishing the existence of such an authority as a requirement to consider the right to data protection as sufficiently guaranteed. Hence, without such an authority, under no circumstances can the governing legal framework be considered acceptable. Precisely one of the key points in the decisions on adequacy approved to date by the European Commission concerning the data protection provided in third countries is the existence of an independent control authority.¹⁷

This provision in the European Charter is not new, although the fact that it is invested with such importance in the document is an innovation. Point 8 of Resolution 45/95 of the United Nations General Assembly, of 14 December 1990, which establishes the guidelines for data protection, states that "The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles [of data protection] set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence". Moreover, the preamble establishes that "supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data". Along the same lines, Article 1.3 provides that "The supervisory authorities shall exercise their functions in complete independence", and point 4 of the same article adds, "Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts". And, of course, Article 28.1 of Directive 95/46/EC clearly states that "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them".

In summary, the principle of protection through an independent authority has now been consolidated as a true principle of the right to data protection.

The Spanish Constitutional Court has also come out clearly and indisputably on the position occupied by the Spanish Data Protection Agency within the system of guarantees of

the fundamental right to data protection. The aforementioned Judgment 290/2000, of 30 November, emphasises the importance of the independent control authority in the data protection system. The Constitutional Court stated that "*With respect to... the Data Protection Agency..., it must first be noted that the legal regulations adopted by various European member states with a view to protection personal data from the dangers of information systems prior to the entrance into effect of our Constitution (Swedish Law of 11 May 1973, Law of the Federal Republic of Germany of 22 January 1977, the French law of 6 January 1978, Norwegian law of 8 June 1978), all envisage an institutional element. Regardless of the various names and organizational forms these laws establish, they all created institutions specialised in public law, invested with various supervisory duties over personal data files subject to automated processing, whether by public bodies or private entities*". And the Court indicates that the Spanish Agency is established as "*a body under Public Law, invested with legal capacity and public and private authority, which acts fully independently of the public administration in the exercise of its duties*". Likewise, the Court justifies the attribution of duties and powers to the Data Protection Agency "*to ensure, via the exercise of the same, that both the restrictions on the use of information systems and the safeguards of the fundamental right to personal data protection will be upheld in all files, whether belonging to public or private entities*".

And the Judgment goes on to say that "*the creation of the aforesaid Public Law body and the duties attributed to it make it possible to guarantee... the exercise by all citizens of all the powers encompassed within the fundamental right*". Thus, the Data Protection Agency "*guarantees the citizens' exercise of their fundamental right to the protection of such data*". And given "*that the guarantee of these rights and those establishing the equality of all Spaniards to enjoy such rights is the goal that guides the Data Protection Agency's actions, such duties and powers must be exercised in whatsoever area within the country where there are automated files containing personal data, regardless of the controllers of such files*".

Thus, the existence of an independent supervisory authority clearly is an integral part of the system behind the fundamental right to personal data protection.

III. CHALLENGES AND CONFLICTS IN THE RIGHT TO DATA PROTECTION

It is important to note that this right, envisaged with recognition of the true and effective power of data subjects to dispose of their personal data, is nonetheless subject to a number of challenges or conflicts that must be borne in mind. I believe that such conflicts may be summarized as follows: data protection *versus* a) freedom of expression; b) transparency and access to information; c) market interests and evolution; and, d), the fight against terrorism and the guarantee of public safety.

Above all, it must be immediately and unquestionably stated that there is no such contradiction between the aforementioned rights or situations and data protection. The European Court of Justice pointed this out, for example, in its well-known Judgment of 20 May 2003, in *Rundfunk et al*, Cases C-465/00, C-138/01 and C-139/01; and in the not lesser-known Judgment of 6 November 2003, *Linqvist*, Case C-101/01¹⁸

¹⁷⁾ Such decision are as follows:
Commission Decision of 26 July 2000 pursuant to Directive 95/46 on the adequate protection of personal data provided in Switzerland.
Commission Decision of 26 July 2000, the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce.
Commission Decision of 20 December 2001 on the adequate protection of personal data provided by the Canadian *Personal Information Protection and Electronic Documents Act*.
Commission Decision of 30 June 2003 on the adequate protection of personal data in Argentina.
Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey.
Commission Decision of 28 April 2004 on the adequate protection of personal data on the Isle of Man.
Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection. This Decision was appealed by the European Parliament before the Court of Justice (Case C-318/04). Advocate General LÉGER published his Conclusions (22 November 2005) in which he proposes annulling the Decision.

¹⁸⁾ Further discussion on these Judgments is available in my previously mentioned study "*El derecho a la protección de datos de carácter personal en la jurisprudencia...*", op. cit, pages 16 and subsequent.

with respect to freedom of expression. Quite the contrary: it is only by upholding the fundamental right of all people to data protection that the suitable stage is set for freedom of expression and the right of access to information, the proper evolution of the market and an effective fight against terrorism.

Moreover, the relationships arising through the development of economic activities in an increasingly globalized world require taking into account not only market needs, but also protection of the fundamental rights and particularly, the right to data protection. Thus, it is crucial to recognise the basic premise that data protection is absolutely not an obstacle to the free evolution of economic activity, but rather a complement to ensure that such activity upholds the rights of citizens. To this purpose, innovative and efficient solutions must be sought that envisage all the various interests involved. A clear example is recourse to tools such as Binding Corporate Rules, which ensure the right to data protection within the framework of a globalized economy.

However, the most apparently conflict situation arises from the relationship between data protection and security, particularly in light of the brutal terrorist attacks suffered in New York, Madrid and London.

Obviously, no one questions the irrefutable fact that effective measures must be taken in the fight against terrorism. But likewise, it is essential to insist time and time again that such measures uphold the fundamental rights; otherwise, we will be offering the terrorists their first and most important victory: the restriction of freedoms and rights which, fortunately, are the foundation of Western societies. And one of those rights is the protection of personal data. Any measure adopted to do away with terrorism and the terrible manifestations of organized crime must uphold the essential content of this right, comprised of the principles referred to previously.

Thus, it is in this scenario where a global data protection model is needed, a model that clarifies the rules of the game at an international level, and in which Directive 95/46/EC on data protection most certainly plays a vital role.

Moreover, this is an increasingly generalised trend. The fundamental right to data protection is currently spreading throughout the world at an extraordinary rate. It may be said that within the framework of globalisation, it is reaching hitherto unknown importance, with significant presence of the European model, not only through the influence of Directive 95/46/EC, but also in the documents drawn up by the Article 29 Group.¹⁹

I cannot now go into greater detail with respect to the four great challenges facing data protection. But an incontrovertibly significant instrument in achieving the desired results is the awareness of citizens and data controllers (both public and private) of the importance vested in a fundamental right that is not all so new, and emphasis on its magnitude in today's modern information society.

Fundamentalne prawo do ochrony danych osobowych, jego istota i wiążące się z nim wyzwania

I. POCHODZENIE PRAWA DO OCHRONY DANYCH JAKO PRAWA FUNDAMENTALNEGO

1. Źródła. „Prawo do bycia pozostawionym w spokoju”

Podstawowe prawo do ochrony danych osobowych jest jednym z najważniejszych praw współczesnych społeczeństw. Jak już wspominałem w moich wcześniejszych pracach,¹ „Traktat Europejski” ustanawiający konstytucję dla Europy wyraźnie wymienia podstawowe prawo do ochrony danych osobowych w dwóch sekcjach. Pojęcie to po raz pierwszy pojawia się w artykule I-51 tytułu VI („Życie demokratyczne Unii”) części pierwszej,² a następnie w artykule II-68 tytułu II („Wolności”) części drugiej, w „Karcie praw podstawowych Unii”.³

Mimo że ewentualne przyszłe zmiany konstytucji europejskiej mogą nas jeszcze w niektórych aspektach zaskoczyć, nie ulega wątpliwości, że nie tylko konstytucja, ale także „Karta praw podstawowych” przyjęta w Nicei w 2000 r. zwiastowały przełom, jeżeli chodzi o uwagę poświęconą podstawowemu prawu do ochrony danych osobowych. Jest to bezsprzecznie najważniejsza przesłanka, o której należy pamiętać w toku niniejszych rozważań.

Thomas Cooley prześledził genezę „prawa do bycia pozostawionym w spokoju”⁴ aż do roku 1888. W roku 1890 *Harvard Law Review*⁵ opublikował obecnie bardzo znany artykuł pióra Samuela Warrena i Louisa Brandeisa zatytułowany „Prawo do prywatności”.⁶ Warren i Brandeis omawiali w nim nowe prawo jednostki: „Zmiany polityczne, społeczne i gospodarcze powodują powstanie świadomości nowych praw, a wiecznie młode prawo zwyczajowe rozwija się, aby sprostać nowym potrzebom społeczeństwa... Obecnie prawo do życia zaczęło oznaczać prawo do czerpania satysfakcji z życia, prawo do bycia

¹) Omawiałem już to zagadnienie w „ECJ Case-Law on the Right to Protection of Personal Data” („Orzecznictwo ETS nt. prawa do ochrony danych osobowych”), *BNA Internacional. World Data Protection Report*, część 1 i część 2, odpowiednio styczeń i luty 2006, jak również w „El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas” („Prawo do ochrony danych osobowych w orzecznictwie Europejskiego Trybunału Sprawiedliwości”), w *Cuadernos de Derecho Público*, nr 19-20, monografia nt. *Protección de Datos* („Ochrony danych osobowych”), strona 45 i następne.

²) Artykuł I-51: Ochrona danych osobowych
1. Każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
2. Ustawa europejska lub europejska ustawa ramowa określa zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

³) Artykuł II-68: Ochrona danych osobowych
1. Każda osoba ma prawo do ochrony danych osobowych, które jej dotyczą.
2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każda osoba ma prawo dostępu do zebranych danych, które jej dotyczą i prawo do dokonania ich sprostowania.
3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

⁴) *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, Callaghan wyd. drugie, Chicago, 1888, p. 29.

⁵) Tom IV, 15 grudnia 1890 r., nr 5.

⁶) Do którego niedawno nawiązał Stefano Rodotà w *Intervista su Privacy e Libertà*, pod redakcją Paolo Contiego, Editori Laterza, Roma-Bari, 2005, strona 7 i następne. Biuro *Garante per la protezione dei dati personali* niedawno opublikowało ponownie dwujęzyczną wersję – po włosku i po angielsku – artykułu Warrena i Brandeisa, Rzym, grudzień 2005.

¹⁹) Group of European Data Protection Authorities established in Article 29 of the Directive.

pozostawionym w spokoju.” Od tego czasu społeczeństwo jest nieustannie obecne w życiu jednostek. Walka o prywatność jest bez wątpienia kluczowym czynnikiem w rozwoju społeczeństw demokratycznych. Nowe palące wyzwanie, któremu należało stawić czoła, to jak nie dopuścić do pojawienia się „Wielkiego Brata”, czyli niemożliwej do zniesienia kontroli nad życiem osobistym przez sektor prywatny czy publiczny. Na tym tle pojawienie się automatycznego przetwarzania danych osobowych zwiastowało kolejny punkt zwrotny, który miał od tej pory wywierać znaczący wpływ na cały proces. W latach sześćdziesiątych i siedemdziesiątych ubiegłego wieku nowe technologie stopniowo wysunęły się na pierwszy plan: ich zastosowanie umożliwiło nie tylko gromadzenie i przechowywanie ogromnych ilości danych, ale także – co bardziej istotne – poddawanie tych danych przetwarzaniu. W niespotykanej dotąd skali wzrosło prawdopodobieństwo naruszenia prywatności, na co prawodawcy nie mogli dłużej pozostawać obojętni.

2. Konflikt pomiędzy ochroną prywatności a komputerowym przetwarzaniem danych osobowych o wartości gospodarczej i odrębnym prawem podstawowym do ochrony danych

W 1967 r.⁷ ustanowiono przy Radzie Europejskiej Komitet Konsultacyjny, który podał analizie technologie informacyjne oraz potencjalne zagrożenia, jakie mogą się z nimi wiązać dla praw osobistych, a szczególnie dla wolności od arbitralnej ingerencji w życie osobiste jednostek (prawo to zdefiniowane jest w „Powszechnej deklaracji praw człowieka”⁸ i w „Międzynarodowym pakcie praw obywatelskich i politycznych” z 1966 r.⁹). Prace Komitetu Konsultacyjnego zaowocowały rezolucją 509 z posiedzenia Rady Europejskiej dotyczącą „Praw człowieka i nowych osiągnięć naukowo-technicznych”, przygotowaną w odpowiedzi na narastający w całej Europie niepokój. Mówi się – i jest to pogląd niepozbawiony słuszności – że u źródeł legislacyjnego ruchu ochrony danych osobowych, który od tego czasu objął Europę, leżała w istocie ta właśnie uchwała.

Często przywoływana jest szeroko znana pionierska ustawa heska oraz niemiecka federalna ustawa z 1977 r., wspomina się także w tej dziedzinie francuską ustawę o technologii informacyjnej, plikach i wolnościach, która po poważnych zmianach dostosowujących ją do Dyrektywy 95/46/WE, została zastąpiona przez ustawę nr 2004-801 z dnia 6 sierpnia 2004 r. o ochronie praw jednostki w zakresie przetwarzania danych osobowych.¹⁰ Dnia 8 maja 1979 r. Parlament Europejski przyjął rezolucję o „Ochronie praw jednostek w związku z rosnącym postępem technicznym w sektorze informatycznym”. W czerwcu 1978 w Danii przyjęto dwie ustawy, z których jedna dotyczyła publicznych rejestrów danych, a druga prywatnych. W 1978 r. w Austrii przyjęto ustawę o ochronie danych osobowych, która dawała wszystkim obywatelom podstawowe prawo do doma-

gania się poufności przy przetwarzaniu i ujawnianiu ich danych osobowych, a w 1979 r. Luksemburg przyjął ustawę o wykorzystaniu danych w systemach informatycznych.

W latach osiemdziesiątych Rada Europy udzieliła zdecydowanego poparcia ochronie prywatności w ramach systemów informatycznych w „Konwencji nr 108” o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (1981). Konwencja ta wprowadza zasady i regulacje prawne, które powinny zostać uwzględnione we wszystkich aktach prawnych dotyczących ochrony danych osobowych.

„Konwencja nr 108” próbuje pogodzić prawo do prywatności z prawem do wolności informacji, co miało ułatwić międzynarodową współpracę w dziedzinie ochrony danych osobowych i ograniczyć ryzyko pojawienia się odstępstw od tych zasad w ustawodawstwach krajowych. Rozdział II „Konwencji” wprowadza podstawowe zasady jakości danych, specjalnej ochrony oraz ich gwarantowanego bezpieczeństwa. Analogicznie, artykuł 8 „Konwencji” uznaje prawo do bycia informowanym o istnieniu zautomatyzowanych plików zawierających dane osobowe, o głównych celach ich przechowywania oraz tożsamości i adresie lub głównej siedzibie administratora danych.

Również OECD opublikowała dwa ważne zbiory wytycznych dotyczące tej tematyki: wytyczne dotyczące „Ochrony prywatności i transgranicznego przepływu danych osobowych” oraz wytyczne dotyczące „Bezpieczeństwa w systemach informatycznych”.

Stanowisko zawarte w wymienionych powyżej aktach prawnych, międzynarodowych konwencjach i dokumentach jest jasne: wszystkie z nich usiłują rozstrzygnąć konflikt pomiędzy coraz powszechniejszym zastosowaniem systemów informatycznych a wiążącymi się z tym trendem zagrożeniami dla prywatności jednostek. „Informacja przeciwko prywatności” – tak właśnie przedstawiał się ten dylemat. Znalazł on także swój wyraz w artykule 18.4 hiszpańskiej Konstytucji z 1978 r.

W latach dziewięćdziesiątych w debacie pojawił się jeszcze jeden aspekt. Jednym z etapów budowy zjednoczonej Europy jest bezsprzecznie utworzenie wspólnego rynku wewnętrznego, który wymaga gwarancji swobodnego przepływu danych osobowych, ze względu na wartość gospodarczą takich danych w transakcjach handlowych, szczególnie w ramach coraz bardziej zglobalizowanej i transgranicznej gospodarki. Takie było tło Dyrektywy 95/46/WE Parlamentu Europejskiego z 24 października 1995 r. o ochronie praw osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnym przepływie tych danych. Trzy pierwsze punkty preambuły tej Dyrektywy mają ogromne znaczenie i objaśniają cały akt prawny.¹¹

⁷⁾ Poniższe uwagi zostały już zaprezentowane w „ECJ-Case Law on the Right...”, część 1, op. cit., strona 3 i następne, jak również w „El derecho a la protección de datos de carácter personal en la jurisprudencia...” („Prawo do ochrony danych osobowych w orzecznictwie...”), op. cit., strona 47 i następne.

⁸⁾ Artykuł 12 stanowi, że: „Nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu.”

⁹⁾ W praktycznie tych samych słowach artykuł 17 „Paktu” stanowi:

„1. 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.

2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami.”

¹⁰⁾ Odnosnie tej ustawy, zob. Alex Türk, „La Ley francesa de protección de datos de carácter personal” („Francuska ustawa o ochronie danych osobowych”), na stronie www.agpd.es. Pełny tekst ustawy jest dostępny na stronie www.cnll.fr oraz na www.agpd.es.

¹¹⁾ (1) Cele Wspólnoty, określone w „Traktacie”, wraz ze zmianami wprowadzonymi „Traktatem o Unii Europejskiej”, obejmują tworzenie coraz ściślej wspólnoty narodów Europy, kształtowanie bliższych stosunków między państwami należącymi do Wspólnoty, zapewnienie postępu ekonomiczno-społecznego poprzez wspólne działania na rzecz likwidacji barier dzielących Europę, pobudzanie ciągłej poprawy warunków życia jej narodów, ochronę i umacnianie pokoju i wolności oraz rozwój demokracji w oparciu o fundamentalne prawa uznane w konstytucjach i ustawodawstwach Państw Członkowskich oraz w „Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności”;

(2) Systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; zważywszy, że muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, respektować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu ekonomiczno-społecznego, rozwoju handlu oraz dobrobytu jednostek;

(3) Utworzenie i funkcjonowanie rynku wewnętrznego, na którym zgodnie z art. 7a „Traktatu”, zapewniony jest swobodny przepływ towarów, osób, usług i kapitału wymaga nie tylko zapewnienia swobodnego przepływu danych osobowych z jednego Państwa Członkowskiego do drugiego, lecz również ochrony podstawowych praw jednostek.

Do konfliktu pomiędzy sferą prywatną a prawem do informacji dołączyła nowa antynomia: gospodarcza wartość danych osobowych a poszanowanie praw, w szczególności prawa do prywatności. Budowa zjednoczonej Europy wiąże się oczywiście z tworzeniem wewnętrznego rynku, w ramach którego przestrzegane są podstawowe prawa, i w tym kontekście sprzeczność pomiędzy wolnym przepływem danych a prawem do prywatności jest uważana za sprawę o najwyższej wadze. Dyrektywa 95/46/WE stanowiła odpowiedź na to nowe wyzwanie i wzniosła fundament pod krajowe ustawodawstwa dotyczące ochrony danych osobowych w Europie, m.in. hiszpańską ustawę 15/1999 z 13 grudnia 1999 r.¹²

W roku 2000 sytuacja uległa radykalnej zmianie, zarówno w Unii Europejskiej, jak i w Hiszpanii. Był to początek nowej ery, w której ochrona danych osobowych została uznana za prawdziwe prawo podstawowe o autonomicznym charakterze i niezależne od prawa do prywatności. Ta radykalna innowacja wynikła głównie za sprawą „Karty praw podstawowych Unii Europejskiej”, ogłoszonej na szczycie w Nicei 7 grudnia 2000 r. Artykuł 8 rozdziału o wolnościach „Karty” stwierdza krótko, lecz jednoznacznie, że *„każdy ma prawo do ochrony dotyczących go danych osobowych”*. Nie ma tu wzmianki o prywatności czy intymności, ani odniesienia do systemów informatycznych.

Duży nacisk kładzie się jednakże na wymóg, zgodnie z którym *„przestrzeganie tych zasad [o ochronie danych osobowych] będzie kontrolowane przez niezależną instytucję”*. Natomiast w artykule 7 wprowadza się osobno prawo do prywatności i życia rodzinnego. Istnieje zatem wyraźne rozróżnienie tych dwóch praw: prawa do prywatności i prawa do ochrony danych. Wymagają one w związku z tym odrębnych uregulowań w przepisach.

W Hiszpanii przesunięcie stanowiska w kierunku uznania prawa do ochrony danych osobowych za w pełni autonomiczne i odrębne nastąpiło w wyniku dwóch ważnych wyroków Trybunału Konstytucyjnego: nr 290 i nr 292 z 2000 r., oba z dnia 30 listopada. Pierwszy z nich zatwierdza istnienie Hiszpańskiej Agencji Ochrony Danych Osobowych, której kompetencje obejmują cały kraj, gwarantując tym samym, że to podstawowe prawo będzie chroniło w sposób jednolity wszystkie osoby (osoby fizyczne).¹³ Drugi z tych wyroków utrwała pewien trend w orzecznictwie Trybunału Konstytucyjnego, za którym od czasu uznania prawa do prywatności podąża ustawodawstwo doty-

czące ochrony danych osobowych. Trend ten obejmuje tzw. prawo do informatycznego lub informacyjnego samodecydowania.¹⁴ W tym zakresie godne uwagi są także wyroki sądu konstytucyjnego 110/84, 254/93, 143/94, 94/98, 11/98, 144/99 i 202/99,¹⁵ w szczególności STC 254/1993,¹⁶ który stwierdza, że Konstytucja z 1978 r. zawiera „prawo do ochrony przeciwko potencjalnym atakom na godność osobistą i wolność mającym u źródła nielegalne wykorzystanie zautomatyzowanego przetwarzania danych.” Co więcej, uznaje się za niedopuszczalną koncepcję, że „treść podstawowego prawa do prywatności jest wyrażana jedynie za pomocą uprawnień negatywnych, wyłączających. Uprawnienia potrzebne, aby dowiedzieć się o istnieniu zautomatyzowanych plików, celu do jakiego służą i instytucjach je kontrolujących (...) są absolutnie niezbędne, aby zagwarantować, że interesy chronione na podstawie artykułu 18 Konstytucji, na których opiera się podstawowe prawo do prywatności, są faktycznie i skutecznie chronione.”

Jednakże dopiero w orzeczeniu STC 292/2000 z dnia 30 listopada Trybunał ostatecznie uznał, że podstawowe prawo do ochrony danych osobowych wynika bezpośrednio z Konstytucji i powinno być traktowane jako prawo autonomiczne i niezależne. Przytoczony poniżej punkt 7 uzasadnienia wyroku jest bez wątpienia kluczowym elementem tej tezy:

7. Wobec powyższego, jasne jest, że treść podstawowego prawa do ochrony danych obejmuje uprawnienia do kontrolowania i dysponowania danymi osobowymi umożliwiające jednostce decydowanie, które z danych zostaną udostępnione stronom trzecim, czy to państwu, czy osobie fizycznej, które dane mogą być gromadzone przez te osoby trzecie i daje jednostkom prawo do informacji, kto jest w posiadaniu ich danych osobowych oraz prawo do sprzeciwu wobec przechowywania lub wykorzystania tych danych. Te prawa do dysponowania danymi osobowymi i ich kontrolowania wpisują się w podstawowe prawo do ochrony danych osobowych i są określane w ustawodawstwie jako prawo do wyrażenia zgody na gromadzenie, pozyskiwanie i dostęp do danych osobowych, na ich późniejsze przechowywanie i przetwarzanie oraz na ich wykorzystanie lub potencjalne wykorzystanie przez osobę trzecią, niezależnie od tego, czy jest nią państwo czy osoba fizyczna.

¹⁴ E. Guichot przeprowadził niedawno całościową analizę orzecznictwa Trybunału Konstytucyjnego na ten temat w *Datos personales y Administración Pública* („Dane osobowe i administracja publiczna”), Thomson-Civitas, Madryt, 2005, strona 68 i następne.

¹⁵ Wyroki zasadniczo dotyczą wniosków o ochronę prawną przeciwko bezprawnemu przetwarzaniu danych osobowych, które narusza zasadę „informatycznego samodecydowania”, wyrażającą się w prawie do kontrolowania danych dotyczących osoby fizycznej, lub, co sprowadza się do tego samego, prawa osób, których dotyczą dane, do kontrolowania wykorzystania ich danych. Stąd wyroki 144/99 oraz 202/1999, sprzeciwiające się wykorzystaniu przez RENFE (hiszpańskie linie kolejowe) danych pracowników dotyczących ich przynależności do związków zawodowych. (Wyroki dotyczące wykorzystania danych przez RENFE są bardzo liczne. Zob. Guichot, *Datos personales...*, op. cit., strona 71). Wcześniejsze orzeczenia wiązały prawo do ochrony danych osobowych z prawem do prywatności (STC 143/1944, 254/1993 oraz 110/1984) i generalnie deklarowały „ogólne uznanie prawa do prywatności lub do życia prywatnego, co obejmuje jego ochronę przez wszelkiego rodzaju ingerencjami w prywatną sferę życia.”

¹⁶ Na temat tego wyroku, zob. E. Guichot, *Datos personales y Administración Pública*, op. cit., strona 69 i następne; Arroyo Yanes, L.M., „El derecho de autodeterminación informativa frente a las Administraciones Públicas (Comentario a la STC 254/93, de 20 de julio)” („Prawo do informacyjnego samodecydowania przed administracją publiczną – komentarze do STS 254/93 z 20 lipca”), w *Revista Andaluza de Administración Pública*, 1993; ASPAS ASPAS, „La libertad informática, un nuevo derecho fundamental desvelado por el Tribunal Constitucional (STC 254/1993, de 20 de julio)” („Wolność systemów informatycznych, nowe fundamentalne prawo wskazane przez Trybunał Konstytucyjny – STC 254/1993 z 20 lipca”), w *Revista Aragonesa de Administración Pública*, no. 4, 1994; Gonzalez Murua, „Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales” („Komentarze nt. STC 254/1993 z 20 lipca. Uwagi nt. artykułu 18.4 Konstytucji i ochrony danych osobowych”), w *Revista Vasca de Administración Pública*, no. 37, 1993; Lucas Murillo de la Cueva, „La construcción del derecho a la autodeterminación informativa” („Utworzenie prawa do informacyjnego samodecydowania”), *Revista de Estudios Políticos*, no. 104, 1999.

¹² Oprócz wspomnianej Dyrektywy 95/46 zagadnienie ochrony danych osobowych zostało także poruszone w innych aktach prawnych, jak np. Dyrektywa 2002/58/WE Rady Europejskiej i Parlamentu Europejskiego z 12 lipca 2002 r., dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej, znana także jako „Dyrektywa o ochronie prywatności i komunikacji elektronicznej”, która zastąpiła Dyrektywę 97/66/WE, dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacji. Oprócz tych aktów prawnych o ochronie danych osobowych dwie kolejne dyrektywy uzupełniają te wspomniane powyżej w dziedzinie e-handlu, tj. Dyrektywa 2000/31/WE, dotycząca handlu elektronicznego oraz Dyrektywa 1999/93/WE, dotycząca podpisów elektronicznych, jakkolwiek żadna z nich nie zastępuje pierwszych dwóch wspomnianych dyrektyw w kwestii ochrony danych osobowych.

¹³ Hiszpania jest państwem zdecentralizowanym, obejmującym podmioty znane jako wspólnoty autonomiczne; model ten stanowi poziom pośredni pomiędzy państwem podzielonym na regiony i państwem federalnym. Warto zapewne znać doktrynę, której przestrzega Trybunał Konstytucyjny odnośnie podziału władzy pomiędzy władzami centralnymi a wspólnotami autonomicznymi w kwestii ochrony danych osobowych. We wspomnianym powyżej wyroku nr 290/2000 Trybunał skupia się na analizie przepisów decydujących o zaistnieniu lub niezaistnieniu naruszenia podziału władzy, ustanowionego przez naszą Konstytucję. W punkcie 7 uzasadnienia wyroku stwierdza się, „że rozpatrywanie rzeczonego sporu dotyczącego kompetencji musi uwzględniać dwie kwestie: treść fundamentalnego prawa do ochrony danych osobowych oraz, po drugie, ogólne kompetencje Agencji Ochrony Danych Osobowych, biorąc pod uwagę fakt, iż obowiązkiem tej instytucji jest zagwarantowanie przestrzegania ustawodawstwa dotyczącego ochrony danych osobowych oraz kontrolowanie jego stosowania”, jak stwierdzono w pierwszym komentarzu do sekcji a) artykułu 36 LORTAD. Do drugiej z tych kwestii odnoszę się w dalszym miejscu w tekście.

Prawo do wyrażania zgody na przechowywanie danych osobowych i ich przetwarzanie, zautomatyzowane czy też nie, wymaga natomiast spełnienia pewnych niezbędnych dodatkowych wymogów, z jednej strony zapewnienia jednostce informacji, aby w każdej chwili wiedziała, kto przechowuje jej dane osobowe i do jakich celów je się wykorzystuje, z drugiej strony prawa sprzeciwu wobec przechowywania i wykorzystywania danych. Podsumowując, wszystkie te elementy charakteryzują konstytucyjną definicję podstawowego prawa do ochrony danych, praw osób, których dane dotyczą, do wyrażenia zgody na ich gromadzenie i wykorzystywanie oraz do informacji o takich działaniach. Aby zagwarantować skuteczność tego prawa, niezbędne jest respektowanie prawa do informacji przez administratora danych i jego celów, prawa do sprzeciwu wobec przechowywania danych i do żądania od podmiotu przetwarzającego dane zaprzestania rzeczonych przechowywania i wykorzystywania danych, np. prawo żądania od tego podmiotu, aby poinformował jednostkę o fakcie posiadania danych osobowych, dostępu do właściwych rejestrów i pozycji rejestru, oraz do jakiego celu dane te zostały wykorzystane, co obejmuje także ich możliwych odbiorców (...) i jeżeli zachodzi taka konieczność, prawo zażądania od kontrolera danych możliwości poprawienia lub usunięcia danych."

Nie trzeba chyba dodatkowo podkreślać wagi tego wyroku, którego znaczenie jest oczywiste. Uznaje on prawo do ochrony danych osobowych za autonomiczne i niezależne od prawa do prywatności; ustala się podstawową treść tego prawa, nawiązując do artykułu 18.4 Konstytucji, jak również do jej artykułu 10.2. Co więcej, punkt 8 uzasadnienia wyroku wymienia konkretnie instrumenty międzynarodowe, w tym „Kartę praw podstawowych”, mimo że dokument ten jeszcze nie obowiązywał w tym czasie (został dopiero przyjęty).

Tak oto koncepcja prawa do ochrony danych została skonkretyzowana, tworząc przedpole dla legislacyjnej koncepcji samodecydowania o dotyczących nas informacjach, która dużo zawdzięcza szeroko znanemu wyrokowi niemieckiego Trybunału Konstytucyjnego w sprawie ustawy o spisie ludności z 15 grudnia 1983 r.

Radykalna zmiana, którą przyniosły wyroki nr 290 i 292/2000 znalazła swoje odzwierciedlenie na szczeblu europejskim w przywoływanej już „Karcie praw podstawowych Unii Europejskiej” i w konstytucji europejskiej (zawarte w niej podstawowe koncepcje ochrony danych osobowych zostały zaprezentowane na początku niniejszego artykułu). Tak oto proces ewolucji prawa do ochrony danych osobowych znalazł w końcu swoje ukoronowanie w uznaniu prawa do ochrony danych za autonomiczne prawo podstawowe.

II. ISTOTA PODSTAWOWEGO PRAWA DO OCHRONY DANYCH OSOBOWYCH

1. Zasady decydujące o istocie podstawowego prawa do ochrony danych osobowych

Kluczową kwestią jest zatem ustalenie podstawowej treści powyższego prawa oraz definiujących je zasad i cech właściwych, bez których nie można o nim mówić. 27 międzynarodowa konferencja w sprawie ochrony danych i komisarzy ds. ochrony prywatności, zorganizowana w Montreux w Szwajcarii, w dniach 13-15 września 2005 r. przyjęła deklarację końcową „Ochrona danych osobowych i prywatności w zglobalizowanym świecie: uniwersalne prawo i poszanowanie dla różnorodności”. Deklaracja ta nawiązywała bezpośrednio do zasad prawa do ochrony danych osobowych:

16. Uznając, że zasady ochrony danych osobowych wywodzą się z wiążących i niewiążących prawnie aktów prawa międzynarodowego, takich jak wytyczne OECD regulujące ochronę prywatności i transgraniczny przepływ danych osobowych, „Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych”, wytyczne Organizacji Narodów Zjednoczonych dotyczące skomputeryzowanych plików danych osobowych, Dyrektywa Unii Europejskiej w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych oraz Platforma Prywatności APEC (Organizacji Współpracy Gospodarczej Azji i Pacyfiku).

17. Zważywszy, że do zasad tych należą w szczególności:

- zasada zgodnego z prawem i rzetelnego gromadzenia i przetwarzania danych;
- zasada dokładności;
- zasada określonego celu i ograniczonego celu;
- zasada proporcjonalności;
- zasada transparentności;
- zasada udziału jednostki i szczególnie gwarancja prawa dostępu osób, których dotyczą dane;
- zasada niedyskryminacji;
- zasada bezpieczeństwa danych;
- zasada odpowiedzialności;
- zasada niezależnego nadzoru i sankcji prawnych;
- zasada dostatecznego poziomu ochrony w przypadku transgranicznego przepływu danych osobowych.

Uważam, że zasady te można podsumować, wymieniając tylko te, które stanowią samą istotę prawa do ochrony danych osobowych. Są to wymogi: zgody, informacji, celu, jakości danych, proporcjonalności i bezpieczeństwa. Wszystkie te zasady są uwzględnione w artykule 4 i kolejnych hiszpańskiej ustawy o ochronie danych osobowych. Można do nich dodać jeszcze następujące zasady: uczciwe wykorzystanie danych i minimalizacja ich wykorzystania (ta ostatnia zasada pokrywa się moim zdaniem z zasadą proporcjonalności). Aby zasady te były skuteczne, wymagane jest uznanie, zagwarantowanie i ochrona prawa dostępu do danych, ich poprawiania, usuwania i sprzeciwu wobec przetwarzania [unormowanych – w naszym przypadku – przez artykuł 15 i kolejne LOPD (hiszpańskiej ustawy o ochronie danych osobowych)].

Należy zauważyć, że pełne znaczenie wspomnianych powyżej zasad uwidacznia się, gdy uznanie podstawowego prawa do ochrony danych osobowych opiera się na uprawnieniu osoby, której dane dotyczą, do dysponowania swoimi danymi i do wyrażania zgody na ich przetwarzanie. Powyższe stwierdzenie oznacza w istocie, że podmioty zajmujące się przetwarzaniem danych osobowych wykorzystują dane osobowe należące do osób trzecich, nie zaś swoje własne, i dlatego prawa jednostek, których dane dotyczą, muszą być rygorystycznie przestrzegane. Sprowadza nas to z powrotem do kwestii poszanowania godności jednostki, która jest fundamentalną podstawą ochrony danych i uwidacznia znaczenie powyższych zasad.

Dlatego też, jeżeli przetwarzane dane należą do osób trzecich a sposób ich wykorzystania musi gwarantować poszanowanie godności jednostki oraz jego/jej prawo do usunięcia tych danych, logiczną konsekwencją jest, że: osobie, której dotyczą dane, musi być przekazana informacja o gromadzeniu jej danych (artykuły 10 i 11 Dyrekty-

wy 95/46/WE); przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów, które przewidują wykorzystanie danych za zgodą osoby, której one dotyczą (artykuł 7 Dyrektywy i artykuł 8 „Karty praw podstawowych”); dane mogą być wykorzystywane wyłącznie do legalnych celów, do których były gromadzone (artykuł 6.1. Dyrektywy); należy respektować zasadę współmierności oraz minimalnej ingerencji w przetwarzanie danych oraz nakaz rzetelności i wykorzystania do zgodnych z prawem celów (artykuł 6 Dyrektywy); oraz że dane osobowe muszą być przetwarzane z uwzględnieniem środków bezpieczeństwa (artykuły 16 i 17 Dyrektywy). Wszystkie z powyższych wymogów są z kolei gwarantowane, jak wspomnieliśmy uprzednio, poprzez respektowanie prawa podmiotów danych do dostępu do swoich danych, ich poprawy, wykreślenia i wyrażenia sprzeciwu (artykuł 12 i następne Dyrektywy), które to uprawnienia stanowią niezbędne gwarancje podstawowego prawa do dysponowania swoimi własnymi danymi osobowymi, leżącego u samych podstaw systemu.

2. Zasada niezależnej kontroli

Europejska „Karta praw człowieka”, w duchu wspomnianych wcześniej dokumentów, czyni decydujący krok w stronę kolejnej z nieodzownych zasad ochrony danych: zasady niezależnej kontroli. Deklarując, że *„Przestrzeganie tych zasad [dotyczących ochrony danych osobowych] podlega kontroli niezależnego organu”*, stwierdza tym samym, że istnienie takiego organu jest wymogiem koniecznym, aby można było mówić o wystarczającej gwarancji prawa do ochrony danych. Jeżeli odnośne uregulowania prawne nie przewidują istnienia takiego organu, nie mogą w żadnym razie zostać uznane za wystarczające. Właśnie dlatego fakt istnienia niezależnego organu kontrolnego¹⁷ był jedną z kluczowych kwestii przy decyzjach w sprawie odpowiedniej ochrony danych osobowych w krajach trzecich podejmowanych dotychczas przez Komisję Europejską.

Powyższe postanowienie europejskiej „Karty praw człowieka” nie jest nowe, chociaż przyznana mu w tym dokumencie ranga stanowi nowość. W punkcie 8 rezolucji 45/95 Zgromadzenia Ogólnego Narodów Zjednoczonych z 14 grudnia 1990 r., która ustanawia wytyczne w sprawie ochrony danych osobowych, stwierdza się, że: *„Ustawodawstwo każdego kraju powinno ustanawiać instytucję, która, zgodnie z zasadami krajowego systemu prawnego, powinna być odpowiedzialna za kontrolowanie przestrzegania zasad [ochrony danych osobowych] przedstawionych powyżej. Powinno się zagwarantować bezstronność tej instytucji, niezależność wobec osób lub instytucji odpowiedzialnych za przetwarzanie i pozyskiwanie danych oraz kompetencje techniczne.”* W preambule stwierdza się

¹⁷⁾ Decyzje te obejmują:
Decyzja Komisji z dnia 26 lipca 2000 r. na mocy Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii.
Decyzja Komisji z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani” oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA.
Decyzja Komisji z dnia 20 grudnia 2001 r. w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych.
Decyzja Komisji z dnia 30 czerwca 2003 r. w sprawie właściwej ochrony danych osobowych w Argentynie.
Decyzja Komisji z dnia 21 listopada 2003 r., w sprawie właściwej ochrony danych osobowych w Guernsey.
Decyzja Komisji z dnia 28 kwietnia 2004 r. w sprawie właściwej ochrony danych osobowych na Wyspie Man.
Decyzja Komisji z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych. Decyzja ta została zaskarżona przez Parlament Europejski przed ETS (Sprawa C-318/04). Rzecznik Generalny LÉGER opublikował swoje konkluzje (22 listopada 2005 r.), w których wniósł o unieważnienie decyzji.

ponadto, że: *„instytucje kontrolne, wykonujące w pełni niezależnie swoje funkcje, są elementem skutecznej ochrony jednostek w zakresie przetwarzania danych osobowych”*. W tym samym duchu artykuł 1.3 stanowi, że: *„Instytucje kontrolne powinny wykonywać swoje funkcje w pełni niezależnie”*, a punkt 4 tego samego artykułu dodaje, że: *„Powinna istnieć możliwość odwołania się przed sądem od decyzji instytucji kontrolujących, które są przedmiotem skargi”*. Artykuł 28.1 Dyrektywy 95/46/WE stwierdza ponadto jasno, że *„Każde Państwo Członkowskie zapewnia, że jeden lub kilka organów publicznych będzie odpowiedzialnych za kontrolę stosowania na jego terytorium postanowień przyjętych przez Państwa Członkowskie na podstawie niniejszej Dyrektywy. Organy te będą postępować w sposób całkowicie niezależny wykonując powierzone im funkcje.”*

Podsumowując, zasada ochrony danych osobowych przez niezależną instytucję kontrolującą została już utrwalona jako jedna z najważniejszych zasad prawa do ochrony danych osobowych.

Również hiszpański Trybunał Konstytucyjny wypowiedział się bardzo jasno i jednoznacznie w sprawie roli hiszpańskiej Agencji Ochrony Danych Osobowych w systemie gwarancji chroniących podstawowe prawo do ochrony danych osobowych. Wspomniany wyrok nr 290/2000 z 30 listopada podkreśla znaczenie niezależnej instytucji kontrolującej w systemie ochrony danych osobowych. Trybunał Konstytucyjny stwierdził, że: *„W odniesieniu do (...) Agencji Ochrony Danych Osobowych (...) należy zauważyć, że, po pierwsze, wszystkie regulacje prawne przyjęte przez różne kraje członkowskie Unii Europejskiej w celu ochrony danych osobowych przed zagrożeniami związanymi z systemami informatycznymi, które zostały przyjęte przed wejściem w życie naszej Konstytucji (szwedzka ustawa z 11 maja 1973 r., zachodnioniemiecka ustawa z 22 stycznia 1977 r., francuska ustawa z 6 stycznia 1973 r., norweska ustawa z 8 czerwca 1978 r.) przewidują wprowadzenie elementu instytucjonalnej kontroli. Niezależnie od zróżnicowania nazw i form organizacyjnych, które wprowadzają te ustawy, wszystkie one tworzą wyspecjalizowane instytucje prawa publicznego, którym powierzają różne obowiązki kontrolne dotyczące plików z danymi osobowymi, poddawanych automatycznemu przetwarzaniu, zarówno przez instytucje publiczne, jak i podmioty prywatne.”* Trybunał zaznacza także, że hiszpańska agencja została ustanowiona jako *„instytucja prawa publicznego, której nadano zdolność prawną oraz zwierzchnictwo nad instytucjami publicznymi i podmiotami prywatnymi i która wykonuje swoje obowiązki działając w pełni niezależnie od administracji publicznej.”* Trybunał uzasadnił też nadanie Agencji Ochrony Danych Osobowych obowiązków i kompetencji, których wykonywanie ma *„zagwarantować, że restrykcje dotyczące wykorzystania systemów informatycznych, jak i gwarancje podstawowego prawa do ochrony danych osobowych będą przestrzegane w przypadku każdego pliku, niezależnie od tego, czy należy on do podmiotu publicznego czy prywatnego”*.

Wyrok w dalszej części stwierdza także, że: *„utworzenie wspomnianej wyżej instytucji prawa publicznego oraz powierzone jej obowiązki umożliwiają zagwarantowanie (...) korzystania przez wszystkich obywateli z uprawnień zawartych w tym podstawowym prawie”*. Dlatego Agencja Ochrony Danych Osobowych *„gwarantuje wykonywanie przez obywateli ich podstawowego prawa do ochrony danych”*. A biorąc pod uwagę *„że celem, który przyświeca działaniom Agencji Ochrony Danych Osobowych jest zagwarantowanie tych praw oraz praw ustanawiających równość wszystkich Hiszpanów w korzystaniu z nich, musi ona wykonywać swoje obowiązki i kompetencje na całym obsza-*

rze kraju, wszędzie gdzie istnieją zautomatyzowane pliki zawierające dane osobowe, niezależnie od rodzaju podmiotów kontrolujących te pliki”.

Istnienie niezależnej instytucji kontrolującej stanowi więc wyraźnie integralną część systemu stojącego za podstawowym prawem do ochrony danych osobowych.

III. WYZWANIA I KONFLIKTY ZWIĄZANE Z PRAWEM DO OCHRONY DANYCH OSOBOWYCH

Należy koniecznie podkreślić, że przedmiotowe prawo, przewidujące respektowanie autentycznego i skutecznego uprawnienia podmiotów do dysponowania swoimi danymi osobowymi, wiąże się niemniej jednak z pewnymi wyzwaniami czy też konfliktami, o których nie należy zapominać. Można tu wyróżnić przede wszystkim następujące sprzeczności: ochrona danych osobowych przeciwko a) wolności wypowiedzi, b) transparentności i dostępowi do informacji, c) interesom gospodarczym i rozwojowi rynku oraz d) walce z terroryzmem i gwarancjom bezpieczeństwa publicznego.

Przede wszystkim, należy od razu i jednoznacznie stwierdzić, że nie istnieje sprzeczność pomiędzy wspomnianymi wyżej prawami lub okolicznościami a ochroną danych osobowych. Europejski Trybunał Sprawiedliwości zwrócił na to uwagę, między innymi, w swoim powszechnie znanym wyroku z 20 maja 2003 w sprawie *Rundfunk et al*, nr C-465/00, C-138/01 i C-139/01; oraz w nie mniej znanym wyroku z 6 listopada 2003 *Linqvist*, nr C-101/01¹⁸ dotyczącym wolności wypowiedzi. Jest dokładnie przeciwnie: tylko przestrzeganie fundamentalnego prawa wszystkich ludzi do ochrony danych osobowych tworzy odpowiednie ramy dla wolności wypowiedzi i prawa do dostępu do informacji, właściwego rozwoju rynku i skutecznej walki z terroryzmem.

Co więcej, nowe relacje powstające w wyniku rozwoju działalności ekonomicznej w coraz bardziej zglobalizowanym świecie wymagają brania pod uwagę nie tylko potrzeb rynku, ale także ochrony praw podstawowych, a w szczególności prawa do ochrony danych osobowych. Dlatego tak ważne jest zrozumienie podstawowego założenia, zgodne z którym ochrona danych osobowych nie jest w żadnym wypadku przeszkodą dla swobody rozwoju działalności gospodarczej, ale raczej jej uzupełnieniem, mającym gwarantować respektowanie praw obywateli. W tym celu należy szukać innowacyjnych i skutecznych rozwiązań, które uwzględniałyby zróżnicowanie interesów. Oczywiście przykładem są takie narzędzia, jak regulaminy korporacji, które gwarantują prawo do ochrony danych osobowych w ramach zglobalizowanej gospodarki.

Najbardziej konfliktowa sytuacja powstaje jednak w wyniku zderzenia ochrony danych osobowych i wymogów bezpieczeństwa, szczególnie w świetle brutalnych ataków terrorystycznych, które miały miejsce w Nowym Jorku, Madrycie i Londynie.

Nikt oczywiście nie kwestionuje niepodważalnego faktu, że w walce z terroryzmem należy sięgać po skuteczne środki. Równie nieodzowne jest jednak żądanie, aby dzia-

łania antyterrorystyczne były prowadzone z poszanowaniem podstawowych praw, w przeciwnym wypadku terroryści odniosą nad nami swoje pierwsze i najważniejsze zwycięstwo: będzie nim ograniczenie tych wolności i praw, które na nasze szczęście stanowią fundament zachodnich społeczeństw. Jednym z tych praw jest ochrona danych osobowych. Każde posunięcie wprowadzone w celu zwalczania terroryzmu i przejawów zorganizowanej przestępczości musi pozostawać w zgodzie z podstawową treścią tego prawa, na które składają się omówione wcześniej zasady.

Dla powyższych przyczyn w scenariuszu walki z terroryzmem potrzebny jest globalny model ochrony danych osobowych, model, który wyjaśniałby reguły gry na poziomie międzynarodowym i w którym Dyrektywa 95/46/WE o ochronie danych osobowych będzie oczywiście odgrywać kluczową rolę.

Mamy tutaj do czynienia z coraz bardziej powszechnym trendem. Podstawowe prawo do ochrony danych osobowych rozpowszechnia się obecnie na świecie w bezprecedensowym tempie. Można powiedzieć, że w warunkach globalizacji prawo to nabiera nieznanego do tej pory znaczenia, przy czym wyraźnie widoczny jest jego model europejski, nie tylko za sprawą oddziaływania Dyrektywy 95/46/WE, ale również dokumentów sporządzonych przez Grupę Roboczą Art. 29.¹⁹

Nie mogę w tej chwili poświęcić więcej uwagi czterem wielkim wyzwaniom, z którymi zmagają się obecnie ochrona danych osobowych. Chciałbym tylko podkreślić, że narzędziem, które może ogromnie pomóc w tych zmaganiach, jest umacnianie świadomości obywateli i kontrolerów danych (zarówno publicznych jak i prywatnych), co do znaczenia tego podstawowego prawa, które nie jest przecież takie nowe, i mocne akcentowanie jego wagi we współczesnych nowoczesnych społeczeństwach informacyjnych.

¹⁸⁾ Dokładniejsze omówienie tych wyroków można znaleźć w mojej przywoływanej już wcześniej pracy „*El derecho a la protección de datos de carácter personal en la jurisprudencia...*”, op. cit., strona 16 i następne.

¹⁹⁾ Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych ustanowiona w art. 29 Dyrektywy.

Biobanks and the Related Challenges

1. Introductory Remarks

The issue of biobanks and the related challenges is of key importance from a personal data protection viewpoint. The core issue has to do with striking the appropriate balance between the requirements of scientific and medical research and the need for stringent safeguards applying to citizens' privacy and the information concerning one's most intimate sphere.

These are the guiding lines of the following analysis, and they should be attached special importance in this context because scientific research – as aimed at fostering the knowledge required to treat and prevent a large number of diseases – and, on the other hand, the protection of privacy and personal data are values that are especially treasured in our societies.

In the wide gamut of biobanks there stand out those processing genetic data, which are peculiar in that they provide information that goes well beyond what is required to identify an individual.

The prejudice caused to an individual's most intimate sphere can be fully appreciated if one considers that the data extracted from the most diverse body parts (saliva, hair, skin, blood) allow to get information of a "predictive" nature as well. Since the genome is the link between different generations, the data concerning a given person provide information on all the members of the respective biological group – which raises the difficult as well as inescapable issue of deciding whose genetic data is being processed and who is actually empowered to control movement and use of the said information. Furthermore, the creation and use of biobanks all over the world might ultimately be shaped by exclusively economic exploitation criteria and go against the interests of patients and society. The unlawful processing of genetic data, where these data are not stored or disclosed appropriately and are held, for instance, by insurance companies or employers, might turn into a tool for causing severe discrimination, possibly affecting the individual's dignity and citizens' professional lives. Who would stipulate a life insurance policy with an applicant that is genetically liable to a given disease?

Therefore, the protection of personal data can be regarded in this sector as a fundamental precondition to ensure respect for the principles of equality and non-discrimination.

2. Biobanks: Recent Experience

Over the past few years, there have been rapid developments in scientific research with a significant increase in the number of biobanks, which are being set up – often

not only for research purposes – at an exponential pace all over Europe and in other continents.

One of the most recent cases has to do with Iceland, where a project is being tested to store genetic and medical information concerning a very high number of Icelanders (275,000 people over a 12-year period). Supporters of the project maintain that the database will provide valuable information for medical research by allowing the detection of new genes and therapies; collection of the information is said to comply with the international rules on data protection.

A project aimed at collecting and storing genetic and medical information on citizens, to be linked with life-style information, has also been started in England. The ultimate purpose of this collection, indeed of the study as a whole, consists in detecting the genes that increase an individual's susceptibility to certain diseases, in order to extract information that can allow researchers to develop better treatments and vaccines.

A project that has been submitted in the Netherlands would appear to raise more complex issues, as it goes beyond exclusively scientific research purposes. The project envisages a nationwide census to be started in January 2007: all the data concerning newborns in the Netherlands will be stored in an electronic database, where all the information on their subsequent lives will be also gathered. Each newborn will be assigned a "serial number", the so-called Citizens Service Number; information on their education, health, family and social relationships – including any problems of a judicial nature, from police reports to judicial orders and measures – will be collected and fed into the database. This initiative has been presented as a measure to protect children, in order to "prevent society's lack of attention and indifference from turning today's children into tomorrow's criminals" (The Independent) and ensure that their adult lives will be safe and without problems. Each file will only be accessed by the persons responsible for the monitoring activities, who will have to point out situations raising alarm or concern and develop solutions that are suitable for each individual case – in particular, on the basis of the information gathered by the bodies participating in the project (social work organisations, schools, police, physicians, etc.).

Additionally, there is the veritable proliferation of practices and experiments that often go beyond national borders and entail, for instance, international transfers of tissue samples, DNA and genetic data, the importation and exportation of embryos, organs, etc. A number of highly sensitive data move freely in the absence of clear-cut, accurate rules. Because of this, in the attempt to meet the real, growing demand for internationally shared ethical criteria in this very delicate sector and thereby provide States with a reference framework within which to adopt their domestic policies, declarations and recommendations concerning bioethics have been adopted.

3. Regulatory Framework at International Level

At the international level, not many instruments deal specifically with biobanks; the existing instruments have affirmed general principles that are shared universally.

Reference can be made to UNESCO's instruments, in particular the Universal Declaration on the Human Genome and Human Rights of 1997, which was followed by the

International Declaration on Human Genetic Data of 2003 – where ethical principles were set out in respect of the collection, processing, storage and use of human genetic data contained in biological samples (blood, tissues, saliva, etc.). Finally, the Universal Declaration on Bioethics and Human Rights adopted in October 2005 should be mentioned. The Declaration addresses the ethical issues related to medicine, social sciences and technologies as applied to human beings, taking account of their social, legal and environmental dimensions. The aforementioned declarations, and in particular the latter one, are aimed at laying out a consistent framework of principles and procedures to guide Member States in adopting domestic policies, legislations and ethical codes. They all reaffirm the principle whereby human dignity and rights must be respected, as the interests and welfare of the individual should have priority over the sole interest of science.

The 2005 Universal Declaration acknowledges the importance of ensuring freedom of scientific research, which is a source of major benefits for mankind as it can increase life expectancy and improve the quality of life. To that end, all medical decisions and practices should be aimed at the welfare of the individuals concerned, minimising any possible harm to such individuals; discrimination and stigmatisation of individuals, families, groups or communities on whatever ground should be prohibited as resulting from genetic information. The Declaration affirms the need to respect the autonomy of individuals in making decisions concerning them. This is why principles are laid down – some of them are actually well-established principles – such as the need to obtain the individuals' free, informed and express consent in connection with scientific research and medical diagnosis and treatment, by affording specific protection to the individuals who are unable to provide their consent. It should be recalled that these principles are largely superimposable with those set forth in the European Convention for the Protection of Human Rights and the Dignity of Human Beings with regard to the applications of biology and medicine, as adopted in Oviedo in 1997.

4. The Situation in Italy

a) Genetic Data: The Work Done by the Italian Data Protection Authority

Although in Italy there have not been significant experiences in this field yet, the Italian Data Protection Authority has addressed issues related to genetics in the attempt to fill in the current regulatory blank. Within this framework, the Authority will draw up a General Authorisation that will apply – pursuant to Section 90 of the Code – to the whole genetics sector with particular regard to the protection of privacy. In a letter of 16 November 2005, the Italian Ministry of Health gave its favourable opinion on the draft Authorisation for the processing of genetic data submitted by the Garante, providing some amendments and additions were made as proposed by the Higher Council for Health Care.

The said Authorisation is aimed at laying down rules and limitations on the processing of genetic data. In particular, it is provided that the processing may only be allowed with the data subject's prior written consent – which may be withdrawn at any time – and after specifically informing the data subject on the purposes sought, the results of the research, and the rights afforded to him/her. To that end, any research using genetic data will have to be carried out on the basis of projects, in which the specific measures adopted to ensure that the data are processed appropriately should be set out also in terms of security measures. Specific obligations are laid down in respect of

the data retention period, which must not be longer than is absolutely necessary for the purposes for which the data were collected; the prohibition against dissemination of genetic data in non-aggregated format is also reaffirmed.

The attempt to regulate the processing of genetic data for research purposes is, therefore, being made by laying down specific rules. However, rules are not enough in this perspective, and there is another key issue to be addressed – namely, the actual role and the supervisory tasks committed to the Data Protection Authority. Indeed, this issue deserves more in-depth, general considerations.

b) More in General: Which Role for the DPA?

The role to be possibly played by the data protection authority in verifying and controlling the processing of genetic data is coming up as an issue to be addressed in Italy as well. Indeed, it has surfaced recently in connection with provisions concerning the fight against terrorism (Act no. 155/2005) – whereby spit samples may be taken coercively if it is impossible to identify an individual detained by the police. In the course of adopting the said measures, proposals were tabled (and subsequently withdrawn) that envisaged entrusting the Italian DPA with specific tasks in keeping the spit samples, or anyway with important tasks related to supervision over processing of these data after their inclusion in the ad-hoc database. It should be pointed out that no specific provisions have been set out so far as regards the mechanisms applying to processing of the data in question.

So far, poor attention has been paid to the question concerning who should control and by what means whether genetic data are really processed exclusively for the purposes for which they were made available; generally speaking, the focus has not been on the safeguards to be verified in concrete, after being laid down, as to the manner in which the research is carried out, the data are processed, and the information obtained in used. However, the issue of control becomes crucial exactly because the data at stake are sensitive and have to do with one's genome, i.e. the most valuable sphere of personal data. It is a multifaceted issue that has to be addressed. One wonders up to what point and in what manner this kind of control can be carried out by data protection authorities. What does it mean for such an authority to perform controls in a penetrating, pervasive manner? To what extent can these authorities also undertake to discharge management tasks, such as those related to the preservation of donors' identification data? To what extent should they be involved in direct managing of such databases?

Indeed, data protection authorities are called upon to play a role that often goes beyond their institutional functions, since the issues at stake are in some respects deeply related to social and ethical components even apart and beyond from the specific case made for genetic data.

In Italy, for instance, problems have arisen following promulgation of Act no. 40/2004 on medically assisted reproduction; they require careful consideration with a view to two main objectives, i.e. protecting the data subjects' confidentiality and ensuring respect for ethical principles.

By a decree of 7 October 2005, the Italian Ministry of Health set up, at the Istituto Superiore di Sanità, the national register including the list of private and public organi-

sations that were authorised by Regions and autonomous Provinces – under Sections 10 and 11(1) of Act no. 40/2004 – to apply medically assisted reproduction techniques, the embryos formed and the children born following application of the said techniques. The register should allow surveying all the entities and organisations in Italy in order to ensure transparency and publicity as regards both the medically assisted reproduction techniques adopted and the results achieved through such techniques. In addition to the data concerning the private and public organisations that apply medically assisted reproduction techniques – including their identification, description, technical features, facilities and organisational mechanisms – the register will include the data concerning the couples that have undergone assisted reproduction, the embryos formed and the children born following application of the said techniques.

The Italian Data Protection Code provides that the Garante's opinion must be obtained by the competent Ministry prior to issuing such decrees. In this case, the Garante issued a favourable opinion, however it pointed out that the register was only to contain data relating to the entities authorised to apply the said techniques insofar as those data were necessary for the survey. The data concerning the couples applying to the centres in question, the embryos formed and the children born thereafter may be collected, communicated and disseminated exclusively in anonymous format – including by way of aggregated data. At all events, the Garante reserved the right to assess the mechanisms for collecting and storing the data in the register, as well as for accessing and inspecting the said data.

As regards, more specifically, the broader ethical implications of this piece of legislation, it should be recalled that, upon adoption of Act no. 40/2004, an issue came up that had already been discussed during Parliamentary readings of the relevant bill – concerning the fate of cryopreserved embryos that are currently totally abandoned. Under Section 17(3) of the said Act, a distinction is to be drawn between cryopreserved embryos awaiting implantation and those that have been established to have been totally abandoned.¹ By a decree of 4 August 2004, the Italian Ministry of Health determined the nature of the said embryos as totally abandoned and ordered them to be transferred from the medically assisted reproduction centres to a National Biobank created on purpose.

The above decree actually provided for setting up a new entity, i.e. a Biobank of embryos located at the Centro trasfusionale e di immunologia dei trapianti of "Ospedale Maggiore" in Milan (which is an IRCSS, i.e. a Hospitalisation and Treatment Institute Pursuing Scientific Research Purposes). The Biobank is currently in operation and it is expected that about 400 "abandoned" embryos will be transferred to it, as established by a survey carried out by the Istituto Superiore di Sanità.

¹⁾ An embryo is considered to have been totally abandoned if any of the following conditions is fulfilled: a) the centre carrying out medically assisted reproduction interventions obtains, from either the parental couple or the single woman (as for the embryos produced prior to passing of the current legislation, by using donated sperm in the absence of a male partner), a waiver statement in writing concerning future implantation of cryopreserved embryos; b) the centre carrying out medically assisted reproduction interventions can document the repeated attempts made, for at least one year, to contact the couple/woman that had requested the embryos to be cryopreserved; only if it is proven that it was really impossible to get in touch with the couple/woman may the embryo be considered as totally abandoned.

Once again, the ethical and moral issues related to the fate of the said abandoned embryos – among the proposals put forward, reference can be made to the one coming from the National Bioethics Centre whereby all excess embryos should be adopted – are closely related to privacy-related legal issues concerning collection, storage and protection of the data held by this new entity. Additionally, it is to be recalled that security of the storage system must be ensured and the purposes for which the Biobank was set up must be respected.

5. The Role of Research Ethics Committees (RECs)

The case described above carries numberless ethical, legal and social implications; this is why it can spark some considerations on the relationship between data protection rules and the rules aimed at ensuring that scientific research is performed by respecting citizens' rights – which requires, by necessity, an in-depth analysis of the relationship between data protection authorities and the so-called Research Ethics Committees (RECs).

This is a difficult issue, and the difficulty is compounded by the fact that RECs carry out functions that are binding on researchers; they are required to lay down rules and provisions, they also are called upon to monitor and supervise. On the other hand, it is unquestioned that research activities entailing the processing of personal data must respect the fundamental principles in this sector, and supervision over compliance with such principles is committed, in principle, to the national data protection authorities. Hence, there is bound to be some measure of overlapping and interaction between the regulatory and supervision tasks discharged by RECs and those carried out by data protection authorities.

Committing all regulatory tasks to RECs, or else to DPAs, is not the right solution; indeed, their tasks, purposes and competences are different, and also the fundamental values they are required to safeguard, though mutually related, are ultimately different.

Still, there is a point to be made here, and a very important one as well. Again, the situation in other countries – starting from the Icelandic experience – clearly shows that this is the case. It is increasingly frequent that separate tasks are committed to RECs on the one hand, and DPAs on the other hand, whenever recommendations are to be issued in respect of genetic researches that entail the creation of biobanks.

Therefore, there is the urgent need to consider these issues, also in order to overcome the conceptual hurdles that continue to crop up in this area. For instance, Recital no. 2 in Directive 2002/20/EC of 4 April 2001, on the approximation of the laws, regulations and administrative provisions of the Member States concerning the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, reads as follows: "The clinical trial subject's protection is safeguarded through risk assessment based on the results of toxicological experiments prior to any clinical trial, screening by ethics committees and Member States' competent authorities, and rules on the protection of personal data". However, no adequate specification is provided on how to harmonize the activities of the various entities involved and, above all, the rules each of them is required to supervise and safeguard.

6. (Tentative) Conclusions

Technological and scientific developments in the human genetics sector and the increased opportunities for gathering all the genetic information on individuals in a single "big container" are leading to an upsurge of the economic, financial and commercial interests focusing on these very peculiar data.

This evolution requires researchers, political authorities and international decision-makers at Community and national level to devise new solutions to new problems – ultimately, to outline a new framework for the relationships between science, technology and society.

The application of biotechnologies to man and gene research are taking on major importance nowadays as they can contribute significantly to the welfare and health of individuals. The huge developments expected in the research for treatments applying to many diseases (including some rare diseases) will have to take place by keeping in mind the related public interests to ensure citizens' safety and confidentiality.

Biobanki i związane z nimi wyzwania

1. Uwagi wstępne

Z punktu widzenia ochrony danych osobowych kwestia biobanków i związanych z nią wyzwań ma ogromne znaczenie. Sedno sprawy polega na zachowaniu odpowiednich proporcji między wymaganiami badań naukowych i medycznych a koniecznością stosowania zabezpieczeń w dziedzinie prywatności obywateli oraz informacji dotyczących najbardziej intymnych sfer ich życia.

Są to przewodnie myśli analizy, którą przedstawię w moim wystąpieniu. W omawianym kontekście należy na nie zwrócić szczególną uwagę, ponieważ badania naukowe – mające na celu pogłębianie wiedzy niezbędnej do leczenia i zapobiegania wielu chorobom – a z drugiej strony ochrona prywatności i danych osobowych są wartościami szczególnie cenionymi w naszym społeczeństwie.

W szerokiej gamie biobanków zwracają uwagę te, które przetwarzają dane genetyczne. Mają one istotne znaczenie z tego względu, że dostarczają większej ilości informacji niż jest to wymagane do identyfikacji jednostki.

Naruszenie najbardziej intymnej sfery jednostki może zyskać określoną wartość, gdy dane otrzymane na podstawie oceny różnorodnych części ciała (śliny, włosów, skóry, krwi) umożliwią „przewidywanie” pewnych informacji. Ponieważ genom jest ogniwem łączącym różne pokolenia, dane dotyczące danej osoby dostarczą również informacji o wszystkich członkach danej grupy biologicznej – co rodzi trudne, ale też nieuniknione pytanie, czyje dane genetyczne są przetwarzane i kto właściwie jest uprawniony do kontrolowania obiegu i wykorzystywania wspomnianych informacji.

Ponadto proces tworzenia i korzystania z biobanków na całym świecie mógłby zostać ostatecznie ukształtowany wyłącznie przez kryteria ekonomiczne, skierowane przeciw-

ko interesom pacjentów i społeczeństwa. Nieprawne przetwarzanie danych genetycznych, kiedy dane te nie są właściwie przechowywane bądź ujawniane, a są w posiadaniu firm ubezpieczeniowych lub pracodawców, może przekształcić się w narzędzie ostrej dyskryminacji, uderzającej w godność człowieka i mającej wpływ na życie zawodowe obywateli. Kto bowiem przyznałby polisę ubezpieczeniową na życie osobie, która jest genetycznie podatna na daną chorobę?

Dlatego też można potraktować ochronę danych osobowych w tej dziedzinie jako podstawowy warunek konieczny do przestrzegania zasad równości i wyeliminowania elementów dyskryminacji.

2. Biobanki: ostatnie doświadczenia

W ciągu kilku ostatnich lat nastąpił gwałtowny rozwój badań naukowych, zwiększyła się także liczba biobanków, które powstają w bardzo szybkim tempie w całej Europie i na innych kontynentach, często nie tylko w celach badawczych.

Jeden z ostatnich projektów został zrealizowany w Islandii. Polega na przechowywaniu informacji genetycznych i medycznych dotyczących bardzo dużej liczby Islandczyków (dane odnoszące się do 275 tys. osób z okresu ponad 12 lat). Zwolennicy projektu utrzymują, że baza danych dostarczy cennych informacji do badań naukowych, gdyż umożliwi odkrycie nowych genów i metod leczenia; zbieranie informacji jest uważane za zgodne z międzynarodowymi regulacjami dotyczącymi ochrony danych.

Również w Anglii rozpoczęto projekt, którego celem jest gromadzenie i przechowywanie danych genetycznych i medycznych dotyczących obywateli, w tym informacji odnoszących się do stylu ich życia. Podstawowym celem zbierania tych danych, a w rzeczywistości całości badań jest odkrycie genów, które zwiększają podatność człowieka na pewne choroby, a następnie wykorzystanie uzyskanych informacji do opracowania lepszych metod leczenia i wynalezienia szczepionek.

Projekt przedłożony w Holandii wydaje się dotyczyć bardziej skomplikowanych spraw, gdyż wykracza poza wyłącznie naukowo-badawcze cele. Zakłada rozpoczęcie w styczniu 2007 roku ogólnokrajowego spisu ludności: wszystkie dane dotyczące noworodków w Holandii będą przechowywane w elektronicznej bazie danych, zbierane też tam będą informacje dotyczące ich późniejszego życia. Każdemu noworodkowi zostanie przydzielony „kolejny numer”, tzw. numer obywatela (Citizens Service Number); w bazie danych będą gromadzone informacje dotyczące wykształcenia, stanu zdrowia i rodziny oraz relacji i spraw społecznych, takich jak jakiegokolwiek problemy o charakterze prawnym, począwszy od raportów policyjnych do nakazów sądowych i zastosowanych środków. Inicjatywa ta ma być środkiem podjętym w celu ochrony dzieci, „zapobiegającym, by ze względu na brak zainteresowania i obojętność ze strony społeczeństwa dzieci nie zmieniły się w przyszłych przestępców” (The Independent) oraz zapewniającym, by ich dorosłe życie było bezpieczne i pozbawione problemów. Do każdego zbioru danych będą miały dostęp tylko osoby odpowiedzialne za ich monitorowanie. Zadaniem tych osób będzie wychwycenie niepokojących sytuacji oraz znalezienie rozwiązania odpowiedniego dla każdego przypadku – przede wszystkim na podstawie informacji zebranych przez komórki uczestniczące w projekcie (organizacje społeczne, szkoły, policja, lekarze itd.).

Ponadto można zauważyć rozpowszechnianie się praktyk i doświadczeń, które sięgają poza granice kraju, a dotyczą na przykład transferu próbek tkanki, DNA i danych genetycznych, przywożenia bądź wywożenia embrionów, organów itd. Z powodu braku przejrzystych, właściwych przepisów te szczególne dane są swobodnie przekazywane. Dlatego też, by sprostac rzeczywistości, zwiększającemu się zapotrzebowaniu na jednoznaczne międzynarodowe kryteria etyczne w tej niezwykle delikatnej dziedzinie życia oraz zapewnić państwom ramy regulacyjne stanowiące podstawę do prowadzenia przez nie wewnętrznej polityki w tej sferze, przyjęto określone deklaracje i rekomendacje.

3. Podstawy regulacyjne na szczeblu międzynarodowym

Niewiele instrumentów na szczeblu międzynarodowym odnosi się do kwestii biobanków; istniejące natomiast kierują się ogólnymi, powszechnie stosowanymi zasadami.

Można w tym miejscu nawiązać do instrumentów UNESCO, zwłaszcza „Powszechnej deklaracji w sprawie ludzkiego genomu i praw człowieka” („Universal Declaration on the Human Genome and Human Rights”) z 1997 roku oraz „Międzynarodowej deklaracji w sprawie danych genetycznych człowieka” („International Declaration on Human Genetic Data”) z 2003 roku, określającej zasady etyczne odnoszące się do zbierania, przetwarzania, gromadzenia i wykorzystywania ludzkich danych genetycznych zawartych w próbkach biologicznych (krwi, tkankach, ślinie itd.). W końcu należy wspomnieć o „Uniwersalnej deklaracji w sprawie bioetyki i praw człowieka” („The Universal Declaration on Bioethics and Human Rights”) przyjętej w październiku 2005 roku. Deklaracja ta zajmuje się sprawami etycznymi związanymi z medycyną, naukami społecznymi i technologią z uwzględnieniem społecznych, prawnych i środowiskowych aspektów. Wymienione wcześniej deklaracje, a zwłaszcza ostatnia, mają na celu przedstawienie spójnych zasad i procedur, które mają być wytycznymi dla Państw Członkowskich w prowadzeniu krajowej polityki w tym zakresie, w ujęciu legislacyjnym czy w odniesieniu do reguł etycznych. Wszystkie potwierdzają przy tym zasadę, że należy szanować ludzką godność i prawa, gdyż interesy i dobro jednostki powinny być priorytetem w stosunku do wyłącznych interesów nauki.

Deklaracja z 2005 roku uznaje znaczenie zapewnienia swobody w prowadzeniu badań naukowych, które przynoszą znaczące korzyści ludzkości, gdyż mogą zwiększyć średnią długość życia oraz poprawić jakość życia. Dlatego też podejmując wszelkie decyzje w sprawach praktyki medycznej, należy kierować się dobrem jednostek, potrzebą minimalizowania wszelkich możliwych krzywd wynikających z nich, a które mogą spotkać te jednostki; zabroniona powinna być także dyskryminacja i prześladowanie jednostek, rodzin, grup bądź społeczności na jakiegokolwiek podstawie w związku z informacjami uzyskanymi z danych genetycznych. Deklaracja potwierdza konieczność respektowania niezależności jednostek w podejmowaniu decyzji ich dotyczących. Dlatego ustanowiono zasady – niektóre z nich już funkcjonują – takie jak konieczność uzyskania od jednostki wyraźnej zgody na badania naukowe, diagnozowanie medyczne i leczenie, zapewniając szczególną ochronę tym, którzy nie mogą takowej zgody udzielić. Należy tu przypomnieć, że zasady te w dużym stopniu nakładają się na zasady zawarte w „Europejskiej konwencji ochrony praw człowieka i godności istoty ludzkiej wobec zastosowań biologii i medycyny”, przyjętej w Oviedo w 1997 roku.

4. Sytuacja we Włoszech

a) Dane genetyczne: praca zrealizowana przez Włoskie Organy Ochrony Danych

Mimo że Włochy nie mają znaczących doświadczeń w tej dziedzinie, włoski organ ochrony danych zajął się zagadnieniami związanymi z genetyką w celu uzupełnienia istniejącej luki w regulacjach prawnych. Organ ten nakreślił ogólne unormowania, które będą obejmować – zgodnie z paragrafem 90 kodeksu – cały sektor genetyki, ze szczególnym uwzględnieniem ochrony prywatności. W liście z 16 listopada 2005 roku Ministerstwo Zdrowia Włoch wyraziło swą przychylną opinię dotyczącą projektu „Upoważnienia do przetwarzania danych genetycznych”, przedłożonego przez Garante*, wprowadziło przy tym pewne poprawki i uzupełnienia zgodnie z sugestiami Wyższej Rady ds. Służby Zdrowia (Higher Council for Health Care).

Wspomniane upoważnienie ma za zadanie ustanowienie zasad i ograniczeń w dziedzinie przetwarzania danych genetycznych. W szczególności ustalono, że przetwarzanie danych może odbywać się tylko za wcześniejszą pisemną zgodą podmiotu, którego dane dotyczą – zgoda ta może być w każdej chwili cofnięta – podmiot musi być też szczególnie poinformowany o celu badań, ich wynikach oraz przysługujących mu prawach.

Dlatego każde badanie z wykorzystaniem danych genetycznych będzie musiało być przeprowadzone na podstawie projektów, w których powinny zostać ujęte środki służące zapewnieniu odpowiedniego przetwarzania danych również pod względem bezpieczeństwa. Przedstawiono także regulacje dotyczące okresu przechowywania danych, nie może on być dłuższy niż jest to konieczne dla celów, dla których dane były gromadzone; ponadto potwierdzono zakaz rozpowszechniania jakichkolwiek niepełnych danych genetycznych.

Podejmowane są zatem wysiłki mające na celu uregulowanie kwestii przetwarzania danych osobowych dla celów badawczych przez ustanawianie szczegółowych przepisów. Jednakże przepisy w tej sferze są niewystarczające, dlatego należy zająć się kolejną zasadniczą kwestią – mianowicie, właściwą rolą organu ochrony danych i jego zadaniami związanymi z nadzorowaniem działań w omawianej dziedzinie. Zagadnienie to wymaga dogłębnego rozważenia.

b) Uogólniając: Jaką rolę ma pełnić organ ochrony danych (DPA)?

Rola, jaką odgrywałyby prawdopodobnie organy ochrony danych w procesie weryfikacji i kontrolowania przetwarzania danych, to kwestia, którą również należy zająć się we Włoszech. Pojawiła się ona niedawno w związku z regulacjami dotyczącymi walki z terroryzmem (ustawa nr 155/2005), zgodnie z którymi można pod przymusem pobrać próbki śliny, jeśli policja nie może ustalić tożsamości zatrzymanej osoby. W trakcie podejmowania omawianych kroków przedstawiono wnioski (a następnie je wycofano), które zakładały powierzenie organom ochrony danych szczególnych zadań związanych z przechowywaniem próbek śliny, czy też ważnych zadań nadzorowania przetwarzania tych danych po włączeniu ich do bazy danych tworzonej *ad hoc*. Należy podkreślić, że dotychczas nie zostały przyjęte żadne przepisy odnoszące się do mechanizmów stosowanych w przetwarzaniu omawianych danych.

* Włoski urząd ochrony danych, przyp. tłum.

Dotychczas niewiele uwagi poświęcono zagadnieniu, kto powinien kontrolować i w jaki sposób, czy dane genetyczne są w rzeczywistości przetwarzane wyłącznie w celach, dla których zostały udostępnione; ogólnie mówiąc, nie skupiano się na weryfikowaniu zabezpieczeń po ich ustanowieniu w odniesieniu do sposobu, w jaki badanie było przeprowadzane, dane przetwarzane, a informacje uzyskane. Kontrola jest jednak zasadniczą kwestią, albowiem dane, o których mowa, należące do kategorii danych szczególnie istotnych, dotyczą genomu, tzn. najcenniejszej sfery danych osobowych. Jest to wieloaspektowa sprawa, którą należy się zająć. Można się przy tym zastanowić, w jakim stopniu i w jaki sposób organy ochrony danych mogą przeprowadzać tę kontrolę. Co oznacza dla tych organów przeprowadzenie kontroli w bardzo wnikliwy sposób? Do jakiego stopnia organy te mogą podjąć się zadań związanych z zarządzaniem danymi, takimi jak zachowanie danych tożsamości dawcy? W jakim stopniu powinny być one bezpośrednio zaangażowane w zarządzanie takimi bazami danych?

W rzeczywistości organom ochrony danych jest przydzielana często rola, która wykracza poza ich funkcje instytucjonalne, gdyż zagadnienia, o których mowa, są pod pewnymi względami ściśle związane z czynnikami społecznymi i etycznymi, wybiegającymi poza specyficzne przypadki dotyczące danych genetycznych.

We Włoszech, na przykład, pojawiły się problemy wynikające z ogłoszenia ustawy nr 40/2004 dotyczącej prokreacji wspomaganą medycznie; należy rozpatrzyć tu dokładnie dwa główne cele, tj. zapewnienie poufności podmiotowi, którego dane dotyczą oraz zapewnienie respektowania zasad etycznych.

Mocą rozporządzenia z 7 października 2005 roku Ministerstwo Zdrowia Włoch utworzyło w Istituto Superiore di Sanità narodowy spis prywatnych i publicznych ośrodków upoważnionych przez władze regionów i autonomicznych prowincji – zgodnie z paragrafem 10 i 11(1) ustawy nr 40/2004 – do stosowania metod medycznego wspomaganie prokreacji, a także embrionów i dzieci narodzonych dzięki zastosowaniu tych technik. Spis ten powinien umożliwić dokonanie przeglądu wszystkich podmiotów i organizacji we Włoszech w celu zapewnienia przejrzystości w tej dziedzinie oraz poinformowania społeczeństwa zarówno o stosowanych technikach, jak i osiągniętych wynikach. Oprócz danych dotyczących prywatnych i publicznych ośrodków stosujących techniki medycznego wspierania prokreacji, takich jak: nazwa, opis, dane techniczne, urządzenia i struktury organizacyjne, rejestr ten będzie zawierał również dane dotyczące par, które poddały się tej metodzie prokreacji, a także embrionów i dzieci narodzonych w wyniku zastosowania tej metody.

Włoski kodeks odnoszący się do ochrony danych stanowi, że przed wydaniem takich rozporządzeń kompetentne ministerstwo musi zapoznać się z opinią Garante. W tym przypadku Garante wydało pozytywną opinię, jednak z zaznaczeniem, że spis powinien zawierać tylko dane ośrodków uprawnionych do stosowania wymienionych wcześniej technik w stopniu niezbędnym do dokonania oceny ich działalności. Dane par zwracających się do omawianych ośrodków, a także embrionów i narodzonych dzieci mogą być gromadzone, przekazywane i rozpowszechniane wyłącznie w formie anonimowej – w postaci pełnych danych. We wszystkich przypadkach Garante ma prawo ocenić mechanizmy zastosowane do gromadzenia i przechowywania danych w spisie, ma też prawo dostępu do tych danych i ich kontroli.

Jeśli chodzi o etyczne implikacje tego prawnego unormowania, należy przypomnieć, że podczas uchwalania ustawy nr 40/2004 pojawiła się kwestia, którą poruszono wcze-

śniej podczas czytania projektu ustawy w Parlamencie, a dotycząca losów zamrożonych embrionów, z których zrezygnowano. Zgodnie z paragrafem 17(3) wspomnianej ustawy należy rozróżnić embriony oczekujące na implantację oraz uznane za „pozostawione”¹ Rozporządzeniem z 4 sierpnia 2004 roku Ministerstwo Zdrowia Włoch określiło te embriony jako całkowicie „pozostawione” i nakazało przekazywanie ich z ośrodków zajmujących się prokreacją wspomaganą medycznie do Narodowego Biobanku utworzonego w tym celu.

Rozporządzenie to uwzględniło powstanie nowego podmiotu, tj. Biobanku embrionów mieszczącego się w Centro trasfusionale e di immunologia dei traioanti „Ospedale Maggiore” w Mediolanie (IRCSS, tj. Instytut Hospitalizacji i Leczenia do Celów Naukowo-Badawczych). Biobank już funkcjonuje i, według Istituto Superiore de Sanità, przewiduje się przekazanie do niego około 400 „pozostawionych” embrionów.

Jeszcze raz chciałbym zwrócić uwagę, że kwestie etyczne i moralne dotyczące losów omawianych embrionów – wśród przedstawionych propozycji należy wspomnieć o jednej, wysuniętej przez Narodowy Ośrodek Bioetyki (National Bioethics Centre), by wszystkie „nadliczbowe” embriony przekazać do adopcji – są ściśle związane ze regulacjami prawnymi dotyczącymi gromadzenia, przechowywania i ochrony danych będących w posiadaniu tego nowego podmiotu. Ponadto, należy zapewnić odpowiedni system bezpieczeństwa i przechowywania danych, muszą być także respektowane cele, dla których Biobank został powołany.

5. Rola komisji etyki badań (RECs)

Opisywany przypadek zawiera liczne etyczne, prawne i społeczne implikacje. Dlatego też mogą pojawić się pytania o zależność między przepisami dotyczącymi ochrony danych a przepisami mającymi na celu zapewnienie, że podczas przeprowadzania badań naukowych są przestrzegane prawa obywateli – konieczna jest więc zatem głęboka analiza relacji między organami ds. ochrony danych i tzw. komisjami etyki badań (Research Ethics Committees).

Jest to trudna kwestia, a trudność tę potęguje jeszcze fakt, że komisje te pełnią funkcje wiążące także dla naukowców. Wymaga się od nich ustanawiania przepisów, jak również monitorowania i nadzorowania. Z drugiej jednak strony, jest rzeczą bezsporną, że podczas przeprowadzania badań naukowych związanych z przetwarzaniem danych osobowych w tym sektorze muszą być przestrzegane fundamentalne zasady, a nadzór nad przestrzeganiem tych zasad sprawują, zazwyczaj, krajowe organy ochrony danych.

W związku z tym zadania regulacyjne i nadzorcze wykonywane przez komisje do spraw etyki i organa ochrony danych w pewnym stopniu zazębiają się i wpływają na siebie nawzajem.

¹) Embrion uznaje się za całkowicie pozostawiony w następujących przypadkach:

a) ośrodek zajmujący się medycznie wspomaganą reprodukcją otrzymuje od rodziców bądź niezamężnej kobiety (dot. embrionów powstałych przed przyjęciem obecnej legislacji, w sytuacji korzystania z przekazanej spermy wobec braku partnera) pisemne oświadczenie, w którym zrzekają się z implantacji zamrożonych embrionów w przyszłości; b) ośrodek zajmujący się reprodukcją wspomaganą medycznie może udokumentować, że podjął wielokrotne próby, przez okres co najmniej roku, skontaktowania się z parą (kobietą), dla której zamrożony embrion był przeznaczony; tylko w przypadku, kiedy można udowodnić, że skontaktowanie się z parą (kobietą) było naprawdę niemożliwe, można uznać, że embrion został całkowicie pozostawiony.

Przydzielenie wszystkich zadań regulacyjnych jednemu bądź drugiemu organowi nie jest właściwym rozwiązaniem. W rzeczywistości ich zadania, cele i kompetencje są różne, także fundamentalne wartości, których mają strzec. Mimo że są wzajemnie powiązane, w rzeczywistości różnią się.

Należy poruszyć jeszcze jeden bardzo ważny aspekt.

Sytuacja w innych krajach – poczynając od doświadczeń Islandii – wyraźnie wskazuje, że należy zająć się tą sprawą. Coraz częściej, kiedy mają być wydane rekomendacje dotyczące badań genetycznych i związanych z tym biobanków, inne funkcje są przydzielane komisjom REC i organom ochrony danych (DPA).

Dlatego też w pilnym trybie należy rozpatrzyć te kwestie, aby pokonać przeszkody pojawiające się w tej dziedzinie. Na przykład punkt 2 Dyrektywy 2002/20/WE z 4 kwietnia 2001 roku, dotyczący ujednolicenia przepisów prawnych, regulacji oraz struktur administracyjnych w Państwach Członkowskich w celu implementacji dobrej praktyki klinicznej w przeprowadzaniu klinicznych testów produktów leczniczych dla użytku człowieka, ustanawia, co następuje: „Ochrona podmiotu poddanego testowi klinicznemu jest zapewniona przez ocenę ryzyka dokonaną przed testami klinicznymi na podstawie wyników eksperymentów toksykologicznych przeprowadzanych przed każdym testem klinicznym pod nadzorem komisji ds. etyki i kompetentnych organów Państw Członkowskich oraz przepisów dotyczących ochrony danych osobowych”. Jednak nie ma odpowiednich ustaleń określających, jak zharmonizować działania różnych podmiotów i przede wszystkim przepisy, które miałyby one stosować.

6. Wnioski

Rozwój techniki i nauki w dziedzinie genetyki oraz większe możliwości gromadzenia informacji genetycznych dotyczących osób w jednym „dużym pudle” są powodem zwiększającego się zainteresowania tymi szczególnymi danymi ze względów ekonomicznych, finansowych i komercyjnych.

Tendencja ta powoduje, że naukowcy, władze polityczne oraz organy międzynarodowe podejmujące decyzje na szczeblu Wspólnoty oraz na szczeblu krajowym muszą znajdować nowe rozwiązania nowych problemów – a w końcu nakreślić nowe ramy regulacyjne dotyczące relacji między nauką, technologią i społeczeństwem.

Zastosowanie biotechnologii w badaniach człowieka i genów jest obecnie sprawą zasadniczą, gdyż może mieć istotny wpływ na pomyślność i zdrowie jednostki. Przewidywany ogromny rozwój w dziedzinie metod leczenia wielu chorób (w tym rzadkich) będzie musiał uwzględniać interes publiczny w celu zapewnienia obywatelom bezpieczeństwa i poufności.

Prof. dr hab. Marek Safjan

Prezes Trybunału Konstytucyjnego, Polska
President of the Constitutional Tribunal, Poland

Katarzyna Berwid-Wilińska

Samodzielne stanowisko do spraw orzecznictwa - Trybunał Konstytucyjny, Polska
Independent Iuris prudence Assistant - Constitutional Tribunal, Poland

Prawo do prywatności osób publicznych¹

1. Uwagi wstępne

Problematyka związana z ochroną prywatności² budzi żywe zainteresowanie nie tylko w środowiskach prawniczych. We współczesnych społeczeństwach działają bowiem dwa przeciwstawne nurty – z jednej strony dążenie do błyskawicznego udostępnienia niemalże każdej informacji (czemu znakomicie sprzyja globalizacja mediów oraz rynku informacyjnego), z drugiej – dążenie do skrywania własnej prywatności za coraz wyższym murem „niedostępności”. Paradoks obecnej sytuacji sprowadza się do tego, że obie te wartości, będąc przeciwstawnymi, jednocześnie wzajemnie się wzmacniają. Im bowiem większy jest nacisk na swobodę przepływu wszelkiej informacji, tym większe jest pragnienie uchronienia się przed zewnętrznym wścibstwem. Konsekwencją tego stanu rzeczy jest więc nieuchronność nasilania się i zaostrzania konfliktów między prywatnością a przepływem informacji.

2. Osoby publiczne

Opozycja między chronioną sferą prywatności a sferą powszechnej dostępności jest szczególnie wyraźnie widoczna w obszarze związanym z działalnością osób publicznych. Jest bowiem oczywiste, że wszystko, co przekłada się na przestrzeń aktywności publicznej, jest objęte publicznym zainteresowaniem. Życie osoby publicznej nie staje się jednak, z racji pełnionej przez nią funkcji, w pełni transparentne i powszechnie dostępne. Co nie oznacza, że zakres dostępności do wiedzy o takiej osobie nie ulega znaczącemu poszerzeniu. Wydaje się, że w tej delikatnej materii konieczne jest unikanie wszelkich skrajności. Z tej też racji należy odrzucić skrajne poglądy: zarówno przekonanie o całkowitej dostępności sfery prywatności osób publicznych, jak i uznanie, że prywatność tych osób podlega takim samym ograniczeniom jak wszystkich innych (osób niepublicznych). Nie można więc

¹ Jest to istotnie zmieniona i zaktualizowana wersja artykułu opublikowanego w: „Prace z prawa prywatnego: Księga pamiątkowa ku czci sędziego Janusza Pietrzykowskiego”, red. Z. Banaszczyk, Warszawa 2000.

² Podstawowa literatura: Z. Bidziński, J. Serda, *Cywilnoprawna ochrona dóbr osobistych w praktyce sądowej*, [w:] *Dobra osobiste i ich ochrona w polskim prawie cywilnym*, pod red. J. St. Piątowskiego, Wrocław-Warszawa-Kraków 1986; A. Cisek, *Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym*, Wrocław 1989; A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego*, S.C., t. XX, 1972 oraz *Ochrona sfery życia prywatnego jednostki w świetle doktryny i orzecznictwa*, ZNUJ, z. 100, 1982; B. Kordasiewicz, *Jednostka wobec środków masowego przekazu*, Wrocław-Warszawa-Kraków 1991; K. Kubiński, *Ochrona życia prywatnego człowieka*, RPEiS 1993, z. 1; J. Panowicz-Lipska, *Majątkowa ochrona dóbr osobistych*, Warszawa 1975; J. St. Piątkowski, *Ewolucja ochrony dóbr osobistych*, [w:] *Tendencje rozwoju prawa cywilnego*, pod red. E. Łętowskiej, Wrocław 1983; St. Rudnicki, *Ochrona dóbr osobistych na podstawie art. 23 i 24 k.c. w orzecznictwie Sądu Najwyższego w latach 1985-1991*, Przegląd Sądowy 1992, nr 1; M. Safjan, *Prawo do ochrony życia prywatnego*, [w:] *Szkola Praw Człowieka*, Helsińska Fundacja Praw Człowieka, Warszawa 1998, t. 4; M. Sośniak, *Funkcje i skuteczność zgody osoby uprawnionej w zakresie ochrony dóbr osobistych*, [w:] *Prace z prawa cywilnego*, Wrocław-Warszawa 1985; A. Szpunar, *Ochrona dóbr osobistych*, Warszawa 1979.

zgodzić ze słynnym stwierdzeniem Lorda Gladstone'a, że „życie prywatne osób publicznych jest publiczne”.³ Można natomiast dopatrzeć się w tym ujęciu większej tolerancji dla wkraczania w sferę prywatności osób publicznych. Nie może to jednak oznaczać zamazywania konturów występujących tu sfer i relatywizowania używanych pojęć. Życie prywatne osoby publicznej nie staje się bowiem publiczne nawet wtedy, kiedy jest ono przedmiotem uzasadnionego zainteresowania. Może być natomiast przedmiotem węższej ochrony i uzasadnionego zainteresowania, *ergo* przedmiotem dopuszczalnej ingerencji.

Jeśli spojrzeć na problem chronionej prywatności z pewnej perspektywy porównawczej, biorąc pod uwagę kształtujące się współcześnie tendencje w tej dziedzinie, można zauważyć kilka wspólnych punktów, co do których istnieje zbieżność poszczególnych systemów prawnych:

- po pierwsze, uznaje się, że prawo do ochrony życia prywatnego musi być, co do zasady, respektowane również w odniesieniu do osób publicznych;
- po drugie, uznaje się, że w wypadku tych osób jest w znacznie szerszym zakresie usprawiedliwione wkraczanie w sferę prywatności, *ergo* obniża się próg niedostępności (co nie znaczy jednak, że prywatność tych osób zmienia swoją naturę i przekształca się w „*sphere publique*”);⁴
- po trzecie, w celu uzasadnienia wciśnięcia mediów poszukiwany jest związek między sferą działalności publicznej, a życiem prywatnym osoby.

Cała reszta zagadnień jest przedmiotem niekończących się kontrowersji, sporów i rozbieżności. Dotyczą one samego pojęcia i zakresu życia prywatnego, granic dopuszczalnej ingerencji w prywatność, sposobu rozumienia sfery aktywności publicznej, a więc i osób publicznych, wreszcie stosowanych sankcji i środków ochrony. Wyróżnić tu można bez wątpienia z jednej strony podejście anglosaskie (amerykańskie), które wyraźnie przyznaje – w odniesieniu do osób publicznych – pierwszeństwo wartościom związanym z prawem do informacji i wolnością wypowiedzi nad prawem do prywatności,⁵ z drugiej strony podejście prawa kontynentalnego, które zdaje się w sposób bardziej zrównoważony balansować pozostające w opozycji wartości.⁶

3. Orzecznictwo europejskie

W orzecznictwie Europejskiego Trybunału Praw Człowieka problematyka ochrony życia prywatnego osób publicznych pojawia się przede wszystkim na tle art. 8 „Konwencji o ochronie praw człowieka i podstawowych wolności”. ETPC dostrzega z całą wyrazistością zagadnienie związane ze zderzeniem się prawa do prywatności z prawem do informacji. Wartością szczególnie podkreślaną w orzecznictwie ETPC jest wolność debaty publicznej i transparentność funkcjonowania wszelkich instytucji publicznych w demokratycznym państwie. W konsekwencji, ujawnienie informacji ze sfery życia prywatnego osoby publicznej będzie usprawiedliwione w takim stopniu, w jakim jest konieczną przesłanką jawności życia publicznego. Jak stwierdził ETPC w orzeczeniu *Lingens przeciwko*

Austrii (orzeczenie z 8 lipca 1986 r., A. 103, par. 42) – osoby publiczne, a zwłaszcza politycy, muszą zaakceptować w stosunku do siebie znacznie szerszy, niż jest to możliwe wobec innych osób, zakres swobody wypowiedzi. Z istoty bowiem osoby te, podejmując się pełnienia funkcji publicznych, świadomie tym samym akceptują istnienie kontroli publicznej swych zachowań zarówno ze strony dziennikarzy, jak i całego społeczeństwa.

Jednocześnie jednak ETPC nie traci z pola widzenia wartości, jaką jest ochrona życia prywatnego. W tym kontekście należy wskazać na charakterystyczne orzeczenie w sprawie *von Hannover przeciwko Niemcom* (wyrok z 24 czerwca 2004 r., sygn. 59320/00), w którym podkreślono, że organy wymiaru sprawiedliwości RFN naruszyły art. 8 „Konwencji” nie zapewniając odpowiedniej ochrony prawa do prywatności skarżącej. Prezentacja faktów, odnoszących się np. do osób publicznych, w debacie publicznej, w społeczeństwie demokratycznym, musi być odróżniona od prezentacji faktów z życia prywatnego podmiotu, który takich funkcji nie pełni (pkt 63 uzasadnienia).

ETPC uznaje zarazem za możliwe rozszerzenie prawa opinii publicznej do uzyskiwania informacji ze sfery życia prywatnego osób publicznych, w tym polityków. O tendencji w kierunku poszerzania sfery dostępności świadczyć może m.in. orzeczenie z 18 maja 2004 r. w sprawie *Éditions Plon przeciwko Francji* (sygn. 58148/00, pkt 43 i n. uzasadnienia), które odnosiło się do publikacji wspomnień lekarza zmarłego prezydenta Republiki Francuskiej. ETPC w tej sprawie uznał bowiem, że władze francuskie, kształtując zakres swobody wypowiedzi w tego rodzaju sytuacjach, dysponują niewielkim zakresem swobody ze względu na konieczność realizacji takiej wartości, jak transparentność życia publicznego.

Warto też zauważyć, że na tle orzecznictwa ETPC pojęcie życia prywatnego jest rozumiane szeroko, w bezpośrednim nawiązaniu do definicji danych osobowych, zawartej w „Konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych” z 28 stycznia 1981 r. [zob. w szczególności uzasadnienie wyroku z 4 maja 2000 r. w sprawie *Rotaru przeciwko Rumunii* (sygn. 28341/95; pkt 43 uzasadnienia)].

4. Stanowisko według prawa polskiego⁷

Wymienione wyżej trzy elementy, charakteryzujące kwestię relacji prawa do ochrony prywatności i prawa do informacji w odniesieniu do osób publicznych, odnoszą się również do prawa polskiego.

⁷⁾ J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, pod red. A. Preisnera i B. Banaszaka, Warszawa 2000, s. 277 i n.; A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego*, Studia Cywilistyczne 1972, t. XX, s. 3 i n.; A. Kopff, *Ochrona życia prywatnego jednostki w świetle doktryny i orzecznictwa*, ZNUJ 1982, z. 100, s. 29 i n.; B. Kordasiewicz, *Jednostka wobec środków masowego przekazu*, Wrocław 1991; B. Kordasiewicz, *Cywilnoprawna ochrona prawa do prywatności*, Kwartalnik Prawa Prywatnego 200, z. 1, s. 19 i n.; B. Kordasiewicz, *Prawo do prywatności – aspekty cywilnoprawne*, [w:] *Prawo do prywatności aspekty cywilno-prawne*, pod red. K. Motyki, Lublin 2001, s. 47 i n.; K. Kubiński, *Ochrona życia prywatnego człowieka*, RPEiS 1993, z. 1, s. 62 i n.; M. Puwalski, *Prawo do prywatności osób publicznych*, Toruń 2003; M. Safjan, *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych*, Kwartalnik Prawa Prywatnego 2002, z. 1, s. 223 i n.; G. Sibiga, *Dostęp do informacji publicznej a prawo do prywatności jednostki i ochrony jej danych osobowych*, Samorząd Terytorialny 2003, nr 11, s. 5 i n.; J. Sieńczyło-Chlabisz, *Prawo do ochrony prywatności osób publicznych w orzecznictwie polskim i zagranicznym*, Glosa 2005, nr 1, s. 34 i n.; R. Stefanicki, *Cywilnoprawna ochrona prywatności osób podejmujących działalność publiczną*, Studia Prawnicze 2004, z. 1, s. 25 i n.; P. Sut, *Czy sfera intymności jest dobrem osobistym chronionym w prawie polskim*, Palestra 1995, z. 7-8, s. 49 i n.; P. Sut, *Ochrona sfery intymności w prawie polskim – uwagi de lege lata i de lege ferenda*, RPEiS 1994, nr 4, s. 104 i n.; M. Wild, *Ochrona prywatności w prawie cywilnym (koncepcja sfer a prawo podmiotowe)*, PiP 2001, s. 51 i n.; H. Zięba-Załucka, *Granice (nie tylko konstytucyjne) krytyki osób sprawujących funkcje publiczne*, Przegląd Sądowy 2005, nr 7-8, s. 3 i n.

³⁾ Cytat za P. Kayser, *La protection de la vie privée*, Aix - en -Provence, Paris 1990, s. 193.

⁴⁾ Niekiedy odmiennie, zob. P. Kayser, op. cit., s. 174; elementy należące do sfery dostępności są wyłączone ze sfery prywatności.

⁵⁾ Inaczej w tej kwestii B. Kordasiewicz, *Jednostka wobec środków masowego przekazu*, Wrocław-Warszawa-Kraków 1991, s. 217, którego zdaniem zakres sfery życia prywatnego jest zawsze uzależniony od istniejących okoliczności.

⁶⁾ P. Kayser, op. cit., s. 151 i n.

Punktem wyjścia powinno być jednak stwierdzenie, że prywatność jest wartością objętą bezpośrednią gwarancją konstytucyjną (art. 47 Konstytucji). Jest to istotne dla określenia konturów tego prawa na poziomie wszystkich regulacji gałęziowych (prawa cywilnego, karnego, administracyjnego). Ustalenie zakresu chronionej prywatności musi jednak uwzględniać inne normy konstytucyjne, które wyznaczać będą granice ochrony, a więc przede wszystkim art. 51 Konstytucji, wskazujący na możliwość istnienia ustawowego obowiązku udostępnienia informacji o sobie, art. 54 Konstytucji, zapewniający każdemu wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji, a także – szczególnie interesujący z punktu widzenia rozważanego zagadnienia art. 61 Konstytucji, gwarantujący obywatelowi prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Istnieje już więc z punktu widzenia samej Konstytucji konieczność zbalansowania wskazanych praw podstawowych. Żadne z nich nie ma bowiem charakteru absolutnego, każde też podlegać może ograniczeniom stosownie do przesłanek określonych w ramach zasady proporcjonalności (art. 31 ust. 3 Konstytucji).

Już na poziomie analizy konstytucyjnej pojawia się więc możliwość sformułowania następujących wniosków:

- po pierwsze, prawo do ochrony życia prywatnego nie jest podmiotowo ograniczone, a wobec tego również osoby publiczne są objęte jego zakresem. Sama dostępność do informacji o działalności osób pełniących funkcje publiczne (art. 61 Konstytucji) nie pozostaje w kolizji z ochroną prywatności jako takiej;
- po drugie, przy określaniu granic dopuszczalnej ingerencji w sferze prywatności – również wobec osób publicznych – muszą być brane pod uwagę enumeratywnie wskazane wartości, które w demokratycznym państwie prawnym uzasadniają ograniczenie tego prawa (bezpieczeństwo lub porządek publiczny, ochrona środowiska, zdrowia, moralności publicznej, wolności i prawa innych osób). Zawężenia chronionej sfery prywatności osób publicznych należy poszukiwać na gruncie naszego prawa w racjach związanych z prawem do otrzymywania informacji i swobodnego wyrażania poglądów.

Warto jednocześnie w tym miejscu zauważyć, że z natury rzeczy wkroczenie w sferę prywatności osoby publicznej nie powinno nigdy prowadzić do unicestwienia tego prawa, a więc naruszenia jego istoty. Na gruncie prawa polskiego dążenie do najbardziej nawet daleko posuniętej transparentności zasad życia publicznego nie może prowadzić do usuwania wszelkich barier niedostępności. W konsekwencji, nawet osoba publiczna może powoływać się na istnienie enklawy „prywatności”, która powinna być respektowana przez środki społecznego przekazu. Wynikają stąd również ważne kryteria w zakresie stosowania i wykładni prawa – już na poziomie regulacji prawa prasowego, cywilnego oraz karnego.

5. Orzecznictwo Trybunału Konstytucyjnego

Konstytucja nie definiuje pojęcia prywatności, a dobra i wartości wymienione w art. 47 Konstytucji obok prywatności, takie jak zwłaszcza życie rodzinne oraz decydowanie o swoim życiu osobistym, należą również do szeroko rozumianej sfery życia prywatnego. W pełni aktualne pozostaje więc stwierdzenie Andrzeja Kopffa sprzed 40 lat, odnoszone do cywilistycznego ujęcia dóbr osobistych w art. 23 i 24 k.c., że prywatność to dobro, które przecina się na wielu poziomach z innymi dobrami osobistymi człowieka. Nie jest celem tego opracowania podejmowanie próby rekonstrukcji definicji prywatności, która jest, jak wiadomo, przedmiotem obfitej literatury światowej, a przyjmo-

wane sposoby jej rozumienia są bardzo zróżnicowane. Można co najwyżej założyć, że istnieją pewne elementy prywatności, które stanowią – przy istniejących różnicowaniach w podejściu do tej kwestii – stały składnik prywatności od czasów, gdy sama koncepcja tego prawa została zarysowana w sławnym artykule Warrena i Brandeisa z końca XIX wieku.⁸ Do składników tych należy przede wszystkim prawo jednostki do samodzielnego wyznaczania sfery dostępności informacji o sobie w stosunku do innych podmiotów. Można to oczywiście ująć od strony negatywnej, co jest często czynione – akcentując prawo jednostki do określenia sfery niedostępności. Stąd zresztą pochodzi klasyczna formuła, syntetycznie określająca już w początkach rozwoju doktryny prywatności jej istotę jako „*right to be alone*”. Drugi zasadniczy składnik prywatności to wolność decydowania o swoim życiu osobistym i rodzinnym, swoiste prawo samostanowienia przysługujące każdej osobie. Obie te tradycyjnie wyróżniane sfery prywatności znajdowały swój wyraz w orzecznictwie konstytucyjnym.

Trybunał Konstytucyjny w swym dotychczasowym orzecznictwie zwracał wyraźnie uwagę na to, że ochrona życia prywatnego, o której stanowi art. 47 Konstytucji, obejmuje między innymi autonomię informacyjną, która oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, jak również prawo do kontrolowania tych informacji, jeżeli znajdują się w dyspozycji innych podmiotów (art. 51 Konstytucji).⁹ Szczególnie znaczący w tym kontekście jest wyrok TK z 20 listopada 2002 r., K 41 /02, dotyczący tzw. deklaracji majątkowej, w którym Trybunał uznał nie tylko, że informacje o majątku i sferze ekonomicznej jednostki mieszczą się w zakresie prywatności i autonomii informacyjnej, ale również – a może nawet przede wszystkim – że ochrona prywatności i autonomia informacyjna nie mają charakteru absolutnego i podlegają takim samym ograniczeniom, jak inne prawa i wolności konstytucyjne, między innymi ze względu na potrzeby życia w zbiorowości – tzw. aspekt „usprawiedliwionego” zainteresowania publicznego. Kluczowe znaczenie ma jednak zasada proporcjonalności. „Obowiązek ujawnienia informacji o sobie, stanowiąc ograniczenie autonomii informacyjnej, może być zatem dokonany tylko w ustawie (...) i tylko w granicach zgodnych z konstytucyjną zasadą proporcjonalności”. Prawo do ochrony prywatności ma bowiem szczególny charakter i rangę w systemie praw i wolności konstytucyjnych (zob. np. art. 233 ust. 1 Konstytucji – nawet w okresie stanu wojennego czy wyjątkowego ustawodawca nie może wprowadzić ograniczeń w zakresie tego prawa).

Dopuszczalności ingerowania w sferze autonomii, obejmującej stosunki rodzinne każdej osoby, dotyczył wyrok TK z 13 lipca 2004 r., K 20/03,¹⁰ którego przedmiotem była ocena zgodności z Konstytucją przepisów zobowiązujących funkcjonariuszy samorządowych do ujawniania informacji o sytuacji majątkowej członków rodziny. Zdaniem TK osoby te, ze względu na wagę informacji o funkcjonowaniu instytucji publicznych, „muszą się liczyć z obowiązkiem ujawnienia przynajmniej niektórych aspektów swego życia prywatnego”. Jakie są jednak granice owej przejrzystości w sytuacji, kiedy ujawniane informacje wkraczają w sferę prywatności nie tylko samego funkcjonariusza, ale także jego bliskich? TK stwierdził: „samo ujawnianie pokrewieństwa czy jego braku, w pewnych sytuacjach może naruszać prywatność zarówno funkcjonariusza, jak i osoby mu

⁸ Por. Warren S.D. Brandeis L.D., The Right to privacy, Harvard Law Review 1890, vol.4.

⁹ Zob. wyrok z 20 listopada 2002 r., K 41/02; OTK ZU nr 6A/2002, poz. 83, oraz wyrok z 19 lutego 2002 r., U 3/01; OTK ZU nr 1A/2002, poz. 3.

¹⁰ OTK ZU nr 7A/2004, poz. 63.

bliskiej (np. w przypadku dzieci pozamałżeńskich, przyrodniego rodzeństwa, wychowywania dziecka, którego funkcjonariusz nie jest rodzicem)”. Stopień ograniczenia prywatności zstępnych, wstępnych i rodzeństwa, wynikający z tak ujętego obowiązku, nie odpowiada więc w konsekwencji warunkom proporcjonalności. Odrębnie już jednak należy ocenić informacje odnoszące się małżonka.

W orzecznictwie Trybunału Konstytucyjnego odnoszącym się do ochrony prywatności, w zakresie szeroko rozumianej autonomii informacyjnej, szczególne miejsce zajmują rozstrzygnięcia dotyczące tzw. ustawy lustracyjnej, której celem było zapewnienie „przejrzystości” życiorysów osób podejmujących się określonych funkcji w organach władzy, a także w pewnych instytucjach zaufania publicznego (adwokatura). Ważąc argumenty przemawiające za i przeciwko dopuszczalności przyjętej formy lustracji, Trybunał Konstytucyjny uznał w wyroku z 21 października 1998 r., K 24/98¹¹ oceniane regulacje za zgodne z Konstytucją. Trybunał stwierdził przy tej okazji, że: „(...) osoba kandydująca do pełnienia funkcji publicznej godzić się musi z takim zainteresowaniem opinii publicznej, wyrażającym się między innymi wolą uzyskania jak najszerszego zakresu informacji o jej życiu (również prywatnym) i przeszłości. (...) Uznać należy, że sfera prywatności naruszana jest przez sam obowiązek złożenia oświadczenia lustracyjnego, jednakże znajduje to uzasadnienie w przyjętej przez racjonalnego ustawodawcę ogólnej koncepcji lustracji i jest bezpośrednią konsekwencją woli pełnienia funkcji publicznej. Wynikłe z samych założeń lustracji ograniczenie prawa do prywatności musi być uznane za konieczne w demokratycznym państwie prawa dla jego bezpieczeństwa, zatem za wyczerpujące przesłanki art. 31 ust. 3 Konstytucji RP. Żaden obywatel nie jest zobowiązany do ubiegania się, ani do pełnienia funkcji publicznej, zaś znając następstwa tego faktu w postaci upublicznienia pewnego zakresu informacji, należących do sfery prywatności, podejmuje on samodzielną i świadomą decyzję, opartą na rachunku pozytywnych i negatywnych konsekwencji, wkalkulowujących określone ograniczenia, oraz dyskomfort związany z ingerencją w życie prywatne”.

W kolejnym orzeczeniu dotyczącym przepisów ustawy lustracyjnej (wyrok z 5 marca 2003 r., K 7/01)¹² Trybunał zwrócił jednak uwagę na nowy element odnoszący się do formy i zakresu ujawnianych informacji o przeszłości osób poddanych lustracji. Uznając samą dopuszczalność ingerowania w sferę prywatności w związku z prowadzoną lustracją, podkreślił zarazem znaczenie, jakie może mieć – z punktu widzenia ochrony dóbr osobistych osób – ścisłość i precyzja informacji podlegających ujawnieniu (dotyczy to dodatkowych informacji o okresie pełnionej funkcji, rodzaju wykonywanych czynności, a także kategorii organów bezpieczeństwa, z którymi osoba współpracowała). Ostatecznie zbyt wąski zakres ujawnienia informacji Trybunał uznał za niezgodny z Konstytucją, zwłaszcza zaś z gwarancjami prawa do ochrony życia prywatnego. „Ujawnianie publicznie informacji niekompletnej, niezawierającej danych, które mogą mieć znaczenie dla danej osoby (choćby nawet było to przekonanie oparte na czysto subiektywnych przesłankach) może być bowiem porównane z niedopuszczalnym ujawnianiem informacji jako takiej i z tej racji stanowi naruszenie art. 47 Konstytucji (...) w konsekwencji trudno nie dostrzegać, że stopień ingerencji w sferze dóbr osobistych

jednostki, jej czci i dobrego imienia, jest w pewnym co najmniej stopniu uzależniony od sposobu ujawnienia charakteru jej aktywności”.

6. Pojęcie osoby pełniącej funkcje publiczne

Bezpośrednio zagadnieniem związanym z granicami ochrony życia prywatnego osób pełniących funkcje publiczne zajął się Trybunał Konstytucyjny w wyroku z 20 marca 2006 r. (K 17/05), uznając konstytucyjność art. 5 ust. 2 zd. 2 ustawy o dostępie do informacji publicznej.¹³ Przedmiotem analizy była regulacja ograniczająca prawo do ochrony prywatności osób pełniących funkcje publiczne w zakresie informacji mających związek z pełnieniem tych funkcji. Podstawowy problem konstytucyjny dotyczył oceny zakwestionowanej regulacji nie tylko z punktu widzenia ochrony prywatności – art. 47 Konstytucji, ale również przesłanek ograniczenia prawa do informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne – art. 61 ust. 3 Konstytucji i zasady proporcjonalności – art. 31 ust. 3 Konstytucji.

Trybunał Konstytucyjny uznał, że realizacja prawa do żądania informacji, o którym mowa w art. 61 Konstytucji, może dotyczyć nie tylko działalności publicznej osób pełniących funkcje publiczne, ale również sfery tzw. pogranicza czy też przenikania się ich życia publicznego i prywatnego. Trudno bowiem w praktyce jednoznacznie rozdzielić obie te sfery (dotyczy to np. dysponowania tzw. funduszem reprezentacyjnym, albo też prezentami otrzymanymi od innej osoby publicznej czy instytucji). Zawsze jednak, gdy realizacja prawa do informacji publicznej będzie wiązała się z wkroczeniem do sfery pośredniej, „tam ocena dopuszczalności ingerencji (...) powinna być dokonywana niezwykle ostrożnie i z wyważeniem racji, które mogłyby przemawiać za uznaniem priorytetu interesu publicznego, wyrażającego się w konstytucyjnej gwarancji prawa do informacji, w stosunku do ochrony prywatności”.

Zdaniem Trybunału Konstytucyjnego samo pojęcie „informacja dotycząca działalności organów władzy publicznej oraz osób pełniących funkcje publiczne” odnosi się również do informacji ze sfery życia prywatnego osób pełniących funkcje publiczne, o ile mają one związek z działalnością publiczną. Nie chodzi tu jednak o wszelkie informacje o osobie pełniącej funkcje publiczne, jakimi dysponuje dana instytucja publiczna. W opinii Trybunału „Niewątpliwie istnieją bowiem takie informacje (dane), które również w przypadku osób publicznych nie będą się mieścić w ramach zakresu przedmiotowego sfery prawa do informacji. Będą to np. co do zasady informacje dotyczące stanu zdrowia czy sfery intymności, w tym życia seksualnego”. Zakres dopuszczalnych informacji, należących do tzw. strefy przenikania się życia prywatnego i publicznego osób pełniących funkcje publiczne, powinien być ustalony przy uwzględnieniu następujących kryteriów: „Po pierwsze, informacje, których natura i charakter może naruszać interesy i prawa innych osób, nie mogą wykraczać poza niezbędność określoną potrzebą transparentności życia publicznego, ocenianą zgodnie ze standardami przyjętymi w demokratycznym państwie. Po drugie, nie mogą to być informacje – co do swej natury i zakresu – przekreślające sens (istotę) ochrony prawa do życia prywatnego. Po trzecie, muszą to być zawsze informacje mające znaczenie dla oceny funkcjonowania instytucji oraz osób pełniących funkcje publiczne”.

¹¹) OTK ZU nr 6/1998, poz. 97. O kontrowersyjności materii świadczy fakt, że wyrokiem w sprawach lustracyjnych towarzyszyły zawsze zdania odrębne (w tym wypadku jedno zdanie odrębne, w następnym zaś orzeczeniu dot. ustawy lustracyjnej K 39/97, OTK 1998, poz. 26, s. 491- 4 zdania odrębne).

¹²) OTK ZU nr 3/A/ 2003, poz. 19.

¹³) Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112, poz. 1198 ze zm.).

Trybunał Konstytucyjny podkreślił jednak, że nie jest możliwe precyzyjne i jednoznaczne określenie zarówno związku między życiem prywatnym a działalnością publiczną, jak i ustalenie okoliczności, które powodują, że daną osobę można uznać za pełniącą funkcję publiczną. Przede wszystkim nie należy mylić pojęć – „osoba publiczna” i „osoba pełniująca funkcje publiczne”. Pojęcia te nie są z całą pewnością równoznaczne, pierwsze z nich ma znacznie szerszy zakres i „obejmuje również osoby zajmujące w życiu publicznym istotną pozycję z punktu widzenia kształtowania postaw i opinii, wywołujące powszechne zainteresowanie ze względu na te lub inne dokonania, np. artystyczne, naukowe czy sportowe”. W przypadku osób pełniących funkcje publiczne chodzi nie tylko o osoby formalnie związane z daną instytucją publiczną, ale o takie, którym przysługuje choćby wąsko ujęty zakres kompetencji decyzyjnej. „Nie każdy zatem pracownik takiej instytucji będzie tym funkcjonariuszem, którego sfera chronionej prywatności może być zawężona z perspektywy uzasadnionego interesu osób trzecich, realizującego się w ramach prawa do informacji. Spod zakresu funkcji publicznej wykluczone są zatem takie stanowiska, choćby pełnione w ramach organów władzy publicznej, które mają charakter usługowy lub techniczny”.

Jeśli natomiast chodzi o związek informacji o życiu prywatnym osoby pełniącej funkcje publiczne z jej działalnością publiczną, to jego istnienie powinno być ustalane zawsze *in concreto*, pod kątem tego, czy dana informacja mogłaby mieć znaczenie dla oceny funkcjonowania danej instytucji publicznej. „Ten choćby pośredni wpływ zdarzeń ze sfery życia prywatnego na sferę publicznego funkcjonowania podmiotu stanowi usprawiedliwienie i uzasadnienie, jak również każdorazowy miernik dopuszczalnego zakresu ingerencji”.

Trybunał Konstytucyjny wyraźnie podkreślił, że zakresy przepisów normujących konstytucyjne prawo dostępu do informacji (art. 61) oraz wolność wyrażania poglądów, pozyskiwania i rozpowszechniania informacji (art. 54) krzyżują się jedynie częściowo, tj. wolność pozyskiwania i rozpowszechniania informacji jest ujęta szerzej niż prawo z art. 61 Konstytucji, które dotyczy jedynie pewnego „wycinka” prawa do pozyskiwania informacji. „Niektóre informacje istotne z punktu widzenia interesu społecznego, a dotyczące sfery życia prywatnego osoby publicznej, mogą być bowiem ujawnione także wtedy, kiedy nie pozostają w związku z pełnieniem funkcji, ale mają znaczenie dla oceny zachowań danej osoby, jej wiarygodności i prezentowanych publicznie poglądów”.

Zdaniem Trybunału Konstytucyjnego kwestionowanej regulacji ustawy o dostępie do informacji publicznej nie można utożsamiać z istniejącą na gruncie prawa prasowego. „Pojęcie działalności publicznej danej osoby jest szersze niż działalność związana z pełnieniem funkcji publicznej w strukturach organów władzy publicznej, której dotyczą informacje objęte prawem dostępu do informacji z art. 61 Konstytucji. Osobą publiczną w rozumieniu art. 14 ust. 6 prawa prasowego są również osoby niepełniące funkcji w strukturach władzy publicznej, ale których aktywność (np. artystyczna, naukowa, sportowa) wywołuje zrozumiałe zainteresowanie opinii publicznej”. Związek między informacją z zakresu życia prywatnego a działalnością publiczną jest mniej rygorystyczny, niż w przypadku osób pełniących funkcje publiczne. „W świetle art. 14 ust. 6 prawa prasowego wchodzi bowiem w grę informacja, które niekoniecznie mają bezpośredni związek z aktywnością publiczną, stanowią jednak istotną przesłankę oceny zachowań tych osób przejawianych w sferze publicznej (np. informacja o życiu rodzinnym polityka głoszącego określone, rygorystycznie ujęte zasady moralności zachowania w relacjach rodzinnych). Poziom, zakres dopuszczalnych informacji o sferze życia

prywatnego jest więc w tym przypadku wyznaczany przede wszystkim uzasadnionym interesem publicznym, który każdorazowo, stosownie do okoliczności, określać będzie głębokość ingerencji w sferę życia prywatnego”. Trybunał Konstytucyjny podkreślił, że regulacja art. 14 ust. 6 prawa prasowego jest przede wszystkim instrumentem realizacji wolności wypowiedzi prasowej. Natomiast celem kwestionowanego unormowania art. 5 ustawy o dostępie do informacji jest zapewnienie jawności funkcjonowania instytucji publicznych. „Nie każda informacja z zakresu życia prywatnego osoby publicznej, która może być opublikowana (w granicach wyznaczonych przez art. 14 ust. 6 prawa prasowego), jest zarazem objęta obowiązkiem udostępnienia przez instytucję publiczną, określonym w ustawie o dostępie do informacji publicznej”.

7. Prywatność osób publicznych na tle szczegółowych regulacji

Do niedawna jeszcze ochrona prywatności jako odrębnego dobra osobistego, o swym własnym, autonomicznym polu zastosowania była z pewnym trudem dedukowana z całości rozwiązań systemowych, związanych z ochroną dóbr osobistych.¹⁴ Dzisiaj prywatność urosła do dobrej rangi konstytucyjnej i stanowi przedmiot wyraźnych regulacji ustawowych, w szczególności w prawie prasowym oraz nowym kodeksie karnym. Okazuje się, że taki stan rzeczy może również wywoływać pewne trudności interpretacyjne, bo niezgodnione są pola i zakresy ochrony przyjęte w poszczególnych aktach normatywnych.

Kluczowe znaczenie ma dla omawianej problematyki regulacja zawarta w art. 14 ust. 6 prawa prasowego,¹⁵ która ma następujące brzmienie: „Nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby”.

Regulacja ta już na pierwszy rzut oka nie jest zsynchronizowana z przepisami prawa karnego, które zdają się strzec prywatności znacznie intensywniej i nie przewidują wyłączenia bezprawności działania sprawcy przestępstwa zniesławienia w sytuacji, gdy naruszona jest prywatność osoby publicznej, choćby nawet istniał bezpośredni związek pomiędzy działalnością publiczną tej osoby a ujawnionymi elementami życia prywatnego. Dowód prawdy co do postawionego zarzutu nie może być bowiem przeprowadzony w przypadku naruszenia prywatności za wyjątkiem sytuacji, gdy postawiony zarzut ma zapobiec niebezpieczeństwu dla życia lub zdrowia człowieka albo demoralizacji małoletniego (art. 213 § 2 k.k.).

Można w drodze racjonalnej wykładni systemowej podjąć próbę przyjęcia, że chronione pole prywatności objęte zakazem prawnokarnym w art. 212 k.k. nie odnosi się do tych sfer prywatności, które przepisami innych ustaw są wyłączone z ochrony. Ustawą taką jest przede wszystkim prawo prasowe (art. 14 ust. 6). Taki zabieg interpretacyjny nie jest jednak pewny, ponieważ zakłada, że informacje odnoszące się do życia prywatnego, jeśli wiążą się z aktywnością publiczną danej osoby, przechodzą do sfery powszechnej dostępności. Jest to założenie co najmniej dyskusyjne, a w konsekwencji kolizje między stosowaniem normy prawnokarnej a przepisem prawa prasowego wydają się być nieuchronne. Trybunał Konstytucyjny w cytowanym wyżej orzeczeniu w

¹⁴ Zob. zwłaszcza wypowiedź A. Kopffa, op. cit.

¹⁵ Ustawa z dnia 26 stycznia 1984 r. - prawo prasowe (Dz.U. Nr 5, poz. 24 ze zm.).

sprawie K 17/05 wskazuje na potrzebę uzgodnienia regulacji prawnych, obecnie nie-spójnych i wzajemnie niezsynchronizowanych. Obok przepisów prawa prasowego można również wymienić szereg innych szczegółowych regulacji ingerujących w sferę prywatności bez zgody osoby zainteresowanej: przepisy ustawy antykorupcyjnej¹⁶ pozwalające na ujawnienie (upublicznienie) wszystkich dochodów uzyskiwanych przez osoby publiczne, określone w tej ustawie (art. 10); przepisy ordynacji podatkowej¹⁷ pozwalające na dokonywanie ustaleń przy wykorzystaniu informacji objętych tajemnicą bankową – art. 82 § 2, art. 182-184; przepisy ustawy lustracyjnej¹⁸ w zakresie, w jakim dochodzi do upublicznienia faktu współpracy ze służbami bezpieczeństwa (art. 11, art. 28 oraz art. 40 ust. 3); przepisy ustawy o ochronie informacji niejawnych¹⁹ w zakresie, w jakim można uznać, że zgoda na zbieranie informacji służących wystawieniu tzw. certyfikatu bezpieczeństwa jest wyrażana jedynie pośrednio i obejmuje przeprowadzenie postępowania, a nie uzyskanie i ujawnienie konkretnej informacji – art. 31 i art. 32.

Wszystkie te szczegółowe regulacje upoważniające do ingerencji w prywatność zawężają pole ochrony i wyłączają zarzut bezprawności działania sprawczego – zarówno w płaszczyźnie prawa cywilnego, jak i karnego. Przepis prawa prasowego wskazujący na dopuszczalność wkraczania w sferę prywatności – o ile istnieje bezpośredni związek z działalnością publiczną danej osoby – stanowi bodaj najszerszy i zarazem najsłabiej sprecyzowany, biorąc pod uwagę ogólnikowość sformułowanych przesłanek – wyłom w obszarze poddany ochronie.

8. Orzecznictwo dotyczące ochrony prywatności osób publicznych

Orzecznictwo co najmniej od początku lat dziewięćdziesiątych przyjmuje zróżnicowane standardy ochrony prywatności w zależności od tego, czy zakres udostępnianej informacji dotyczy osoby publicznej czy też innego podmiotu. Zakres dopuszczalnej ingerencji w sferze prywatności osób publicznych jest ujmowany znacznie szerzej. Kontratypem bezprawności naruszenia jest w takim przypadku silnie podkreślany interes ogólny nakierowany na transparentność życia publicznego. Prywatność osób publicznych musi więc – w zderzeniu z wolnością wypowiedzi prasowej, której granice wyznacza m.in. art. 14 ust. 6 prawa prasowego – ulec ograniczeniu.²⁰ Poszerzenie sfery dostępności nie oznacza jednak wyłączenia ochrony sfery życia prywatnego. Wkroczenie w sferę prywatności osób publicznych musi być więc zawsze uzasadnione istotnymi racjami interesu publicznego, pozostawać w związku z wykonywaną działalnością publiczną.²¹

Istnienie związku między działalnością publiczną a życiem prywatnym, jest konieczną przesłanką uchylenia bezprawności udostępnienia informacji o życiu prywatnym osoby

publicznej.²² Nie jest możliwe ustalenie jednoznacznych i ogólnych kryteriów, które mogłyby się odnosić do wszystkich sytuacji. Z tej też racji, ocena będzie z natury rzeczy zależeć od okoliczności konkretnej sprawy.

9. Ingerencja w sferę prywatności dokonywana na podstawie art. 14 ust. 6 prawa prasowego

Rozwiązanie przejęte na gruncie art. 14 ust. 6 prawa prasowego realizuje postulat dostępu do informacji, które z racji swojego charakteru znajdują się w polu społecznego zainteresowania. Jednak założenia wyjściowe regulacji zawartej w art. 14 ust. 6 muszą być poszukiwane w znacznie szerszym kontekście normatywnym i mieć na uwadze, że:

- po pierwsze, ingerowania w sferę prywatności nie należy traktować jako reguły, ale raczej jako wyjątek, a osoby publiczne (bez względu na to, jak zostaną zdefiniowane w kontekście tego przepisu) korzystają również z ochrony życia prywatnego;
- po drugie, publikacja prasowa ujawniająca dane z życia prywatnego musi być uzasadniona rzeczywistym interesem społecznym (samo istnienie związku sfery życia prywatnego z działalnością publiczną nie jest jeszcze wystarczające; podanie informacji musi realizować określony, konkretny w danej sytuacji interes);
- po trzecie, nieprawdziwość ujawnionej informacji zawsze będzie się kwalifikowała jako podstawa do uznania danego działania za bezprawne (tu działa zawsze zobiektywizowana ochrona z art. 24 k.c.).²³

Dopiero spełnienie tych wyjściowych założeń umożliwia ustalenie przesłanek dopuszczalnej ingerencji w prywatność.

Kluczowe znaczenie ma niewątpliwie ustalenie kręgu podmiotów, które objęte są wyłączeniem ochrony swej prywatności z mocy art. 14 ust. 6 prawa prasowego. Jak już to wskazano wcześniej, nie jest uzasadnione stawianie znaku równości między „osobą publiczną” a osobą, która „prowadzi działalność publiczną” – potwierdza to orzeczenie TK w sprawie K 17/05. Są to więc osoby, których aktywność z racji wykonywanych obowiązków podlegać powinna kontroli publicznej – w tym też sensie ta kategoria osób zbliża się (choć – co należy podkreślić – nie jest tożsama) do pojęcia „osób pełniących funkcje publiczne” w rozumieniu art. 61 Konstytucji. Paradoksalnie do osób prowadzących działalność publiczną niekoniecznie zaliczymy te, które są publicznie znane. O ile z pewnością polityk z pierwszych stron gazet jest osobą prowadzącą działalność publiczną, to jest nią również mało znany sędzia z sądu okręgowego, który z racji pełnionych funkcji jest obdarzony społecznym zaufaniem (w takim znaczeniu, jak można sądzić, używał tego sformułowania Sąd Najwyższy

¹⁶ Ustawa z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz.U. Nr 106, poz. 679 ze zm.).

¹⁷ Ustawa z dnia 29 sierpnia 1997 r. - ordynacja podatkowa (Dz.U. Nr 137, poz. 926 ze zm.).

¹⁸ Ustawa z dnia 11 kwietnia 1997 r. o ujawnieniu pracy lub służby w organach bezpieczeństwa państwa lub współpracy z nimi w latach 1944-1990 osób pełniących funkcje publiczne (tj.: Dz. U. z 1999 r. Nr 42, poz. 428 ze zm.).

¹⁹ Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (tj. Dz. U. z 2005 r. Nr 196, poz. 1631).

²⁰ Por. np. orz. z 12 września 2001 r., V CKN 440/00, OSN 2002, nr 5, poz. 68 – dot. publikacji o zarobkach prezesa spółdzielni mieszkaniowej.

²¹ Por. wyrok SN z 11 października 2001 r., II CKN 559/99, OSN 2002, nr 6, poz. 82 – dot. ujawnienia informacji o życiu rodzinnym wicemarszałka Sejmu.

²² Por. np. węższe, bezpośrednie ujęcie tego związku w wyroku SN z 17 kwietnia 2002 r., IV CKN 925/00, OSP 2003, nr 5, poz. 60; szersze ujęcie w orz. SN z 6 marca 1991 r., I PR 469/90, OSP 1992, nr 5, poz. 117, w którym dopuszczalność szerszej ingerencji w sferę życia prywatnego odnosi się do zawodów związanych ze szczególnym stopniem społecznego zaufania; podobnie orz. SN z 7 czerwca 2001 r., III CKN 266/00, LEX nr 52377 – odnoszące się do szerokiego ujęcia pojęcia działalności publicznej.

²³ Zob. uchwałę (7) SN z 18 lutego 2005 r., III CZP 53/04 (OSNC 2005, nr 7-8, poz. 114), w której SN uznał, że: „Wykazanie przez dziennikarza, że przy zbieraniu i wykorzystywaniu materiałów prasowych działał w obronie społecznie uzasadnionego interesu oraz wypełnił obowiązek zachowania szczególnej staranności i rzetelności, uchyła bezprawność działania dziennikarza. Jeżeli zarzut okaże się nieprawdziwy, dziennikarz zobowiązany jest do jego odwołania”; oraz glosy krytyczne: J. Sieńczyło-Chłabczyk, PiP 2005, z. 7, s. 113 i n., Z. Radwańskiego, OSP 2005, z. 9, poz. 110 i P. Sobolewskiego, OSP 2005, z. 12, poz. 144, do których się przychylamy.

w znanym orzeczeniu z 6 marca 1992 r., sygn. I PR 469/90, OSP 1992, Nr 5, poz. 117;²⁴ podobnie kształtuje się np. orzecznictwo francuskie). Znany aktor, zabiegający o popularność, udzielający licznych wywiadów w mniej lub bardziej ambitnej prasie, jest oczywiście osobą publiczną. Jednakże dostępność do jego prywatności – nie wynika z tego, że prowadzi on działalność publiczną, która ze swej natury angażuje interes ogólny i powinna być jako taka monitorowana przez szerszą publiczność w różnorodnych jej aspektach, ale z tego, że w istocie, prowokując zainteresowanie mediów, wyraża zgodę, co najmniej w sposób dorozumiany, na naruszenie swojej prywatności (choć oczywiście należy uczynić zastrzeżenie, że z ową dorozumianą zgodą trzeba się także obchodzić ostrożnie i z wyczuciem – zabieganie o względy publiczności nie oznacza, że godzimy się na wszystko i na każdą formę reklamy; podać można liczne przykłady ujawniania intymnych informacji z życia rodzinnego szerszemu ogółowi). Oczywiście, dystynkcje między osobą publiczną w pierwszym i drugim znaczeniu nie zawsze będą łatwo uchwytne, jeśli zważyć, że prowadzenie działalności publicznej nie wyczerpuje się w formach instytucjonalnie przypisanych państwu czy ogólniej – władzy publicznej.

Równie trudne jest, bez wątpienia, określenie granic wdzierania się przez prasę (media) w sferę prywatności osoby publicznej. Regulacja prawa prasowego jest w tym względzie niejednoznaczna, dając jedynie ogólną wskazówkę, że mogą być ujawniane jedynie te fakty, które pozostają w bezpośrednim związku z działalnością publiczną danej osoby. Nie lekceważąc intuicji i zwyczaju dla kształtowania się tendencji w tej wrażliwej dziedzinie, podejmijmy próbę przyłożenia do tego sformułowania nieco bardziej precyzyjnych narzędzi jurydycznej wykładni, odwołując się do celu i funkcji przyjętej regulacji. Określa je, przypomnijmy, przede wszystkim szeroko rozumiany interes ogólny związany z prawem do informacji o wszystkim, co wywiera wpływ, ma znaczenie dla funkcjonowania mechanizmów życia publicznego. Nie mamy wątpliwości, że istnienie bezpośredniego związku powinno wskazywać na zależność między zachowaniem danej osoby w sferze publicznej aktywności a jej zachowaniami w sferze prywatnej, ale chyba nie o samo istnienie owej zależności tu chodzi. Nie każdy fakt ma jednak równą doniosłość i znaczenie, a opieranie się na samym istnieniu związku między prywatnością a sferą publiczną może być ryzykowne. Każda osoba jest jednością i łatwo udowodnić w większości przypadków, że tworzenie czyjegoś obrazu w pieleszach domowych może być interesującym przyczynkiem do charakterystyki tej osoby na innych polach jej aktywności. Zapewne obraz polityka leniwie spędzającego czas przed telewizorem w każdy weekend, będącego rygorystą wobec swych własnych dzieci, albo układającego namiętnie klocki lego w każdej wolnej chwili jest interesujący i może wyjaśniać niekiedy zachowanie tego polityka w sferze publicznej aktywności, ale zapewne nie taki jednak „związek” między prywatnością a sferą publicznej działalności usprawiedliwiałby ujawnienie tych faktów szerszej publiczności. Słusznie zauważa się bowiem w doktrynie nie tylko polskiej,²⁵ że uwzględnione być powinny takie fakty z dziedziny prywatności, których nieujawnienie byłoby dla interesu publicznego niekorzystne lub wręcz szkodliwe. Nie chodzi tu więc o zaspokajanie czystej ciekawości wobec osób publicznych, zawsze zrozumiałej, ale o fakty, które określają lub wyjaśniają bezpośrednio zachowania danej osoby w sferze aktywności publicznej. W literaturze wskazuje się obszary dostępności w odniesieniu do osób publicz-

nych, pomimo że należą one zarazem do życia prywatnego, m.in. stan finansowy, światopogląd czy przekonania polityczne, stan zdrowia etc. Wszystko jednak zależy od konkretnych okoliczności, rodzaju wykonywanej działalności. Wiedza o stanie zdrowia polityka z pierwszych stron gazet może mieć kluczowe znaczenie dla biegu spraw publicznych w państwie, i chociaż mamy tu do czynienia z bardzo wrażliwą sferą prywatności, jej udostępnienie jest zrozumiałe.²⁶ Przejrzystość stanu majątkowego i jawność wysokości płaconych podatków ze strony osób pełniących funkcje publiczne – należą już dzisiaj do kanonów życia publicznego.²⁷ Osoba publiczna musi też liczyć się niekiedy z tym, że jej prywatne wypowiedzi dotyczące określonych przekonań moralnych, światopoglądowych lub politycznych zostaną ujawnione (trudno byłoby np. zaprzeczyć, że dla wyborcy przyszłego posła lub senatora jest istotny stosunek kandydata na parlamentarzystę do kary śmierci, nad którą parlament będzie głosował). Dla opinii publicznej nie będzie też obojętne w pewnych sytuacjach ujawnienie informacji dotyczących życia rodzinnego polityka, który wzywając do szanowania wartości życia rodzinnego, sam umieścił swoje dzieci w placówkach opiekuńczo-wychowawczych. Zaufanie do wiarygodności wypowiedzi osoby publicznej, którą niekiedy ocenić można dopiero po ujawnieniu pewnych informacji z życia prywatnego, uzasadnia takie zainteresowanie i stwierdzenie bezpośredniego związku między obiema sferami aktywności.

Istnieje też w naszej tradycji przekonanie, że nieprzekraczalną barierę prywatności – również w odniesieniu do osób publicznych – stwarza sfera intymności życia. Pogląd ten uzyskał mocne oparcie w polskiej doktrynie prawa cywilnego, poczynawszy od znanych wypowiedzi prof. A. Kopffa, który – nawiązując do doktryny francuskiej – operował dla określenia tej sfery prywatności terminem „*la zone irreductible d'intimite*”. Pogląd ten wydaje się trafny co do samej zasady, chociaż i tu przecież natrafiamy niejednokrotnie na kontrowersje związane z pytaniem, gdzie przebiega granica intymności życia. Jak bowiem poucza doświadczenie może być ona różnie sytuowana. Co więcej, nie możemy przecież zapominać, że w pewnych sytuacjach prawo czyni wprost podstawę do ingerowania w sferę intymności życia, wtedy np. kiedy dopuszcza ustalanie więzi filiacyjnych, jeśli prowadzone jest postępowanie w sprawie o przestępstwa przeciwko obyczajności, czy wreszcie, kiedy zaangażowany jest interes związany z ochroną małoletnich przed demoralizacją oraz z ochroną życia i zdrowia człowieka. W tych ostatnich przypadkach ingerencja w prywatność jest zresztą wyraźnie dopuszczona przez przepisy prawa karnego (art. 213 § 2 k.k.). Przy poczynionych tu zastrzeżeniach nie można mieć jednak żadnych wątpliwości co do tego, że publikacje ujawniające fakty z życia intymnego osób publicznych będą wkraczały bezprawnie w chronioną prywatność tych osób.

10. Wnioski

Im bardziej doniosła jest aktywność danej osoby, tym większe muszą być ustępstwa na rzecz sfery dostępności, bo też i w takim przypadku obie sfery pokrywają się w znaczącym stopniu. I odwrotnie, im mniejsza jest skala działalności publicznej, tym większa musi być ostrożność w poszukiwaniu bezpośrednich związków między sferą prywatności a aktywnością publiczną.

²⁴) Teza wyroku SN z 6 III 1992 r.: 1. *Istnieją zawody, z którymi wiąże się szczególny stopień społecznego zaufania i dla pełnienia których niezbędne jest przestrzeganie szczególnych reguł godnego zachowania się, a zachowanie to może odnosić się również do sfery życia prywatnego i rodzinnego.*

²⁵) Por. P. Kayser. op. cit., s. 151 i n.

²⁶) Zob. P. Kayser, op. cit., s. 195.

²⁷) Zob. np. decyzję Rady Konstytucyjnej (Conseil Constitutionnel z 29 XII 1983 nr 83-164 DC JO 30 décembre 1983, p. 3874); zob. też orzeczenie SN cyt. przez B. Kordasiewicza, op. cit., na s. 217 – o dostępie do informacji o sytuacji majątkowej.

Nie należy bowiem tracić z pola widzenia faktu, że w sytuacji sądowego sporu, na dziennikarzu będzie spoczywał ciężar przeprowadzenia dowodu co do tego, że przekazane i upublicznione informacje należące do sfery prywatności, mają znaczenie dla opinii publicznej z powodów wyżej określonych. Obowiązuje tu bowiem w pełni zasada domniemania bezprawności zachowania sprawcy naruszenia dobra osobistego, której konsekwencją jest przerzucenie ciężaru dowodu na naruszającego to dobro (art. 24 k.c.).

Wydaje się, że najbardziej nawet abstrakcyjne i precyzyjne rozważania doktrynalne oraz podejmowane próby interpretacyjne nie zastąpią zwyczaju, wrażliwości i wycucia zarówno po stronie odbiorcy informacji, jak i jej nadawcy. Albowiem to nie prawnicy, ale opinia publiczna będzie określała, gdzie przebiega granica chronionej prywatności osób publicznych. Wrażliwość społeczeństwa i związane z tym poczucie tolerancji na informację, a także poczucie estetyki i dobrego smaku będą zatem powoli kształtować standard ochrony tego prawa.

The right to privacy of public figures¹

1. Introductory remarks

The problems of privacy protection² are of great interest not only in legal circles. Modern societies experience two opposite tendencies – one is to immediately publish nearly all information (which is perfectly supported by the globalisation of the media and the information market) and the other is to conceal one's privacy behind a still higher wall of "unavailability". The paradox of the current situation comes down to the fact that both these values, however contrasting they might be, at the same time

¹ This is a significantly altered and updated version of the article published in: „Prace z prawa prywatnego: Księga pamiątkowa ku czci sędziego Janusza Pietrzykowskiego” [“Works on private law; memorial book in honour of Judge Janusz Pietrzykowski”, ed. Z. Banaszczyk, Warsaw 2000.

² Basic bibliography: Z. Bidziński, J. Serda, *Cywilnoprawna ochrona dóbr osobistych w praktyce sądowej* [Civil law protection of personal interest in judicial practice] [in:] *Dobra osobiste i ich ochrona w polskim prawie cywilnym* [Personal interests and protection thereof in Polish civil law] ed. J. Svol. Piąkowski, Wrocław-Warsaw-Kraków 1986; A. Cisek, *Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym* [Personal interest and their non-property protection in the Civil Code] Wrocław 1989; A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego* [The idea of rights to intimacy and to privacy of personal life] S.C., vol. XX, 1972 and *Ochrona sfery życia prywatnego jednostki w świetle doktryny i orzecznictwa* [Protection of the private sphere of individuals in the view of doctrine and jurisprudence] ZNUJ, No. 100, 1982; B. Kordasiewicz, *Jednostka wobec środków masowego przekazu* [The individual in relation to mass media] Wrocław-Warsaw-Kraków 1991; K. Kubiński, *Ochrona życia prywatnego człowieka* [Protection of human private life] RPEiS 1993, No. 1; J. Panowicz-Lipska, *Majątkowa ochrona dóbr osobistych* [Property protection of personal interest] Warsaw 1975; J. Svol. Piąkowski, *Ewolucja ochrony dóbr osobistych* [The evolution of protection of personal interest] [in:] *Tendencje rozwoju prawa cywilnego* [Tendencies in the development of civil law] ed. E. Łętowska, Wrocław 1983; Svol. Rudnicki, *Ochrona dóbr osobistych na podstawie art. 23 i 24 k.c. w orzecznictwie Sądu Najwyższego w latach 1985-1991* [Protection of personal interests on the grounds of Art. 23, 24 Civil Code in the jurisprudence of Supreme Court between 1985-1991], Przegląd Sądowy 1992, nr 1; M. Safjan, *Prawo do ochrony życia prywatnego* [The right to privacy protection] [in:] *Szkoła Praw Człowieka* [A School of Human Rights] Helsinki Human Rights Foundation, Warsaw 1998, vol. 4; M. Sośniak, *Funkcje i skuteczność zgody osoby uprawnionej w zakresie ochrony dóbr osobistych* [The functions and effectiveness of consent of authorised individual in the protection of personal interest] [in:] *Prace z prawa cywilnego* [Works on civil law] Wrocław-Warsaw 1985; A. Szpunar, *Ochrona dóbr osobistych*, [Protection of personal interest] Warsaw 1979.

strengthen each other. The higher the pressure on free flow of any information, the greater the desire to protect oneself from external inquisitiveness. So, eventually, this situation leads to inevitable and aggravating conflicts between privacy and information flow.

2. Public figures

The contrast between the protected sphere of privacy and the sphere of public accessibility is particularly clearly presented in the area of the activity of public figures. It is obvious that everything that can be reflected in the sphere of public activity, lies in the scope of public interest. However, the life of public figures does not become fully transparent and generally accessible because of the function they perform. It does not mean that the scope of accessible knowledge about such person is not significantly broadened. It seems that in this sensitive matter any extremes should be avoided. This is why extreme points of view should be rejected, both the opinion that the private sphere of a public person should be completely accessible, and that their privacy is subject to the same limitations as that of all others (non-public figures). Hence, one cannot agree with the famous statement of Lord Gladstone that “the private life of public figures is public.”³ It is possible, though, to see this approach as more tolerant to intrusions into the private sphere of public figures. However, this cannot lead to blurring the borders of the spheres in question or to relativising of used terms. The private life of a public person does not become public, even if it is subject to justified interest. On the other hand, it might be subject to more narrow protection and to justified interest, *ergo* subject to acceptable intrusion.

If we look at the problem of protected privacy from a comparative perspective, taking into consideration the currently formed trends in this area, it is possible to notice several common points that specific legal systems agree upon:

- firstly, it is acknowledged that the right to protection of private life must be, as a rule, respected also in reference to public figures;
- secondly, it is acknowledged that in case of such individuals, intrusions into the private sphere are justified in a significantly wider extent, *ergo* the threshold of inaccessibility is lowered (which, however, does not imply that the privacy of these people changes its nature and transforms into “*sphere publique*”);⁴
- thirdly, in order to justify the inquisitiveness of the media a connection is sought between the sphere of public activity and the private life of the individual.

The remaining issues are subject to endless controversies, disputes and discrepancies. They refer to the very notion and scope of private life, the limits of acceptable intrusion into privacy, the understanding of the sphere of public activity, and therefore also of “public figures”, finally of applied sanctions and safeguards. Undoubtedly, two approaches can be distinguished here – on one hand the Anglo-Saxon (American) approach, that – in reference to public figures – gives clear priority to the values connected with the right to information and freedom of speech over the right to

³ Quotation: P. Kayser, *La protection de la vie privée*, Aix-en-Provence, Paris 1990, p. 193.

⁴ Sometimes differently, see P. Kayser, op. cit., p. 174; elements that belong to the accessible sphere are excluded from the private sphere.

privacy,⁵ on the other hand the continental legal approach, that seems to balance the contrasting values in a more temperate manner.⁶

3. European jurisprudence

In the jurisprudence of the European Court of Human Rights the problems of protecting private life of public figures appear mainly on the basis of Article 8 of the "Convention for Protection of Human Rights and Fundamental Freedoms". The ECHR clearly notices the issue connected with the clash between the right to privacy and the right to information. The value that is particularly emphasised in the jurisprudence of ECHR is the freedom of public debate and the transparency of functioning of all public institutions in a democratic state. As a result, disclosing information from the private life sphere of a public person will be justified to such extent, to which it is a necessary prerequisite for the transparency of public life. As ECHR judged in the case *Lingens vs. Austria* (sentence of 8 July 1986, A. 103, par. 42) – public figures, especially politicians, have to accept a broader scope of freedom of speech in reference to themselves, than it is possible to accept for other individuals. By definition, these people, when undertaking to perform public functions, accept with full awareness the existing public control of their behaviour, on the part of journalists as well as of the whole society.

At the same time, the value that is the protection of private life, does not drop out of sight of the ECHR. In this context the characteristic judgement in case *von Hannover vs. Germany* (sentence of 24 June 2004, No. 59320/00) must be recalled, where it is emphasised that the judicial institutions of Germany had violated Article 8 of the Convention by means of failing to ensure a proper protection of the applicant's right to privacy. Presentation of facts, that refer for example to public figures, in public debate, in a democratic society, must be distinguished from presentation of facts from the private life of a subject that does not perform such functions (point 63 of substantiation).

At the same time ECHR considers it possible to extend the right of public opinion to obtain information from the private sphere of public figures, including politicians. The evidence of the tendency towards extending the sphere of accessibility can be seen, among others, in the sentence of 18 May 2004 in the case *Éditions Plon vs. France* (No. 58148/00, point 43 and following substantiation), that referred to the publication of memoirs of the physician of the late President of French Republic. In this case, the ECHR recognised that in forming the scope of freedom of speech in such situations, French authorities have a limited extent of freedom, due to the necessity to execute the value of public life transparency.

It is worth mentioning, that in the context of jurisprudence of ECHR, the term "private life" is broadly understood in close reference to the definition of personal data, contained in the Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981. [see especially the substantiation of the sentence of 4 May 2000, in the case *Rotaru versus Romania* (No. 28341/95; point 43 of substantiation)].

⁵ A different view on that issue: B. Kordasiewicz, *Jednostka wobec środków masowego przekazu* [The individual in relation to mass media] Wrocław-Warsaw-Krakow 1991, p. 217, in whose opinion the scope of the private sphere is always dependent on existing circumstances.

⁶ P. Kayser, op. cit., p. 151 and following.

4. Position of Polish law⁷

The three above mentioned elements that characterise the issue of relations between the right to privacy protection and the right to information in reference to public figures, refer to Polish law as well.

The starting point should be the statement that privacy is a value guaranteed directly by the Constitution (Art. 47 of the Constitution). This is essential for determining the borders of this right on the levels of all branch regulations (civil, criminal and administration law). However, establishing a scope of protected privacy must take into account other constitutional norms that will set the limits for protection, in particular Article 51 of the Constitution, that points out the possible existence of a legal obligation to make information about oneself accessible, Article 54 of the Constitution, that grants to everybody the freedom to express their opinions and to obtain and broadcast information, and finally the article which is particularly interesting from the point of view of the question under discussion – Article 61 of the Constitution that grants citizens the right to obtain information about the activities of public authorities and of individuals that perform public functions. So, already in the point of view of the Constitution, there is a necessity to balance these fundamental rights. This is because none of them is of absolute nature, and each of them can be subject to limitations with respect to the prerequisites defined in the principle of proportionality (Art. 31 (3) of the Constitution).

Thus, already on the level of constitutional analysis, a possibility emerges to formulate the following conclusions:

- firstly, the right to protection of private life is not limited as for subject, and as such, its scope encompasses public figures, too. The accessibility of information

⁷ J. Braciak, *Prawo do prywatności* [The right to privacy] [in:] *Prawa i wolności obywatelskie w Konstytucji RP* [Citizens' rights and freedoms in the Constitution of the Republic of Poland] ed. A. Preisner and B. Banaszak, Warsaw 2000, p. 277 and following; A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego* [The idea of the right to privacy and intimacy of private life] *Studia Cywilistyczne* 1972, vol. XX, p. 3 and following; A. Kopff, *Ochrona życia prywatnego jednostki w świetle doktryny i orzecznictwa* [Protection of the private sphere of individuals in the view of doctrine and jurisprudence] *ZNUJ* 1982, No. 100, p. 29 and following; B. Kordasiewicz, *Jednostka wobec środków masowego przekazu* [The individual in relation to mass media] Wrocław 1991; B. Kordasiewicz, *Cywilnoprawna ochrona prawa do prywatności* [Civil law protection of the right to privacy] *Kwartalnik Prawa Prywatnego* 200, No. 1, p. 19 and following; B. Kordasiewicz, *Prawo do prywatności – aspekty cywilnoprawne* [The right to privacy – civil law aspects] [in:] *Prawo do prywatności aspekty cywilnoprawne* [The right to privacy – civil law aspects] ed. K. Motyka, Lublin 2001, p. 47 and following; K. Kubiński, *Ochrona życia prywatnego człowieka* [Protection of human private life] *RPEiS* 1993, No. 1, p. 62 and following; M. Puwalski, *Prawo do prywatności osób publicznych* [The right to privacy of public figures] Toruń 2003; M. Safjan, *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych* [Reflections upon the constitutional conditions for the development of personal interests protection] *Kwartalnik Prawa Prywatnego* 2002, No. 1, p. 223 and following; G. Sibiga, *Dostęp do informacji publicznej a prawo do prywatności jednostki i ochrony jej danych osobowych* [Access to public information and the individual's right to privacy and data protection] *Samorząd Terytorialny* 2003, No 11, p. 5 and following; J. Sieńczyło-Chłabisz, *Prawo do ochrony prywatności osób publicznych w orzecznictwie polskim i zagranicznym* [The right to protection of privacy of public figures in Polish and foreign jurisprudence] *Głosa* 2005, No 1, p. 34 and following; R. Stefanicki, *Cywilnoprawna ochrona prywatności osób podejmujących działalność publiczną* [Civil law protection of privacy of individuals who undertake public activity] *Studia Prawnicze* 2004, No. 1, p. 25 and following; P. Sut, *Czy sfera intymności jest dobrem osobistym chronionym w prawie polskim* [Is the sphere of intimacy a protected personal interest under Polish law?] *Palestra* 1995, No. 7-8, p. 49 and following; P. Sut, *Ochrona sfery intymności w prawie polskim – uwagi de lege lata i de lege ferenda* [The protection of the sphere of intimacy in Polish law – de lege lata and de lege ferenda] *RPEiS* 1994, No 4, p. 104 and following; M. Wild, *Ochrona prywatności w prawie cywilnym (konceptcja sfer a prawo podmiotowe)* [Privacy protection in the civil law (the idea of spheres and subject law)] *PIP* 2001, p. 51 and following; H. Zięba-Załucka, *Granice (nie tylko konstytucyjne) krytyki osób sprawujących funkcje publiczne* [Limitations (not only constitutional) of criticism towards individuals performing public functions] *Przegląd Sądowy* 2005, No 7-8, p. 3 and following.

- about the activities of individuals who perform public functions (Article 61 of the Constitution) does not remain in conflict with the protection of privacy as such;
- secondly, when determining the limits for acceptable intrusion in the private sphere – also for public figures – one has to take into consideration the enumeratively shown values that justify the limitations of this right in a democratic legal state (safety, public order, protection of the environment, health, public morality, freedoms and rights of other individuals). The limitations of the protected sphere of privacy of public figures can be found in our laws in the arguments connected with the right to obtaining information and free expression of opinions.

At the same time, it is worth mentioning here, that, naturally, the intrusion into the private sphere of a public figure should never lead to submergence of this right, and so to the violation of its essence. On the basis of Polish law, attempts at pursuing even the furthest transparency of principles of public life cannot lead to the removal of all inaccessibility barriers. In consequence, even a public figure can plead the existence of a “privacy enclave” that should be respected by public media. This results in important criteria for the application and interpretation of law – already on the level of regulations of press law, civil law and criminal law.

5. Jurisprudence of the Constitutional Tribunal

The Constitution does not define the notion of privacy, and the rights and values listed in Art. 47 of the Constitution apart from privacy, such as, in particular, family life and deciding about one’s personal life, also belong to the broadly understood sphere of private life. So, the declaration of Andrzej Kopff from 40 years ago, that refers to civil law interpretation of personal interests in Art. 23 and 24 of Civil Code, that privacy is a right that interferes on several levels with other human personal interests, still remains fully valid. This study does not aim at attempting to reconstruct a definition of privacy, which is, as it is well known, the topic of numerous publications throughout the world, and is understood in numerous varied accepted ways. At the most, it can be assumed that there are some elements of privacy, that have constituted – with the existing varied approaches to this issue – a constant element of privacy since the times when the very idea of this right was outlined in the famous article by Warren and Brandeis dated on the end of 19th century.⁸ These elements include, first of all, the right of individuals to determine the sphere of accessibility of information about themselves in relation to other subjects, on their own. Obviously, one could stress the negative aspect, as it is often practised, by emphasising the right of individuals to determine their sphere of inaccessibility. Here lies the origin of the classic formula, that has defined the essence of privacy since the origin of the doctrine of privacy, the “*right to be alone*”. Another essential element of privacy is the freedom to decide about one’s personal and family life, the specific right to self-determination that is granted to each individual. Both these traditionally distinguished spheres of privacy were expressed in constitutional jurisprudence.

The Constitutional Tribunal in its jurisprudence so far has clearly pointed out the fact that the protection of private life, as defined in Art. 47 of the Constitution, includes among others autonomy of information, which means the right to decide on one’s own

about disclosing to others information about oneself, as well as the right to control this information, if it is at the disposal of other bodies (Art. 51 of the Constitution).⁹ In this context, the sentence of CT of 20 November 2002 is particularly significant. The sentence referred to the so called property declaration, and the Tribunal acknowledged in it not only that the information about possessions and property of an individual belongs to the privacy sphere and to the autonomy of information, but also – or maybe even first of all – it stated that the protection of privacy and autonomy of information are not of absolute nature and are subject to the same limitations as other constitutional rights and freedoms, due to, among others, the needs of life in community – the so-called aspect of “justified” public interest. However, the key element here is the principle of proportionality: “The obligation to disclose information about oneself, that constitutes a limitation of autonomy of information, can be thus executed only by Act of Parliament (...) and only within the limits compliant with the constitutional principle of proportionality”. The right to privacy protection is of specific nature and position in the system of constitutional rights and freedoms (see e.g. Art. 233 (1) of the Constitution – even during martial law or state of emergency the legislator cannot introduce limitations to this right).

The acceptability of intrusions into the sphere of autonomy, that encompasses family relationships of each individual, was expressed in the sentence of CT dated 13 July 2004, K 20/03¹⁰, regarding the evaluation of compliance with the Constitution of the regulations that oblige the local authority members to disclose information about the property status of members of their families. According to CT, these people, due to the importance of information about functioning of public institutions, “must take into account the obligation to disclose at least some aspects of their private lives.” But what are the limits to such transparency in situations when such revealed information interferes not only with the privacy of the agents themselves but also with that of their relatives? CT stated that: “the sole disclosure of relationship, or absence of it, in some situations can violate the privacy both of the agent and that of his relative (e.g. in the case of children out of wedlock, step siblings, custody of a child of whom the agent is not a parent)”. The degree of limitation of the privacy of ascendants, descendants and siblings, that results from obligation interpreted in such manner, eventually does not comply with the conditions of proportionality. Although information related to spouses should be evaluated separately.

In the jurisprudence of the Constitutional Tribunal referring to protection of privacy, in the scope of widely understood autonomy of information, judgements related to the so-called vetting act occupy a separate place. The aim of this act was to ensure “transparency” of lives of individuals who undertake to perform certain functions in bodies of authority, as well as in some institutions of public trust (the Bar). Considering the arguments for and against the acceptability of the existing form of vetting, the Constitutional Tribunal declared, in the sentence dated 21 October 1998, K 24/98,¹¹ the regulations under evaluation compliant with the Constitution. The Tribunal stated that: “(...) candidates to perform public functions have to accept such form of interest of

⁹⁾ See sentence of 20 November 2002., K 41/02; OTK ZU No. 6A/2002, pos. 83, and sentence of 19 February 2002, U 3/01; OTK ZU No. 1A/2002, item 3.

¹⁰⁾ OTK ZU No. 7A/2004, item 63.

¹¹⁾ OTK ZU No. 6/1998, item. 97. the controversy of the issue is confirmed by the fact that sentences in cases related to vetting were always accompanied by separate votes (one separate vote in this case, in the next sentence on the Vetting Act K39/97, OTK 1998, item. 26, p. 491-4 separate votes).

⁸⁾ Cf. Warren S.D. Brandeis L.D., The Right to Privacy, Harvard Law Review 1890, vol. 4.

public opinion that is expressed, among others, by the will to obtain the broadest possible scope of information about their lives (also private) and past. (...) It should be acknowledged that the sphere of privacy is violated by the obligation to present a vetting statement itself, but it is justified by the general idea of vetting accepted by rational legislator and it is a direct consequence of the will to perform a public function. The limitation of the right to privacy that results from the core assumptions of vetting must be considered necessary in a democratic state of law for the sake of its safety, so we consider the prerequisites of Art 31 (3) of the Constitution of Republic of Poland exhaustive. No citizen is obliged to apply for, or to perform a public function, and knowing the consequences of this fact that mean publishing some range of information belonging to the sphere of privacy, the citizen takes a self-determined, conscious decision based on the balance of positive and negative consequences, that take into account certain limitations, and the discomfort connected with the intrusion into private life."

In a further judgement related to the regulations of the vetting act (sentence of 5 March 2003, K 7/01)¹² the Tribunal did, though, point to the new element that refers to the form and scope of revealed information about the past of individuals subject to the vetting. While acknowledging the acceptability of intrusion into the private sphere in connection with the course of vetting, at the same time it emphasised the significance of accuracy and precision of disclosed information (this refers to additional information about the period of performing function, the kind of activities, as well as the category of law enforcement agency that the person had cooperated with) from the point of view of protection of personal interests of these individuals. Finally, the Tribunal deemed that too narrow scope of disclosed information was non-compliant with the Constitution, in particular with the guarantees of the right to private life protection. "Public disclosure of incomplete information, that does not contain data that might be of importance for a given person (even if such belief is based only on subjective grounds), can be compared with unacceptable disclosure of information itself, and thus it constitutes a violation of Art. 47 of the Constitution (...), as a result it is difficult not to notice that the degree of intrusion in the sphere of personal interests of individuals, their honour and reputation, is at least to some extent dependent on the manner in which the character of their activity is disclosed".

6. The notion of individual performing public functions

In the sentence of 20 March 2006, (K 17/05), the Constitutional Tribunal considered directly the issue related to the limits of protection of private life of individuals performing public functions, acknowledging the compliance with Constitution of Art. 5 (2) sentence 2 of the Act on Access to Public Information.¹³ The subject of analysis was the regulation limiting the right to protection of privacy for individuals who perform public functions, in the aspect of information that remains in connection with performing these functions. The basic constitutional problem referred to evaluation of the regulation in question not only from the point of view of protecting privacy – Art. 47 of the Constitution – but also the prerequisites for limiting the right to information about the activity of public government authorities and of individuals performing public functions – Art. 61 (3) of the Constitution and the principle of proportionality – Art. 31 (3) of the Constitution.

The Constitutional Tribunal acknowledged that the execution of the right to demand information, as defined in Art. 61 of the Constitution, may refer not only to public activity of individuals who perform public functions, but also to the so called border sphere, or the sphere where their private and public lives interfere with each other. It is difficult to firmly separate these spheres (it might concern, for example, the use of the so-called entertainment allowance, or the use of gifts received from other public figure or institution). Always, wherever the execution of the right to public information is connected with intrusion into the border sphere, "there the evaluation of acceptability of the intrusion (...) should be done particularly carefully, weighing arguments that might speak for acknowledging the priority of public interest, expressed in the constitutional guaranteed right to information, in reference to privacy protection."

According to the Constitutional Tribunal, the notion "information referring to the activity of governmental authorities or individuals performing public functions" refers also to information that belongs to the sphere of private life of the individuals performing public functions, provided that they are connected with their public activity. However, this does not mean all information about a public figure, that a given public institution possesses. In the opinion of the Tribunal "There undoubtedly exist such information (data) that also in the case of public figures will not fit into the subjective scope of the sphere of the right to information. This will be, as a rule, information related to health status or the sphere of intimacy, including sexual life". The scope of acceptable information, belonging to the so-called border sphere of interference between private and public lives of individuals performing public functions, should be determined taking into account the following criteria: "Firstly, information whose nature and character might violate the rights and interests of other individuals, cannot exceed the necessity determined by the need for transparency of public life, evaluated in accordance with the standards accepted in a democratic state. Secondly, this must not be information, that – in its nature and scope – subverts the sense (essence) of the protection of the right to private life. Thirdly, this must always be information that is significant for the evaluation of functioning of institutions and of individuals performing public functions".

However, the Constitutional Tribunal pointed out that it is not possible to precisely and firmly determine either the relation between private life and public activity or to determine the circumstances that result in the possibility to consider a given individual as an individual performing public functions. First of all, it is crucial not to confuse the terms "public figure" and "individual performing public functions". Without doubt, these terms are not synonymous, the first one has a much wider scope and it "includes as well individuals who occupy a significant position in public life from the point of view of forming attitudes and opinions, or who arise general interest because of their achievements of any nature, such as artistic, scientific or sports achievements." In case of individuals performing public functions not only individuals in formal relation with a given public institution are considered, but also these who are accrued with even a narrow scope of decisive competences. "So, not each employee of such institution will be the agent, whose sphere of protected privacy can be limited due to justified interest of third parties that is executed within the right to information. Thus, the scope of public function excludes such jobs, even if performed within the framework of public authority institution, that are of service or technical nature".

¹²) OTK ZU No. 3/A/ 2003, item. 19.

¹³) The Act of 6 September 2001. on Access to Public Information (Journal of Laws No. 112, item 1198 amended).

As for the connection between the information about private life of individuals who perform public functions and their public activity, its existence should be always determined in concreto, taking into consideration whether a given information could be significant for the evaluation of the functioning of a given public institution. "Such, even indirect influence of events from the private sphere on the sphere of public functioning of a subject constitutes the justification and substantiation, as well as a measure of acceptable degree of intrusion at any time".

The Constitutional Tribunal has clearly emphasised that the scope of regulations that govern the constitutional right to access information (Art. 61) and the freedom of expressing opinions, obtaining and broadcasting information (Art. 54) interfere only partly, which means that the freedom to obtain and broadcast information is more widely defined than the right from Art. 61 of the Constitution that refers only to a certain "segment" of the right to obtain information. "Some information significant from the point of view of public interest, that refers to the sphere of private life of a public figure, can be disclosed even in cases when they are not in relation with performing the function, but they are relevant for the evaluation of the behaviour of the given individuals, their credibility and publicly expressed opinions".

According to the Constitutional Tribunal, the questioned regulation of the Act on Access to Public Information cannot be treated identically as that which already exists on the basis of press law. "The term public activity of a given individual is broader than the activity connected with performing public function in the structures of public authority institutions, that is referred to by the information included in the right to access information from Art. 61 of the Constitution. Public figures as determined in Art. 14 (6) of the press law are also individuals who do not perform functions in the structures of public authority, but whose activity (e.g. of artistic, scientific, sport nature) creates an understandable interest of the public opinion". The connection between information from the private sphere and public activity is less strict than in cases of individuals performing public functions. "Art. 14 (6) of the press law, takes into account information that does not have to be in close relation with public activity, but which constitutes an important basis for evaluation of the behaviour of these individuals expressed in the public sphere (e.g. the information about family life of a politician who propagates exact, strict moral principles of behaviour in the sphere of family). The level and degree of acceptable information about the private sphere is in such cases determined, first of all, by justified public interest, which at any time, with respect to the circumstances, will determine the degree of intrusion into the private sphere". The Constitutional Tribunal emphasised that the regulation of Art. 14 (6) of the press law is mainly an instrument to execute the freedom of speech in press, whereas the questioned regulation of Art. 5 of the Act on Access to Information aims at ensuring the transparency of functioning of public institutions. "Not every information from the private life of a public figure, that may be published (within the limitations determined in Art. 14 (6) of the press law), is also encompassed by the obligation to disclose information by public institution, as determined in the Act on Access to Public Information.

7. Privacy of public figures in the view of specific regulations

Until recently, the protection of privacy as a separate personal interest, of its own autonomous field of application, was deducted with some difficulty from the whole

framework of system solutions related to the protection of personal interests.¹⁴ Nowadays, privacy has been promoted to be a right of constitutional rank and it is subject to clear legislative regulations, especially in the press law and in the new criminal code. However, it seems that such status can also lead to certain problems of interpretation, as the fields and degrees of protection are not harmonised in the specific regulations.

The key to the matter in question is the regulation determined in Art. 14 (6) of the press law,¹⁵ which contains the following: "it is not allowed to publish without the consent of the person in question any information or data related to the private sphere of life, unless it is directly connected with the public activity of the given person".

It is clear at the first glance, that this regulation is not synchronised with the regulations of criminal law, which seem to protect privacy more intensely and which do not foresee the exclusion of unlawfulness of the perpetrator of defamation in the case when the privacy of a public figure is violated, even if there exists a direct connection between the public activity of the individual and the disclosed elements of private life. The evidence of truth for the posed charge cannot be conducted in the case of privacy violation, with the exception of situations when the charge is to prevent imminent danger for human life or health or the demoralisation of a minor (Art. 213 § 2 Criminal Code).

By means of rational system interpretation one could attempt to accept that the protected area of privacy included in the prohibition of criminal law in Art. 212 of the Criminal Code does not refer to these spheres of privacy that are excluded from protection by other regulations. Such other regulation is, first of all, the press law (Art. 14 (6)). Such method of interpretation is not certain, though, as it assumes that information referring to private life, if it is connected with the public activity of a given individual, moves to the sphere of general accessibility. Such assumption is at least debatable, and as a consequence, conflicts between the application of criminal law and the regulations of press law seem inevitable. The Constitutional Tribunal in the above-quoted sentence in case K 17/05 emphasises the need to harmonise legal regulations which are incompatible and not synchronised with each other at the moment. Apart from the regulations included in the press law, several other specific regulations can be distinguished that interfere with the private sphere without the consent of the person in question: the regulations of the Act against Corruption¹⁶ that allow to disclose (publish) all income gained by public figures, determined in this Act (Art. 10); regulations of the Taxation Law¹⁷ (that allow to use the information that is a bank secret – Art. 82 §2, Art. 182-184); the regulations of the Vetting Act¹⁸ in the scope in which the fact of cooperation with law enforcement agencies is published (Art. 11, Art. 28, and Art. 40 (3)); the regulations of the Act on the Protection of Confidential Information¹⁹ (to the extent to which one agrees that the consent to obtain information necessary for issuing the so-

¹⁴ See in particular the declaration of A. Kopff, op. cit.

¹⁵ The Act of 26 January 1984 – Press Law (Journal of Laws No. 5, item 24 amended).

¹⁶ Act of 21 August 1997 on limiting economic activity of individuals performing public functions (Journal of Laws No. 106, item 679 amended)

¹⁷ Act of 29 August 1997 – Taxation Law (Journal of Laws No. 137, item 926 amended).

¹⁸ Act of 11 April 1997 on the disclosure of work or service in law enforcement agencies or cooperation with such in the years 1944-1990 of individuals performing public functions (Journal of Laws of 1999 No. 42, item 428 amended).

¹⁹ Act of 22 January 1999 on the protection of confidential information (Journal of Laws of 2005 No. 196, item 1631).

called security certificate is expressed only indirectly and encompasses the due procedure, and not the obtaining and disclosing of a specific information – Art. 31 and 32).

All these specific regulations that give authorisation to interfere with privacy, narrow the area of protection and exclude the charge of unlawfulness of the perpetrating action, both on the levels of civil and criminal law. The regulation of the press law that points to the acceptability of intrusion into the private sphere if there is a direct connection with the public activity of a given individual – creates probably the widest and as well the least precise, as for the generality of formulated prerequisites – break in the area under protection.

8. Jurisprudence related to the protection of privacy of public figures

At least since the beginning of the 1990s the jurisprudence has recognised varied standards of privacy protection, depending on whether the scope of published information refers to a public figure or a different body. The scope of acceptable intrusion into privacy of public figures is defined more broadly. The countertype for unlawfulness of intrusion is here the strongly emphasised public interest focusing on the transparency of public life. The privacy of public figures thus has to – in clash with the freedom of press, whose limits are determined, among others in Art. 14 (6) of the press law – be subject to limitations.²⁰

The extension of the accessible sphere does not mean the exclusion of protection of the sphere of private life. The intrusion into the private sphere of public figures must be thus always justified by strong arguments of public interest, and to remain in connection with the performed public activity.²¹

The existence of a connection between public activity and private life is a necessary prerequisite for cancellation of the unlawfulness of publishing information about the private life of a public figure.²² It is not possible to determine firm and general criteria that could be applicable in all situations. So, the evaluation will naturally depend on the circumstances of a specific case.

9. Intrusion into the private sphere made on the basis of Art. 14 (6) of press law

The solution adopted on the basis of Art. 14 (6) of the press law executes the demand for access to information, whose nature places it in the scope of public interest. But the initial assumptions of Art. 14 (6) must be sought in a much wider normative context and take into account that:

Firstly, the intrusion into the private sphere cannot be treated as a rule, but rather as an exception, and public figures (regardless of how they are defined in the context of this regulation) also benefit from the protection of private life;

Secondly, a press publication that discloses facts from private life has to be justified by true public interest (the sole existence of a connection between the sphere of private life and public activity is not sufficient yet; the disclosure of information must fulfil a specific, concrete interest in a given situation);

Thirdly, the untruthfulness will always qualify as a basis for considering the given action as unlawful (here the objectified protection of Art. 24 of the Civil Code is always in force).²³

Only fulfilment of these initial assumptions enables to determine the prerequisites for acceptable intrusion into privacy.

The key factor here is to determine the circle of bodies that are included in the cancellation of privacy protection on the basis of Art. 14 (96) of the press law. As it was mentioned here above, it is not justified to treat identically a “public figure” and an individual who “performs public functions”, which is confirmed by the sentence of Constitutional Tribunal in the case K 17/05. So, the latter are individuals, whose activity should be subject to public control due to the nature of their function – in this aspect this category is near (but, what needs to be stressed, it is not identical with) the term “individuals performing public functions” as determined in Art. 61 of the Constitution. Paradoxically, individuals performing public functions will not always be those who are publicly well known. Whereas a top politician certainly is an individual who performs public functions, such individuals as a district court judge who enjoys public trust because of his function, belongs to the same category (or so it was understood, as it can be believed, by the Supreme Court in the famous sentence of 6 March 1992, ref. no. I PR 469/90, OSP 1992, No. 5, item 117;²⁴ and it is seen in a similar way by French jurisprudence). A famous actor, who strives for popularity and gives numerous interviews to tabloid or broadsheet press, of course is a public figure. However, as for the accessibility of his private sphere – this does not imply that he performs a public function, that of its nature involves public interest and as such should be monitored in its various aspects by wide audience, but, as he indeed provokes media interest and so expresses consent, at least presumable consent, for intrusion of his privacy (although it is obviously necessary to make the provision that such presumable content must be also treated carefully and tactfully – striving for public attention does not mean that one agrees to everything and to every form of advertising; numerous examples of disclosure of personal information about family life to the public could be given here). Obviously, the distinction between a public figure in the first and second meaning of the term is not always easily visible, if we take into consideration that performing public functions is not limited to forms institutionally associated with the state or general public authority.

²⁰ Cf. sentence of 12 September 2001, V CKN 440/00, OSN 2002, No. 5, item 68 – on publishing the earnings of the president of a tenants’ cooperative.

²¹ Cf. sentence of SC of 11 October 2001, II CKN 559/99, OSN 2002, No. 6, item 82 – on the disclosure of information related to family life of the speaker of the Parliament.

²² Cf. e.g. a narrower, more direct view of this connection in the sentence of SC of 17 April 2002, IV CKN 925/00, OSP 2003, No. 5, item 60; broader view in sentence of SC of 6 March 1991, I PR 469/90, OSP 1992, No. 5, pos. 117, in which the acceptability of a broader intrusion into private life sphere refers to jobs connected with a special degree of public trust; similarly sentence of SC of 7 June 2001, III CKN 266/00, LEX No. 52377 – that refers to the broad view of public activity.

²³ See Act (7) SC of 18 February 2005, III CZP 53/04 (OSNC 2005, No. 7-8, item 114), in which the SC stated that: „proving by the journalist that while collecting and using press materials he acted in defense of publicly justified interest and that he fulfilled the obligation to keep due care and diligence, cancels the unlawfulness of the journalist’s action. If the charge proves untrue, the journalist will be obliged to recall it”; and critical opinions: J. Sieńczyło-Chłabicz, PiP 2005, No. 7, p. 113 and following, Z. Radwański, OSP 2005, No. 9, item 110 and P. Sobolewski, OSP 2005, No. 12, pos. 144, which we support.

²⁴ Thesis of sentence of SC z 6 III 1992: 1. *There are jobs, which are connected with a specific degree of public trust and in order to perform them it is necessary to obey certain rules of proper behaviour, and that behaviour may also refer to the spheres of family and private life.*

Doubtlessly, it is equally difficult to determine the limits for intrusion of the press (media) into the private sphere of a public figure. The regulations of the press law are unclear in this aspect, they only give a general guideline that only these facts may be disclosed that remain in direct relation to the public activity of a given individual. Without underestimating the role of intuition and custom in shaping tendencies in this sensitive area, let us try to use some more accurate instruments of legal interpretations to this formula, referring to the aim and function of the adopted regulation. These are determined, as I would like to remind, first of all by the widely understood general interest related to the right to information about everything that influences or is significant for the mechanisms of functioning of public life. There is no doubt that the existence of a direct connection should point to the relation between the behaviour of a given individual in the sphere of public activity and his behaviour in the private sphere, but it is probably not only the existence of such dependence that is important here. Not all facts are of equal value and importance, and basing solely on the existing connection between privacy and the public sphere may be risky. Every individual is a whole, and it is easy to prove in most cases that creating the image of someone at their home can be an interesting supplement to the characteristics of this person in other areas of activity. Presumably, the image of a politician who spends his weekends lazily in front of the TV, who is a very strict parent to his children, or who passionately plays with LEGO building blocks in his free time, might be interesting and could sometimes explain the behaviour of this politician in his sphere of public activity, but probably it is not this kind of "connection" that would justify disclosing these facts to wider audience. It is rightly emphasised not only in Polish doctrine,²⁵ that such facts from the private sphere should be taken into account which, if not disclosed, would violate the public interest. So, the point is not to satisfy curiosity which is always understandable if directed towards public figures, but to show facts that determine or explain directly the actions of a given individual in the sphere of public activity. In literature some areas of accessibility are determined for public figures, although they also belong to the private sphere, such as financial status, outlook on life, political views, health status, etc. However everything depends on specific circumstances, the kind of function performed. The knowledge about the health of a top state politician could be crucial for the course of political affairs in the state, and, although we deal here with a very sensitive sphere of privacy, the publication of it is understandable.²⁶ Transparency of the financial status and openness of taxes paid by individuals who perform public functions, nowadays both belong to standards of public life.²⁷ Public figures also sometimes have to count with the fact that their private declarations referring to certain moral beliefs, outlooks or political views will be disclosed (it would be difficult to deny that the approach of a candidate for Member of Parliament towards, for example, capital punishment, is essential for his potential voters). Sometimes, it might make difference to the public opinion if information is disclosed about the private life of a politician, who, while urging to respect traditional family values, had himself placed his own children in foster homes. The trust in the credibility of a public figure, which can be sometimes evaluated only after disclosing certain information from the private sphere, justifies such interest and is a basis for acknowledging a direct connection between both spheres of activity.

²⁵) Cf. P. Kayser. *op cit.*, p. 151 and following.

²⁶) See P. Kayser, *op. cit.*, p. 195.

²⁷) See e.g. the decision of the Council of Constitution (Conseil Constitutionnel of 29 XII 1983 nr 83-164 DC JO 30 d(cembre 1983, p. 3874); see also the sentence of SC quoted by B. Kordasiewicz, *op. cit.*, p. 217 – on access to information in property situation.

There is also a belief that is present in our tradition, that the impassable limit of privacy – also in reference to public figures – is created by the sphere of intimacy of life. This view has received strong support in the Polish doctrine of civil law, since the famous declarations of Professor A. Kopff who, referring to the French doctrine, used the term "*la zone irréductible d'intimité*" to describe this sphere. This view seems right as for its core principle, although here also controversies emerge related to the question where lies the limit of life intimacy. As it is known from the experience, it can be placed differently. Moreover, one must not forget that in some situations, the law creates a direct basis for the intrusion into the sphere of intimacy, for example if it allows the establishing of filial relations in the course of proceeding in case of crime against morality, or finally if interest related to protection of minors from demoralisation or to protection of human life and health is involved. In these last cases intrusion into privacy is even clearly accepted by the regulations of criminal law (Art. 213 § 2 Criminal Code). However, with respect to the provisions made here, it is certainly doubtless that publications disclosing facts from the intimate life of public figures, will unlawfully intrude into the protected privacy of such figures.

10. Conclusion

The more significant the activity of a given individual, the greater concessions to the sphere of accessibility have to be made, as in such case both spheres overlap to a great extent. And, on the contrary, the smaller the scale of public activity, the more care is required while seeking direct connections between the private sphere and the public sphere.

One must not lose sight of the fact, that in the situation of court trial, it is the journalist who will have to prove that the transmitted and published information that belong to the private sphere, are significant for the public opinion due to reasons determined here above. The principle of presumed unlawfulness of the violator of personal interest is fully in force here, which in consequence transfers the obligation to present evidence to the violator of this interest (Art. 24 Civil Code).

It seems that even the most abstract and precise doctrinal deliberations and the attempts at interpretation cannot substitute the custom, sensitivity and tact both on the part of recipients and publishers of information. That is because not lawyers but the public opinion will determine where to set the limit of protected privacy of public figures. The sensitivity of society and the related sense of tolerance for information, as well as a sense of aesthetics and good taste will gradually form the standard for the protection of this right.

Enlargement of the common European data protection basis in the Third Pillar

The creation of an area of freedom, security and justice is one of the objectives formulated in the draft European Constitution (Article I-3 para 2). The Hague Programme adopted on 4 November 2004 by the European Council tries to concretise this objective with a view to reaching a broad co-operation in police and judicial matters. The key concept is the general "availability" of police data. This means that information, which is available in one EU Member State for law enforcement purposes, shall also be available for the same purposes to the competent authorities of the other Member States. By the end of 2005 at the latest, the EU Commission had to present respective proposals for the realisation of this principle of availability which also have to take data protection into consideration. In the subsequent period, both the European Parliament and the Conference of the European Data Protection Commissioners have emphatically spoken out in favour of an act of law concerning the protection of personal data within the framework of the Third Pillar. The proposal of a Council framework decision on the protection of personal data which are processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final), presented by the Commission in October 2005, shall take account of those requirements. In my following explanation, I would like to focus particularly on this proposal and also point out the consequences for the data protection level in the Member States.

This proposal is intended to close the most essential gap in the regulation in the field of data protection in the European Union after various earlier initiatives for the protection of personal data in the framework of the Third Pillar did not prove to be successful (among others the Proposal from Italy of 1998, Council document 8321/98 JAI 15). In addition, the Charter of Fundamental Rights in the European Union emphatically recognises the right to privacy (Article 7) and the right of the protection of personal data (Article 8). Although police and judicial co-operation does not take place in an area not regulated by law, the respective regulations of the Data Protection Convention of the Council of Europe, which are also binding for the EU Member States, seem to be too general in view of modern information technology. The general Data Protection Directive (Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data – EC Data Protection Directive) does explicitly not apply (Article 3 II EC Data Protection Directive) to activities which do not fall under the area of Community Law. Thus, it does not apply to activities which fall, for example, under Title VI of the EU-Treaty in the area of criminal law. Insofar, Member States are entitled to take their own decisions regarding the regulation of data protection. However, within the scope of Title VI, data protection has already been regulated by individual acts of law, among others, one of them is for example, the EUROPOL Convention. Accordingly, a regulation covering the whole scope of the Third Pillar is imperative, in order to

guarantee the 450 million EU citizens an adequate level of data protection which is harmonized as far as possible. This also applies to the police and judicial area.

The Commission's proposal bases to a large extent on the regulations of the EC Data Protection Directive, however, with specific regulations pursuant to the requirements of the police and judicial co-operation in criminal matters and in consideration of the principle of proportionality. By following a recommendation of the European Data Protection Commissioners, also the principles of Recommendation (87) 15 of the Council of Europe 1987 regulating the use of personal data in the police sector, are being respected to a large extent. As an act of law, the Commission proposes the form of a framework decision which aims to harmonize the legal provisions in the Member States with regard to the protection of personal data being processed for the purpose of preventing and fighting crime.

At the beginning of the deliberations, the purpose and scope of application of this proposal still require some clarification. Pursuant to the recitals, the harmonization of the Member States' legal provisions should not result in rendering data protection less stringent, but rather in guaranteeing a high protection level within the whole Union. By achieving this, the data protection requirement is taken into account which demands that a harmonization of data protection at a high level is an indispensable condition for an intensified data exchange between security services. This means that the framework decision has to apply to all police and judicial data, regardless whether they have been transferred previously or whether they have been made available in another way by the competent authorities of another Member State. On the other hand, it would be insufficient to limit the harmonization to the data transferred between the Member States, because in the course of investigation proceedings, those data are inevitably added to other data which were not the object of transfer.

Also the scope of application of the proposal concerning the processing system requires further clarification. With regard to the premise stipulating that the regulations shall apply to all kinds of personal data, a limitation to the automated processing would not be acceptable. It would be problematic as well if the manual processing were only covered as far as it is carried out within a data file, because then, the large scope of information processing in files and/or in other documents would remain outside this proposal's area of protection.

Thus, as an interim result one can state that the double restriction foreseen in the draft does not only result in unacceptable gaps in protection, but also in an impediment of the regulation's aim, which is a data exchange between police authorities that should be as free as possible.

A highly clear and final definition of the circle of persons whose data may be processed by authorities responsible for law enforcement and for the protection against threats, is particularly important. It is insofar necessary to improve the proposal, as it contains, in addition to convicted persons, suspected persons, contact persons and accompanying persons, an opening clause pursuant to which also data of persons not belonging to the circle of the previously mentioned categories can be recorded. Just for its vagueness, the clause should be deleted, because for the very reason that the security services' activities are highly intrusive, a clear limitation to data processing, which is

regulated by law and which can be verified by courts of justice and by data protection authorities, is particularly important.

Following the respective regulations in the Data Protection Directive, the data subject's rights, among others, the rights of notification and information, are included in the proposal. However, the reasons for a refusal are regulated in a very comprehensive way. This requires an amendment in order to decide in the individual case, whether information has to be provided or can be denied while respecting the data subject's interest. As a corrective of the exceptions of the obligation to provide information, the data subjects have to be told that they are entitled to turn to the independent data protection authorities, which have the means to evaluate the lawfulness of the data processing.

The proposal also contains institutional guarantees concerning data protection. For example, with a view to implementing this framework decision, Member States are obliged to establish supervisory authorities assuring the respect of the regulations in the area of data protection. Their authorisations are listed in detail. Moreover, Article 31 of the proposal provides for an advisory data protection forum, which should emulate the Article 29 Working Party as a model for its organisation. This proposal should be welcomed, because with regard to the area of the Third Pillar, this proposal assures that for the first time, an advisory panel is established providing the possibility of a comprehensive exchange of opinions and experience between the supervisory data protection authorities of the EU Member States and the European Data Protection Supervisor (EDPS).

The adoption of the framework decision for the protection of personal data within the context of police and judicial co-operation in criminal matters, would be a milestone on the way to a comprehensive data protection within the EU. This can and has to result in a far-reaching harmonization of the right to privacy with regard to police information processing at national level and also with regard to exchanging information at cross-border level. Therefore, this proposal is of fundamental importance. Without an adequate data protection level, the data exchange in the area of police and justice between the Member States cannot and must not be intensified in a way desirable and required for an effective law enforcement and protection against threats in a Europe without internal borders. Therefore, we hope that this framework decision will be adopted in the near future.

Rozbudowanie wspólnej europejskiej podstawy prawnej o zagadnienia dotyczące ochrony danych w „trzecim filarze”

Ustanowienie obszaru swobody, bezpieczeństwa i sprawiedliwości to jeden z celów ujętych w projekcie konstytucji europejskiej (art. 1-3, ustęp 2). Program haski przyjęty 4 listopada 2004 roku przez Radę Europejską próbuje sprecyzować ten cel w odniesieniu do kwestii daleko idącej współpracy w sferze policyjnej i sądowej. Zasadniczym pojęciem w tej dziedzinie jest ogólna „dostępność” danych policyjnych. Oznacza ono, że dostęp do informacji niezbędnych do egzekwowania prawa w jednym Państwie Członkowskim Unii Europejskiej powinny mieć dla tych samych celów również kompetentne organa pozostałych Państw Członkowskich. Najpóźniej do końca 2005 r. Komisja Unii Europejskiej miała przedstawić propozycje dotyczące realizacji zasa-

dy „dostępności”, uwzględniające przy tym ochronę danych osobowych. W późniejszym czasie zarówno w Parlamencie Europejskim, jak i podczas Konferencji Europejskich Rzeczników Ochrony Danych Osobowych stanowczo opowiadano się za przyjęciem aktu prawnego o ochronie danych osobowych w ramach tzw. trzeciego filaru. Wniosek dotyczący decyzji ramowej o ochronie danych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych [COM (2005) 475 wersja ostateczna], przedstawiony przez Komisję w październiku 2005 r., powinien uwzględniać przedstawione uwarunkowania. W moim wystąpieniu chciałbym skoncentrować się przede wszystkim na tym wniosku, a przy tym zwrócić uwagę na znaczenie poziomu ochrony danych osobowych w Państwach Członkowskich.

Wniosek ten ma na celu wypełnienie istotnej luki w regulacjach prawnych dotyczących ochrony danych w Unii Europejskiej, zwłaszcza że wcześniejsze inicjatywy mające na celu ochronę danych w ramach „trzeciego filaru” okazały się nieudane (m.in. propozycja włoska z 1998 r., dokument Rady 8321/98 JAI 15). Ponadto „Karta praw podstawowych w Unii Europejskiej” uznaje prawo do prywatności (art. 7) i prawo do ochrony danych osobowych (art. 8). Mimo że o współpracy policyjnej i sądowej w obszarach nieuregulowanych prawnie nie może być mowy, poszczególne przepisy Konwencji Rady Europy o ochronie danych osobowych, obowiązujące również w Państwach Członkowskich Unii Europejskiej, wydają się zbyt ogólnikowe, biorąc pod uwagę nowoczesną technologię informacyjną.

Ogólna zaś Dyrektywa o ochronie danych (Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych – „Dyrektywa o ochronie danych osobowych WE”) nie ma bezpośredniego zastosowania (art. 3 II WE – „Dyrektywa o ochronie danych”) do czynności, które nie wchodzą w zakres prawa Wspólnoty. Nie stosuje się jej zatem w przypadku czynności, które podlegają, na przykład, pod Tytuł VI „Traktatu o Unii Europejskiej” w obszarze prawa karnego. Państwa Członkowskie są przy tym uprawnione do podejmowania suwerennych decyzji w dziedzinie ochrony danych. Jednakże w ramach tego Tytułu ochrona danych została już uregulowana odrębnymi aktami prawnymi. Przykładem takiego aktu jest „Konwencja o Europolu”. Konieczna jest zatem regulacja obejmująca cały „trzeci filar” w celu zapewnienia 450 milionom obywateli Unii Europejskiej właściwej, w możliwie największym stopniu zharmonizowanej, ochrony danych osobowych. Dotyczy to również sfery działań policyjnych i sądowych.

Wniosek Komisji opiera się przede wszystkim na regulacjach „Dyrektywy o ochronie danych WE” z uwzględnieniem jednak szczególnych przepisów odnoszących się do współpracy policyjnej i sądowej w sprawach karnych oraz do zasady proporcjonalności. Dzięki rekomendacji europejskich Rzeczników ochrony danych, zasady rekomendacji (87) nr 15 Rady Europy z 1987 r. regulującej wykorzystanie danych osobowych w sektorze policyjnym są w dużym stopniu przestrzegane. Komisja proponuje zatem rodzaj aktu prawnego w postaci decyzji ramowej, która miałaby na celu zharmonizowanie w Państwach Członkowskich przepisów prawnych dotyczących ochrony danych osobowych, które są przetwarzane dla zapobiegania i zwalczania przestępczości.

Na początku należy omówić cel i zakres stosowania tego wniosku. Zgodnie z ustaleniami, harmonizacja przepisów prawnych Państw Członkowskich nie powinna prowadzić

do swobodnej interpretacji ochrony danych osobowych, lecz raczej gwarantować wysoki poziom ochrony w całej Unii. Zapewni to spełnienie wymogu, który stanowi, że niezbędnym warunkiem zwiększonej wymiany danych między służbami bezpieczeństwa jest harmonizacja ochrony danych na wysokim poziomie. Oznacza to, że decyzja ramowa musi być stosowana w przypadku wszystkich danych policyjnych i sądowych bez względu na to, czy były one wcześniej przekazywane lub też zostały udostępnione w inny sposób przez kompetentne organa innego Państwa Członkowskiego. Z drugiej jednak strony ograniczenie harmonizacji do danych przekazywanych między Państwami Członkowskimi byłoby niewystarczające, gdyż w trakcie postępowania karnego dane te są nieuchronnie łączone z innymi, które nie były przedmiotem zainteresowania.

Zakres stosowania wniosku musi być dokładnie określony z podaniem szczegółowych wyjaśnień. Jeżeli chodzi o stwierdzenie, że przepisy mają mieć zastosowanie w przypadku wszelkiego rodzaju danych osobowych, nie do przyjęcia byłoby ograniczenie ich tylko do automatycznie przetwarzanych danych. Problematyczne byłoby również uwzględnienie tylko ręcznie przetwarzanych danych w bazach danych, ponieważ w takiej sytuacji informacje przetwarzane w tych bazach i (albo) w innych dokumentach w dużym zakresie pozostawałyby poza obszarem ochrony określonym we wniosku dotyczącym przetwarzania danych.

Jako stan przejściowy można potraktować sytuację, gdy podwójne ograniczenia przewidziane w projekcie nie tylko prowadzą do powstawania luk w ochronie, które są nie do przyjęcia, ale również utrudniają realizację założeń przepisu stanowiącego o wymianie danych między organami policji, która powinna być na tyle swobodna, na ile to możliwe.

Szczególnie ważne jest jednoznaczne i ostateczne zdefiniowanie kręgu osób, których dane mogą być przetwarzane przez organa odpowiedzialne za egzekwowanie przestrzegania prawa oraz ochronę przed zagrożeniami. Uwzględnienie tych uwarunkowań we wniosku jest konieczne. Oprócz bowiem danych osób skazanych lub podejrzanych o popełnienie przestępstwa, jak również osób zapewniających kontakt z wymienionymi osobami, a także osób uczestniczących w czynach przestępczych – uwzględnionych we wspomnianym wniosku, zgodnie z otwartą klauzulą również dane osób nienależących do wymienionych kategorii mogą być rejestrowane. Ze względu na swą niejasność klauzula ta powinna zostać wykreślona, gdyż właśnie z powodu, że działania służb bezpieczeństwa są raczej niepożądane, bardzo ważne jest jasne określenie granic do przetwarzania danych, które jest usankcjonowane prawnie i weryfikowane przez organy sprawiedliwości oraz organy ochrony danych.

Zgodnie z poszczególnymi przepisami zawartymi w „Dyrektywie o ochronie danych”, we wniosku są zawarte ujednolicone prawa podmiotu, którego dane są przetwarzane, między innymi prawo do notyfikacji i informacji. W obszerny sposób omówiono przyczyny odmowy dostępu do danych. Dlatego konieczne jest wprowadzenie poprawki umożliwiającej podejmowanie decyzji w indywidualnych sprawach, czy należy udzielić informacji, czy też odmówić ich udzielenia, respektując interesy podmiotu, którego dane dotyczą. Dla przestrzegania przepisów związanych z ochroną danych należy poinformować osoby, których te dane dotyczą, o przysługującym im prawie do zwrócenia się do odpowiednich niezależnych organów ochrony danych osobowych, które dysponują środkami do oceny legalności przetwarzania tych danych.

Wniosek ten zawiera również gwarancje instytucjonalne dotyczące ochrony danych. Dla przykładu, Państwa Członkowskie, mając na celu implementację decyzji ramowej, są zobowiązane do ustanowienia organów nadzorczych kontrolujących przestrzeganie przepisów w zakresie ochrony danych. Ich uprawnienia są szczegółowo wymienione. Poza tym art. 31 wniosku stanowi o powstaniu forum doradczego w dziedzinie ochrony danych, który jako wzór powinien przyjąć Grupę Roboczą Art. 29. Wniosek ten powinien być przyjęty, gdyż zapewnia w ramach „trzeciego filaru” ustanowienie po raz pierwszy doradczego forum umożliwiającego wszechstronną wymianę opinii i doświadczeń między organami nadzorczymi ochrony danych w Państwach Członkowskich Unii Europejskiej i Europejskim Inspektorem Ochrony Danych.

Przyjęcie decyzji ramowej dotyczącej ochrony danych osobowych w dziedzinie współpracy policyjnej i sądowej w sprawach karnych stanowiłoby kamień milowy na drodze do pełnej ochrony danych w UE. Rezultatem może i musi być pełna harmonizacja prawa do prywatności w zakresie przetwarzania informacji policyjnych na szczeblu krajowym, ale również wymiana informacji na szczeblu międzypaństwowym. Dlatego też wniosek ten ma fundamentalne znaczenie. Bez odpowiedniego bowiem poziomu ochrony danych wymiana informacji w sferze działań policyjnych i sądowych między Państwami Członkowskimi nie może być prowadzona z takim natężeniem, jakie jest niezbędne do skutecznego egzekwowania prawa i ochrony przed zagrożeniami w Europie bez wewnętrznych granic. Dlatego mamy nadzieję, iż decyzja ramowa zostanie przyjęta w niedalekiej przyszłości.

The multiplicity and flexibility of enforcement

I) Prologue

This is my humble tribute to Ewa Kulesza, because she is such an effective protector of personal data.

My argument about enforcement (through independent authorities) of the right to protection of personal data is that its multiplicity and flexibility are particularly appropriate to attain its purposes.

II) Multiplicity

A) Instrumental powers

The Directive 95/46/EC and the national laws attribute normally to the authorities a series of means or instrumental powers of different nature and effects that contribute to a final act or decision of personal data protection.

A first set of those tools may be characterized as powers of inquiry. Their effectiveness may be presented from the lightest to the strongest, their application being adopted to each situation and circumstances. Those means go from the mere putting of questions, to the active getting of information and, finally, to the inspection, the direct observation and/or manipulation of equipment or of documents or any other objects. The instrumental means may also consist of provisory decisions, aimed to avoid the possible worthlessness of the final decisions.

In this field the blocking and the temporary prohibition of data processing are specially considered.

Another kind of instrumental powers of the data protection authorities concerns some faculties of starting the activity of other entities or of intervention in their procedures. Those are powers such as the right of intervention in judicial procedures, or the faculties of presentation of cases to the parliament, the courts or the state prosecutors.

B) Final positions

1) Non-decisive positions

Some of the final positions of the authorities have not a decisive nature – i.e. they do not consist in coercible acts imposed to other entities, public or private.

This does not mean that such remedies are irrelevant, or even less important. Their strength derives from the public respect conquered by the data protection authorities.

The best-known of these means is the recommendation – the typical weapon of the Ombudsmen. Some of the data protection authorities are well-known Ombudsmen. The recommendation is, indeed, a very democratic way of obtaining a certain result. When it is followed, its aim is attained not by force, but because it is voluntarily appreciated and accepted by those whom it is directed to. The recommendation is, besides, not a mere opinion or advice. It is a manifestation of will, although not binding. It pushes the addressee to adopt a certain activity. When it is not followed, the addressee remains subject to public dispraise.

This appeal to the public means, finally, the recourse to the real core of the democratic system – the citizens.

A somewhat weaker weapon can also be used by data protection authorities – the advice or legal opinion. The authorities have often the capacity to express their position in this way, namely about laws in preparation and special processing such as the transfer of data to the countries outside the EU, which do not offer an adequate level of protection. The legal opinion or advice can, nevertheless, be a non-despicable means of enforcement of the right to data protection. Their value depends on the respectfulness reached by the person or persons that constitute the data protection authority.

There is, in the end, still another type of non-coercible definitive measure with a certain enforcement effect in data protection. It is the warning, either public or not, to a data controller that has violated or in any case put in risk personal data. The warning has two effects over the data controller: immediately, it has the character of a sanction or negative appreciation; mediately or indirectly, it pushes that data controller in order to avoid repeating the censured activity. This is, certainly, although of a light character, a way to enforce personal data rights.

2) Decisive position

a) Registration

Most data protection authorities have the duty to maintain a public registry of data processing.

The information given to the public by these registries – about data processing, their controllers, their purposes – contribute, naturally, to the effectiveness or enforcement of their data protection rights.

This is especially evident in those systems where the inclusion of the processing in the public registry is preceded by an appreciation by the data protection authority, aimed to ascertain if they comply with all the legal conditions or requisites.

b) Prior checking

Perhaps the more efficient means of direct enforcement of data protection is prior checking, normally exercised through acts of authorisation.

Those acts are a prior condition for the processing of the most important personal data, generally sensitive data.

They may also appear as the prerequisite of certain processing with deeper effects, such as the processing of data for purposes different from those that justified their collection.

The prior checking has the character of the enforcement tool because the admissibility and legality of certain personal data processing depend on it.

Its relevance comes from the fact that the acts – normally administrative acts – that constitute such control are decisive and coercible.

Because of the independence of these authorities, those acts can, in general, only be challenged through an appeal to the courts.

c) Sanctions

The application of sanctions to those who have violated any rights to protection of personal data are, as coercible reactions, perhaps the hardest and strongest way to enforce those rights.

The sanction is, because of its retributive nature, something as the restitution or the recomposition of the affected legal system.

Those sanctions are very often administrative sanctions.

But they can also assume the form of prohibition of processing and/or the erasure or destruction of illegally processed data.

In extreme cases, the breach of data protection rules can even be a criminal offence, subject to criminal penalties, the first investigated by state prosecutors and the latter applied by the courts – all of them are also means of enforcement.

3) Preventive effects

Some of the means considered above can have a secondary effect, that is, indeed, also a modality of enforcement.

This is what can be called, in general, the preventive effect.

As those means contribute to avoiding future violations of rights to data protection, convincing the possible violators not to commit them, they become a way to enforce those rights. A curious thing is that this kind of result can be reached not only by decisions, but also by instrumental means.

The fact of having been subject to an inspection can frequently discourage the data controller from committing illegalities related to that act of investigation.

But the preventive effects of the final decisions are more frequent and evident.

This happens very often after the application of the administrative sanction or the warning.

And even the annual report of the authorities, describing data protection breaches of these kinds of rights and the reaction of the control authorities is able to cause the preventive result.

This prevention may even concern the third persons or entities, as they take conscience of the warnings, sanctions and the content of the reports applied to the correspondent addressees.

C) The importance of being multiple

The above-described multiplicity of means is particularly favourable to the appropriate enforcement of the rights concerning personal data.

As the personal data are not uniform or equal, it is comprehensible that the means to enforce them must also be variegated.

On the other hand, as the data controllers are numerous and different, the influence – psychological or even exerting the legal coercion – pushing them to enforce the correspondent rights will be more effective and successful if it assumes diverse forms or configurations.

III) Flexibility and openness

The ways to enforce the rights on personal data are, however, not only multiple, but also flexible and open.

This means that the faculties that constitute enforcement are not limited by law, nor standardised.

Those characteristics concern, not only the instrumental means of enforcement, but also the final acts included in this concept.

As those faculties are not limited, they cannot be exhaustively enumerated. It is only possible to point out some possible examples.

Speaking about the instrumental tools it is important, first of all, to say that, although neither the Directive nor the national laws normally speak expressly about them, nothing impeaches the data protection authorities to intervene in a case or situation "*sponte sua*" (by their own initiative), and not necessarily after receiving a claim or complaint in that sense.

On the other hand, the authorities may, before giving a formal legal opinion or advice about draft legislation, decide to accept to participate (through any of the members or collaborators) in the preparatory work of those texts.

This procedure may have practical advantages: avoiding the texts received by the authorities being already in the final version – and so allowing the authorities to intervene more efficiently in the previous and preventive occasion.

However – once there is the risk of compromising the independent position of the authority – it must be always clear that such a procedure can not be a precedent in what concerns the final opinion or advice of the authority.

And (still thinking about instrumental interventions) the authorities may, even independently of a formal inspection or inquiry, decide to follow up closely specific personal data processing as, for instance, the Portuguese authority has recently decided about the experiences of electronic vote organized in our country.

In respect to final positions, it shall be remarked that even those authorities that are not entitled by law to make formal recommendations can issue such type of suggestions. They have not the same legal value as the proper ones, for instance, their addressees are not legally bound to answer, nor to motivate their eventual non-acceptance. Nevertheless, they have a clear psychological strength – and perhaps also sociological – if they are known by the public.

The imagination can in this context help the authorities to find new and appropriate means of enforcement.

It is with this appeal to imagination that I close this homage to Ewa Kulesza who was able to organize so perfectly, with scarce time and means, the European and world conferences that we remember so gratefully.

Różnorodność i elastyczność w metodach egzekwowania prawa do ochrony

I) Wstęp

Niniejszy artykuł jest moim skromnym hołdem dla Pani Ewy Kuleszy w uznaniu jej skutecznych dokonań jako obrońcy prawa do ochrony danych osobowych.

Chciałbym zaprezentować stanowisko, że egzekwowanie (przez niezależne instytucje) prawa do ochrony danych osobowych jest najbardziej skuteczne przy zastosowaniu różnorodnych metod oraz elastycznego podejścia.

II) Różnorodność

A) Instrumenty prawne

Dyrektywa 95/46/WE i ustawy krajowe nadają zwykle instytucjom zajmującym się ochroną danych osobowych szereg uprawnień lub instrumentów prawnych, które mogą mieć zróżnicowany charakter i sposób działania. Instrumentarium to jest pomocne w wydaniu ostatecznej decyzji w sprawie ochrony danych osobowych.

Pierwszy zestaw tych narzędzi można określić jako uprawnienia śledcze. Można je uszeregować pod względem skuteczności od najsłabszych do najsilniejszych – sposób użycia jest dostosowywany do każdorazowej sytuacji i okoliczności. Uprawnienia śledcze sięgają od zwykłego zadawania pytań do aktywnego zdobywania informacji aż po przeprowadzanie kontroli, bezpośrednie obserwacje i/lub manipulacje dotyczące sprzętu, dokumentów, czy innych obiektów. Omawiana grupa instrumentów może także obejmować decyzje wstępne, podejmowane w sytuacji, gdy odwołana w czasie decyzja ostateczna mogłaby się okazać bezwartościowa.

Często stosowane są też blokady i tymczasowy zakaz przetwarzania danych.

Inny rodzaj uprawnień agencji ochrony danych osobowych obejmuje możliwości nakłaniania innych podmiotów do podjęcia działań, czy też prawo ingerowania w ich procedury. Do grupy tych uprawnień zalicza się prawo do uczestniczenia w postępowaniach sądowych i zgłaszania spraw parlamentowi, sądom oraz prokuratorom.

B) Opinie końcowe

1) Opinie niewiążące

Niektóre z opinii końcowych wydawanych przez instytucje ochrony danych osobowych nie mają natury wiążącej, tzn. nie przewidują zastosowania środków przymusu wobec innych instytucji, czy to publicznych czy prywatnych. Nie oznacza to, że tego typu środki naprawcze są nieistotne, czy mniej ważne. Ich siła bierze się z publicznego szacunku, jaki zyskały instytucje ochrony danych osobowych.

Najlepiej znanym z tych środków jest rekomendacja – typowa broń rzeczników praw obywatelskich. Niektóre instytucje ochrony danych osobowych są szeroko znane jako rzecznicy praw obywatelskich.

Rekomendacja jest rzeczywiście bardzo demokratycznym sposobem uzyskania określonego rezultatu.

Jeśli adresaci rekomendacji przestrzegają jej zaleceń, cel zostaje osiągnięty nie za pomocą przymusu, ale ponieważ rekomendacja została dobrowolnie rozważona i zaakceptowana przez jej adresatów.

Oprócz tego rekomendacja jest czymś innym niż zwykła opinia czy rada.

Jest manifestacją woli, aczkolwiek niewiążącą.

Skłania adresata do podjęcia określonych działań.

Jeśli nie zostanie zastosowana, adresat staje się obiektem nagany społecznej.

To odwołanie się do opinii publicznej oznacza wreszcie odwołanie się do samego rdzenia systemu demokratycznego – do obywateli.

Instytucje ochrony danych osobowych mogą także użyć nieco słabszej broni: zalecenia lub opinii prawnej.

Instytucje te mają często sposobność do wyrażania swojego stanowiska w tej formie, mogą się mianowicie wypowiadać na temat przygotowywanych ustaw i specjalnych przypadków przetwarzania danych, jak np. przekazywanie danych za granicę do krajów spoza UE, które nie zapewniają wystarczającego poziomu bezpieczeństwa.

Opinia prawna czy zalecenie mogą jednakże odgrywać niebagatelną rolę jako środek egzekwowania prawa do ochrony danych osobowych.

Ich wartość zależy od poważania, jakie zdobyła sobie osoba bądź osoby tworzące instytucję ochrony danych osobowych.

Istnieje jeszcze jeden typ środka prawnego, który również nie posiada charakteru przymusowego, ale jest do pewnego stopnia skuteczny w egzekwowaniu prawa do ochrony danych. Jest nim ostrzeżenie, zarówno publiczne jak i niepubliczne, wobec administratora danych, jeżeli naruszył on reguły albo w inny sposób naraził dane osobowe.

Ostrzeżenie ma dwojaki wpływ na administratora danych: skutek natychmiastowy ma charakter sankcji lub negatywnej oceny; skutek pośredni to nakłonienie administratora danych do unikania napiętnowanych działań. Ostrzeżenie jest więc także metodą egzekwowania prawa do ochrony danych osobowych, aczkolwiek o subtelny charakterze.

2) Opinie wiążące

a) Rejestracja

Większość instytucji ochrony danych osobowych ma obowiązek prowadzić publiczny rejestr dotyczący przetwarzanych danych. Informacje, które opinia publiczna uzyskuje dzięki tym rejestrom – o operacjach na przetwarzanych danych, ich administratorach, celach przetwarzania – przyczyniają się naturalnie do skuteczności egzekwowania prawa obywateli do ochrony ich danych osobowych.

Jest to szczególnie widoczne w tych systemach, gdzie wpisanie operacji przetwarzania danych do publicznego rejestru jest poprzedzone badaniem przez instytucję ochrony danych osobowych, czy administrator danych spełnia wszystkie wymogi prawne.

b) Upřednia weryfikacja

Skuteczniejszym środkiem bezpośredniego egzekwowania ochrony danych osobowych jest być może upřednia weryfikacja, zwykle dokonywana przez wydawanie zgody na przetwarzanie danych.

Otrzymanie zgody stanowi warunek wstępny, który należy spełnić, aby móc legalnie przetwarzać najważniejsze dane osobowe, ogólnie mówiąc dane wrażliwe. Uzyskanie zgody może być także konieczne w przypadku operacji na danych mających daleko idące konsekwencje, jak np. przetwarzania danych w innych celach, niż te, którymi uzasadniano ich gromadzenie.

Procedura upředniej weryfikacji ma charakter instrumentu służącego do egzekwowania prawa, ponieważ zależą od niej dopuszczalność i zgodność z prawem niektórych operacji na danych osobowych.

Znaczenie tej procedury wynika z faktu, że decyzje ustanawiające ten typ kontroli mają wiążący charakter i mogą się wiązać z zastosowaniem środków przymusu – są to zwykle akty administracyjne.

Z uwagi na niezależność instytucji ochrony danych osobowych, w większości przypadków decyzje te można podważyć jedynie na drodze apelacji sądowej.

c) Sankcje

Zastosowanie sankcji wobec winnych naruszenia prawa do ochrony danych osobowych jest, jako odpowiedź wiążąca się ze środkiem przymusu – zapewne najostrejszą i najmocniejszą metodą zapewnienia egzekwowania tychże praw.

Ze względu na swój karzący charakter sankcja stanowi coś w rodzaju przywrócenia do stanu poprzedniego czy przywrócenia stanu równowagi w odniesieniu do naruszonego stanu prawnego.

Sankcje te są bardzo często sankcjami administracyjnymi. Mogą jednak także przybrać formę zakazu przetwarzania i/lub nakazu usunięcia lub zniszczenia nielegalnie przetwarzanych danych.

W ekstremalnych przypadkach złamanie zasad ochrony danych osobowych może stanowić przestępstwo kryminalne, zagrożone odpowiedzialnością karną – przestępstwo jest przedmiotem śledztwa prowadzonego przez prokuraturę, a odpowiedzialność karną wymierzają sądy – są to zatem także środki egzekucji.

3) Skutek prewencyjny

Niektóre z zaprezentowanych powyżej środków mogą mieć skutki uboczne, które zaliczają się także do jednej z form egzekwowania prawa. Możemy je ogólnie nazwać skutkiem prewencyjnym.

Ponieważ zaprezentowane powyżej instrumenty prawne przyczyniają się do zmniejszenia liczby naruszeń prawa do ochrony danych osobowych, powstrzymując potencjalnych sprawców naruszeń, stają się tym samym sposobem egzekwowania tego prawa.

Interesujące jest, że tego typu rezultat można osiągnąć nie tylko za pomocą decyzji, ale także przy pomocy innych instrumentów.

Doświadczenie kontroli może powstrzymać w przyszłości administratora danych od popełniania naruszeń związanych z przedmiotem kontroli.

Skutki prewencyjne dużo częściej wiążą się jednak z decyzjami i są wówczas bardziej widoczne.

Mamy z nimi bardzo często do czynienia po zastosowaniu sankcji administracyjnych lub wystosowaniu ostrzeżenia.

Publikacja przez instytucję ochrony danych osobowych corocznego raportu, w którym opisane są naruszenia i odpowiedź na nie organów kontrolnych, może już wywołać skutek prewencyjny.

Skutki prewencyjne mogą się rozciągać nawet na osoby czy podmioty trzecie, które dowiadują się o ostrzeżeniach, sankcjach i treści raportów wystosowanych do odpowiednich adresatów.

C) Zalety dywersyfikacji metod

Opisana powyżej różnorodność metod jest bardzo korzystna z punktu widzenia skutecznego egzekwowania praw dotyczących danych osobowych.

Ponieważ dane osobowe nie są ani jednorodne, ani identyczne, zrozumiałe jest, że związane z nimi metody egzekwowania także muszą być zdywersyfikowane.

Z drugiej strony, ponieważ administratorów danych jest tak wielu i tak bardzo różnią się oni między sobą, aby móc skuteczniej na nich wpływać – w drodze oddziaływania psychologicznego czy przez przymus prawny – nakłaniając do stosowania prawa, należy sięgać po możliwie zróżnicowane formy i kombinacje środków.

III) Elastyczność i otwartość

Metody egzekwowania prawa do ochrony danych osobowych cechuje oprócz różnorodności również elastyczność i otwarty charakter.

Oznacza to, że przedmiotowe uprawnienia nie są ograniczone przepisami prawa, ani zestandaryzowane.

Właściwości te cechują nie tylko instrumenty egzekwowania, ale także ostateczne decyzje objęte tym modelem.

Ponieważ uprawnienia te nie mają zamkniętego charakteru, nie można podać ich wyczerpującej listy. Można jedynie wskazać kilka możliwych przykładów.

Mówiąc o instrumentach, należy przede wszystkim stwierdzić, że chociaż w Dyrektywie oraz zwykle w ustawach krajowych brak jest o nich wyraźnych wzmianek, nie istnieją zakazy powstrzymujące instytucje ochrony danych osobowych od interwencji *sponte sua* (z własnej inicjatywy) w pewnych sytuacjach czy okolicznościach, a nie koniecznie dopiero po otrzymaniu prośby lub skargi.

Z drugiej strony, przed wydaniem formalnej opinii prawnej lub zalecenia w sprawie projektu aktu prawnego instytucje mogą zgodzić się uczestniczyć (poprzez swoich członków lub współpracowników) w pracach grup roboczych przygotowujących te akty.

Taki sposób postępowania może mieć praktyczne korzyści, unika się w ten sposób sytuacji, gdy projekty przedstawiane do zaopiniowania tym instytucjom są już w wersji finalnej, umożliwiając wcześniejszą i bardziej efektywną interwencję.

Z uwagi na ryzyko narażenia niezależnego stanowiska instytucji zawsze musi być jasne, że tego typu postępowanie w kwestii jej ostatecznej opinii lub zalecenia nie może stanowić precedensu.

Kontynuując wątek interwencji przy pomocy instrumentów: instytucje mogą ponadto zdecydować, że będą śledzić uważnie konkretne operacje przetwarzania danych osobowych (nie musi to przyjmować formy oficjalnej kontroli czy dochodzenia), jak, na przykład, zrobiła to ostatnio instytucja portugalska w kwestii głosowań drogą elektroniczną w naszym kraju.

Jeżeli chodzi o końcowe stanowiska należy zauważyć, że nawet instytucje, których nie uprawniono na podstawie przepisów prawa do przedkładania oficjalnych rekomendacji, mogą wydawać tego typu zalecenia.

Nie mają one wówczas takiej samej wartości prawnej, jak właściwe rekomendacje, na przykład, ich adresaci nie mają obowiązku na nie odpowiadać ani uzasadniać ich odrzucenia.

Tym niemniej mają one wyraźną siłę psychologiczną, a być może także socjologiczną, jeżeli są znane opinii publicznej.

W świetle powyższych rozważań, inwencja w działaniu może pomóc instytucjom ochrony danych osobowych znaleźć nowe i najwłaściwsze metody egzekwowania.

Tym właśnie apelem o inwencję i wyobraźnię kończę moje wystąpienie, dedykowane Pani Ewie Kuleszy, która w krótkim czasie i dysponując skromnymi środkami zdołała w sposób perfekcyjny zorganizować europejską i światową konferencję o ochronie danych osobowych, które wspominamy z wielką wdzięcznością.

Dorota Skolimowska

Dyrektor Departamentu Prawnego,
Biuro Generalnego Inspektora Ochrony Danych Osobowych, Polska
Director, Legal Department,
Bureau of the Inspector General for Personal Data, Poland

Adekwatność przetwarzania danych osobowych

Zasada adekwatności danych jest jedną z podstawowych zasad związanych z przetwarzaniem (w szczególności ze zbieraniem) danych osobowych. Gromadzone dane osobowe powinny być adekwatne w stosunku do celów, w jakich są przetwarzane. Ani kategoria ani treść danych osobowych nie może wykraczać poza cele, dla których dane są gromadzone. Przestrzeganie przez podmioty wykorzystujące dane osobowe zasady adekwatności gwarantuje osobom, których dane dotyczą, że podmioty te będą pozyskiwać tylko niezbędne minimum informacji, uzależniając zakres zbieranych danych od celów, w jakich dane te mają zostać wykorzystane. W takim przypadku poziom ingerencji w prywatność osób fizycznych jest maksymalnie ograniczony.

Dlatego też zasada adekwatności wprowadzona została do najważniejszych europejskich regulacji dotyczących przetwarzania danych osobowych. „Konwencja Nr 108” Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, w rozdziale II, wśród podstawowych zasad ochrony danych wymienia zasadę adekwatności. Zgodnie z art. 5 pkt c tej Konwencji, dane osobowe będące przedmiotem automatycznego przetwarzania powinny być odpowiednie (adekwatne), rzeczowe, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone. Podobna regulacja pojawiła się w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dn. 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Art. 6 pkt c Dyrektywy stanowi bowiem, że Państwa Członkowskie zapewnią, aby dane osobowe były stosowne, istotne i niewykraczające poza konieczne w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone. Jasne określenie celów oraz ocena adekwatności gromadzonych danych musi nastąpić najpóźniej w czasie gromadzenia danych (punkt 28 preambuły Dyrektywy).

Od czasu wprowadzenia w Polsce ochrony danych osobowych¹ zasada ta budziła liczne kontrowersje, być może dlatego, że adekwatność zbierania danych w stosunku do celu przetwarzania danych należy oceniać w każdym przypadku odrębnie, uwzględniając konkretną sytuację zbierania danych przez administratora. W konsekwencji nie jest możliwe, aby Generalny Inspektor Ochrony Danych Osobowych co do zasady określił w sposób precyzyjny, jaki zakres danych osobowych administrator może zbierać, bez narażenia się na zarzut zbierania danych nieistotnych lub danych o zbyt dużym stopniu

¹⁾ Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.).

szczegółowości. Każda sytuacja zbierania danych osobowych wymaga odrębnej analizy i oceny, przy czym – i to jest kwestia wywołująca najwięcej emocji – kryteria tej analizy i oceny oparte są o nieostre, niejednokrotnie dyskusyjne kryteria. Stawia to administratorów danych w niezwykle trudnej sytuacji wymagającej każdorazowej oceny, czy przetwarzanie danych osobowych następuje z uwzględnieniem art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, a więc w sposób merytorycznie poprawny i adekwatny do realizowanego celu.² Decyzję administratora danych dotyczącą zakresu zbieranych danych weryfikuje w toku wykonywania swoich ustawowych zadań Generalny Inspektor, a w przypadku sporu między organem ochrony danych i administratorem danych sądy administracyjne.

Zagadnieniem, które budzi wiele kontrowersji jest – do niedawna bardzo powszechna – praktyka pozyskiwania danych osobowych za pomocą kopiowania dokumentów tożsamości, w szczególności starych dowodów osobistych, zawierających liczne dodatkowe informacje (m.in. poprzednie, nieaktualne adresy zamieszkania, informacje o zatrudnieniu, dane dzieci). Istotne wskazówki dotyczące tej kwestii wskazał Naczelny Sąd Administracyjny (wyrok z dnia 19 grudnia 2001 r., II SA 2869/00, ONSA 2003, Nr 1, poz. 29) stwierdzając, że „gromadzenie danych osobowych, przez wykonanie kopii dokumentu zawierającego te dane jest kwestią techniczną, obojętną dla prawodawcy, reglamentującego w ustawie o ochronie danych osobowych przetwarzanie tego rodzaju danych. Inaczej mówiąc, posługiwanie się taką czy inną techniką utrwalania danych (...) nie przesądza samo przez się o legalności albo nielegalności tego utrwalania (przetwarzania). Dla takich ocen istotne znaczenie mają przede wszystkim: podstawa prawna przetwarzania danych (art. 23 ustawy), rodzaj przetwarzanych danych (art. 27) oraz granice przetwarzania (art. 26 ust. 1 pkt 3). Nie można wobec tego uwzględnić zarzutu, że posługiwanie się techniką kopiowania dokumentu prowadzi do naruszenia wspomnianej zasady adekwatności przetwarzania danych w stosunku do celów, w jakich są przetwarzane.”

Sprawa pozyskiwania danych osobowych w związku z zawieraniem umów (m.in. ubezpieczenia, prowadzenia rachunku bankowego, świadczenia usług telekomunikacyjnych) poprzez kopiowanie dokumentów tożsamości była przedmiotem wielu rozstrzygnięć Generalnego Inspektora. Zbieranie danych osobowych w celu zawarcia i wykonania umowy musi być poprzedzone szczegółową analizą i oceną, zmierzającą do ustalenia, jakie dane będą niezbędne. Analiza poszczególnych decyzji Generalnego Inspektora oraz orzecznictwa sądów administracyjnych wskazuje, że zakres danych osobowych przetwarzanych w związku z koniecznością wywiązania się z umowy powinien być zróżnicowany, w zależności od charakteru i znaczenia umowy. „W drobnych umowach ze sfery życia codziennego kontrahenci mogą zachować wobec siebie anonimowość. Nie jest to już dopuszczalne w przypadku umów o znacznym ciężarze gospodarczym lub społecznym. Bezpieczeństwo obrotu prawnego wymaga wtedy dokładnej identyfikacji stron zawierających umowę, i co za tym idzie – może uzasadniać gromadzenie przez nie danych osobowych w zakresie gwarantującym należyte wywiązanie się z zobowiązania.”³

² Por. wyrok Naczelnego Sądu Administracyjnego z dnia 27 listopada 2003 r., II SA 209/3, http://www.gioudo.gov.pl/data/filemanager_pl/497.doc.

³ Wyrok Naczelnego Sądu Administracyjnego z dnia 10 grudnia 2001 r., SA 2869/00, ONSA 2003 Nr 1 poz. 29.

Generalny Inspektor uwzględniając orzecznictwo sądów administracyjnych i szczególną specyfikę sektora bankowego pozytywnie odniósł się do nowelizacji „Prawa bankowego” (art. 112 b), która zezwoliła bankom przetwarzać dla celów prowadzenia działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych.⁴ Ustawodawca w art. 112 „Prawa bankowego” wprowadził normę, która zalegalizowała pozyskiwanie przez banki informacji z dowodów tożsamości, przy czym wyraźnie zaznaczył, iż źródłem danych mogą być wyłącznie dokumenty, które służą potwierdzeniu tożsamości (np. dowód osobisty, paszport). Jak wskazano w Sprawozdaniu z działalności Generalnego Inspektora w 2004 roku banki rozszerzają stosowanie tego przepisu do pozyskiwania danych poprzez kopiowanie innych dokumentów (np. prawo jazdy).⁵ Tymczasem na taki sposób interpretacji nie pozwalają zarówno przepisy prawa, jak i orzecznictwo sądowe. Dokumentem stwierdzającym tożsamość, stosownie do przepisów ustawy o ewidencji ludności i dowodach osobistych oraz ustawy o paszportach, jest dowód osobisty i paszport. Natomiast stosownie do ustawy „Prawo o ruchu drogowym”, prawo jazdy jest dokumentem stwierdzającym uprawnienia do kierowania pojazdami silnikowymi.⁶ Słuszność powyższego stanowiska potwierdził Sąd Apelacyjny w Białymstoku.⁷

Niejednokrotnie przepisy prawa enumeratywnie określają zakres danych osobowych, do których przetwarzania uprawniony jest administrator danych; pojawienie się takich przepisów w Polsce łączy się z wejściem w życie ustawy o ochronie danych osobowych. Przykładem takiego rozwiązania legislacyjnego może być art. 11 ust. 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (tekst jednolity: Dz.U. z 2001 r. Nr 87, poz. 960 ze zm.), w którym wymienione zostały precyzyjnie dane, które osoba zobowiązana do zameldowania na pobyt stały musi zgłosić właściwemu organowi gminy. Wojewódzki Sąd Administracyjny rozpatrując skargę administratora danych na decyzję administracyjną Generalnego Inspektora stanął na stanowisku, że przepisy, w których ustawodawca określa zakres przetwarzanych danych należy traktować jako *lex specialis* wobec przepisu art. 26 ustawy o ochronie danych osobowych, w konsekwencji w takich sytuacjach – zdaniem Sądu – wyłączone jest zastosowanie zasady adekwatności danych, która jest jedną z głównych zasad przy przetwarzaniu danych osobowych.⁸ To sam ustawodawca rozstrzyga bowiem, jakie konkretnie dane są adekwatne do celu ich przetwarzania. Odnosząc się do wyroku Sądu należy jednak podkreślić, że jeżeli przepis prawa nie przesądza ostatecznie o dopuszczalnym zakre-

⁴ Ustawa z dnia 1 kwietnia 2004 r. o zmianie ustawy „Prawo bankowe” oraz o zmianie innych ustaw (Dz.U. Nr 91, poz. 870).

⁵ http://www.gioudo.gov.pl/data/filemanager_pl/727.doc.

⁶ Stosownie do art. 1 ust. 3 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz.U. z 2001 r. Nr 87, poz. 960 ze zm.) „dowód osobisty jest dokumentem stwierdzającym tożsamość, poświadczającym obywatelstwo polskie, uprawniającym obywateli polskich do przekraczania granic między Państwami Członkowskimi UE. Natomiast art. 1 ustawy z dnia 29 listopada 1990 r. o paszportach (Dz.U. Nr z 1991 r. Nr 2, poz. 5 ze zm.) wskazuje, iż paszport jest dokumentem urzędowym uprawniającym do przekraczania granicy i pobytu zagranicą oraz poświadczającym obywatelstwo polskie, a także tożsamość osoby, w zakresie danych, jakie ten dokument zawiera. Natomiast w myśl art. 88 ustawy „Prawo o ruchu drogowym”, prawo jazdy jest dokumentem stwierdzającym uprawnienia do kierowania pojazdami silnikowymi.

⁷ Sąd w uzasadnieniu wyroku z dnia 29 kwietnia 2003 r. stwierdził, iż „faktem jest natomiast, że pokrzywdzony w wyniku rozboju utracił nie dowód osobisty, a dowód rejestracyjny na samochód i prawo jazdy. Nie są to dokumenty stwierdzające tożsamość. Dokumentami stwierdzającymi tożsamość są: dowody osobiste, tymczasowe dowody osobiste oraz tymczasowe zaświadczenia tożsamości (...), paszporty, dokumenty paszportowe należące do cudzoziemca, karty stałego i czasowego pobytu, tymczasowe dokumenty podróży i tymczasowe zaświadczenia tożsamości (...). Z punktu widzenia prawa, prawo jazdy nie posiada charakteru dokumentu stwierdzającego tożsamość” (II AKA 84/2003 OSA 2003/11 poz. 111, str. 29).

⁸ Wyrok Wojewódzkiego Sądu Administracyjnego z dnia 23 czerwca 2005 r., II SA/Wa 417/05.

sie danych osobowych,⁹ to organ ochrony danych osobowych jest nie tylko uprawniony, ale nawet zobowiązany do ustalenia w toku kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, czy kontrolowany podmiot przetwarza dane w zakresie proporcjonalnym do celu ich pozyskania.

Jak trafnie wskazuje A. Drozd „każdą operację na danych osobowych należy oceniać odrębnie w świetle art. 26 ust. 1 pkt 3. Oznacza to, że inny może być zakres danych osobowych adekwatnych do celu zbierania lub przechowywania, a jeszcze inny do celu udostępniania albo przekazywania do państwa trzeciego” (Andrzej Drozd *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*. LexisNexis, 2005, s. 155).

Warto wskazać, że nie tylko Generalny Inspektor Ochrony Danych Osobowych i inne krajowe organy ochrony danych osobowych w Unii Europejskiej rozstrzygając konkretne sprawy, czy tworząc kodeksy postępowania, za niezbędne uznają badanie zgodności przetwarzania danych z zasadą adekwatności.¹⁰ Niejednokrotnie w opiniach Grupy Roboczej Art. 29¹¹ wskazuje się na konieczność proporcjonalnego, „nienadmiarowego” zbierania i wykorzystywania danych osobowych.¹² Zasada adekwatności przetwarzania danych osobowych jako jedna z głównych zasad przetwarzania danych ma bowiem kluczowe znaczenie dla realnego zapewnienia obywatelom ich prawa do prywatności.

The Adequate Processing of Personal Data

The principle of data adequacy is one of the basic principles related to the processing (and in particular, the collection) of personal data. Personal data that has been stored should be adequate in relation to the purposes for which it is processed. Neither the category nor the content of the personal data can exceed the scope of the purposes for which the personal data is stored. Entities and institutions that observe the principle of adequacy guarantee the individuals whose personal data is concerned that they will retrieve only the minimum amount of essential information with the scope of

data collection and processing dependent on the purposes for which the data is to be used. In this way, the level of intrusion into the privacy of individuals is limited to the maximum.

The above reason is also why the principle of adequacy has been introduced into the most important of European regulations concerning the protection of personal data. Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, of 28 January 1981 lists the principle of adequacy amongst the basic principles of the protection of data in Chapter II. According to Article 5, point C of this Convention, personal data undergoing automatic processing shall be adequate, relevant and not excessive to the purposes for which they are stored. Similar regulation appears in Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 6, point C of the Directive specifies that Member States ensure that personal data are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Such purposes must be explicit and legitimate and must be determined no later than at the time of collection of the data (point 28 of the Recitals of the Directive).

From the introduction of the protection of personal data¹ in Poland, this principle has caused considerable controversy. Perhaps due to the fact that the adequacy of data collection in relation to the purposes of data processing should be judged individually in every case, taking into consideration the particular situation in which the controller collected the data. It follows that it is not possible for the Inspector General for the Protection of Personal Data to precisely outline in principle the scope of the data that can be collected by the controller without running the risk of being accused of collecting data which is irrelevant or data which is far too detailed. Every situation in which data are collected and stored requires a separate analysis and assessment, although, the criteria of this analysis and assessment are based on – and this issue leads to a great deal of controversy – vague and often debatable factors. This places data controllers in an extremely difficult situation that requires assessment every time data are collected to see if the processing of personal data takes place in consideration of Article 26 (1), point 3 of the Act on the Protection of Personal Data, that is whether they are relevant and adequate with regards to the purposes of collection.² The decision to collect data taken by the data controller with regard to its scope is verified by the Inspector General for the Protection of Personal Data throughout the course of fulfilling his statutory duties. In cases of a dispute between the Data Protection Authority and a data controller, this is verified by the Administrative Courts.

The issue that is of most concern and controversy, which has been commonplace until very recently, is the practice of retrieving personal data by copying forms of ID, in particular old identity cards that contain a large amount of additional information (for example, former, invalid addresses, employment information or data concerning

⁹ Np. przepis art. 161 ustawy z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne” (Dz.U. Nr 171, poz.1800 ze zm.).

¹⁰ Np. włoski kodeks postępowania i praktyki zawodowej w sprawie systemów informatycznych, zarządzanych przez podmioty prywatne, w odniesieniu do kredytu konsumenckiego, rzetelności oraz terminowości płatności, Alessandro del Ninno, *New Regulations Regarding the Processing of Personal Data in Italy: Part I*, World Data Protection Report, BNA International (Nr 4 2005 r.) s. 19-22.

¹¹ Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana została na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r., w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych jako niezależny podmiot o charakterze doradczym, zajmujący się m.in. badaniem kwestii dotyczących stosowania krajowych środków przyjętych na mocy wskazanej powyżej Dyrektywy, w celu przyczynienia się do jednolitego stosowania tych środków. Więcej informacji o Grupie Roboczej Art. 29 znajduje się na stronie internetowej: http://www.europa.eu.int/comm/justice_home/fsj/privacy/working-group/index_en.htm.

¹² Np. Dokument roboczy Nr 105 w sprawach ochrony danych związanych z technologią RFID (radio-identyfikacja), http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm.

¹ Act on the Protection of Personal Data, 29 August 1997 (unified text, Law Gazette 2002, No. 101, item 926 with amendments).

² Ruling of the Supreme Administrative Court of 27 November 2003, II SA 209/3, http://www.giodo.gov.pl/data/filemanager_pl/497.doc.

children). The Supreme Administrative Court in a ruling of 19 December 2001, II SA 2869/00, ONSA 2003, No. 1, 29 noted significant pointers with regard to this issue claiming that the "collection of personal data through the copying of forms of ID is a technical issue which is immaterial to the employer rationing within the Act on the Protection of Personal Data the processing of this type of data. In other words, the use of this type of technique of data storage (...) does not in itself determine the legality or illegality of this storage (processing). For this kind of assessment, the following have crucial meaning: the legal foundation for data processing (Article 23 of the Act), the type of data processed (Article 27) as well as the limitations of the processing (Article 26 (1), point 3). In light of this, one cannot respect the charge that using the technique of copying a form of ID is an infringement of the aforementioned principle of adequacy of the processing of personal data in relation to the purposes for which they are processed."

The retrieving of personal data in order to sign a contract (for example, an insurance contract, opening a bank account, telephone contract) by the copying of forms of ID has been the subject of many resolutions by the Inspector General. The collection of personal data for the purpose of signing and execution of a contract should be preceded by a detailed analysis and assessment, which aims at establishing what kind of data will be indispensable. The analysis of the decisions of the Inspector General as well as the judicial rulings of the Administrative Courts indicate that the scope of personal data that is processed in relation to the necessity of fulfilling a contract should be varied depending, of course, on the nature and meaning of the contract. "In small contracts in the sphere of everyday life, the contracting parties can be anonymous in the face of each other. However, this is not admissible in cases where the contract is of particular economic or social weight. The security measures require that both contracting parties are precisely identified. Therefore, it follows that data can be collected and stored on the parties in order to guarantee that the contract is properly fulfilled or executed."³

The Inspector General for the Protection of Personal Data taking into consideration the ruling of the Administrative Courts and the particular nature of the banking sector has positively reacted to the amendment to Banking Law (Article 112 b), which permitted banks, for the purposes of undertaking banking activities, to process the information found in the IDs of individuals.⁴ In Article 112 of the Banking Law, the legislators introduced a norm, which legalised the retrieval of information from forms of ID by banks, although, it is clearly stated that the source of this information can only be documents that serve to verify the identity of an individual (for example, ID cards, passports). It follows from the 2004 Report of the work of Inspector General that banks tend to extend their application of the rule concerning the retrieval of information by copying other documents (such as driving licences).⁵ However, both legal regulations and judicial rulings do not allow for such an interpretation. The document which serves to verify an individual's identity, in accordance with the Act on Census and ID

cards as well as the Passport Act is the ID card and passport, whereas in accordance with the Road Traffic Law, the driving licence is a document verifying the individual's right and qualifications to drive a motor vehicle.⁶ The legitimacy of the above-mentioned position was confirmed by the Court of Appeal in Białystok.⁷

The regulations of law often define the scope of personal data that can be processed legally by a data controller. The appearance of these regulations in Poland is strictly linked to the introduction of the Act on the Protection of Personal Data. An example of a legislative solution can be found in Article 11 of the Act of 10 April 1974 on Census and ID cards (unified text: Law Gazette, 2001, No. 87, item 960 with amendments), in which the data that shall be submitted by an individual responsible for registering at a permanent residence to the appropriate local authority is precisely specified. The Provincial Administrative Court investigating the complaint of a data controller concerning an administrative decision of the Inspector General took the position that the regulations, in which the legislators define the scope of the processing of data, should be treated as a *lex specialis* in the face of Article 46 of the Act on the Protection of Personal Data. In consequence, in these situations, according to the Court, the principle of adequacy, which is one of the main principles in data processing, is not applied.⁸ In the same way, the legislator determines which particular data is adequate for the purposes of processing. In reference to the ruling of the Court, one needs to highlight the fact that if a legal regulation does not determine the final scope of the admissibility of personal data processing,⁹ then the Personal Data Protection authority is not only authorised, but has a responsibility to establish, through investigation, the conformity of the processing of data with the regulations on Protection of Personal Data, or if the body under investigation is processing data proportionally to the purposes of the original data retrieval.

As A. Drozd so succinctly indicates: "every operation using personal data needs to be assessed individually in light of Article 26 (1), point 3. This means that the scope of the purpose can be different for the collection and storage of personal data and different for the access to personal data or its transfer to a third party" (Andrzej Drozd, *Act on the Protection of Personal Data*. Commentary. LexisNexis, 2005, p. 155).

It is worth noting that not only the Inspector General for the Protection of Personal Data but also national Personal Data Protection authorities in other EU states while

³⁾ Ruling of the Supreme Administrative Court of 10 December 2001, SA 2869/00, ONSA 2003, No. 1, item 29.

⁴⁾ Act of 1 April 2004 on the amendment to the act – Banking Law as well as amendments to other acts (Law Gazette, No. 91, item 870).

⁵⁾ http://www.gioudo.gov.pl/data/filemanager_pl/727.doc.

⁶⁾ In accordance with Article 1 (3) of the Act of 10 April 1974 on Census and ID cards (Law Gazette, 2001, No. 87, item 960, with amendments), "the ID card is a document verifying the identity of an individual, authenticating Polish citizenship, authorising Polish citizens to freely traverse EU Member State borders. Meanwhile, Article 1 of the Passport Act of 29 November 1990 (Law Gazette, 1991, No. 2, item 5 with amendments) stipulates that a passport is an official document authorising the crossing of borders and stay abroad as well as authenticating Polish citizenship and the identity of the individual in the scope of the personal data that this document contains. Furthermore, Article 88 of the Road Traffic Law stipulates that a driving licence is the legal document verifying the individuals right and qualifications to drive a motor vehicle.

⁷⁾ The court in justifying the ruling of the 29 April 2003 ascertained that "the fact is that the victim while being mugged lost not his ID card but his vehicle registration and driving licence. These are not identity documents. Documents for the verification of one's identity are: ID cards, temporary ID cards, as well as temporary identity certificates... passports, passport documents belonging to foreign nationals, permanent residency cards, temporary residency cards, temporary travel documents, and temporary identity certificates... From the point of view of the law, a driving licence is not a form of identity document." (II AKa 84/2003 OSA, 111, p. 29).

⁸⁾ Ruling of the Provincial Administrative Court of 23 June 2005, II SA/Wa 417/05.

⁹⁾ For example, Article 161, Act of 16 July 2004 on Telecommunications Law (Law Gazette, No. 171, item 1800 with amendments).

settling particular cases or creating procedure rules regard the assessment of conformity of processed data to the principle of adequacy as essential.¹⁰ Many times in the opinions of the Article 29¹¹ Working Party the necessity to undertake proportional, “not excessive” collection and exploitation of data is emphasized.¹² The principle of adequacy of the processing of personal data being one of the main principles of data processing has a crucial meaning in the real provision of citizen’s right to privacy.

Richard Thomas

Information Commissioner, United Kingdom
Rzecznik Informacji, Zjednoczone Królestwo

Enforcement activities – the UK’s approach

Dr Ewa Kulesza has provided powerful and widely admired leadership as the first Inspector General for Personal Data Protection in Poland. She has recognised that every independent data protection supervisory body must discharge its responsibilities, within the common EU legal framework, in ways which share with – and learn from – our fellow supervisors.

All data protection supervisory bodies face similar decisions when considering how best to use their enforcement powers and to what end. Within the UK and also within Europe there is a growing recognition of the need to use regulatory powers wisely, if we do not we risk undermining the hard work of most organisations in trying to get things right and will ultimately fail the public by misdirecting our attention away from where it will do the most good.

As the Information Commissioner for the United Kingdom, I am delighted to pay my own tribute to Ewa Kulesza by sharing our “British” strategy for taking purposeful action as a data protection regulator.

Why a strategy?

The over-riding data protection imperative of the Information Commissioner’s Office is to “*take a practical down to earth approach – simplifying and making it easier for the majority of organisations who seek to handle personal information well and tougher for the minority who do not.*” This “carrots and sticks” approach means that we will adopt a targeted, risk-driven approach to regulatory action – not using our legal powers lightly or routinely, but taking a tough and purposeful approach on those occasions where that is necessary.

This Regulatory Action Strategy elaborates that approach, setting out the nature of our various powers and when and how we plan to use them. The Commissioner intends that this Strategy should send clear and consistent signals to those who fall within the scope of data protection and related laws, to the public whom the law protects and empowers, and to the staff who act on his behalf.

What is regulatory action?

The Information Commissioner has powers to change the behaviour of organisations and individuals that collect, use and keep personal information. These powers are designed to bring about compliance with the Data Protection Act 1998 (the Act) and

¹⁰ For example, the Italian Code of Procedure and Industrial Practice in cases of information systems managed by private companies in relation to consumer credit, reliability and punctual payments, Alessandro del Ninno, *New Regulations Regarding the Processing of Personal Data in Italy: Part 1*, World Data Protection Report, BNA International (No. 4, 2005), p. 19-22.

¹¹ Working Party on the Protection of Individuals with regard to the Processing of Personal Data was introduced by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as an independent body of an advisory nature concerned with, amongst other things, the assessment of issues relating to whether the national authorities introduced by force of the Directive actually apply to the Directive in order to create a uniform application of it. More information about the Working Party Article 29 can be found on the following webpage: http://europa.eu.int/comm/justice_home/fsj/privacy/working-group/index_en.htm.

¹² For example, the Working Document No. 105 on data protection issues related to RFID technology: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm.

related laws. They include criminal prosecution, non-criminal enforcement and audit. Regulatory Action is the term used to describe the exercise of these powers.

Our aim

Our aim is to ensure that personal information is properly protected. We will do so by taking purposeful Regulatory Action where this is at risk because:

- obligations are deliberately or persistently ignored; or
- examples need to be set; or
- issues need to be clarified.

Targeted, proportionate and effective Regulatory Action will also contribute to the promotion of good practice and ensuring we remain an influential office.

Guiding principles

Regulatory Action taken by the Information Commissioner will be consistent with the five Principles of Good Regulation established by the Better Regulation Task Force.

These are:

- Transparency – We will be open about our approach to Regulatory Action and open about the action we take and the outcomes we achieve.
- Accountability – We will include information on the use of our Regulatory Action powers in our annual report to Parliament. We will make sure that those who are subject to Regulatory Action are aware of their rights of appeal.
- Proportionality – We will put in place systems to ensure that Regulatory Action we take is in proportion to the harm or potential harm done. We will not resort to formal action where we are satisfied that the risk can be addressed by negotiation or other less formal means.
- Consistency – We will apply our decision making criteria consistently in the exercise of our Regulatory Action powers.
- Targeting – We will target Regulatory Action on those areas where it is the most appropriate tool to achieve our goals. Our own targets will be based on outcomes rather than how often we use our Regulatory Action powers.

Forms of regulatory action

There are a number of tools available to the Information Commissioner for Regulatory Action. Where a choice exists, the most effective will be chosen for each situation, bearing also in mind the deterrent or educative effect on other organisations. The main options are:

- Criminal Prosecution – A sanction available where there has been a criminal breach of the Act (Section 60 Data Protection Act 1998).
- Caution – An alternative to prosecution where a criminal offence under the Act has been admitted but a caution is a more appropriate response than prosecution.

- Enforcement Notice – A formal notice requiring an organisation or individual to take the action specified in the notice in order to bring about compliance with the Act and related laws. Failure to comply with a notice is a criminal offence (Section 40 Data Protection Act 1998 and Regulation 31 Privacy and Electronic Communications (EC Directive) Regulations 2003).
 - Section 159 Order – An order requiring a credit reference agency to add a “notice of correction” to a consumer’s file (Section 159 Consumer Credit Act 1974).
 - Application for an Injunction – An injunction issued by a court under the Unfair Terms in Consumer Contracts Regulations 1999 to prevent the continued use of an unfair contract term (Regulation 12 Unfair Terms in Consumer Contract Regulations 1999).
 - Application for an Enforcement Order – An order issued by a court requiring a person to cease conduct harmful to consumers. (Section 213 Enterprise Act 2002).
 - Audit – An assessment made, with the consent of an organisation, as to whether the organisation’s processing of personal data follows good practice (Section 51(7) Data Protection Act 1998).
 - Inspection – An inspection of personal data recorded in certain European law enforcement systems in order to check compliance with the Act (Section 54A Data Protection Act 1998).
 - Negotiation – Not a formal regulatory power but a form of Regulatory Action that will be used widely in order to bring about compliance with the Act and related laws. Negotiated resolution can be backed by a formal undertaking given by an organisation to the Commissioner.
- The Commissioner also has powers available to him that can be used in connection with Regulatory Action. These are:
- Information Notice – A notice requiring an organisation or person to supply the Commissioner with the information specified in the notice for the purpose of assessing whether the Act or related laws have been complied with. Failure to comply with a notice is a criminal offence (Sections 43 and 44 Data Protection Act 1998 and Regulation 31 Privacy and Electronic Communications (EC Directive) Regulations 2003).
 - Search Warrant – Powers of entry and inspection, on application to a judge, where there are reasonable grounds for suspecting an offence under the Act has been committed or the data protection principles have been contravened (Section 50 and Schedule 9 Data Protection Act 1998).

Initiation of regulatory action

We will adopt a selective approach to initiating and pursuing Regulatory Action. Our approach will be driven by concerns about significant actual or potential **detriment**

caused by non-compliance with data protection principles or other relevant legal requirements. The criteria set out below will guide decisions about our priorities at all stages – fact-finding, initiation of action and follow-through. We will always be clear about the outcome(s) we are aiming to achieve.

The initial drivers will usually be:

- issues of general public concern (including those raised in the media);
- concerns that arise because of the novel or intrusive nature of particular activities;
- concerns raised with us in complaints that we receive;
- concerns that become apparent through our other activities.

We will initiate Regulatory Action ourselves, as well as in response to matters raised with us by others. We will undertake compliance checks with a view to identifying sectors or specific organisations for more focussed activity. In selecting areas for attention we will bear in mind the extent to which market forces can themselves act as a regulator. Thus the public sector, particularly where processing is hidden from view and where the risks of a “surveillance society” may be greater, might well receive more attention from us than the private sector.

Through these compliance checks and information that we gain from our other activities we will target particular sectors or organisations for attention. This will include audit. We will work with other EU data protection authorities, to coordinate the initiation of Regulatory Action in appropriate cases.

We will not place unreasonable demands on organisations that are selected for attention. In return we expect organisations to cooperate with us even if they are not under a legal obligation to do so. We will be prepared to identify organisations where we do not receive a reasonable level of cooperation. In return we will work with outside providers to encourage and support the development of reputable data protection audit services. We will also examine whether we can offer meaningful benefits to organisations that make use of such services or cooperate with us in other ways.

Complaints received about breaches of the law by organisations or individuals will be one driver for Regulatory Action. Not all complaints where it appears that compliance is unlikely will be referred for Regulatory Action. We will build up intelligence based on the number and nature of complaints received about particular organisations. Cases will only be taken on in the Regulatory Action Division where:

- our criteria are satisfied; and
- either a sanction for a criminal breach or formal action to bring about compliance is both a proportionate response and an outcome that is reasonably achievable.

Decision making

We will ensure that Regulatory Action we take is proportionate to the mischief it seeks to address. Both good regulatory practice and the efficient use of our limited resources require us to be selective. In determining whether to take action, the form of any action and how far to pursue it, we will apply the following criteria:

- is the past, current or prospective detriment for a single individual resulting from a “breach” so serious that action needs to be taken?
- are so many individuals adversely affected, even if to a lesser extent, that action is justified?
- is action justified by the need to clarify an important point of law or principle?
- is action justified by the likelihood that the adverse impact of a breach will have an ongoing effect or that a breach will recur if action is not taken?
- are the organisation and its practices representative of a particular sector or activity to the extent that the case for action is supported by the need to set an example?
- is the likely cost to the organisation of taking the remedial action required reasonable in relation to the issue at stake?
- does a failure by the organisation to follow relevant guidance, a code of practice or accepted business practice support the case for action?
- does the attitude and conduct of the organisation both in relation to the case in question and more generally in relation to compliance issues suggest a deliberate, wilful or cavalier approach?
- how far do we have a responsibility to organisations that comply with the law to take action against those that do not?
- would it be more appropriate or effective for action to be taken by other means (e.g. another regulator, legal action through the courts); is the level of public interest in the case so great as to support the case for action?
- given the extent to which pursuing the case will make demands on our resources, can this be justified in the light of other calls for regulatory action?
- what is the risk to the credibility of the law or to our reputation and influence of taking or not taking action?

We will give organisations an opportunity to make representations to us before we take Regulatory Action that affects them unless matters of urgency or other circumstances make it inappropriate to do so.

Attached to this strategy are some illustrative examples of where we will or will not be likely to take Regulatory Action.

Delivery

The Regulatory Action Division will be charged with delivery of this strategy. It will do so through four units:

Remedies Unit –	Responsible for the negotiated resolution of non-criminal cases where there appears to be a breach of the law and remedial action is required from the organisation in question.
Audit Unit –	Responsible for systematically checking an organisation’s compliance with the requirements of good practice.
Enforcement Unit –	Responsible for non-criminal enforcement action in cases where it is not possible or it is inappropriate to achieve remedial action by negotiation. Responsible for the initial assessment and coordination, of preprosecution work in criminal cases.
Investigations Unit –	Responsible for bringing professional investigatory skills to bear on all aspects of the Division’s work, in particular in relation to criminal cases.

These functions will require a mix of skills which will be brought to bear on project work that runs across more than one unit. This will include compliance checks.

In the interests of effective and efficient working the Commissioner will give delegated authority to the Deputy Commissioner (Data Protection) acting in consultation with either the Legal Director or Principal Solicitor to issue enforcement notices. He will give delegated authority to the Head of the Regulatory Action Division and the Head of Remedies and Audit to issue Section 159 notices.

The Regulatory Action Division (RAD) will work closely with other parts of the office. In particular, this will involve the Casework and Advice Division from which RAD will receive much of its work and the Guidance and Promotion Division (GPD) which will be giving guidance to the same organisations that RAD will be considering for Regulatory Action.

EU Third Pillar

The Third Pillar is the area of EU actually concerned with cooperation in the fields of justice and home affairs. Within the Third Pillar there are several European law enforcement institutions including Europol, Eurojust, the Schengen Information System and the Customs Information System. Each of these institutions has its own data protection supervisory body on which the Information Commissioner is represented. We are committed to making an active and effective contribution to these regulatory activities at European level. This work will be supported by the Regulatory Action Division.

Transparency

In line with the Information Commissioner’s Transparency Policy we will be open about Regulatory Action we take. We will make information available on the number of cases we pursue, their nature and the outcomes. We will also publish an occasional bulletin summarising the details of illustrative cases that have been considered for Regulatory Action.

In some cases, particularly where audit is involved; we must currently rely on the consent of an organisation as the basis for Regulatory Action. In these circumstances we may be willing to give the organisation concerned an undertaking of confidentiality

subject to our reserving the right to act on serious breaches of the law and to comply with legal obligations placed on us.

Where Regulatory Action reveals problems that are common to a particular business sector or activity and it is apparent that there is a need for general advice on the issue in question, we will make such advice available.

Regulatory Action Examples

The following are some examples of the types of conduct which will lead the Information Commissioner to consider using his formal regulatory powers. The examples are intended to be illustrative rather than exhaustive or binding. In practice all the relevant circumstances of a case will be taken into account and, in the case of criminal conduct, the Code for Crown Prosecutors will be followed.

Likely (especially after warning)

- Repeated failure to take adequate security measures.
- Collecting and retaining detailed or sensitive personal information on a “just in case” basis.
- Inaccurate or long out-dated information which impacts on career prospects.
- Seriously intrusive marketing – e.g. repeated failure to observe Telephone Preference Service requirements.
- “Professional” breaches of Section 55 (unlawful obtaining), e.g. by private investigation agencies.
- Failure to notify despite reminders.
- Denial of subject access where it is reasonable to suppose significant information is held.

Unlikely

- “Accidental” non-compliance with the Data Protection Principles – which is recognised and where effective remedial action is swiftly taken.
- Single non-criminal breaches by small businesses caused by ignorance of requirements.
- Non-compliance which is not particularly intrusive and has not caused significant detriment – e.g. a single mail shot.
- Non-compliance where other pressures – e.g. damage to reputation, may be swifter and more effective than action by a regulator.
- Business vs. business disputes where there is no detriment to customers.
- “Domestic” breaches of Section 55 (unlawful obtaining), e.g. feuding spouses or work colleagues – except where a significant abuse of trust is involved.

Dr Ewa Kulesza jako pierwszy Generalny Inspektor Ochrony Danych Osobowych w Polsce okazała się silnym i powszechnie szanowanym autorytetem. Uznała ona, że każdy niezależny organ nadzoru ochrony danych musi wypełniać swoje obowiązki wynikające ze wspólnego prawodawstwa unijnego, czerpiąc z doświadczeń organów nadzorczych z innych krajów oraz dzieląc się z nimi swoimi własnymi doświadczeniami.

Każdy organ nadzoru ochrony danych musi decydować, w jaki sposób oraz w jakim celu najlepiej wykorzystać swoje uprawnienia egzekucyjne. Zarówno w Wielkiej Brytanii, jak i w krajach europejskich, coraz silniej dostrzega się potrzebę rozważnego korzystania z uprawnień regulacyjnych, w przeciwnym razie możemy zniweczyć wysiłki wielu organizacji dobrze wykonujących swoje zadania i w efekcie zawiadziemy swoich obywateli, tracąc z oczu sprawy, które najbardziej wymagają naszej uwagi.

Jako Rzecznik Informacji Brytanii, przedstawiając strategię „brytyjską”, z przyjemnością składam swój osobisty hołd Ewie Kuleszy za podejmowanie skutecznych stanowisk regulatora ochrony danych.

Po co strategia?

Nadrzędnym obowiązkiem Rzecznika Informacji w zakresie ochrony danych jest „*przyjęcie praktycznego podejścia – upraszczać i ułatwiać działanie znajdującym się w większości organizacjom dbającym o prawidłowe traktowanie danych osobowych oraz utrudniać życie mniejszości, która to zaniedbuje*”. Taka metoda „kija i marchewki” polega na przyjęciu podejścia do postępowania regulacyjnego, opartego na analizie celów i ryzyka – a więc zamiast korzystać z naszych uprawnień w sposób łagodny lub rutynowy należy, wówczas, gdy jest to konieczne, stosować podejście stanowcze i celowe.

Strategia postępowania regulacyjnego zawiera obszerniejszy opis tego podejścia oraz przedstawia charakter naszych poszczególnych uprawnień, a także wyjaśnia, kiedy i w jaki sposób planujemy z nich skorzystać. Rzecznik pragnie, aby strategia stanowiła wyraźny i konsekwentny sygnał dla podmiotów podlegających przepisom ustawy o ochronie danych oraz ustaw pokrewnych – dla społeczeństwa, któremu ta ustawa zapewnia ochronę oraz uprawnienia, jak również dla urzędników w jego imieniu działających.

Co to znaczy postępowanie regulacyjne?

Rzecznik Informacji posiada uprawnienia umożliwiające mu zmianę zachowania organizacji oraz osób gromadzących, wykorzystujących oraz przechowujących dane osobowe. Uprawnienia te służą zapewnieniu zgodności z ustawą o ochronie danych osobowych z 1998 r. (konkretną ustawą) oraz ustawami pokrewnymi. Należą do nich postępowanie karne, egzekucja cywilna oraz kontrola. Postępowanie regulacyjne to ogólny termin obejmujący korzystanie z tych uprawnień.

Nasz cel

Naszym celem jest zapewnienie odpowiedniej ochrony danych osobowych. Będziemy to osiągać, podejmując celowe działania egzekucyjne w przypadkach, gdy ochrona danych osobowych jest zagrożona, ponieważ:

- dochodzi do umyślnego lub nagminnego naruszania obowiązków;
- potrzebne są działania podejmowane dla przykładu;
- w celu wyjaśnienia pewnych kwestii.

Odpowiednio zorientowane, współmierne oraz skuteczne postępowanie regulacyjne przyczyni się również do promowania dobrych praktyk oraz do tego, aby nasz urząd pozostał urzędem wpływowym.

Naczelne zasady

Postępowanie regulacyjne podejmowane przez Rzecznika Informacji musi spełniać pięć zasad dobrej regulacji ustalonych przez zespół zadaniowy ds. udoskonalenia regulacji.

Są to:

- | | |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Przejrzystość – | będziemy otwarcie przedstawiać nasze podejście do postępowania regulacyjnego oraz podejmowane przez nas działania, jak również osiągnięte przez nas wyniki. |
| Odpowiedzialność – | informacje na temat wykorzystanych uprawnień w zakresie postępowania regulacyjnego zawierane będą w naszym rocznym sprawozdaniu dla Parlamentu. Zadbamy o to, aby podmioty podlegające postępowaniu regulacyjnemu były świadome swoich praw do odwołania się od naszych decyzji. |
| Współmierność – | uruchomimy systemy zapewniające współmierność podejmowanego przez nas postępowania regulacyjnego do dokonanych lub potencjalnych szkód. Nie będziemy uciekać się do działań formalnych w przypadkach, gdy będziemy zdania, iż ryzyko można zażegnać na drodze negocjacji lub innych mniej formalnych działań. |
| Konsekwencja – | przy korzystaniu z naszych uprawnień w zakresie postępowania regulacyjnego będziemy dbać o konsekwentne stosowanie naszych kryteriów decyzyjnych. |
| Właściwa orientacja – | postępowanie regulacyjne będziemy koncentrować na obszarach, gdzie stanowi ono najważniejsze narzędzie dla osiągnięcia naszych celów. Nasze własne cele opierać się będą o wyniki, nie zaś o częstotliwość wykorzystania przez nas uprawnień w zakresie postępowania regulacyjnego. |

Formy postępowania regulacyjnego

Rzecznik Informacji dysponuje szeregiem narzędzi z zakresu postępowania regulacyjnego. Kiedy dostępnych ich będzie kilka do wyboru, wybrane zostanie najbardziej skuteczne dla danej sytuacji, przy czym należy mieć na względzie odstraszący lub wychowawczy wpływ na inne organizacje. Główne możliwości obejmują:

Postępowanie karne –	sankcja dostępna w przypadku karnego naruszenia ustawy (paragraf 60 ustawy o ochronie danych osobowych 1998).
Upomnienie –	alternatywa wobec postępowania karnego w przypadku, gdy doszło do popełnienia przestępstwa na mocy ustawy, lecz upomnienie stanowi bardziej odpowiednią reakcję niż postępowanie karne.
Zawiadomienie o egzekucji –	formalne zawiadomienie zawierające żądanie podjęcia przez organizację lub osobę będącą jego adresatem działań określonych w zawiadomieniu, w celu zapewnienia zgodności z ustawą oraz ustawami pokrewnymi. Niezastosowanie się do zawiadomienia stanowi przestępstwo [paragraf 40 ustawy o ochronie danych osobowych 1998 oraz rozporządzenie 31 o prywatności i łączności elektronicznej – <i>Privacy and Electronic Communications</i> (Dyrektywa WE) Rozporządzenie 2003].
Nakaz na mocy paragrafu 159 –	nakaz zobowiązujący agencję informacji kredytowej do dodania adnotacji „wezwanie do poprawy” do akt konsumenta (paragraf 159 ustawy o kredycie konsumenckim – <i>Consumer Credit Act 1974</i>).
Wniosek o wydanie nakazu sądowego –	nakaz sądowy wydany na mocy rozporządzenia o nieuczciwych warunkach umów konsumenckich – <i>Unfair Terms in Consumer Contracts</i> 1999 – w celu zapobiegnięcia dalszemu stosowaniu niedozwolonych postanowień umownych (rozporządzenie 12 <i>Unfair Terms in Consumer Contract</i> 1999).
Wniosek o wydanie nakazu egzekucyjnego –	nakaz sądowy zobowiązujący daną osobę do zaprzestania postępowania szkodliwego dla konsumentów (paragraf 213 ustawy o przedsiębiorstwach – <i>Enterprise Act</i> 2002).
Audyt –	przeprowadzona za zgodą danej organizacji ocena zgodności stosowanych przez organizację procedur przetwarzania danych osobowych z zasadami dobrej praktyki [paragraf 51(7) ustawy o ochronie danych osobowych 1998].
Inspekcja –	inspekcja danych osobowych zarejestrowanych w niektórych systemach egzekucji prawa europejskiego w celu zbadania zgodności z ustawą (paragraf 54A ustawy o ochronie danych osobowych 1998).
Negocjacje –	nie jest to formalne uprawnienie regulacyjne, lecz forma postępowania regulacyjnego, która będzie powszechnie stosowana w celu zapewnienia zgodności z ustawą oraz ustawami pokrewnymi. Wynegocjowane rozwiązanie można poprzeć formalnym zobowiązaniem złożonym wobec Rzecznika przez organizację.

Rzecznik dysponuje również uprawnieniami, z których może skorzystać w związku z postępowaniem regulacyjnym. Są to:

Wezwanie do udzielenia informacji –	wezwanie zobowiązujące organizację lub osobę do udzielenia Rzecznikowi informacji określonej w wezwaniu w celu dokonania oceny zgodności z ustawą lub ustawami pokrewnymi. Niezastosowanie się do zawiadomienia stanowi przestępstwo [paragraf 43 i 44 ustawy o ochronie danych osobowych 1998 oraz rozporządzenie 31 o prywatności i łączności elektronicznej – <i>Privacy and Electronic Communications</i> (Dyrektywa WE) rozporządzenie 2003].
Nakaz rewizji –	uprawnienie do wkroczenia na teren oraz dokonania inspekcji, na wniosek sędziego, w przypadku istnienia uzasadnionych podstaw do podejrzenia popełnienia przestępstwa na mocy ustawy oraz naruszenia zasad ochrony danych (paragraf 50 oraz załącznik 9 do ustawy o ochronie danych osobowych 1998).

Wszczęcie postępowania regulacyjnego

W zakresie wszczęcia i realizacji postępowania regulacyjnego przyjmujemy podejście selektywne. Podejście to wynika z problemów związanych z istotnymi, aktualnie zachodzącymi lub potencjalnymi **zjawiskami szkodliwymi**, spowodowanymi nieprzestrzeganiem zasad ochrony danych lub innych istotnych wymogów prawnych. Poniższe kryteria stosowane będą do decyzji podejmowanych w sprawie naszych priorytetów na wszystkich etapach – zbieranie informacji, wszczynanie działań i kontynuacja działań. Zawsze będziemy w sposób jasny określać cele, które pragniemy osiągnąć.

Początkowo głównymi podstawami do wszczynania postępowania regulacyjnego będą:

- kwestie związane z interesem publicznym (łącznie z problemami opisywanymi w mediach);
- kwestie wynikające z nowatorskiego lub konfliktowego charakteru poszczególnych działań;
- problemy zgłaszane nam w otrzymywanych przez nas skargach;
- problemy ujawniające się w trakcie realizowania przez nas innych działań.

Zamierzamy wszcząć postępowanie regulacyjne z własnej inicjatywy, jak również w odpowiedzi na problemy zgłaszane nam przez inne osoby. Przeprowadzać będziemy badania zgodności w celu identyfikacji konkretnych sektorów lub organizacji, co pozwoli na lepsze pozycjonowanie naszych działań. W trakcie selekcji obszarów naszego zainteresowania uwzględniać będziemy to, w jakim zakresie regulacją może zająć się sam wolny rynek. Dlatego też w większym stopniu, niż sektorem prywatnym, zajmować się będziemy sektorem publicznym, zwłaszcza w sytuacjach, gdy przetwarzanie danych będzie tam niejawnie i w przypadku, gdy większe może być zagrożenie pojawienia się „społeczeństwa pod nadzorem”.

Realizując wspomniane badania zgodności oraz analizując dane zebrane w trakcie innych działań, identyfikować będziemy określone sektory lub organizacje, które stano-

wić będą przedmiot naszych działań, co obejmować będzie również kontrole. Będziemy współpracować z innymi unijnymi organami ds. ochrony danych, w celu koordynacji realizacji postępowania regulacyjnego w odpowiednich przypadkach.

Nie będziemy stawiać nierealistycznych wymagań organizacjom wybranym przez nas jako przedmiot zainteresowania. Oczekujemy natomiast od nich współpracy nawet, jeżeli nie zobowiązują ich do takiej współpracy wymogi prawne. Będziemy również identyfikowali organizacje, które nie będą z nami współpracować w wystarczającym stopniu i współdziałali z niezależnymi dostawcami tak, aby stymulować i wspierać rozwój renomowanych usług kontrolnych związanych z ochroną danych. Będziemy także rozważać możliwość zaoferowania istotnych korzyści organizacjom korzystającym z takich usług lub współpracującym z nami w inny sposób.

Jedną z podstaw do wszczęcia przez nas postępowania regulacyjnego będą otrzymywane przez nas skargi dotyczące przypadków naruszenia prawa przez organizacje lub osoby fizyczne. Nie wszystkie skargi sugerujące brak zgodności będą podstawą do wszczęcia postępowania regulacyjnego. Będziemy gromadzić informacje w oparciu o liczbę i charakter otrzymywanych przez nas skarg dotyczących konkretnych organizacji. Postępowanie w pionie postępowań regulacyjnych wszczynać będziemy tylko w przypadku, gdy:

- spełnione będą nasze kryteria;
- sankcja z tytułu popełnienia przestępstwa lub postępowanie formalne mające wymusić zgodność jest współmierne do skali naruszenia oraz gdy w rozsądnym zakresie możliwe jest w ten sposób osiągnięcie założonych celów.

Podejmowanie decyzji

Będziemy upewniać się, że podejmowane przez nas postępowania regulacyjne będą współmierne do rozmiaru przewinienia, na które będą odpowiedzią. Zarówno dobre praktyki regulacyjne, jak i wydajne korzystanie z naszych ograniczonych zasobów wymagają działania w sposób selektywny. W celu ustalenia, czy konieczne jest podjęcie działań, w jakiej formie i na jaką skalę należy te działania podjąć, stosować będziemy następujące kryteria:

- czy poprzednie, aktualne lub potencjalne szkody przypadające na jedną osobę, wynikające z „naruszenia” są tak istotne, że należy zareagować;
- czy szkodliwy wpływ wynikający z „naruszenia” dotyka tak dużej liczby osób, że usprawiedliwia to reakcję;
- czy działania usprawiedliwione są koniecznością wyklarowania istotnej kwestii związanej z przepisami prawa lub innymi zasadami;
- czy działania usprawiedliwia prawdopodobieństwo tego, że negatywne skutki naruszenia będą mieć trwałe konsekwencje lub, że w przypadku niepodjęcia działań naruszenie powtórzy się;
- czy dana organizacja i jej praktyki są typowe dla określonego sektora lub rodzaju działalności do tego stopnia, że podjęcie działań jest konieczne „dla przykładu”;

- czy prawdopodobne koszty, które dana organizacja poniesie w wyniku podjęcia wymaganych działań zaradczych, są współmierne do skali problemu;
- czy nieprzestrzeganie przez organizację odpowiednich zaleceń, zasad postępowania lub przyjętych praktyk usprawiedliwia reakcję;
- czy postawa i zachowanie się organizacji zarówno w odniesieniu do danej kwestii, jak i w bardziej ogólnym ujęciu, w odniesieniu do przestrzegania zasad ochrony danych sugerują, że są to działania podejmowane celowo, umyślnie lub arogancko;
- jak bardzo jesteśmy zobowiązani – względem organizacji, które przestrzegają prawa – do podejmowania działań wobec organizacji, które prawa nie przestrzegają;
- czy bardziej właściwa lub skuteczna byłaby realizacja innych środków (np. przez inny organ nadzoru, poprzez wszczęcie postępowania sądowego); czy interes publiczny jest w tym przypadku tak istotny, że usprawiedliwiałby takie działania;
- uwzględniając to, jak bardzo podjęcie danych działań obciążać będzie nasze zasoby, czy działania te są usprawiedliwione w obliczu konieczności wszczynania innych postępowań regulacyjnych;
- jakie są zagrożenia dla wiarygodności przepisów prawa lub naszej reputacji i jakie będą skutki podjęcia działań oraz ich niepodjęcia.

Zaoferujemy organizacjom możliwość składania nam deklaracji przed wszczęciem przez nas postępowania regulacyjnego, które będzie miało wpływ na daną organizację, chyba że uniemożliwi nam to wymóg pilnego rozpatrzenia danej sprawy lub inne okoliczności.

Do niniejszej strategii dołączyliśmy kilka przykładowych sytuacji, w których raczej będziemy lub raczej nie będziemy wszczynać postępowania regulacyjnego.

Realizacja

Realizacją strategii zajmować się będzie pion postępowań regulacyjnych. Realizacja ta odbywać się będzie za pośrednictwem następujących jednostek:

- | | |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jednostka Zaradcza – | zajmować się będzie negocjowaniem rozwiązań w przypadkach niemających znamion przestępstwa, w sytuacjach, w których domniemane jest naruszenie prawa, a w stosunku do danej organizacji wymagane jest podjęcie czynności zaradczych. |
| Jednostka Kontrolna – | odpowiedzialna za systematyczną kontrolę zgodności danej organizacji z wymogami dobrych praktyk. |
| Jednostka Wykonawcza – | odpowiedzialna za działania egzekucyjne w sprawach niemających znamion przestępstw, w przypadkach, w których niemożliwe lub niewłaściwe będzie zrealizowanie działań zaradczych w drodze negocjacji. Odpowiedzialna za wstępną ocenę i koordynację oraz działania poprzedzające czynności prokuratorskie w przypadkach, w których dojdzie do przestępstw. |

Jednostka Badawcza – odpowiedzialna za zapewnienie profesjonalnych usług badawczych dotyczących wszystkich aspektów działania pionu, w szczególności w odniesieniu do przestępstw.

Funkcje te będą wymagać połączenia wielu umiejętności, które będą wykorzystywane w ramach projektu realizowanego przez wiele jednostek. Dotyczy to również kontroli zgodności.

W celu zapewnienia skuteczności i wydajności działań, Rzecznik nada Zastępcy Rzecznika (Ochrony Danych), działającemu w porozumieniu z Dyrektorem Prawnym lub Głównym Radcą Prawnym, odpowiednie uprawnienia do wystawiania zawiadomień o egzekucji. Nada on również Kierownikowi Pionu Postępowań Regulacyjnych oraz Kierownikowi Działu Środków Zaradczych i Kontroli uprawnienia do wystawiania zawiadomień z tytułu paragrafu 159.

Pion postępowań regulacyjnych (RAD) będzie ściśle współpracować z innymi jednostkami urzędu. W szczególności obejmować to będzie Pion Pomocniczo-doradczy, który w dużym stopniu wspierać będzie RAD oraz Pion ds. Zaleceń i Promocji (GPD), który udzielać będzie zaleceń organizacjom typowanym przez RAD do wszczęcia postępowania regulacyjnego.

Trzeci filar UE

Trzeci filar to obszar UE związany ze współpracą w wymiarze sprawiedliwości i w zakresie spraw wewnętrznych. Trzeci filar obejmuje różne europejskie instytucje wymiaru sprawiedliwości, takie jak Europol, Eurojust, System Informacyjny Schengen (Schengen Information System) oraz System Informacji Celnej (Customs Information System). Każda z tych instytucji posiada własne organy nadzoru zajmujące się ochroną danych, w których Komisarz ds. Informacji ma swoich przedstawicieli. Pragniemy w sposób aktywny i skuteczny wspomagać te działania regulacyjne na poziomie europejskim. Prace te wspierane będą przez pion postępowań regulacyjnych.

Przejrzystość

Zgodnie z polityką przejrzystości Komisarza ds. Informacji będziemy udostępniać informacje na temat wszczynanych przez nas postępowań regulacyjnych. Będziemy upubliczniać informacje na temat liczby prowadzonych przez nas spraw, ich charakteru oraz wyniku postępowania. Będziemy również, co pewien czas publikować biuletyn podsumowujący szczegóły przykładowych spraw, które typowane były do postępowania regulacyjnego.

W niektórych przypadkach, szczególnie w sytuacji, gdy przeprowadzana ma być kontrola, do wszczęcia postępowania regulacyjnego niezbędna będzie nam zgoda danej organizacji. W takim przypadku możemy być skłonni do złożenia zobowiązania do zachowania poufności na rzecz danej organizacji, z zastrzeżeniem prawa do podjęcia stosownych działań w przypadku poważnego naruszenia przepisów prawa oraz z zastrzeżeniem wymogu spełniania wiążących nas zobowiązań prawnych.

W przypadku, gdy postępowanie regulacyjne ujawni problemy, które są powszechne w danym sektorze gospodarki lub w danej działalności i oczywistym stanie się, że istnieje

potrzeba sformułowania ogólnych zaleceń dotyczących danej kwestii, zalecenia takie zostaną przez nas przygotowane.

Przykłady postępowań regulacyjnych

Poniżej zamieściliśmy przykłady zachowań, które mogą być dla Komisarza ds. Informacji podstawą do skorzystania z przysługujących mu uprawnień regulacyjnych. Przykłady mają charakter poglądowy, a nie wyczerpujący lub wiążący. W praktyce uwzględniane będą wszystkie istotne okoliczności sprawy, a w przypadku postępowania karnego przestrzegany będzie „Kodeks Prokuratorów Korony” (*Code for Crown Prosecutors*).

Postępowanie regulacyjne prawdopodobne (zwłaszcza po udzieleniu upomnienia)

- Częste przypadki niepodjęcia właściwych środków bezpieczeństwa.
- Zbieranie i przechowywanie szczegółowych lub poufnych danych osobowych „na wszelki wypadek”.
- Przechowywanie informacji błędnych lub dawno nieaktualnych, wpływających na możliwości rozwoju kariery.
- Wyjątkowo nachalny marketing – np. częste przypadki nieprzestrzegania wymogów usługi *Telephone Preference Service*.
- Naruszenia paragrafu 55 (bezprawne pozyskanie) w ramach realizacji działalności zawodowej, np. przez prywatne agencje detektywistyczne.
- Niepowiadamianie pomimo monitów.
- Nieudzielanie dostępu w sytuacjach, gdy istnieją uzasadnione przesłanki, aby sądzić, że przechowywane są istotne informacje.

Postępowanie regulacyjne mało prawdopodobne

- „Niezamierzona” niezgodność z zasadami ochrony danych – po jej uznaniu i po szybkim podjęciu skutecznych środków zaradczych.
- Pojedyncze naruszenia niemające znamion przestępstwa, popełniane przez małe przedsiębiorstwa w wyniku nieznamienności wymogów.
- Przypadki niezgodności, które nie powodują poważnych komplikacji ani znaczących szkód – np. pojedyncza akcja mailingowa.
- Niezgodność w przypadku, gdy inne formy nacisku – np. groźba utraty reputacji – mogą zadziałać szybciej i bardziej skutecznie niż postępowanie wszczęte przez organ regulacyjny.
- Konflikty pomiędzy przedsiębiorstwami niepowodujące szkody dla klientów.
- „Wewnętrzne” naruszenia paragrafu 55 (bezprawne pozyskanie), np. przez skłóconych małżonków lub kolegów z pracy – w przypadku, gdy doszło do istotnego nadużycia zaufania.

Alex Türk

President, French Data Protection Authority
Przewodniczący Komisji Ochrony Danych Osobowych, Francja

Contribution of CNIL to the work, as a tribute to Mrs Kulesza

Ensuring confidentiality of personal data in court decisions published on the Internet

The openness of the hearing, the open nature of court decisions and freedom of communicating verdicts and rulings to any person that requires to be informed thereof are among the basic guarantees that were sanctioned, in particular, by Article 6 of the European Convention on the Protection of Human Rights and Fundamental Freedoms and have long been introduced in various national law provisions.

Nevertheless, it would be hard to find it natural that the open nature of a court decision containing names of the parties and recorded in a database is sufficient to digitalize it and make it generally available for an indefinite time. Moreover, if a judge in France may for certain disputes order that a given decision be made public or published in the printed press or using any audio-visual communication medium, then this publication is governed by certain rules. It is time-limited and must be detailed as to the decision itself, but in a way it is an additional punishment, at least in penal terms. In the light of such provisions, is it not therefore, a new punishment in a form of „digital announcement“ to publish court decisions containing names of the parties on the Internet?

The development of information technology has made it much easier to use judicial decisions and made it possible to create judicial databases. Consequently, courts in France started creating databases as early as in the 1980s, collecting their decisions there to assist court members in internal document searches. At the same time, data banks containing judicial decisions were created, at the initiative of both private and state institutions, to be remotely available on the Internet for those who paid the subscription or for the public at large.

For some years now, it has been enough to enter any person's name in the search engine to obtain, free of charge, any related details of various type dispersed on the global net, although originating from many remote locations. That means that if a person's name was mentioned in any court decision available on the Internet and if that decision is indexed by a search engine, it will be automatically made available for each user. An Internet user does not even have to go to a specific website, and the decision does not have to be the subject of the search. Going beyond the open nature of proceedings and of the decision itself, which may be available to any enquiring party, the universal and permanent availability of personal data poses a serious risk of breaches of privacy and makes the right to erase an act ineffective.

This conclusion made the French Data Protection Agency (CNIL) adopt on 29 November 2001 guidelines on publishing personal data on the Internet by data banks containing judicial decisions,¹ and then, four years later, develop a summary report of compliance with the guidelines. That was an opportunity to analyze the approach of the remaining European Union countries in this respect.

I. Recommendation of CNIL of 2001

According to this Recommendation, court decisions that are generally available on the Internet and only those decisions, may no longer contain names or addresses of the parties to the proceedings, regardless of the nature of the proceedings.

The Recommendation emphasizes the risks involved in publishing court decisions that reveal the parties' identity in the context of these persons' rights and liberties, especially considering that those decisions may still not be final. Consequently, a legal document search engine might become a real personal data catalogue. Regardless of the nature of dispute, the information on being a party or a witness is itself enough to cause prejudice: a trivial dispute between neighbours may lead one to believe that the plaintiff is a litigant and the respondent is difficult to get along with, free dissemination of court decisions on the Internet might discourage an employer from hiring such a person and a lessor from entering into a lease agreement etc.

CNIL even recommended that names and addresses of witnesses be removed from decisions freely available on the Internet.

The Recommendation also introduced a distinction between databases which are freely available on the Internet and those which provide paid access. This distinction was mainly based on the assumption that the alleged risk of abusing the information coming from court decisions is lesser if such information is not available through search engines, that is, it can only be reached either through a paid website, or it is stored on a CD-ROM that one would have to buy to use. Not to blow the issue out of proportion, CNIL recognized that for paid websites and CD-ROMs there are no grounds to conceal the identity of parties and witnesses if their names are mentioned, which is not a general rule. However, taking into account the fact that court decisions and rulings sometimes provide parties' addresses which are of no value for the records while they might help locate a particular person, CNIL found it advisable to keep confidential addresses of parties in court decisions that might be published in the future on CD-ROMs or on specialized, limited-access websites.

Was the recommendation complied with?

The fundamental measure was taken when in 2002 the government decided to implement the CNIL's Recommendation undertaking to ensure, until September 2002, the anonymity of court decisions available online, on the official Légifrance legal website, and then, within two years, to ensure the anonymity of all previous decisions. Consequently, the major and generally available French website with databases containing

¹⁾ Resolution 01-057 of 29 November 2001 on guidelines on the dissemination of personal data on the Internet by data banks containing judicial decisions, enclosed as an appendix.

court decisions is being adapted to comply with the CNIL's recommendation. Nevertheless, the process of ensuring anonymity of court decisions passed before 2002 could not be finalized, mainly due to technical restraints and costs. The requirement will be met no sooner than in 2008, which is when the IT system of official journals allows speeding up the process of ensuring anonymity.

As concerns private website operators, one can conclude that, even though there has been a great improvement in the performance of software anonymity ensuring, making it much faster to anonymize data and easier to ensure confidentiality, some websites, especially the ones run by professional lawyers which provide public access to court decisions, do not always ensure the anonymity of these decisions. As for limited-access databases of judicial decisions, the ensuring of anonymity for penal cases is a rule and parties' addresses are usually deleted.

Despite those successes, the 2001 Recommendation is still being questioned by some individuals whose responsibility is to maintain legal documents or by some judicial bodies, for example by the highest level of the administrative judiciary, the Council of State, which keeps publishing decisions containing disclosed personal data on its own website. The Council of State believes that *„ensuring the anonymity of administrative court decisions on a regular basis makes it difficult for the lawyers to search for the adequate judicial decisions and use them. As it happens, decisions have always been identified by parties' names in the administrative law, which helps to memorize by the legal rule and invoke it before the judge. Making data confidential undermines this traditional practice".*

Taking such continuous objections into consideration, CNIL adopted a decision in February 2005 on summarizing the applicability of the recommendation. Among the major issues to be provided in the summary was the comparison of methods in which the anonymity of decisions was addressed in other European Union countries. Such analysis was made possible by the cooperation with those European data protection authorities which were kind enough to respond to the questionnaire sent by CNIL. We wish to take this opportunity to thank them once again, as their contribution was of vital importance for the direction taken by CNIL's in its further considerations.

II. Ensuring the confidentiality of personal data contained in court decisions in European Union countries

1. First note: in some countries there exists a tradition of complete confidentiality of personal data contained in court decisions, whatever the medium used.

In **Germany** and **Austria**, confidentiality of all court decisions is traditionally ensured, which helps avoid the issue of reconciling publication of court decisions on the Internet with the observance of the principle to protect personal data. Courts themselves are concerned with ensuring confidentiality of personal data. If a person's name is accidentally disclosed, the error is immediately corrected.

Poland also decided to keep confidential personal data contained in court decisions published. Decisions are identified by their numbers rather than by parties' names.

In **Hungary**, compilations of major court decisions are made in compliance with anonymity requirement, whatever the medium used. Moreover, the Hungarian data protection authority determined that a court decision may be published on the Internet only when approved by a person mentioned in such decision, unless a statutory provision expressly provides otherwise.

Note that in most countries the national legislation admits cases where, due to the nature of a decision (disputes concerning the degree of relationship, sexual violence etc.), parties' names may not be disclosed, whatever the medium used. Of course, this duty remains in force for publishing decisions on the Internet.

For instance, the **Maltese** law enforces the confidentiality of personal data contained in court decisions depending on the nature of a decision (medical case, impropriety, nullity of marriage, separation). This rule applies to decisions published on the Internet while other legal decisions published on the Internet are not anonymous.

2. Some countries have adopted special legislation, with applicable provisions to govern the publication of court decisions not covered by the principle of personal data confidentiality.

In **Estonia**, the publishing of court decisions on the Internet is subject to the provisions of the code of criminal procedure and the code of civil procedure passed in 2004, which provide that published court decisions may enable the identification of the parties (confidentiality of names, birthdate, address etc.), if such identification might breach the privacy of such a person. For persons whose personal data were published before 2004, the Estonian data protection authority admits the possibility of requesting that the aforementioned provisions be applied.

In **Italy**, the publishing of court decisions is subject to special legislative provisions which are, to a great extent, based on the approach adopted on that matter by the Italian personal data protection authority. The Italian legislation gives every person having reasonable grounds the right to file with the court's office a request to remove personal data related to that person from a decision, if the decision is to be published, whatever the medium used. The decision whether or not to grant that request is taken by the court that passed a decision to which the request refers.

The publishing of **Swedish** court decisions is subject to the provisions of the resolution of 1999 which, on the one hand, introduces the principle of free access to information, and on the other hand, governs the terms on which to publish personal data. All Swedish courts must ensure access – also through the Internet – to decisions that they consider of importance. Decisions are identified by date and number. They may not contain data of personal nature. Such data may be only recorded in decisions by the European Court of Justice (together with decisions passed by Swedish courts), as they are not subject to the anonymity ensuring procedure.

In **Luxembourg**, although the matter of publishing court decisions is not governed by special legislative provisions, principles based on practice apply. The personal data confidentiality procedure is constantly applied to judicial decisions made by administrative courts, as available on the Ministry of Justice website. Court databases are not yet available on the Internet, but the database managed by the General Public Prose-

cutor's Office, which can be used by professional lawyers, ensures the confidentiality of personal data. In penal law, full transcripts of court decisions may be made available only in anonymized versions, unless they are issued to individuals to whom they directly relate (attorneys, parties to the proceedings etc.). In civil law, the decision whether or not to provide transcripts to third parties is to be taken by the president of the court that passed a given decision. For divorce, adoption, affiliation or bastardy cases, determining the legal status etc., only copies with concealed personal data are issued. These provisions do not prevent professional lawyers from being able to hold complete sets of decisions containing disclosed personal data.

3. In some countries, the issue of publishing court decisions on the Internet was related to the **approach adopted by the personal data protection authority**.

In **Finland**, even though the personal data protection authority recognized it is not competent to determine the manner in which courts should fulfill the duty to inform the public, it still suggested that court decisions published on the Internet should not contain personal data.

In 2000, a complaint was filed with the **Portuguese** personal data protection authority regarding the publishing of penal court decisions containing parties' names on the Ministry of Justice website. The authority has decided to block the access to the website until the anonymity of those decisions is ensured.

The Portuguese authority issued an official statement in which it spoke in favour of applying the provisions on personal data protection to databases containing judicial decisions. If such databases do not ensure anonymity, the data protection authority should be notified thereof. The Portuguese authority in principle recommends that data should be anonymized in those databases and enforces anonymity in penal cases, affiliation cases, divorces and any other disputes which may affect private lives of parties involved. In practice, this recommendation resulted in all court decisions published on the Internet being anonymous.

The **Dutch** personal data protection authority officially decided in favour of ensuring a full anonymity of court decisions published on the Internet, due to the specific nature of this medium and due to there being no way of controlling the manner in which data can be used. The authority published its recommendations as to the ensuring of anonymity. Consequently, all decisions published on the official website (www.rechtspraak.nl) contain anonymized data.

In **Greece**, the Council of State filed an inquiry with the data protection authority, which in its decision of 25 October 2000 found that publishing court decisions in legal reviews should be compliant with the data confidentiality requirement. Usually, no published court decisions contain personal data, whatever the medium used.

The **Belgian Commission** addressed the issue of judicial decisions' databanks. It recognized that the technological progress which creates greater opportunities for information searching should go hand in hand with greater restraints on the entering of data allowing party identification to automated chronicles of judicial decisions. The Commission also found that the methods of using the electronic media intended for

publishing judicial decisions allow distorting the purpose of processing the data contained in documents by formulating queries based on parties' names.

Therefore, the Belgian commission recommends that names of third parties (witnesses) to disputes should not be provided in decisions. It also invokes Article 2 of the royal resolution of 7 July 1997 on publishing decisions by the Council of State, which provides that every party to a dispute has a right to refuse to have its name published. This provision does not, however, stipulate the ways of informing the parties or manners of enforcing the right of refusal. The Commission recommends that as soon as the court proceedings commence, all parties should receive a form clearly informing them of the aforementioned right and providing the ways of enforcing this right. The Commission believes that the right to refuse to have one's name published by the parties should be accompanied by the court's ability to make such a decision, whereby the court should decide whether or not to ensure anonymity of a given decision.

The Belgian Commission is of the opinion that, as an alternative, the right to give consent could be established: at the time of initiating a dispute in court, the parties would be requested to state using an official form whether or not they agree to have their personal data processed when the decision is published. In case of missing consent or a refusal, it would be required to „*depersonalize*” data each time the decision is published electronically.

The **Latvian** data protection authority received an enquiry from the Ministry of Justice on the conditions under which court decisions can be published in compliance with legal requirements. The authority decided that to protect privacy of the parties involved, court decisions published on the generally available websites must be anonymized.

In the **Czech Republic**, Internet access is only provided for decisions by the Supreme Administrative Court, only for 15 days and without ensuring the anonymity of personal data. The data protection authority generally recommended, considering the prospects of publishing all decisions of Czech supreme courts, that the anonymity of such decisions must be ensured due to the risks run by the parties involved and due to the fact that data publication might be considered as an additional punishment.

The **Irish** law protects the parties' identities in decisions concerning rape cases or in disputes subject to family law. The Irish data protection authority recommended that anonymity of decisions be ensured provided that the statutory information obligations applicable to respective courts are complied with.

In the **United Kingdom**, the issue of publishing court decisions is governed neither by law, nor by practice. When court decisions are published on the Internet, some of them do not contain disclosed personal data.

III. January 2006: CNIL reaffirms and strengthens its position

As has already been said, the comparative analysis was one of the decision-making elements that drove CNIL not only to reaffirm its position expressed in 2001 but also to strengthen it.

Recognizing that, in terms of ensuring anonymity, that position was not isolated and that some countries went even further, CNIL decided that the French practice of publishing databases containing judicial decisions on the Internet – whatever the access method – or on CD-ROMs must be kept in line with the European tendency of heightened protection of individuals.

Looking from that perspective, the arguments related to the technological progress seemed too weak. It was found that by applying adequate technical tools the risk involved in publishing court decisions on the Internet can be reduced and that a distinction should be made between respective websites, depending on whether decisions published therein might be directly indexed by search engines. Technical changes implemented on the Légifrance website made court decisions published therein no longer available through a query entered in a public search engine. Moreover, there is a technical possibility of removing the option to use the database of judicial decisions to search for a court decision by entering the name of any of the parties.

CNIL is in favour of using adequate technical tools to control Internet access to databases containing judicial decisions, but it also stresses that none of such methods will effectively and permanently prevent abuse of such databases available on the Internet.

Moreover, if a given website's operator no longer ensures the possibility of submitting a query related to names of parties into the judicial decision database, such a query can still be created using the so-called global search, that is using the option generally enabled by every website. The Légifrance website also provides such an option. This means that the risk of privacy breach resulting from the possibilities offered by the Internet may only be prevented by ensuring universal anonymity of court decisions published on the publicly available websites.

Irrespective of technical debates, CNIL dealt with the consequences of the transposition of the Directive of the European Parliament and of the Council 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which transposition was delayed and took place during the adoption of the law of 6 August 2004.

Databases containing judicial decisions, if they include personal data of the parties, automatically process personal data and thus are subject to the provisions of the law of 6 January 1978, amended in August 2004. Moreover, where databases contain verdicts passed by penal courts, then such data processing falls under a specific category of processing data of criminal convictions.

Therefore, amendments to the personal data protection law introduced by the law of 6 August 2004 have consequences for the system used for databases containing judicial decisions, whatever the access method.

Directive 95/46 also stipulates in Recital 30 that in order to be lawful, the processing of personal data must, in addition, be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a

natural or legal person, provided that the interests or the rights and freedoms of the data subject do not prevail. These principles were in particular explained in Article 7 of the Directive, which provides that Member States admit personal data processing only when the data subject has given its express consent to do so or if any of the conditions listed in Article 7 was met, for example performance of the contract or compliance with a legal obligation.

Article 7 of the French law amended in August 2004 also provides that personal data may be processed only if the data subject has unambiguously given his consent or upon meeting one of the following conditions:

"1° Processing is necessary for compliance with a legal obligation to which the data processing controller is subject.

2° Processing is necessary in order to protect the vital interests of the data subject.

3° Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

4° Performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

5° Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, provided that the interests for fundamental rights and freedoms of the data subject are not breached."

Consequently, clause 3° expressly permits the courts that issue given decisions to create databases containing these judicial decisions, keeping the names and strictly for internal use as long as this meets the definition of performing a public interest task. On the other hand, private operators of databases containing judicial decisions may not effectively invoke clause 5°. Publishing databases containing judicial decisions on websites with limited access or on CD-ROMs may be consistent with a reasonable interest of individuals responsible for such data processing, but it means breaching the rights and basic liberties of the individual to which the data relate. Therefore, taking into account the special nature of information contained in such databases, CNIL believes that the objection formulated in Article 7-5° of the law is not applicable in this case.

Paragraph 5 of Article 8 of the Directive* 95/46 provides that „Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of the official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of the official authority."

This provision was transposed to the French law (Article 9) in August 2004, which reads as follows:

„Personal data relating to offences, criminal convictions or security measures may be carried out only by:

* For the official translation of the Directive go to: www.europa.eu.int/eur-lex/pl (translator's note.).

1° Courts, national authorities and legal persons in charge of government services acting within their delegated powers.

2° Law enforcement employees strictly for the purposes of duties entrusted to them pursuant to applicable regulations.”

CNIL concluded that creation of databases of the criminal courts’ decisions specifying names of convicted individuals, by private operators would constitute an offence. Besides, CNIL believes that the laws require private operators to keep confidential details of parties and witnesses related to decisions published as part of their activities.

Lastly, contrary to the expectations of certain milieus, CNIL did not soften its position of 2001. On the contrary – it has strengthened it, by removing an exception previously provided for databases with limited, and particularly paid access.

Summarizing the above activities was not only interesting because it showed the extent of work carried out by CNIL. Most of all, it showed that the European Directive on the Protection of Personal Data plays a vital role in the harmonization of approaches throughout different European countries, even in those areas in which every country and every national data protection authority enjoys the broadest freedom. It would be difficult to believe that any single country would choose its own path without considering the choices made by its partners. Considering that the Internet is an area of expertise particularly difficult to regulate by a single country, such approach would be highly unreasonable.

Wkład CNIL w dzieło, jako wyraz uznania dla Pani Kuleszy

Utajnianie danych osobowych w decyzjach sądowych publikowanych w Internecie

Jawność rozpraw, jawny charakter decyzji sądowych oraz swobodne przekazywanie wyroków i orzeczeń każdej żądającej tego osobie należą do podstawowych gwarancji, usankcjonowanych w szczególności przez artykuł 6 europejskiej „Konwencji o ochronie praw człowieka i podstawowych wolności” i od dawna wprowadzonych w różnych przepisach prawa krajowego.

Niemniej jednak, trudno byłoby uznać za naturalne, że jawny charakter decyzji sądowej, w której figurują nazwiska stron i umiejscowionej w bazie danych, wystarcza do jej cyfryzacji i powszechnego udostępnienia na czas nieokreślony. Ponadto, jeśli we Francji w przypadku pewnych określonych sporów sędzia może zarządzić podanie do publicznej wiadomości lub publikację konkretnej decyzji w prasie drukowanej lub za pomocą dowolnego środka komunikacji audiowizualnej, to taka publikacja odbywa się zgodnie z określonymi zasadami. Jest ograniczona w czasie i musi być uszczegółowiona w samej decyzji, jednak w pewnym sensie stanowi dodatkową karę, przynajmniej w dziedzinie karnej. Czy w świetle takich postanowień wprowadzenie do Internetu decy-

zji sądowych zawierających nazwiska stron nie stanowi swego rodzaju nowej kary polegającej na „obwieszczeniu cyfrowym”?

Rozwój informatyki znacznie ułatwił korzystanie z orzecznictwa i umożliwił tworzenie prawniczych baz danych. I tak, sądy we Francji już od lat 80. zaczęły tworzyć bazy danych, gromadząc w nich wydane przez siebie decyzje po to, by ułatwić swoim członkom wewnętrzne wyszukiwanie dokumentów. Równocześnie, z inicjatywy państwowej lub prywatnej powstawały banki danych zawierające orzecznictwo, dostępne zdalnie przez Internet, po wykupieniu abonamentu lub bez niego.

Od kilku lat wystarczy wpisać do wyszukiwarki nazwisko dowolnej osoby, aby bezpłatnie otrzymać wszystkie dotyczące jej, różnorodne informacje, rozproszone w globalnej sieci, pochodzące z wielu odległych geograficznie lub zróżnicowanych stron. Oznacza to, że jeśli nazwisko jakiejś osoby pojawiło się w dowolnej decyzji sądowej dostępnej w Internecie i jeśli decyzja ta jest indeksowana przez wyszukiwarkę, automatycznie stanie się dostępna dla każdego użytkownika. Internauta nie musi nawet wchodzić do specjalistycznej witryny, a decyzja nie musi być przedmiotem prowadzonego przez niego wyszukiwania. Wykraczając ponad jawny charakter posiedzeń oraz samej decyzji, która może trafić do dowolnej, pytającej o to osoby, powszechna i stała dostępność danych osobowych stwarza poważne ryzyko naruszenia prywatności i czyni nieskutecznym prawo do puszczania w niepamięć.

Ta konstatacja skłoniła Krajową Komisję ds. Informatyki i Wolności (CNIL) do przyjęcia w dniu 29 listopada 2001 r. zalecenia w sprawie publikowania danych osobowych w Internecie przez banki danych zawierające orzecznictwo,¹ a następnie, cztery lata później, do opracowania podsumowania realizacji tego zalecenia. Stało się to okazją do przeanalizowania podejścia pozostałych krajów Unii Europejskiej do tego tematu.

I. Zalecenie CNIL z 2001 r.

Zgodnie z tym zaleceniem, decyzje sądowe, które są ogólnie dostępne w Internecie, i tylko te decyzje, nie mogą odtąd zawierać nazwisk ani adresów stron uczestniczących w postępowaniu, niezależnie od charakteru tego postępowania.

W zaleceniu podkreślono zagrożenia, jakie publikowanie decyzji sądowych ujawniających tożsamość stron może powodować w świetle praw i wolności tych osób zwłaszcza, że decyzje te mogą nie mieć charakteru ostatecznego. Tym samym, legalne narzędzie do wyszukiwania dokumentów mogłoby się stać prawdziwym „katalogiem informacji” o ludziach. Niezależnie od charakteru sporu, sam fakt występowania jako strona lub świadek jest informacją sprzyjającą powstawaniu uprzedzeń: banalny spór sąsiedzki może dać powód do myślenia, że strona skarżąca jest pieniaczem, a pozwany jest trudny we współżyciu; swobodne udostępnienie decyzji sądu w Internecie mogłoby zniechęcić pracodawcę do zatrudnienia takiej osoby, a wynajmującego do zawarcia umowy najmu itp.

CNIL zalecił nawet usunięcie z decyzji swobodnie dostępnych w Internecie nazwisk i adresów świadków.

¹ Uchwała nr 01-057 z dnia 29 listopada 2001 r. dotycząca zalecenia w sprawie rozpowszechniania w Internecie danych osobowych przez banki danych zawierające orzecznictwo, zamieszczona w załączniku.

Zalecenie wprowadzało ponadto rozróżnienie między bazami danych swobodnie dostępnymi przez Internet a tymi, do których dostęp jest płatny. Rozróżnienie to opierało się głównie na założeniu, że domniemane ryzyko nadużycia informacji pochodzących z decyzji sądowych jest mniejsze, jeśli informacje te nie są dostępne przez wyszukiwarki, czyli można do nich dotrzeć albo przez płatną witrynę, albo znajdują się na płytach CD-ROM, które trzeba kupić. W trosce o zachowanie umiaru i odpowiednich proporcji CNIL uznał, że w przypadkach witryn płatnych oraz płyt CD-ROM nie ma podstaw do ukrywania tożsamości stron i świadków, jeśli są wymienieni, co nie jest zasadą ogólną. Biorąc jednak pod uwagę fakt, że na orzeczeniach i wyrokach figurują niekiedy adresy stron, które nie mają wartości dokumentacyjnej – mogłyby natomiast ułatwić zlokalizowanie konkretnej osoby – CNIL uznał za wskazane zatajanie adresów stron w decyzjach sądowych, jakie w przyszłości będą publikowane na płytach CD-ROM lub w specjalistycznych witrynach o ograniczonym dostępie.

Czy zalecenie było przestrzegane?

Zasadniczy krok został wykonany, kiedy w 2002 r. rząd podjął decyzję o zastosowaniu zalecenia CNIL, zobowiązując się do zapewnienia od września 2002 r. anonimowości decyzji sądowych dostępnych w sieci, w oficjalnej witrynie prawnej Légifrance, a następnie, w ciągu dwóch lat, do zapewnienia anonimowości wszystkich wcześniejszych decyzji. Tym samym, główna, powszechnie dostępna francuska witryna z bazami danych zawierającymi orzecznictwo dostosowuje się do zalecenia CNIL. Niemniej jednak, proces zapewniania anonimowości decyzji sądowych sprzed 2002 r. nie mógł się zakończyć, głównie z powodu ograniczeń technicznych oraz kosztów. Spełnienie wymagania nastąpi dopiero w roku 2008, kiedy system informatyczny dzienników urzędowych pozwoli na przyspieszenie procesu zapewniania anonimowości.

Jeśli chodzi o prywatnych operatorów witryn, można stwierdzić, że mimo znacznego podniesienia skuteczności oprogramowań zapewniających anonimowość, dzięki którym utajnienie danych zachodzi znacznie sprawniej i daje się łatwiej wdrożyć, niektóre witryny, zwłaszcza założone przez zawodowych prawników, udostępniających powszechnie decyzje sądowe, nie zawsze zapewniają anonimowość tych decyzji. Jeśli chodzi o bazy danych zawierające orzecznictwo, do których dostęp jest ograniczony, zapewnienie anonimowości decyzji sądowych w dziedzinie karnej jest regułą i adresy stron są na ogół usuwane.

Mimo tych sukcesów, zalecenie z 2001 r. wciąż jest kwestionowane przez część osób zawodowo prowadzących dokumentację prawną oraz przez niektóre organa sądownicze, choćby przez najwyższy organ w sądownictwie administracyjnym – Radę Stanu, która we własnej witrynie internetowej wciąż zamieszcza decyzje z jawnymi danymi osobowymi. Rada Stanu uważa bowiem, że „systematyczne zapewnianie anonimowości decyzji sądów administracyjnych utrudnia wyszukiwanie właściwego orzecznictwa i jego wykorzystywanie przez prawników. Tak się składa, że w prawie administracyjnym decyzje tradycyjnie zawsze były identyfikowane po nazwiskach stron, co pozwala lepiej zapamiętać zasadę prawną i powoływać się na nią przed sędzią. Utajnianie danych podważa tę tradycyjną praktykę”.

Biorąc pod uwagę takie utrzymujące się zastrzeżenia, CNIL podjął w lutym 2005 r. decyzję o dokonaniu podsumowania stosowania zalecenia. Jedną z ważnych kwestii przewidzia-

nych w podsumowaniu było porównanie sposobów, za pomocą których kwestia anonimowości decyzji została rozwiązana w pozostałych państwach Unii Europejskiej. Przeprowadzenie analizy było możliwe dzięki współpracy z europejskimi organami odpowiedzialnymi za ochronę danych, które zechciały odpowiedzieć na kwestionariusz wysłany przez CNIL. Korzystając z okazji, pragniemy jeszcze raz im podziękować, ponieważ ich wkład miał decydujący wpływ na kierunek, w jakim poszły rozważania prowadzone przez CNIL.

II. Utajnianie danych osobowych zawartych w decyzjach sądowych krajów Unii Europejskiej

1. Pierwsza obserwacja: w niektórych krajach istnieje tradycja całkowitego utajniania danych osobowych zawartych w decyzjach sądowych, niezależnie od używanego nośnika.

W **Niemczech** i **Austrii** tradycyjnie zapewnia się anonimowość wszystkich decyzji sądowych, co pozwala na uniknięcie kwestii pogodzenia publikowania decyzji sądowych w Internecie i przestrzegania zasady ochrony danych osobowych. Sądy same dbają o utajnianie danych osobowych. Jeśli nazwisko jakiejś osoby zostanie pomyłkowo ujawnione, korekta jest wprowadzana natychmiast.

Polska także zdecydowała się na utajnianie danych osobowych zawartych w publikowanych decyzjach sądowych. Decyzje identyfikowane są po numerach, a nie po nazwiskach stron.

Na **Węgrzech** kompilacji najważniejszych decyzji sądowych dokonuje się z zachowaniem anonimowości, niezależnie od użytego nośnika. Ponadto, węgierski urząd odpowiedzialny za ochronę danych stwierdził, że decyzję sądową można publikować w Internecie tylko pod warunkiem uzyskania zgody osoby wymienionej w takiej decyzji, chyba że istnieje przepis ustawowy, który w sposób wyraźny stanowi inaczej.

Trzeba zauważyć, że w większości państw ustawodawstwo krajowe przewiduje przypadki, w których ze względu na charakter decyzji (spory dotyczące stosunków pokrewieństwa, przemoc seksualnej itp.) nazwiska stron nie mogą być ujawniane, niezależnie od rodzaju używanego nośnika. Obowiązek ten oczywiście istnieje w przypadku publikowania decyzji w Internecie.

Przykładowo, prawo **maltańskie** narzuca utajnianie danych osobowych zawartych w decyzjach sądowych w zależności od charakteru decyzji (sprawa medyczna, niezgodność z dobrymi obyczajami, nieważność małżeństwa, separacja). Ta zasada stosuje się do decyzji publikowanych w Internecie. Natomiast pozostałe decyzje prawne publikowane w Internecie nie są anonimowe.

2. Niektóre kraje przyjęły specjalne ustawodawstwo, regulując odpowiednimi przepisami publikowanie decyzji sądowych nieobjętych zasadą utajniania danych osobowych.

W **Estonii** publikowanie decyzji sądowych przez Internet podlega przepisom kodeksu postępowania karnego i kodeksu postępowania cywilnego, przegłosowanym w 2004 r., które stanowią, że publikowane decyzje sądowe nie mogą pozwalać na identyfikację stron (utajnianie nazwisk, daty urodzenia, adresu itp.), jeśli taka identyfikacja mogła-

by naruszyć prywatność danej osoby. W przypadku osób, których dane osobowe zostały opublikowane przed 2004 r., estoński urząd ochrony danych dopuszcza możliwość złożenia wniosku o zastosowanie wyżej wspomnianych postanowień.

We **Włoszech** publikowanie decyzji sądowych podlega specjalnym przepisom ustawodawczym, które w bardzo szerokim zakresie opierają się na stanowisku przyjętym w tej sprawie przez włoski urząd ochrony danych osobowych. Włoskie ustawodawstwo daje każdej osobie kierującej się uzasadnionymi przesłankami prawo zwrócenia się do kancelarii sądowej o usunięcie z decyzji danych osobowych dotyczących tej osoby, jeśli decyzja ma być opublikowana, niezależnie od rodzaju nośnika. Decyzję o uwzględnieniu wniosku podejmuje sąd, który wydał decyzję stanowiącą przedmiot składanego wniosku.

Publikowanie **szwedzkich** decyzji sądowych podlega przepisom zawartym w rozporządzeniu z 1999 r., które z jednej strony wprowadza zasadę swobodnego dostępu do informacji, a z drugiej reguluje zasady publikowania danych osobowych. Wszystkie sądy szwedzkie muszą zapewnić dostęp – również przez Internet – do decyzji, które uważają za ważne. Decyzje identyfikowane są po dacie i numerze. Nie mogą one zawierać danych o charakterze osobowym. Dane takie mogą figurować wyłącznie w decyzjach Europejskiego Trybunału Sprawiedliwości (razem z decyzjami sądów szwedzkich), ponieważ nie podlegają procedurze zapewniania anonimowości.

W **Luksemburgu**, mimo że kwestia publikowania decyzji sądowych nie podlega specjalnym przepisom ustawodawczym, stosuje się zasady wynikające z praktyki. Orzecznictwo sądów administracyjnych, dostępne na stronie internetowej Ministerstwa Sprawiedliwości, jest poddawane systematycznej procedurze utajniania danych osobowych. Sądowe bazy danych na razie jeszcze nie są dostępne przez Internet, ale za to baza zarządzana przez Prokuraturę Generalną, z której mogą korzystać zawodowi prawnicy, zapewnia poufność danych osobowych. W dziedzinie prawa karnego pełne odpisy decyzji sądowych można udostępniać tylko w wersjach anonimowych, chyba że wydawane są osobom, których bezpośrednio dotyczą (adwokatom, stronom w postępowaniu itp.). W dziedzinie prawa cywilnego o wydawaniu odpisów osobom trzecim decydują prezesi sądów, które te decyzje wydały. W przypadku rozwodu, adopcji, dochodzenia lub kwestionowania ojcostwa, stanu cywilnego itp. wydawane są tylko kopie z utajnionymi danymi osobowymi. Postanowienia te nie wykluczają możliwości posiadania zbiorów decyzji, zawierających jawne dane osobowe, przez zawodowych prawników.

3. W niektórych krajach sprawa publikowania decyzji sądowych w Internecie była związana ze **stanowiskiem zajętym przez urząd odpowiedzialny za ochronę danych osobowych**.

W **Finlandii**, mimo że urząd odpowiedzialny za ochronę danych osobowych uznał, że nie jest powołany do określania sposobu, w jaki sądy powinny wypełniać obowiązek informowania społeczeństwa, to jednak ocenił, że decyzje sądowe publikowane w Internecie nie powinny zawierać danych osobowych.

Portugalski urząd ochrony danych osobowych otrzymał w 2000 r. skargę dotyczącą publikowania w witrynie Ministerstwa Sprawiedliwości decyzji sądowych w dziedzinie karnej, w których pojawiają się nazwiska stron. Urząd zdecydował o zablokowaniu dostępu do witryny dopóty, dopóki nie zostanie zapewniona anonimowość tych decyzji.

Urząd portugalski wydał oficjalne stanowisko, w którym opowiedział się za stosowaniem przepisów o ochronie danych osobowych do baz danych zawierających orzecznictwo. Jeśli bazy takie nie zapewniają anonimowości, należy je zgłaszać do urzędu ochrony danych. Urząd portugalski z zasady zaleca utajnianie danych w tych bazach, a narzuca anonimowość w sprawach kryminalnych, dochodzenia ojcostwa, rozwodów lub wszelkich innych sporach, które mogą mieć wpływ na życie prywatne zainteresowanych osób. W praktyce zalecenie to doprowadziło do tego, że wszystkie decyzje sądowe publikowane w Internecie są anonimowe.

Holenderski urząd ochrony danych osobowych oficjalnie opowiedział się za zapewnieniem całkowitej anonimowości decyzji sądowych publikowanych w Internecie, ze względu na specyficzny charakter tego nośnika i brak możliwości kontrolowania sposobu wykorzystania danych. Urząd opublikował zalecenia w zakresie zapewnienia anonimowości. W konsekwencji, wszystkie decyzje publikowane w oficjalnej witrynie (www.rechtspraak.nl) zawierają dane utajnione.

W **Grecji** Rada Stanu skierowała zapytanie do urzędu ochrony danych, który w decyzji z 25 października 2000 r. uznał, że publikowanie w przeglądach prawniczych decyzji sądowych powinno się odbywać z zachowaniem poufności danych. Zwyczajowo, żadne publikowane decyzje sądowe nie zawierają danych osobowych, niezależnie od rodzaju nośnika.

Komisja belgijska wypowiedziała się na temat banków danych zawierających orzecznictwo. Uznała, że rozwojowi technologii, zwiększającemu możliwości wyszukiwania informacji, musi towarzyszyć większy umiar przy wprowadzaniu do zautomatyzowanych kronik zawierających orzecznictwo danych, które mogą umożliwić identyfikację stron. Komisja stwierdziła także, że sposoby korzystania z nośników elektronicznych służących do publikacji orzecznictwa pozwalają na wypaczanie celu przetwarzania danych zawartych w dokumentach przez formułowanie pytań opartych na nazwiskach stron. W związku z tym, komisja belgijska zaleca, by w decyzjach nie podawać nazwisk osób trzecich (świadków) w sporach. Powołuje się też na artykuł 2 rozporządzenia królewskiego z 7 lipca 1997 r. w sprawie publikacji decyzji Rady Stanu, który przewiduje, że każda strona w sporze ma prawo do odmowy publikacji swego nazwiska. Postanowienie to nie przewiduje jednak sposobów informowania stron ani sposobów realizacji prawa do odmowy. Komisja zaleca, by już w chwili rozpoczęcia postępowania sądowego wszystkie strony otrzymywały formularz informujący w sposób jasny o wspomnianym prawie oraz podający sposoby wykonania tego prawa. Komisja uważa, że odmowę publikacji nazwiska przez strony powinna uzupełniać możliwość podjęcia decyzji przez sam sąd, który zadecyduje o zapewnieniu anonimowości konkretnej decyzji. Komisja belgijska jest zdania, że można by alternatywnie ustanowić prawo udzielania zgody: w chwili rozpoczynania sporu sądowego strony byłyby proszone o podanie na oficjalnym formularzu, czy zgadzają się na przetwarzanie dotyczących ich danych osobowych z chwilą elektronicznej publikacji decyzji. W przypadku braku zgody lub odmowy, istniałby obowiązek „depersonalizacji” danych przy każdej elektronicznej publikacji decyzji.

Łotewski urząd ochrony danych otrzymał zapytanie od Ministerstwa Sprawiedliwości w sprawie warunków, na jakich można publikować decyzje sądowe zgodnie z wymogami prawa. Urząd uznał, że ochrona prywatności zainteresowanych osób wymaga, aby decyzje sądowe publikowane w ogólnie dostępnych witrynach spełniały wymóg anonimowości.

W **Republice Czeskiej** przez Internet dostępne są jedynie decyzje Najwyższego Sądu Administracyjnego, tylko przez okres 15 dni i bez zachowania anonimowości danych osobowych. Urząd ochrony danych zalecił ogólnie, mając na uwadze perspektywę publikacji wszystkich decyzji czeskich sądów najwyższych, zapewnienie anonimowości takich decyzji ze względu na zagrożenia dla zainteresowanych osób oraz fakt, że publikacja danych mogłaby być odebrana jako dodatkowa kara.

Prawo **irlandzkie** chroni tożsamość stron w decyzjach dotyczących spraw o gwałt lub w sporach podlegających prawu rodzinnemu. Irlandzki urząd ochrony zalecił zapewnianie anonimowości decyzji, pod warunkiem spełnienia obowiązków ustawowych w zakresie informowania, stosowanych do konkretnych sądów.

W **Wielkiej Brytanii** sprawy publikowania decyzji sądowych nie reguluje ani prawo, ani praktyka. Kiedy decyzje sądowe są zamieszczane w Internecie, część z nich nie zawiera jawnych danych osobowych.

III. Styczeń 2006 r.: CNIL potwierdza i zaostrza stanowisko

Jak już zostało powiedziane wcześniej, analiza porównawcza stała się jednym z elementów decyzyjnych, które doprowadziły CNIL nie tylko do potwierdzenia stanowiska wyrażonego w 2001 r., ale nawet do jego zaostrzenia.

Stwierdzając, że w kwestii zapewniania anonimowości stanowisko to nie było odosobnione i że inne kraje poszły nawet jeszcze dalej, CNIL uznał, że francuska praktyka w zakresie publikowania baz danych zawierających orzecznictwo przez Internet – niezależnie od sposobu dostępu – lub na płytach CD-ROM musi wpisywać się w europejską tendencję zwiększonej ochrony osób.

Z tej perspektywy argumenty wysuwane w związku z rozwojem technologicznym wydały się zbyt słabe. Zauważono, że wprowadzenie odpowiednich narzędzi technicznych pozwala na ograniczenie ryzyka związanego z publikowaniem decyzji sądowych w Internecie i że należałoby dokonać rozróżnienia między poszczególnymi witrynami w zależności od tego, czy publikowane w nich decyzje mogą być bezpośrednio indeksowane przez wyszukiwarki. Zmiany techniczne wprowadzone w witrynie Légifrance sprawiły, że publikowane w niej decyzje sądowe nie są już dostępne przez zapytanie wprowadzone do ogólnej wyszukiwarki. Ponadto istnieje techniczna możliwość usunięcia opcji wyszukiwania decyzji sądowej w bazie danych zawierającej orzecznictwo przez zapytanie o nazwisko którejś ze stron.

CNIL opowiada się za używaniem narzędzi technicznych regulujących dostęp przez Internet do baz danych zawierających orzecznictwo, ale przypomina też, że żadna z takich metod nie zdoła skutecznie i trwale zapobiec ryzyku nadużycia takich baz danych dostępnych w Internecie.

Ponadto, jeśli operator danej witryny nie zapewnia już możliwości zapytania bazy danych zawierającej orzecznictwo o nazwisko stron, to jednak takie zapytanie wciąż można utworzyć, stosując tzw. wyszukiwanie „w całym tekście”, czyli korzystając z opcji, jaką na ogół oferuje każda witryna. Witryna Légifrance również daje taką możliwość.

Oznacza to, że ryzyku naruszenia prywatności, jakie powstaje w tym zakresie w związku z możliwościami Internetu, może zapobiec tylko powszechne zapewnienie anonimowości decyzji sądowych publikowanych w ogólnie dostępnych witrynach.

Niezależnie od dyskusji o charakterze technicznym, CNIL zatroszczył się o wyciągnięcie konsekwencji z transpozycji Dyrektywy 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 tych danych, która nastąpiła z opóźnieniem, w chwili przyjęcia ustawy z dnia 6 sierpnia 2004 r.

Bazy danych zawierające orzecznictwo, jeśli zawierają dane osobowe stron, dokonują zautomatyzowanego przetwarzania danych osobowych i jako takie podlegają postanowieniom ustawy z 6 stycznia 1978 r., zmienionej w sierpniu 2004 r. Poza tym w przypadkach, gdy bazy zawierają wyroki sądów karnych, takie przetwarzanie należy do specyficznej kategorii przetwarzania danych dotyczących wyroków skazujących.

Dlatego właśnie zmiany w ustawie o ochronie danych osobowych wprowadzone ustawą z 6 sierpnia 2004 r. wywołują skutki dla systemu stosowanego do baz danych zawierających orzecznictwo, niezależnie od sposobu dostępu.

Dyrektywa 95/46 wskazuje ponadto w punkcie 30 preambuły, że aby przetwarzanie danych osobowych było zgodne z prawem, musi odbywać się za zgodą osoby, której dane dotyczą, lub być konieczne dla zawarcia lub realizacji umowy wiążącej daną osobę, bądź mieć charakter wymogu prawnego lub też służyć realizacji zadania wykonywanego w interesie publicznym lub związanego ze sprawowaniem władzy publicznej, bądź służyć realizacji uzasadnionego interesu dowolnej osoby, pod warunkiem, że interesy lub prawa i wolności osoby, której dane dotyczą, nie mają charakteru nadrzędnego. Zasady te zostały w szczególności wyjaśnione w artykule 7 Dyrektywy, który stanowi, że kraje członkowskie dopuszczają przetwarzanie danych osobowych tylko wówczas, gdy osoba, której te dane dotyczą, jednoznacznie wyraziła zgodę lub, gdy został spełniony którykolwiek z zamkniętej listy warunków wymienionych w artykule 7, taki jak wykonywanie umowy lub przestrzeganie zobowiązania prawnego.

Artykuł 7 ustawy francuskiej zmienionej w sierpniu 2004 r. przewiduje też, że dane osobowe mogą być przetwarzane dopiero po otrzymaniu zgody osoby, której dotyczą, lub spełnieniu któregoś z poniższych warunków:

„1° Przestrzeganie zobowiązania prawnego spoczywającego na administratorze odpowiedzialnym za przetwarzanie.

2° Ochrona życia osoby, której dane dotyczą.

3° Realizacja zadania wykonywanego w interesie publicznym, które zostało powierzone osobie odpowiedzialnej za przetwarzanie danych lub odbiorcy tych danych.

4° Wykonanie bądź umowy, w której zainteresowana osoba jest stroną, bądź działań poprzedzających zawarcie umowy, podjętych na wniosek tej osoby.

5° Realizacja słusznego interesu, jakiego dochodzi osoba odpowiedzialna za przetwarzanie danych lub odbiorca tych danych, pod warunkiem nielekceważenia interesu lub praw i podstawowych wolności osoby, której te dane dotyczą.”

Tym samym, punkt 3° zezwala w sposób wyraźny na tworzenie baz danych zawierających orzecznictwo sądom wydającym decyzje, z zachowaniem formy imiennej i na

użytek ściśle wewnętrzny, o ile wpisuje się to w zakres realizacji zadania wykonywanego w interesie publicznym.

Z kolei prywatni operatorzy baz danych zawierających orzecznictwo nie mogą skutecznie powoływać się na punkt 5°. Publikowanie baz danych zawierających orzecznictwo na stronach internetowych z ograniczonym dostępem lub na płytach CD-ROM może być zgodne z uzasadnionym interesem osób odpowiedzialnych za takie przetwarzanie danych, ale oznacza lekceważenie praw i podstawowych wolności osoby, której te dane dotyczą. W związku z tym, biorąc pod uwagę szczególny charakter informacji znajdujących się w takich bazach danych, CNIL uważa, że zastrzeżenie sformułowane w artykule 7-5° ustawy nie ma w tym przypadku zastosowania.

Ustęp 5 artykułu 8 Dyrektywy* 95/46/WE stanowi, że „przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą władz publicznych lub też, jeżeli zgodnie z prawem krajowym ustanowiono określone środki zabezpieczające, z zachowaniem odstępstw, których Państwo Członkowskie może udzielić zgodnie z obowiązującymi przepisami prawa krajowego, zapewniając zachowanie odpowiednich zabezpieczeń. Jednak kompletny rejestr przestępstw kryminalnych może być prowadzony tylko pod kontrolą władzy publicznej.”

Powyższe postanowienie zostało przetransponowane do prawa francuskiego (artykuł 9) w sierpniu 2004 r. w następującym brzmieniu:

„Dane osobowe dotyczące naruszeń, wyroków lub środków bezpieczeństwa mogą być przetwarzane wyłącznie przez:

1° Sądy, organy władzy państwowej i osoby prawne kierujące służbą państwową, działające w ramach przyznanych im uprawnień.

2° Przedstawicieli prawa, ściśle na potrzeby realizacji zadań powierzonych im na mocy przepisów prawa.”

CNIL uznał, że operatorzy prywatni, którzy utworzyliby bazę danych zawierających orzeczenia sądów karnych z podanymi nazwiskami osób skazanych, dopuściliby się naruszenia prawa. Ponadto, CNIL uważa, że przepisy prawa nakładają na operatorów prywatnych obowiązek utajniania nazwisk stron i świadków związanych z decyzjami publikowanymi w ramach prowadzonej przez nich działalności.

I wreszcie, wbrew oczekiwaniom pewnych środowisk, CNIL nie złagodził swego stanowiska z 2001 r. Wręcz przeciwnie – uległo ono zaostrzeniu, ponieważ usunięto wyjątek początkowo poczyniony na rzecz baz danych o ograniczonym, a w szczególności płatnym dostępie.

Podsumowanie powyższych działań było interesujące nie dlatego, że pokazuje zakres prac wykonanych przez CNIL. Przede wszystkim pokazuje ono, że Dyrektywa europejska z 1995 r. w sprawie ochrony danych osobowych odgrywa istotną rolę w ujednoliceniu podejścia w poszczególnych krajach europejskich, nawet w tych dziedzinach, w których każdy kraj i każdy krajowy urząd ochrony danych posiada najszerszy zakres swobody. Trudno raczej uwierzyć, by jakiś kraj miał pójść własną drogą, nie oglądając się na wybory dokonane przez partnerów. W dziedzinie Internetu, która tak trudno poddaje się jakimkolwiek regulacjom na obszarze krajowym, takie stanowisko byłoby wyjątkowo nierozsądne.