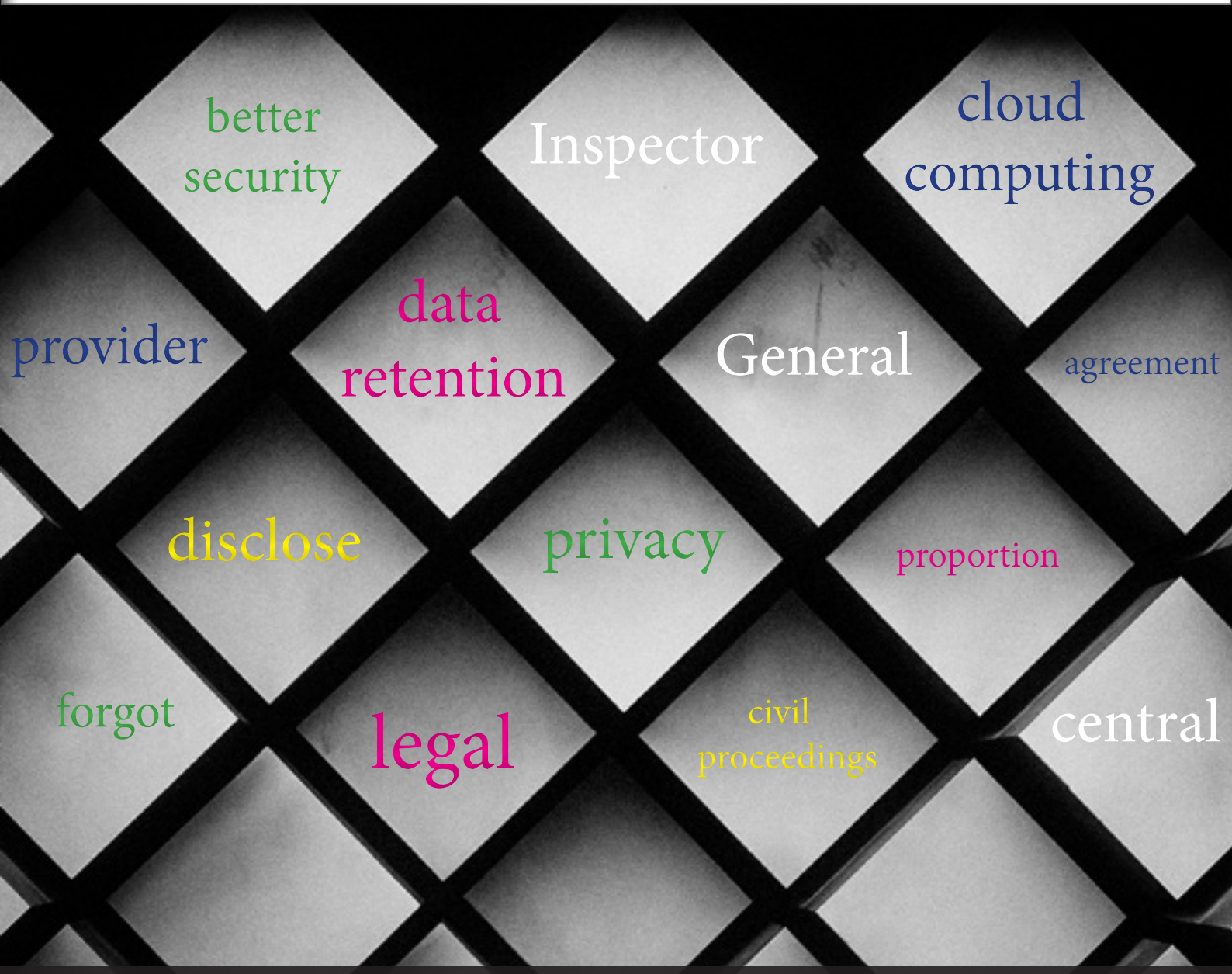
Przegląd Prawa Technologii Informacyjnych
ICT Law Review

1/2013

Kwartalnik Wydziału Prawa i Administracji
Uniwersytetu Mikołaja Kopernika
w Toruniu

Quarterly of the Faculty of Law and Administration
of Nicolaus Copernicus University
in Torun



Ochrona danych osobowych
Personal data protection

Spis treści / Contents

I. Wydarzenia / Events 3

II. Artykuły / Articles

A.Adamski,
The telecommunication data retention in Poland: does the legal regulation pass the proportionality test? 4

P. Balboni, F. Fontana,
Cloud computing: A guide to evaluate and negotiate cloud service agreements in the light of the actual European legal framework 12

K. Dobrzeniecki,
Konflikty wartości konstytucyjnych związane z funkcjonowaniem Internetu 18

P. Litwiński,
Udostępnianie danych osobowych na potrzeby postępowań cywilnych 24

M. Kawecki,
Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej 38

III. Varia

Felieton / Feature article

A. Pietrzak,
Spam -niechciana poczta elektroniczna 45

Sprawozdanie / Report

D. Gęsicka,
Sprawozdanie z konferencji „CopyCamp” 48

Wywiad / Interview

B. Marek,
Rozmowa z dr Wojciechem Wiewiórowskim - Generalnym Inspektorem Ochrony Danych Osobowych 50

Drogi Czytelniku,

Z przyjemnością oddaję w Twoje ręce pierwszy numer Kwartalnika, którego tematem przewodnim jest ochrona danych osobowych. Dlaczego taki temat? W styczniu 2012r. Komisja Europejska zaprezentowała propozycję reformy ochrony danych osobowych. Reforma, choć wciąż dyskutowana, może wiele zmienić począwszy od harmonizacji prawa dotyczącego ochrony danych osobowych w całej Unii. Styczeń 2013r. to dobry czas by przyjrzeć się zagadnieniom, które wciąż budzą wątpliwości. Warto także wziąć pod uwagę ciekawe postulaty *de lege ferenda*. Zapraszam do lektury.

Beata Marek
Redaktor Naczelna

Dear reader,

I am very glad to present you the first issue of ICT Law Review. It focuses on personal data protection and there are at least two reasons for that. In January 2012 the proposal of personal data protection reform was made publicly known by the European Commission. This new regulation, still under discussion, will be directly applicable in all Member States. In view of the forthcoming enhanced harmonization of data protection law in Europe, January 2013 provides a good opportunity to look upon selected issues of personal data protection from the current perspective of national and EU legislation.
I would like to thank the authors for their contributions and wish our readers a very happy, safe and successful new year.

Beata Marek
Editor-In-Chief

Czasopismo Open Access, wydawane na licencji Creative Commons Uznanie Autorstwa 2.5 Polska

The Open Access Quarterly, issued under Creative Commons Attribution 2.5 Poland

Rada Naukowa / Scientific Council

Prof. dr hab. Andrzej Adamski (Przewodniczący / Chairperson)
Dr hab. Arkadiusz Lach
Dr Karol Dobrzeniecki
Dr inż. Jerzy Kosiński
Dr Michał Polasik
Dr Monika Wałachowska
Dr Zofia Zawadzka
Dr Konrad Zacharzewski
Mirosław Maj

Redakcja / Editorial Team
Beata Marek (Redaktor Naczelna / Editor-In-Chief)
Daria Gęsicka (Zastępca RN / Assistant E-i-C)
Szymon Ludwiczak (Sekretarz / Secretary)

Wydawca / Publisher
Wydział Prawa i Administracji
Uniwersytet Mikołaja Kopernika
Ul. Władysława Bojarskiego 3, 87-100 Toruń

Contact
ictlaw@umk.pl

ISSN:

Nr rejestracji / Registration Nr: Pr 337

Data wydania / Issue data: 28.01.2013
Tumaczenia / Translation: Daria Gęsicka

Okładka / Cover: Voltiostudio
DTP: Beata Marek

Luty - Marzec / Ferbuary - March

04.02 - 06.02
6th Annual Corporate Data Protection and Privacy Compliance Conference,
Amsterdam

05.02
ISSA European Conference 2013,
London

14-15.02
9th Annual Asian ITechLaw Conference,
Bangladore

19.02
Cloud Computing Gigacon,
Poznań

20.02
9 Kongres Bezpieczeństwa Sieci,
Warszawa

21.02
5th Annual Data Protection Conference,
Dublin

24.02 - 01.03
6th International Conference on Digital Society,
Nice

24.02 - 01.03
CYBERLAWS 2013,
Nice

27.02
IV Forum Prawa Nowych Technologii: Prawo komunikacji elektronicznej w praktyce gospodarki i administracji,
Warszawa

04.03 - 06.03
ISS World MEA,
Dubai

05.03
Data Protection Officer Conference 2013,
Manchester

05.03 - 06.03
SEMAFOR 2013,
Warszawa

06.03 - 08.03
IAPP Global Privacy Summit,
Washington, DC

13.03
Cloud Computing Gigacon,
Gdańsk

18.03 - 19.03
III ogólnopolska konferencja „Ataki sieciowe",
Toruń

POLECAMY / WE RECOMMEND

20.03
Debata :
Prywatność w nowych technologiach,
Warszawa

Więcej informacji s.58

20.03 - 21.03
Online Privacy: Consenting to your Future,
Portomaso

21.03 - 22.03
Living on e-Discovery's Cutting Edge,
San Diego, CA

Andrzej Adamski*

The telecommunication data retention in Poland: does the legal regulation pass the proportionality test?

Cite: A. Adamski, *The telecommunication data retention in Poland: does the legal regulation pass the proportionality test?*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, vol. 1/2013, p. 4-11.

Abstract

The purpose of this paper is to find whether Polish legal regulations on the telecommunication data retention based on the Directive 2006/24/EC are a necessary and proportional measure in view of the relevant provisions of the Constitution of the Republic of Poland and the principles of the European law, including EctHR case law.

The paper consists of four sections; the first section provides background information on the subject matter, the second section is an attempt to scrutinize the effects of the Directive into the Polish legal system. In the third section, the proportionality of existing legal regulations on the data retention is evaluated. In this respect, an attempt is made to demonstrate as how to apply the proportionality test in order to examine the issue under consideration against the requirements of proportionality. Last but not least, the author presents complaints concerning implementation of the Directive 2006/24/EC.

Key words: Constitutional Tribunal, criminal proceedings, data retention, data preservation, telecommunication data, proportionality test, right to privacy

1. Background

The confidentiality of communications is guaranteed by the Polish Constitution of 1997 in Article 49 which stipulates that any limitations of this right "may be imposed only in cases and in a manner specified by statute". The regulation has two basic implications. First, the telecommunication traffic data has been recognized as legally protected information under the definition of "telecommunication secrecy" provided by the Law on Telecommunications of 2000. Secondly, due to the statutory limits of the telecommunication secrecy, the right of access to traffic data was granted to the law enforcement and criminal justice authorities, for the first time on the basis of Article 67(4) of the Law of Telecommunications of 2000. Initially, however, the legitimate goal of gathering and storing traffic data by telecom providers was determined by business matters (i.e. payments charging and payment disputes solving). As such it was carried out in compliance with the Directive 1997/66/EC and the Directive 2002/58/EC and the relevant provisions of the Law on Telecommunications.

The legal regime of mandatory phone-traffic data retention for the purposes of law enforcement and national security agencies in Poland dates back to 2003. Both, the regulation of the Ministry of Infrastructure of 2003 and the Law on Telecommunications of 2004 as amended in 2005, provided twelve month period for the retention of data concerning on-line interactions of subscribers and users of telecommunication services. In 2005 the period has been extended up to two years, however the MPs group proposal for its further extension (up to 5 years) was not accepted by the parliamentary commission in 2006 despite the governmental support claiming that the extension would increase "efficiency in combating crime and terrorism." The legislative draft was rejected by the commission as incompatible with the Directive 2006/24/EC.

2. Implementation of the Directive

In 2009 the Directive was transposed into Polish legal system in a two-stage manner. In April 2009 pursuant to the amended Law on Telecommunication of 2004 the obligation of the telephone data retention was imposed on telecommunication operators and service providers. However, it was not until 15th March 2009 that the retention of „communications data relating to Internet access, Internet telephony and Internet e-mail" became enforceable. The respective regulation of the Minister of Infrastructure, covering inter alia the retention of Internet data, was enacted on 28th December 2009.

In Poland, the implementation of the data retention directive resulted in legal changes mostly in the field of the telecommunications law where new obligations were imposed on operators and providers. In consequence, the detailed regulations were required in the business sector. There were only a few amendments in the Law on the Police and the Criminal Procedure Code facilitating access of the law enforcement authorities to traffic, location and subscribers data held by telecom providers.

2.1. Telecommunications law regulations

In Poland the scope of data retention complies with Article 5 of the Directive and covers all types of data specified therein. The Articles 3, 4, 6 and 7 of the Regulation of the Minister of Infrastructure of 28th December 2009 enumerate in detail the categories of data to be retained. These categories include data necessary to identify the following matters:
- the source and destination of the communication, including: the telephone number or (for the Internet e-mail and telephony) user id, and the identity of the subscriber or registered user;
- the type, date, time and duration of the communication act;
- users' communication equipment;
- the location of mobile equipment.

The subscriber's data or "data concerning a user" (as provided in Article 159 of the Law on Telecommunications) is a subject to legal protection under the telecommunications secrecy and personal data regime. Providers of the publicly available telecommunications services are entitled to process the following data on users who are natural persons (Article 161 of the Law on Telecommunication):
1) surnames and first names; 2) parents' first names; 3) place and date of birth; 4) address of permanent residence; 5) personal number (PESEL) – in the case of a citizen of the Republic of Poland; 6) name, series and number of documents confirming the identity, and in the case of a foreigner being a citizen of a country which is not a member of the European Union or the European Economic Area – a passport number or a residence card number; 7) data included in documents confirming the capacity to perform an obligation towards a provider of publicly available telecommunications services resulting from an agreement on the provision of telecommunications services. Basically, these data in combination with traffic data (e.g. IP address of a computer) allow for identification of the fixed network telephony and mobile telephony subscribers.

The retention period is equal for both means of communication, the telephone and the Internet, and amounts up to 24 months from the date of the communication act[1]. Upon the expiry of the date a telecom operator or provider is obliged to destroy transmission data, unless it was provided otherwise by the law. The provision of the Article 180a of the Law on Telecommunications paves the way for the unlimited-in-time storage of traffic data which is inconsistent with the Directive.

2.2. Access to the data

According to Article 180d of the Law on Telecommunications, operators and providers of publicly accessible telecommunication services are obliged to submit on their own expense the traffic and location data to the police, secret services, state prosecutors and courts in compliance with the rules and procedures prescribed by other legal provisions. Respectively, corresponding regulations are to be found in the Law on the Police (Article 20c), the Criminal Procedure Code (Article 218) and other laws concerning various state agencies of social control, which include: the Internal Security Agency, Central Anticorruption Bureau, Fiscal Intelligence, Border Guard, Military Police and Military Counter -Intelligence Service. The instrument of state agencies authorization for having access to the retained data was upheld and the relevant provisions were only slightly modified in 2009.

The statutory authorization of access to the telecommunications traffic data "for the purpose of prevention and detection of crime" was granted to the police and secret service (Urząd Ochrony Państwa) in 2000. What aroused criticism in the literature at that time were the inappropriate control mechanisms of making this data available to the police (Adamski

2000, Adamski, 2001). High standard of an independent oversight, stemming from the ruling in the Malone case was not adopted by the legislator. Instead, a procedure of an authorization upon written or oral request of the duly authorized police officer was introduced. In case of an oral request, the only protective mechanism was the Police Commander's notification by telecom network provider about data disclosure to the policeman. This legal safeguard, however, is no longer valid. The provision was effaced from the recently amended Law on the Police despite the negative opinion of the Prime Minister Legislative Council concerning its removal from the draft law (Rada Legislacyjna 2009). The legislation in force allows the police and secret services for direct (on-line) access to the data. In such circumstances any assistance or intermediation of telecom operator staff is necessary, and neither written nor oral request is required. Against the comparative background it would be more than difficult to find an example of any other EU member state where access to such specific and sensitive information on private life of citizens - as the telecommunication data is- would depend exclusively on the decision of the state agent. The present Polish data retention regime arouses concerns for two other reasons. In contrast to Article 1 of the Directive these regulations do not introduce a criterion of the crime seriousness as an accessibility premise and allow for the wide use of traffic and location data. The data might be used not only for the purpose of detection and prosecution of crime but also for the prevention of crime, which enables "data mining" practices.

On the basis of the recently amended Article 218 of the Criminal Procedure Code, every entity operating in the telecommunication sector is obligated to provide the court or state prosecutor, upon their demand included in their order, with any correspondence and data specified in Article 180c and Article 180d of the Law on Telecommunications under condition that the abovementioned data is significant to the pending proceedings. It may seem that Polish prosecutors take advantage of such possibility quite frequently. As the recent survey depicts prosecutors examine billing data of suspects in 70 per cent of preparatory proceedings concerning drugs possession cases. In search for evidence of their possible involvement in drug trafficking activity, the prosecutor's office workers summon as witnesses those people who were previously identified as frequent callers for. There, the summoned are interrogated and questions on the location, frequency and quantity of drugs are posed (E. Kuźmicz at al., 2009).

Access to retained data is restricted to the police, national security agencies, and judicial authorities. All the authorities designated by relevant laws are entitled to access traffic, subscribers and localisation data in case of any crime, trivial crimes inclusive. There is no legal requirement for seriousness of crime nor independent mechanism that would allow control of the data disclosure by telecom providers. These legal flaws in terms of data accessibility do not constitute the most current problem; still no steps have been taken to improve the regulation. In addition to that, it is these flaws that may account for the recently disclosed Polish scandal concerning surveillance of ten journalists by the secret services exploiting intensively (2005-2007) the traffic and location data of the journalist's mobile phones. Allegedly, the practices were carried out in order to reveal their informants in politically motivated investigation. Moreover, reveled data shows that the agencies were not collecting these information in order to fulfill functions ascribed to them such as preventing and combating serious crime that threaten vital interest of the state (Człuchowski 2010).

3. Proportionality of data retention regime

Under the data retention regime, each and every use of fixed-line or mobile telephone, fax, e-mail, the Internet telephony is recorded as to the identity of the individuals involved, the time and place of communications and other details. Massive collection and storage of the telecommunication data in a modern "information" society enable those to whom the data is available to reproduce a "map" of private life of almost every citizen (see: Malte Spitz 2009). Additionally, mandatory data retention increases a scope of social control of citizens beyond the legally determined boundaries. As indicated in the literature, it not only affects communications taking place

in public or business premises but for a large part also affects communications in private homes, despite the fact that monitoring a citizen's behaviour in their home is generally permissible only in exceptional circumstances (Bryer 2005).

Keeping the above in mind, there is no cast of a doubt whether the blanket retention of telecommunications data constitutes an interference with the right to privacy guaranteed in Article 8 ECHR and other individual rights guaranteed in the constitutional law of many countries, including Poland. In the case of Poland, the blanket data retention stays in conflict with the right to privacy (Article 47 of the Constitution), the right to confidentiality of communications (Article 49 of the Constitution) and the right to self-determination of personal data processing (Article 51 of the Constitution). A very important provision in the present context is paragraph 2 of Article 51("Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state governed by the rule of law"). However, all of them are relevant and necessary legal basis for the proportionality test.

In most jurisdictions, the proportionality test is carried out on the grounds of constitutional law and focuses on specific constitutionally guaranteed rights and freedoms in order to establish whether their restriction in the public interest is justified or not. This effort usually involves a rigorous four-stage enquiry, through which the court needs to examine:
1) whether the purpose of any right restriction is legitimate (namely, whether the instrument in question is stipulated in statues or is determined by the court to be a legitimate democratic purpose);
2) whether the measure in question is suitable to attain the identified purpose;
3) whether the measure is necessary for the attainment of the purpose (namely whether it is the least restrictive measure available for achieving the purpose in question) ;
4) whether the measure is proportionate in the strict sense (namely whether it strikes a proper balance between the purpose and the individuals' rights in question) (Goold, at al. 2007).

A similar approach has been adopted by the Polish Constitutional Tribunal in a number of judgments (Zasada, 2009). In the judgment of 12th December 2005 (K 32/04), the Constitutional Tribunal declared that determination of the police surveillance measures proportionality requires examination of whether such measures : (a) are capable of leading to the intended results, (b) are indispensable for the protection of the public interest with which they are connected, and (c) their results are proportional to the burdens they place on the citizen (Judgment K32/04). Access to and the use of the retained telecommunications data by the law enforcement and secret service agencies are ranked among the surveillance measures (Taracha, 2006). Therefore, it is clear that legal provisions governing an application of the data-retention-based surveillance should undergo proportionality test in order to examine whether it is necessary in a democratic society.

The examination of data retention legislation against the proportionality rule conducted by the German Constitutional Court in the judgment of 2nd March 2010 enabled the Court to declare that in the context of Article 10 of the German Constitution (protecting the privacy of telecommunication) the data retention regulations are not proportional with respect to a number of issues (Federal Constitutional Court 2010). Disproportionality was found in regulations concerning data security and the use of traffic and location data by the police against the principles of purpose limitation, transparency, judicial control and effective remedies (De Vries at al.2011).

- Is retention of data suitable to attain its purpose?

The aim of the Directive in terms of telecommunications data retention is to ensure that the data be available for the purposes of the investigation, detection and prosecution of serious crime. Obviously, it is difficult to discredit usefulness of traffic and location data for such purposes. Both, literature and media provide us with variety of reports on real criminal cases which support this standpoint (Who Knows 2004). Notwithstanding, more systematic analyses showing, for instance, the relation of the

crime solution due to the use of telecommunication data are hardly available. Instead, we are faced with general assertions on this subject, like the recent one coming from the UK („Communications data provides evidence in court to secure convictions of those engaged in activities that cause serious harm. It has played a role in every major Security Service counter-terrorism operation and in 95 per cent of all serious organised crime investigations") (UK Government). The statement on Poland ("in the years 2000-2005 traffic data obtained by the prosecutors from telecom operators was crucial for the effective prosecution of offenders in 402 serious crime cases") represents a similar approach (Projekt 2006). In view of such reports, the usefulness of telecommunications data for the purposes of law enforcement and criminal justice cannot be denied. However, this does not mean that the data retention regime is a necessary condition for a successful operation of the criminal investigation system nor does it mean that the abovementioned purposes cannot be attained by less restrictive measures.

● Is retention of data necessary for the attainment of the purpose?

The widely spread among experts and the public opinion has it that the data retention regime is deficient in many respects. Furthermore, it is believed that the measure has serious disadvantages, especially when approached from the protection of individual rights perspective. In comparison with its main alternative – the preservation of data regime adopted in Article 16 of the 2001 CoE Convention on Cybercrime and many national legislations, the disadvantages are even more visible (Convention on Cybercrime 2001). The leading argument in favor of the data preservation is that it does not require a service provider to collect data prospectively nor does it permit the government to preserve anything in a provider's system. Only these data is retained which relates to a particular investigation. The solution complies with the requirements for human rights protection (Explanatory Report, 152 and 161).

In addition, the research has shown that the data preservation at least in some countries has proven to be a very efficient measure. In Germany, for an instance, the efficiency of the communication service providers under the data preservation regime was high enough to satisfy almost entirely the needs of the law enforcement authorities concerning requested traffic data. As findings of two German studies suggest, under the so-called "quick freeze" approach the rate of unsuccessful data requests (i.e., the share of criminal cases in which traffic data had been requested by German authorities but had already been deleted by the communications service providers) was very low. In a survey of the Max Planck Institute carried out on the sample of 467 criminal cases from 2003 and 2004 in which 1,257 traffic data requests were made, only 4 % constituted unsuccessful data. Taking into account that in 2005 40,000 telecommunications data requests were made, this would represent only 0.01% of the 4.9 million criminal investigations nationwide (Albrecht et al. 2008). In other words, for 99.99% of annual criminal investigations, the data preservation might be viable alternative for data retention regime (DeSimone 2010).

The parallel analysis was conducted by the Bundeskriminalamt (Federal Office of Criminal Investigation), and it revealed that in 2005 there were only 381 cases nationwide—0.001% of the 6.4 million annual crimes in Germany—in which unavailable data was requested from communication service providers (DeSimone 2010). The most recent empirical evidence coming from the German Federal Republic provides additional argument against the data retention regime. A study of the criminological department of the Max Planck Institute for Foreign and International Criminal Law has demonstrated that the clearance rates for both serious and computer-related crime did not increased under the data retention legislation (2008-2009) (Albrecht et al. 2011). In other words, the security of the population appears to be unrelated with the mandatory data retention regime. Furthermore, in terms of the police statistics it is approximately on the same level that was observed earlier, under the data preservation scheme.

Needless to say, the above findings may undermine

the belief that data retention is necessary.

- Is the measure proportionate in the strict sense?

Finally, the proportionality assessment of the constitutional rights and freedoms restrictions (Article 31(3) of the Polish Constitution) requires answer to the question on whether the law of data retention in Poland is proportional to the burdens it places on the citizen. The present author's answer to this question is definitely negative. In view of the foregoing discussion on the effects of the Directive implementation to the Polish legal system it is clearly visible that the present regulation of data retention lacks any guarantees and safeguards for individuals rights and freedoms recognized both at the international (European) and national levels.

The Constitutional Tribunal in its judgment of 12th December 2005 (K 32/04) specified what checks and balances the legislator should impose on surveillance measures when introducing them to the legal system. According to this ruling, the police surveillance "should be accompanied by appropriate substantial guarantees, including a definition of limits on interference within the sphere of privacy, as well as procedural guarantees such as: the obligation to report the control and to legalise it by an external organ; the obligation to make available, even if only in a limited scope and from a certain moment, the information regarding the control and its results to the concerned person; control mechanisms in case of abuse on the part of the controlling organ". However, none of these guarantees is included into a legal framework of data retention. Simply speaking, such an intrusive measure is largely unregulated and its application remains beyond the scope of any external control.

Having approached the following issue from the perspective, one should not be astonished with an incredibly high number (1,06 million) of requests for access to traffic and location data submitted by the law enforcement and intelligence services in 2009, and even higher (1,8 million) in 2011 (Office for Electronic Communications).

4. Awaiting for the ruling of the Constitutional Tribunal

In 2011 two complaints concerning implementation of the Directive 2006/24/EC to the Polish legal system were lodged to the Constitutional Tribunal. On 28th January 2011 a group of deputies representing the Democratic Left Alliance party (Sojusz Lewicy Demokratycznej) applied to the Constitutional Tribunal with a motion requesting to consider nonconformity of the data retention legislation to the Constitution. On 1st August 2011 a similar motion was submitted to the Tribunal by the Commissioner for Citizens' Rights. Both of these complaints plead the infringements of identical provisions of the Constitution (i.e., Articles 31 sec.3, 47, 49, 51 sec. 2) and the European Convention on Human Rights (Article 8). Also, in both complaints there is consistency in pointing out failures of the statutory regulations against that background (i.e. the lack of an independent oversight on the access to data, the lack of a precise legal provision that exactly determines the purposes of gathering and use of data, the lack of notification of the person who was the target of the measure, the lack of obligation to delete data which are no longer necessary for the original purpose, etc.). Nevertheless, considerable discrepancy between the two writs can be noted. The complaint of deputies of the Democratic Left Alliance party was based on the argument that the data retention itself is a disproportional intrusion into the private lives; thus, must be regarded as a constitutionally objectionable regulation. Comparatively, the Commissioner's complaint is not as far-reaching as the Democratic Left Alliance party's is and does not question constitutionality of data retention per se. The argument raised by the deputies, however, is no longer valid - it expired along with the mandates of the deputies in the last parliamentary elections. Consequently, it will not be taken into consideration by the Constitutional Tribunal whose decision on the motion of the Commissioner for Citizens' Rights is expected to arrive soon. ■

* Andrzej Adamski (aadamski@law.umk.pl) is a professor in criminal law and computer law at the Faculty of Law & Administration, Nicolaus Copernicus University, Toruń, Poland.

[1] The Telecommunication Law amendment of 16 November 2012 has reduced the data retention period up to 12 months.

Endnotes:

Article 20c of the Law of 6th April 1990 on the Police (amended):
1. Data that identify a telecommunications network subscriber, termination points of a network or telecommunications device, data about completed or attempted connections between specific telecommunications devices or network termination points, and the circumstances and type of the connection may be disclosed to the Police and processed by the Police only with the view to crime prevention or detection.
2. The data referred to in Paragraph 1 may be disclosed:
(1) at a written request of the Police Commander in Chief or a Voivodship Police Commander,
(2) verbal request of a police officer being in possession of a written authorization issued by the persons referred to in Subparagraph 1 above.
3. Telecommunications network operator shall notify disclosure of the data referred to in Paragraph 2 (2) to the territorially competent Voivodship Police Commander.
4. Telecommunications network operators shall disclose the data referred to in Paragraph 1 to the police officers specified in the request lodged by a Police authority.
5. The data referred to in Paragraph 1 may be disclosed via a telecommunications network.
6. The Police shall forward the materials obtained as a result of activities provided for in Paragraph 2 and containing information important for criminal proceedings to the territorially and technically competent prosecutor.
7. Materials obtained as a result of the activities provided for in Paragraph 2 and not containing any information which could be important for criminal proceedings shall be immediately destroyed in the presence of a committee, the fact being officially recorded.
8. The costs of disclosure of the data referred to in Paragraph 1 shall be incurred by the telecommunications network operator.

Article 16 of the Council of Europe Convention on Cybercrime – Expedited preservation of stored computer data:
1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

REFERENCES:

Adamski Andrzej, Obywatel bezpieczny, ale przezroczysty. Nowelizacja ustawy o policji a ochrona danych osobowych (Citizen safe, but transparent. Data protection and the law on the Police Act amendment) „Rzeczpospolita" daily, 18.08.2000.

Adamski Andrzej, Kontrola dostępu do danych telekomunikacyjnych podlegających obowiązkowi retencji na tle ustawodawstwa wybranych państw Unii Europejskiej (Control of access to the retained telecommunication data in the legislation of some EU member states), Warszawa 2012.

Adamski Andrzej: Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy,(Crime in Cyberspace. Legal countermeasures in Poland and the Council of Europe Draft Convention), Toruń 2001, pp. 75 and 94.

Albrecht Hans-Jörg et. al, Rechtswirklichkeit der Auskunftserteilung über Telecommunicationsverbindungsdaten nach chapter 100g, 100h StPO, Max-Planck-Institute for Foreign and International Criminal Law [Reports on Research in Criminology] (February 2008)

Albrecht, Hans-Jörg; Kilchling Michael, Die Überwachung von Telekommunikations-Verkehrsdaten. Surveillance of Telecommunications Traffic Data 2009; http://www.mpg.de/408947/forschungsSchwerpunkt

Albrecht Hans-Jörg, Brunst Phillip, De Busser Els, Grundies Volker, Kilchling Michael, Rinceanu Johanna, Kenzel Brigitte, Nikolova Nina, Rotino Sophie, Tauschwitz Moritz, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Max-Planck-Instituts für ausländisches und internationales Strafrecht, Freiburg i.Br., Juli 2011

Breyer Patric, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR (2005) 11 European Law Journal 365.

Convention on Cybercrime (ETS No.185), Explanatory Report, 152 and 161, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm; http://conventions.coe.int/treaty/en/reports/html/185.htm

Człuchowski Wojciech, Dziennikarze na celowniku służb specjalnych (Journalists Targeted by the Intelligence Agencies), Gazeta Wyborcza 2010-10-08 ; http://wyborcza.pl/1,76842,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html#ixzz1u4r0XEgW

DeSimone Christian, Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive, German Law Journal 2010, vol. 1, issue 3, p. 311.

De Vries Katja, Bellanova Rocco, De Hert Paul and Gutwirth Serge, The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?), Springer 2011 (draft chapter to be published), p. 4.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union of 13.4.2006, No. L 105/54.

European Commission, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 COM(2011) 225 final, pp.9-12.

Federal Constitutional Court - Press office -Press release no. 11/2010 of 2 March 2010, Judgment of 2 March 2010 http://www.bundesverfassungsgericht.de/en/press/bvg10-011en.html

Goold Benjamin, Lazarus Liora, Swiney Gabriel, Public Protection, Proportionality, and the Search for Balance, Ministry of Justice Research Series 10/07, September 2007, p.1.

Judgment of the Constitutional Tribunal of 12 December 2005, (K 32/04), available at http://www.trybunal.gov.pl/index2.htm

Kuźmicz Ewelina, Mielecka-Kubień Zofia, Wiszejko-Wierzbicka Dorota (ed.) Karanie za posiadanie. Artykuł 62 ustawy o przeciwdziałaniu narkomanii – koszty, czas, opinie. Raport z badań, (Sentencing for possessing. Article 62 of the Drug Control Act – costs, time and opinions. Report from the survey) Instytut Spraw Publicznych, Warszawa 2009, s. 58.

Malone v. United Kingdom (1984) 7 EHRR 14 at paragraph 68.

Malte Spitz data retention 2009 http://www.zeit.de/datenschutz/malte-spitz-data-retention

Office for Electronic Communications, Statistical data provided in pursuant to Article 10 of the 2006/24/EC Directive.

Projekt ustawy o zmianie ustawy - Prawo telekomunikacyjne (Draft law on the Law of telecommunication) http://www.pis2.home.pl/dokumenty.php?s=rzad&iddoc=49&st=1

Rada Legislacyjna przy Prezesie Rady Ministrów, Opinia o projekcie ustawy o zmianie ustawy Prawo telekomunikacyjne oraz niektórych innych ustaw, RL-0303-32/09 (Legislative Council to the Prime Minister, Opinion on the draft law amending the Law on the Police and some other laws); http://radalegislacyjna.gov.pl/dokumenty/opinia-z-6-pazdziernika-2009-r-o-projekcie-ustawy-o-zmianie-ustawy-prawo-telekomunikacyjne

Rozporządzenie Ministra Infrastruktury z dnia 28 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego [Dz. U. Nr 19, poz. 166]. (Regulation of the Minister of Infrastructure of 28 January 2003 on the performance of duties related with the national defence, safety and public order in the State by the telecommunication providers) http://www.abc.com.pl/serwis/du/2003/0166.htm

Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania [Dz. U. Nr 226. poz.1828]. (Regulation of the Minister of Infrastructure of 28 December 2009 on a detailed specification of data and types of operators of public telecommunications networks or providers of publicly available telecommunications services obliged for its retention and storage, Journal of Laws of 2009, No 226 item 1828.

Taracha Adam, Czynności operacyjno-rozpoznawcze, aspekty kryminalistyczne i prawno dowodowe (Operational powers of the police. Forensic and Legal Aspects) Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2006, p.75.

UK government to store all internet traffic data http://www.v3.co.uk/v3/news/2271947/uk-government-store-internet

Ustawa z dnia 6 kwietnia 1990 r. o Policji [Dz. U. 2002, Nr 7, poz.58 ze zm.] (Law of 6 April 1990 on the Police, Journal of Laws of 2002, No. 7, item 58 with amendments), in English at http://www.policja.pl/portal/pol/90/4889/Polish_National_Police.html

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego [Dz. U. 1997, Nr 89, poz. 555 ze zm.] (Law of 6 June 1997 – The Code of Criminal Procedure, Journal of Laws of 1997, No. 89, item 555 with amendments).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne [Dz.U. Nr 174, poz. 1800 ze zm.] (Law of 16 July 2004 on Telecommunications , Journal of Laws of 2004, No. 174, item 1800 with amendments).

Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw [Dz. U. 2009.85.716.]

Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, Harvard Journal of Law & Technology, Volume 18, Number 1 Fall 2004 http://jolt.law.harvard.edu/articles/pdf/v18/18HarvJLTech307.pdf

Zasada proporcjonalności (w odniesieniu do prawa publicznego) w tezach Trybunału Konstytucyjnego (The principle of proportionality in the public law in the Constitutional Tribunal decisions), Biuro Trybunału Konstytucyjnego, Zespół Orzecznictwa i Studiów, 2009.

Paolo Balboni, Francesca Fontana*

Cloud computing: A guide to evaluate and negotiate cloud service agreements in the light of the actual European legal framework

Cite: P. Balboni, F. Fontana, *Cloud computing: A guide to evaluate and negotiate cloud service agreements in the light of the actual European legal framework*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, vol. 1/2013, p. 12-17.

Abstract

Cloud computing technology fulfills the need of on-demand, scalable, and interoperable outsourced services: nevertheless, in the actual, fragmented European legal framework, it poses many issues from a legal point of view. The article provides an overview of such issues, and of the most relevant documents that have been published in Europe during 2012 in order to correctly manage the use of cloud computing services from a legal point of view, with a special focus on the European Cloud Strategy and on Article 29 Working Party Opinion 5/2012 on Cloud Computing.

This last document, in fact, provides cloud clients with a useful checklist which contains all the elements that should be present in an agreement between a cloud service provider and a cloud client. Finally, the article's last paragraph is dedicated to the processing of sensitive data in the cloud.

Key words: cloud computing, cloud service provider, data protection, European Cloud Strategy, privacy, sensitive data, service agreements

1. Introduction

Cloud computing technology enables the transition to on-demand, scalable, and interoperable outsourced services. This makes the cloud very attractive to businesses, as it may help reduce costs and increase IT capabilities, (e.g., storage and computational capabilities). Moreover, higher data protection and data security standards can be achieved by leveraging the competences of reputable Cloud Service Providers ('CSPs'). Altogether, widespread adoption of cloud technology may not only result in economic benefits, but also in higher data protection and security. Nevertheless, businesses, governments and public administrations ('PAs') at large lack trust towards CSPs. One of the main reasons rests in the lack of transparency on CSPs' personal data processing. This actually poses concerns in terms of security and confidentiality of information, instead of making businesses, governments and PAs feel more secure.

Cloud computing is a relatively new technology, and, at present, still poses a number of issues, such as: a lack of international agreement on common terminology; the development of an unlimited and still-in-progress-technology; the huge amounts of data that are being accumulated and concentrated; the fact that data processing has become global; the lack of transparency with respect to CSPs processes, procedures and practices, including information on possible sub-contractors and the characteristics and locations of their processing. Europe is in the process of preparing itself for the change. During the last months, several documents have been published in order to correctly manage the use of cloud computing services from a legal point of view. The most relevant ones follow:

- article 29 Working Party Opinion 5/2012 on Cloud Computing (07.01.2012);
- ICO Guidance on the use of Cloud Computing (27.09.2012);
- Guidelines on Cloud Computing issued by the Irish Data Protection Commissioner (07.03.2012);
- CNIL Recommendations for companies planning to use Cloud computing services (06.25.2012);
- Italian Data Protection Authority Guidance on Cloud Computing – Cloud Computing – Proteggere i dati per non cadere dalle nuvole ("Vademecum del Garante sul Cloud Computing", may 2012);
- the Sopot Memorandum (04.24.2012), which is a very interesting working paper on Cloud Computing - Privacy and data protection issues, published by The International Working Group on Data Protection in Telecommunications; and, last but not least;
- the European Cloud Strategy, dated 27.09.2012.

This last one, in particular, has shown the key areas where actions are needed: (i) fragmentation of the digital single market due to differing national legal frameworks and uncertainties over applicable law; (ii) problems with contracts related to worries over data access and portability, change control and ownership of the data; (iii) a jungle of standards that generates confusion by, on one hand, a proliferation of standards and, on the other hand, a lack of certainty as to which standards provide adequate levels of interoperability of data formats to permit portability.

In the authors' opinion, the European Cloud Strategy clearly identifies the most significant needs around cloud, such as the "need for a chain of confidence-building steps to create trust in cloud solutions", and the key actions proposed to achieve is vital to devise a solid and globally integrated European Cloud Strategy. Standards should not be imposed top-down but identified together with the industry. Certification mechanisms, in order to really contribute at building trust in cloud, need to be operated by independent trusted entities, meaning that the main elements for a trustworthy certification need to be present: (i) certifier independency, (ii) impartiality in the auditing procedure, (iii) technical security of the e-seal, (iv) active monitoring of the certificate owner practice, (v) certifier enforcement power, (vi) and certifier accountability.

Despite the specific goals of the European Cloud Strategy, cloud clients still have to face a number of practical issues when entering a contract with a CSP. In fact, the privacy legislations throughout the 27 member States are different from one another. It is very likely that in 2014 the EU Commission Proposal for a General Data Protection Regulation[1] ('Draft Regulation') – directly applicable throughout all Europe - will enter into force: this will hopefully solve the problem. In the meantime, cloud clients can count on a very useful tool to deal with some practical difficulties. In fact, the above mentioned Art.29 WP Opinion 5/2012 provides a very practical 'privacy checklist' which may help cloud clients negotiate with CSPs, or at least evaluate terms and conditions set forth in the relevant cloud service agreement.

2. Privacy checklist

Art.29 WP Opinion 5/2012 states that "security, transparency and legal certainty for clients should be key drivers behind the offer of cloud computing services". The most important aspect to clarify prior to start a negotiation, is the allocation of privacy roles. On the one hand, it is clear that the cloud client acts as data controllers. On the other hand, the entire Art.29 WP Opinion 5/2012 is drafted under the assumption that the CSP is a processor. However, in our opinion, this should be carefully evaluated on a case-by-case basis[2]. Clients and CSPs should not rely too much on the definitions: it is fundamental to clearly state in the agreement who is responsible for doing what and the relevant liabilities in case of wrongful conduct.

Let us now see what information CSP should disclose to potential clients, on the one hand; and clients should carefully analyse before entering into a contract, on the other hand. This last obligation on the clients must be underlined, because they act as data controllers and thus are the ones that primarily bear data protection responsibilities and liabilities.

● A CSP MUST:

1. Share information about its identity (and its representative in the EU, if applicable), its data protection role (i.e., processor or controller), and the contact details of the Data Protection Officer or of a 'privacy contact person';

2. Describe in which ways personal data will be processed, the locations in which data may be stored or processed, the sub-contractors that may be involved in the processing, and whether the service requires installation of software on cloud customer's systems;

3. Specify whether/how data transfer outside the European Economic Area (EEA) – to countries without 'adequate level of data protection – takes place and on which legal ground (e.g., model contracts, binding corporate rules – Safe Harbor principles alone have not been recognised as an adequate means of transfer in the WP29 Opinion 5/2012);

4. Indicate the data security measures in place, with special reference to the availability of data, integrity, confidentiality, transparency, isolation (purpose limitation) and intervenability;

5. Describe how customers can monitor CSP data protection and security levels and whether there is the possibility to run audits for customers or trusted third parties;

6. Describe how customers can monitor CSP data protection and security levels and whether there is the possibility to run audits for customers or trusted third parties;

7. Disclose breach notification policies;

8. Provide information on data portability, migration and transfer back assistance;

9. Disclose data retention, restitution and deletion policies;

10. Prove accountability by showing policies and procedures the CSP has in place to demonstrate compliance throughout the CSP value chain (e.g., sub-contractors);

11. Ensure cooperation with clients to be in compliance with data protection laws, e.g., to ensure the exercise of data protection rights;

12. Provide information on how law enforcement requests to access data are managed;

13. Clearly describe remedies available for the customers in case of the CSP breaching the contract.

In consideration of the above, we would like to highlight some practical issues. Art.29 WP Opinion 5/2012, for the sake of transparency, states that the CSP:
- is obliged to disclose the name of all existing and potential sub-contractors that may process personal data, the type of service subcontracted and the characteristics of such sub-contractors (e.g., in a public digital register);
- has to guarantee that the sub-contractors will comply with the applicable EU data protection law.

Considering the significant number of potential sub-contractors that may process personal data, the turnover of such service providers and that this is sensitive business information for CSPs, the first obligation of transparency seems to be very cumbersome and disproportionate (not to say impossible to respect in practice). We believe that what really counts is the second obligation imposed on CSPs, that is, to guarantee sub-contractors' compliance with applicable EU data protection law; true expression of the accountability principle.

A similar comment has to be made as to the obligation for CSPs to disclose the list of locations where the data may be processed. In fact, it is very hard for CSPs to identify the locations of all data centres where personal data may be processed, especially in public cloud services. Furthermore, it may again be considered as CSP's sensitive business information. We believe that the most important thing for (potential) customers is that CSP guarantees about lawful data transfer outside the EEA and respects the agreement signed with customers in terms of territorial limitation of personal data flow.

Finally, we would like to point out a particular issue regarding sub-processing agreements. If a cloud client acts as a data controller, nulla quaestio: but what if the cloud client is a processor acting on behalf of a data controller? E.g., Company A, acting as a data processor, relies on a CSP to provide data storage to Company B. Art.29 WP Opinion 5/2012 explicitly foresees the possibility for a processor to appoint another processor, as long as it is accepted in advance by the controller; which retains at all times the possibility to terminate the contract in case of changes it does not accept, and it must be previously informed of. The Draft Regulation also foresees the possibility for a processor to appoint another processor. Even the Directive 95/46 on the protection of personal data - from which the 27 member States' national privacy legislations derive - does not forbids it. Consequently, in countries such as, e.g., in France, UK, Germany, Austria, Luxembourg, Por-

tugal, The Netherlands a data processor can appoint another data processor (sub-processor). In Italy, however, the current data protection legislation only allows a data controller to appoint a data processor. In this case, the non-homogeneous European legal framework creates some practical difficulties that professionals have to cope with in a way to reduce the possible risk of privacy sanctions. Hopefully the enactment of the Draft Regulation will finally put an end to this type of inconsistencies.

3. Specific remarks on the processing of sensitive data in the cloud

Let us now make some considerations on the use of cloud computing for processing sensitive data, taking into consideration the application of mobile cloud computing technologies in healthcare.

The exponential increase of chronic diseases amongst the rapidly aging population, the progressive patient demand of home care, and the need of several EU national governs to strain healthcare budgets are demanding new approaches to healthcare. Cloud computing can help change this scenario and shift from a set of eHealth technologies to a portfolio of services running in the cloud. Moreover, the service model of the cloud could contribute to simplify the hardware and delay the investment for a larger infrastructure or for system maintenance. The mobile approach, largely encouraged by the cloud, could fill the needs of innovative technologies to support the design of distributed healthcare services, in particular provided at the patient's house. In fact, eHealth represents one of the sectors that could largely benefit by the ubiquity of mobile cloud services. The main applications are: (i) monitoring of patients, particularly of blood pressure, heart pulse, ECG (electrocardiogram), respiratory rate, body temperature and oxygen saturation; (ii) access to the patient medical summary from everywhere and sharing the therapy data; (iii) enabling personal care services; (iv) scheduling and managing of people and assets for at home care of chronic patients. Geriatrics, palliative cares, heart dysfunctions, post-surgery or rehabilitation are the main therapeutic areas, while personal care has a more preventive purpose. At-home healthcare probably provides one of the most complete scenarios for mobile cloud computing. Typically, such solutions allow medical organizations running home services to design every day activity by scheduling personnel (doctors, nurses, technicians, etc.) and assets (drugs, measurement and therapy equipment), considering several constraints, such as, patient location or therapy requirements. Furthermore, tools are offered for sharing patient's health data, taking and sharing notes, communicating within the organization, and storing data. Finally, geo-localization features available on the mobile interface help the operators to reach the patients in the shortest time.

Nevertheless, ensuring security of health related data while allowing patients' global cross-boarder healthcare, and determining responsibility and accountability for data protection breach are crucial factors to be taken into consideration for the correct development of the eHealth sector. Starting from the last factor, let us point out that there is a significant number of players involved in the eHealth services: PAs, Local Healthcare Authorities, hospitals, private practices, doctors, administrative staff, etc. – to whom we refer as Healthcare Provider(s). The data controller is the individual or entity that determines purpose and means of processing of personal data. The data processor is the individual or entity that processes personal data on behalf of the controller (Article 2.d Directive 95/46/EC). It looks quite clear the Healthcare Provider is clearly a data controller, but the question is: is the CSP is a data controller or a data processor? The fact is that in the e-Health sector, the CSP can be qualified either as a controller or as a processor, depending on factual circumstances. In fact, in this field a CSP normally independently decides on data security measures and on the purpose of the processing related to the service provided[3], while the cloud user, i.e. the Healthcare provider, independently decides on the purpose of the processing related to the use of the service provided by the CSP, on some of the essential means of processing. Basically, in the eHealth (mobile) cloud environment both the Healthcare Provider and the CSP will most likely be data controllers with respect to different phases of the data processing related

to patient care. Legal responsibility for controllers (Healthcare provider and CSP) shall thus be limited to issues concerning purposes, means and the security related to their relevant data processing. As a consequence, the CSP could be in a legal position close to that of any Information Society Provider as defined under Directive 2000/31/EC.

As far as data transfers are concerned, Article 29 Working Party has already stressed the importance of adequately protecting the health-related data in the (WP 131/2007) working document on the processing of personal data relating to health in electronic health records (EHR). Health-related data should be stored within jurisdiction applying the Directive 95/46/EC or an adequate data protection legal framework. Furthermore, transfer of such data to countries outside the European Economic Area (EEA) can only occur either on the basis of prior patient's explicit consent or on the condition that the data are anonymised (or, at least, pseudonymised). And it is worth recalling that there are countries where in principles health-related data cannot exit their borders (e.g., UK). As a further consideration, we believe that the legislator should enable other lawful ways to transfer sensitive data (such as, health related data) than the data subject's consent, anonymisation or pseudonymisation. More precisely, we believe that assuring adequate data security and clear allocation of responsibility/accountability throughout multiple transfers from the Healthcare provider(s) to the CSP(s) (but also among the subjects involved in the care of the patient) would be better than relying on patient consent. In fact, very often data subjects/patients do not even know what they consent to, and in this way, we may achieve de facto a protection of data subjects and their personal data (as opposed to formal protection), and enable global cross-border healthcare for patients.

Finally, pursuant to Article 17 of the Directive 95/46/EC, appropriate technical and organizational measures have to be implemented by the data controller and by its processors to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Given the sensitivity of the data processed in the healthcare environment, Article 29 Working Party has explicitly recommended that access to data by unauthorized persons must be virtually impossible and prevented. Concurrently, availability of the system for authorized professionals must be virtually unlimited where there is a genuine need to know. Furthermore, some of the key security requirements in such environment are:
- reliable and effective system of electronic identification and authentication;
- comprehensive logging and documentation of all processing steps which have taken place within the system;
- preventing unauthorised access to or alteration of data at the time of transfer or of back up storage, e.g., by using cryptographic algorithms.

Such requirements apply both to the Healthcare(s) provider and to the CSP(s), irrespective of whether the latter is to be considered data controller or data processor. We believe that data security may benefit from cloud services, due to the fact that large CSPs have generally more recourses, including better trained personnel, to dedicate to data security than the average Healthcare provider. The problem may rest in assuring necessary data security requirements throughout the whole data flow (in and out the cloud). In this respect, we consider that rigorous identity and access management, and deployment of robust (mobile) networks, are key to compliance with the aforementioned obigations.

4. Conclusions

Prior to migrate to the cloud, businesses, governments and PAs should carefully verifying data privacy and data security policy of the CSPs and choose the one that offers better level of data protection. Cloud clients should also regularly monitor data protection compliance of the selected CSP and look into limitations and exclusions of liability clauses. CSPs that do not provide transparency and have unreasonable limitations and exclusions of liability clauses in their conditions of service should be avo-

ided. More generally, businesses, governments and PAs should focus on the cloud service agreement. There, clear duties and obligations for the parties needs to be laid down. In this respect, the privacy checklist provided in WP29 Opinion 5/2012 (see above Section 2) can be very useful evaluation. Moreover, in WP29 Opinion 5/2012 it is underlined that security, transparency and legal certainty for clients should be key drivers behind the offer of cloud computing services. In this respect, it is very important to have a tool for structured disclosure of relevant CSP privacy and data protection practices. This way, CSPs can offer transparency about their privacy policies and (potential) customers can compare CSPs and take informed and responsible decisions. To this end, we would like to draw attention to Cloud Security Alliance ("CSA")'s initiative on Privacy Level Agreement ("PLA"). In a nutshell, PLA is meant to be similar to services level agreement ("SLA") for privacy. In the PLA (typically an attachment to cloud services agreement), CSP will clearly declare the level of privacy and data protection that it undertakes to maintain with respect to the relevant data processing, in a format similar to what is used by other CSPs. ■

* Dr Paolo Balboni (paolo.balboni@ictlegalconsulting.com), Scientific Director of European Privacy Association, Cloud Computing Sector Director and responsible for Foreign Affairs of Italian Institute for Privacy, Lawyer admitted at the Bar in Milan specialised in ICT, new technologies law and personal data protection, Paolo Balboni is partner at ICT Legal Consulting. He provides legal advice to multinational companies, especially concerning personal data protection, e-contracts, e-commerce, e-marketing, advertising, cloud computing, Web 2.0 service providers' liability, Internet content providers' liability, e-signatures, digital retention of documents and intellectual property rights. He also advises celebrities on privacy and copyright matters. He has considerable experience in the following areas: IT, media & entertainment, e-Health, fashion and banking. He is the author of the book 'Trustmarks in E-commerce', Paolo Balboni is a Research Associate for Tilburg University (The Netherlands). He co-chairs the Privacy Level Agreement (PLA) Working Group of Cloud Security Alliance and he was the legal counsel chosen for the projects of European Network and Information Security Agency (ENISA) on 'Cloud Computing Risk Assessment', 'Security and Resilience in Governmental Clouds', 'Procure Secure: A guide to monitoring of security service levels in cloud contracts' and 'Common Assurance Maturity Model – Beyond the Cloud (CAMM)', Paolo Balboni is often involved in European Commission studies on new technologies and data protection, and also participates on several speaking engagements at international conferences on these matters. He obtained his Law degree with distinction from the University of Bologna in 2002, Ph.D. from Tilburg University (the Netherlands) in 2008 by defending a thesis on Comparative ICT Law titled: Trustmarks: Third-Party Liability of Trustmarks Organisations in Europe. He speaks fluent Italian, English and Dutch and has a good knowledge of German, French and Spanish.

Francesca Fontana (francesca.fontana@ictlegalconsulting.com), associate of ICT Legal Consulting and Fellow of the European Privacy Association, she is specialized in privacy and data protection. Ms. Fontana has considerable experience in the healthcare, media and entertainment sectors. Graduated in law at the University of Bologna, she is fluent in Italian, English, Spanish and has a good knowledge of French.

[1] COM(2012) 11 final of 25/1/2012.

[2] WP29 Opinion 5/2012 explicitly refers to WP29 Opinion 1/2010 on the concepts of 'controller' and 'processor' and to the Draft Regulation, which both state that if a processor processes data beyond the purpose for which they are collected, it becomes a controller. In fact, this happens very frequently in the cloud environment, where a CSP usually decides where to store or transfer data according to its own business and security reasons. This seems to be sufficient to make the CSP a controller. So, one must be careful in assuming that a CSP is merely a data processor.

[3] Cfr. WP29 Opinion 1/2010 on the concepts of 'controller' and 'processor'.

Karol Dobrzeniecki*

Konflikty wartości konstytucyjnych związane z funkcjonowaniem Internetu (The conflicts of constitutional values connected with Internet)

Cytowanie: K. Dobrzeniecki, *Konflikty wartości konstytucyjnych związane z funkcjonowaniem Internetu*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, nr 1/2013, s. 18-23.

Abstrakt

Wraz z rosnącą popularnością Internetu, wciąż pojawiają się nowe kwestie prawne. Niektóre z nich są o charakterze czysto technicznym, ale część ma znaczenie fundamentalne i dotyczy wprost materii konstytucyjnej. Powstaje szereg pytań, na które nie ma prostych odpowiedzi. Czy wolności i prawa obywatelskie powinny przysługiwać w takim samym stopniu niezależnie od tego, przy użyciu jakich środków technicznych uprawnieni z nich korzystają? Jakie znaczenie ma elektroniczna forma realizowania indywidualnej, społecznej lub politycznej aktywności? Jak chronić poszczególne wartości konstytucyjne wobec specyfiki internetowej komunikacji i jaka powinna być reakcja państwa wobec faktu, że nowe media jednocześnie poszerzają faktyczną sferę wolności, ale także stanowią zagrożenie dla pewnych wartości konstytucyjnych, jak np. prywatność, życie rodzinne czy własność intelektualna? Następuje gwałtowny wzrost podaży różnorodnych treści w formie elektronicznej dla szerokiej publiczności. Pojawiają się przekazy, które są potencjalnie groźne dla moralności i bezpieczeństwa publicznego, co mogłoby uzasadnić interwencję ze strony ustawodawcy. To z kolei pociąga za sobą kwestię oceny konstytucyjności przyjmowanych aktów. Podawane przeze mnie przykłady dotyczyć będą przede wszystkim debaty konstytucyjnej toczącej się w Stanach Zjednoczonych, ale globalny zasięg Internetu sprawia, że podobne dylematy pojawiają się w większości konstytucyjnych państw Zachodu.

Można zaryzykować tezę, że w związku z funkcjonowaniem Internetu państwa są zmuszone na nowo wytyczać granice pomiędzy różnymi wartościami konstytucyjnymi. Zdaniem niemieckiego socjologia prawa, Günthera Teubnera, digitalizacja jest, obok prywatyzacji i globalizacji, jednym z najważniejszych wyzwań, przed którymi stoi współczesna teoria konstytucyjna podobnie jak konieczność odpowiedniego dostosowania dziedzictwa konstytucyjnego państw zachodnich do tych zjawisk.

Słowa kluczowe: digitalizacja, kontrola normatywna, prawa i wolności obywatelskie, uprywatniona regulacja

---

Cite: K. Dobrzeniecki, *Konflikty wartości konstytucyjnych związane z funkcjonowaniem Internetu*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, vol. 1/2013, p. 18-23.

Abstract

Ever-rising popularity of the Internet has provoqued new legal issues to emerge. Some of them are mainly of technical nature; whereas, others - of a constitutional one. Thus, important questions have appeared. The questions require immediate response. However, there is no simple answer to most of them. For example, should the civil rights and obligations remain unchanched regardless of the technical means which are used by citizens? What meaning do the digital forms of social as well as individual or political activity have? How can constitutional values be protected in the digital communication? What response should be given by the authorities facing the fact that new means of communication enlarge the scope of freedom but at the same time threaten constitutional rights and freedoms such as: privacy right, family life protection or intellectual property? The amount of information is growing and simultaneously the number of potential recipents is on increase. Some of the digital communication include content which is demoralizing or threatens public safety. Such instances leads to legislative interventions the result of which does not always comply with the Polish Constitution.

The author concentrates mainly on the debate concerning new technologies and constitution which takes place in the USA. Still, the remarks and hypotheses presented in the article can be transposed into the European legal systems which due to the global scope of the Internet can experience similar challenges.

The hypothesis stated by the author is that the Internet has forced the contemporary legal systems to rethink and redefine constitutional rights and obligations. According to German sociologist of law, Gunther Teubner, besides privatisation and globalisation, digitalisation is one of the most significant consitutional challenges which requires redefinition of the constitutional values in the European legal system.

Key words
civil rights and freedom, digitalization, normative control, regulation

1. „Aczasowość" Internetu

Jedną z właściwości komunikacji internetowej jest jej swoista „aczasowość". Manifestuje się to w zwiększeniu tempa powstawania stosunków społecznych za pośrednictwem Sieci, a także ich względnej nietrwałości oraz przełamywaniu wielu barier czasowych w relacjach międzyludzkich. Również technologie tworzące światową sieć komputerową podlegają szybkiej transformacji. W efekcie, wiele ocen prawnych dotyczących poszczególnych aspektów Internetu szybko ulega dezaktualizacji. Analogicznie wygląda sytuacja orzeczeń sądowych. Podczas rozpatrywania przez Sąd Najwyższy USA pierwszej w historii sprawy dotyczącej Internetu (Reno v. ACLU, 1997) sędzia Antonin Scalia, w jednej z ustnych wypowiedzi na rozprawie doszedł do następujących wniosków. „Mamy do czynienia ze strukturą podlegającą niezmiernie gwałtownej zmianie. Czy nie jest więc możliwe, że ustawa której konstytucyjność badamy i którą w dniu dzisiejszym uznajemy za niezgodną z konstytucją stanie się konstytucyjna np. w przyszłym tygodniu, w przyszłym roku albo za dwa lata?"[1].

W tym kontekście państwowe systemy stanowienia reguł prawnych jawią się jako powolne, scentralizowane, biurokratyczne molochy. Często nie potrafią przystosowywać swoich struktur do szybkich zmian zachodzących w dziedzinie techniki. Tworzą reguły, które zazwyczaj okazują się regułami zaprojektowanymi dla „wczorajszych" rozwiązań technicznych. Gwałtowność przemian na polu techniki nie znajduje również odzwierciedlenia w tempie działania państwowego wymiaru sprawiedliwości. W czasie od momentu wszczęcia procesu sądowego do chwili jego zakończenia może ulec zmianie model prowadzenia działalności e-przedsiębiorstwa. W wielu przypadkach prowadzi to do perturbacji przy wykonywaniu orzeczeń.

2. Moralność publiczna

Według badań przeprowadzanych w USA, na początku XXI wieku, nawet najmłodsi użytkownicy Internetu byli wystawiani na oddziaływanie przekazów o silnym nacechowaniu seksualnym. Często miało to miejsce niezależnie od ich woli, ani tym bardziej od woli opiekunów. W przypadku nastolatków problem ten dotyczył już praktycznie co drugiej badanej osoby[2]. Amerykański ustawodawca podjął próbę znalezienia rozwiązań prawnych, które pozwoliłyby chronić małoletnich. Przyjmowane w tym celu ustawy, począwszy od roku 1996, kiedy wydano Communications Decency Act, były kolejno uznawane przez Sąd Najwyższy USA za sprzeczne z Pierwszą Poprawką do Konstytucji[3]. Sąd stwierdził, że prawodawca, chroniąc dzieci, nie był w stanie zabezpieczyć praw osób dorosłych[4]. Wszelkie ograniczenia wolności słowa ze względu na treść przekazu podlegają w Stanach Zjednoczonych ścisłej i surowej analizie pod kątem ich zgodności z Ustawą Zasadniczą (ang. *strict scrutiny analysis*). Internet stał się siłą napędową dyskursu obejmującego z jednej strony rozważania poświęcone wartościom konstytucyjnym i zasadom techniki prawodawczej, z drugiej zahaczającym o pogłębioną analizę właściwości systemów przetwarzania i transmisji danych. Technika, do której nowe ustawy się odnosiły, podlegała i podlega ciągłej, szybkiej transformacji. W tych warunkach niezwykle trudne okazywało się tworzenie norm, które mogłyby w sposób precyzyjny i adekwatny do potrzeb realizować uzasadniony interes społeczny (ang. *compelling interest*), a zarazem byłyby w najmniejszym, możliwym stopniu obciążające dla innych interesów i wartości. Ustawodawca amerykański ponosił kolejne porażki są dowe w starciach z obrońcami wolności obywatelskich, ponieważ nie potrafił pogodzić ochrony małoletnich z ochroną wolności słowa.

W kontekście sporu o ochronę dzieci pojawił się pogląd, że model bezpośredniej kontroli normatywnej nie jest dobrym rozwiązaniem tego problemu w USA. Ze względu na zobowiązania państwa w zakresie wolności słowa, regulację prawną mogą następować różne formy autocenzury albo samoregulacji, dyskretnie wspierane przez rząd. Regulacją pośrednią, czy też sterowaniem przez bodźce ekono-

miczne będzie przykładowo uzależnienie przyznawania szkołom i bibliotekom subsydiów rządowych od tego, czy zostaną w nich zastosowane aplikacje pozwalające na elektroniczne blokowanie niepożądanych treści na poziomie użytkownika (software blocking). Otwiera to nowy rozdział w zakresie kontrowersji konstytucyjnych. Po pierwsze dotyczą one określenia zakresu zautomatyzowanego blokowania. Nazbyt szerokie jego rozciągnięcie, obejmie treści, które podlegają ochronie konstytucyjnej (np. informacje na temat chorób wenerycznych, zaburzeń seksualnych itp.). Zbyt wąski zakres byłby równoznaczny z nieefektywnością systemu. Pozostaje też wątpliwość co do tego, kto ma ustalać kryteria selekcyjne, na bieżąco oceniać legalność obrazów, dźwięków i tekstów. Zasoby ludzkie i materialne organizacji produkujących „elektroniczne filtry" są zazwyczaj zbyt małe w porównaniu z potencjałem przemysłu internetowego (ang. *content industry*) i produkcji informacyjnej. Prawo stoi przed wyzwaniem opracowania metody oceny konstytucyjności instrumentów regulacji, w sytuacjach, gdy cele polityczne nie są realizowane drogą stanowienia reguł behawioralnych, ale np. poprzez promowanie określonego standardu technicznego[5].

Ze zjawiskiem digitalizacji wiąże się również potrzeba dokonania nowej wykładni niektórych klauzul generalnych. W prawie amerykańskim sytuacja taka powstała w zakresie konstytucyjnych standardów traktowania wypowiedzi mających charakter podżegania (ang. *incitement*) do naruszenia prawa lub do użycia przemocy[6]. Przy niezwykle liberalnym podejściu Sądu Najwyższego, który zezwala na zakazywanie jedynie najbardziej skrajnych przypadków tego rodzaju wypowiedzi, zaistniała potrzeba wypracowania modelu traktowania wypowiedzi rozpowszechnianych przez Internet, które mają swoją własną specyfikę. W tym kontekście, oryginalność nowej formy komunikacji polega, między innymi, na braku tradycyjnej relacji zachodzącej zazwyczaj pomiędzy mówcą a publicznością. Według istniejących standardów, wypowiedź utraci ochroną ze strony pierwszej poprawki tylko wówczas, gdy jest ona nakierowana bezpośrednio na wywołanie natychmiastowego (ang. *imminence*) skutku w postaci bezprawnych działań, a jej adresatami jest dająca się wyodrębnić grupa ludzi. Komunikacja w trybie sieciowym przebiega w taki sposób, że od biorcy opublikowanej informacji bardzo często pozostają nieznani jej nadawcy. Wiele przemawia więc za tym, że standard powinien być przeformułowany, szczególnie wobec potwierdzonych przypadków negatywnego oddziaływania przekazów internetowych na zachowanie się różnych grup i środowisk[7].

3. Uprywatnienie regulacji

Wzmiankowane przez Teubnera zjawisko „uprywatnienia" można odnieść do stosunków własnościowych panujących w obrębie infrastruktury Internetu, zarówno w zakresie urządzeń, jak i oprogramowania. Znajduje się ona przeważnie w rękach prywatnych. W kontekście pogłębiającej się zależności społeczeństwa od sprawnie działającej komunikacji elektronicznej nasila się problem wpływu podmiotów niepaństwowych na sposób korzystania ze swobód i wolności obywatelskich. W szczególności dotyczy to „uprywatnionej regulacji" wolności słowa, przez różnego rodzaju elektroniczne blokady komunikacyjne stosowne przez operatorów, dostawców Internetu, itp. Pod wpływem przewrotu informatycznego, w niektórych dziedzinach życia społecznego zatarciu ulega rozróżnienie, na to, co jest, a co nie jest działaniem państwa, za które bierze ono odpowiedzialność. Działania „czysto" prywatne powstają na gruncie uregulowań z zakresie własności i zobowiązań, które pozwalają na egzekucję „prywatnych reguł umownych" przy użyciu państwowego przymusu. Swoboda „ekspresji" w postaci rozpowszechniania różnego rodzaju wytworów kultury wpływa niekiedy destrukcyjnie na stan „majątku" (własność intelektualną), podczas gdy rozbudowana ochrona informacyjnego „majątku" może z kolei tłumić wolność wypowiedzi[8]. Państwo. przyznając albo definiując prawa ochronne dla coraz to nowych wytworów ludzkiej myśli, stwarza, tym samym, „mikromonopole" na korzystanie z fragmentów domeny publicznej. Wiele przemawia za tym, że działania takie powinny być objęte kontrolą zgodności z ustawą zasadniczą. Konstytucja przyznaje obywatelom określone prawa, ale również wyraża treść wartości podzielanych przez społeczeństwo. Te war-

tości mogą zostać naruszone tak przez podmioty prywatne, jak i publiczne. Popularyzacja korzystania z dóbr intelektualnych za pośrednictwem Internetu skłania do poważnej debaty na temat rozwinięcia doktryny publicznych praw podmiotowych, objęcia jej zakresem nie tylko wymiaru wertykalnego, pomiędzy państwem a obywatelem (w jurysprudencji amerykańskie tzw. *state action doctrine*), ale także horyzontalnego, między podmiotami prywatnymi (ang. *private action*). W przeciwnym wypadku może okazać się, że życie społeczne „wyemigrowało" do przestrzeni prywatnej, przy czym określenie „prywatna" będzie oznaczać „wyzwolona" z wartości konstytucyjnych[9].

Trzecim wzmiankowanym wyzwaniem dla współczesnej teorii konstytucyjnej jest fenomen globalizacji. Zygmunt Bauman zalicza nowoczesne środki komunikacji do najważniejszych czynników stymulujących mobilność we współczesnym świecie. Prowadzi to do kurczenia się czasu i przestrzeni. Sprzyja powstawaniu wspólnot o charakterze ogólnoświatowym i równoległej erozji wspólnot tradycyjnych, które na skutek przewrotu informatycznego utraciły ważny atut. „Komunikacja wewnątrzgrupowa nie posiada żadnej przewagi nad procesem wymiany informacji pomiędzy wspólnotami, jeżeli obydwa te procesy odbywają się w okamgnieniu"[10].

4. Lokalne standardy w globalnej Sieci

Pojawia się potrzeba przeformułowania niektórych klauzul konstytucyjnych odnoszących się do standardów zachowań, typowych dla społeczeństw przedindustrialnych. Jedną z nich są popularne w prawie amerykańskim tzw. community *standards*, np. „bieżące standardy lokalnej społeczności w zakresie opisu lub przedstawiania treści seksualnych"[11]. Ocena stopnia „nieprzyzwoitości" (ang. *obscenity*) oferowanych do sprzedaży książek, czasopism, publicznie dostępnych pokazów i widowisk została w Stanach powierzona ocenie według kryteriów przyjmowanych w społecznościach lokalnych (tzn. tych, z których wywodzą się sędziowie przysięgli). Zastosowanie tego rodzaju standardów w środowisku cyfrowym wydaje się szczególnie trudne, ponieważ *community standards* opierają się na wzorcach ocennych, powstałych w ramach społeczności zorganizowanych na gruncie fizycznego sąsiedztwa[12]. Wiele przemawia za tym, że doktryna w zakresie „nieprzyzwoitości" powinna ulec rekonceptualizacji, ponieważ zmienia się znaczenie pojęcia „społeczności", tracąc stopniowo swój dawny, terytorialny charakter. Przeobraża się też sposób dystrybucji tego rodzaju materiałów. Dotychczasowa konstrukcja normatywna prowadzi do nieracjonalnego wniosku, iż każdy podmiot publikujący w Sieci powinien zapoznać się ze standardami obowiązujących w setkach, o ile nie tysiącach lokalnych społeczności. Globalizacja środków horyzontalnej komunikacji elektronicznej może zatem przyspieszyć proces ujednolicenia i uniwersalizacji sztandarów ocennych, do ich liberalizacji albo zmiany, w taki sposób, aby stały się niezależne od terytorialnych przesłanek[13].

Globalna dostępność treści publikowanych w Internecie stworzyła także okazję do powstawania konfliktów dotyczących stopnia ochrony różnych wartości konstytucyjnych. Dochodzi do nich również pomiędzy krajami o reżimach demoliberalnych, takimi jak np. Francja i USA. Przykładowo, prawo francuskie zabrania publicznego przedstawiania umundurowania, symboli i emblematów organizacji odpowiedzialnych za zbrodnie przeciwko ludzkości. Dotyczy to m.in. byłej niemieckiej partii nazistowskiej. Pierwsza Poprawka do Konstytucji USA chroni tymczasem również taką formę ekspresji. Umieszczenie przez amerykańskiego operatora (Yahoo! Inc.) w serwisie aukcyjnym, ogłoszenia o sprzedaży nazistowskich pamiątek doprowadziło do procesu przed francuskim sądem przeciwko lokalnemu przedstawicielowi firmy. Sąd nakazał zastosowanie wszelkich możliwych środków technicznych, aby uniemożliwić Francuzom dostęp do tego typu aukcji. Sąd amerykański orzekł z kolei, że decyzja sądu francuskiego nie mogłaby zostać wykonana na terytorium USA, ponieważ godzi ona w chronioną prawem wartość konstytucyjną[14]. Podobnie przedstawia się sytuacja z publicznym zaprzeczaniem zbrodniom nazistowskim oraz tzw. mowie nienawiści (ang. *hate speech*), które są kryminalizowane w wielu krajach europejskich, a także w bliskiej USA Kanadzie[15]. Wzrost znaczenie Internetu wywołuje

wzrost częstotliwości tego rodzaju konfrontacji pomiędzy uregulowaniami konstytucyjnymi. Stwarza presję na rzecz harmonizacji prawa, wypracowanie wspólnego standardu ochrony powszechnie uznawanych, choć różnie rozumianych wartości konstytucyjnych. Z drugiej strony istnienie różnych standardów narodowych stawowi swoista tamę przed próbami ocenzurowanie globalnej sieci przez którekolwiek państwo.

Powyższe przykłady pokazują, że z funkcjonowaniem Internetu wiążą się sytuację w których określone wartości konstytucyjne wykluczają się nawzajem, wskutek czego urzeczywistnienie jednej wartości nie może się dokonać inaczej, jak poprzez poświęcenie innej albo przynajmniej jej ograniczenie1. Jak widać, szczególnie wyraźne są konflikty wartości w obrębie praw i wolności obywatelskich. Taki stan rzeczy powinien słaniać do refleksji. E.J. Koops zwraca uwagę na to, że nowe technologie zmieniają stosunki sił pomiędzy stronami tradycyjnie traktowanymi przez prawo jako te słabsze i te silniejsze np. obywatelami i urzędnikami, pracownikami i pracodawcami, konsumentami i przedsiębiorcami. Te przesunięcia nie mają jednostronnego charakteru – przez co sposób kompensacji przez prawo powstających nierówności również nie jest oczywisty. Możliwość korzystania z Internetu i technologii informacyjnych w jednych obszarach prowadzi do zmniejszenia wcześniejszych nierówności, w innych powiększa istniejące wcześniej różnice pomiędzy słabymi a silnymi stronami. Koops postuluje uzupełnienie istniejących środków ochrony prawnej o takie, które pozwolą adekwatnie zadośćuczynić szkodom powstającym w ramach funkcjonowania złożonych systemów zarządzania ryzykiem. Byłyby to z jednej strony środki o charakterze administracyjnym, jak np. niezależne audyty monitorujące prawidłowość prowadzonych polityk, z drugiej skorzystanie z instrumentów prawnych innych niż tradycyjne stanowienie norm, w szczególności posłużenie się „socjo-techniczną infrastrukturą" np. technologiami podnoszącymi prywatność (ang. *privacy enhancing technologies*) i technologiami podnoszącymi transparentność (ang. *tranparency enhancing technologies*)[17]. Zastosowanie każdego z możliwych sposobów łagodzenia konfliktów wartości konstytucyjnych w środowisku internetowym, musi być jednak każdorazowo poprzedzone gruntownym rozpoznaniem regulowanej materii, jej specyfiki i kierunków ewolucji. ■

* Karol Dobrzeniecki (karol.dobrzeniecki@law.umk.pl), doktor nauk prawnych, adiunkt w katedrze Teorii Prawa i Państwa na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu.

W artykule wykorzystane zostały fragmenty monografii autora pt. Lex informatica, Toruń 2008.

[1] Zapis ustnej dyskusji, [w:] Reno v. ACLU, 521 U.S. 844 (1997) (No. 96-511), 1997 WL 136253, at *49 (19 marca 1997 r.)

[2] D. Thornburgh, H. S. Lin (red.), Youth, Pornography, and the Internet, National Academy Press, 2002.

[3] Zakazem rozpowszechniania objęto nie tylko treści obsceniczne (obscene), które już wcześniej zostały wyłączone z zakresu zastosowania pierwszej poprawki do Konstytucji USA jako pozbawione społecznej wartości. Rozciągnięto go także na treści dotąd uznawane za nieprzyzwoite (indecent) ale objęte konstytucyjną ochroną.

[4] Kwestionowano konstytucyjność m.in. Child Pornography Prevention Act z 1996 r., Child Online Protection Act (1998), Child Internet Protection Act (2000), Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (2003). Por. S.H. Kosse, Try, Try Again: Will Congress Ever Get It Right? A Summary of Internet Pornography Laws Protecting Children and Possible Solutions, „University of Richmond Law Review", vol. 38 2003-2004.

[5] L. Lessig, Code and the Other Laws of the Cyberspace, New York 1999, s. 181.

[6] W USA tzw. incitement standard ustalił Sąd Najwyższy w sprawie Brandenburg v. Ohio 395 U.S. 444 (1969).

[7] J.P. Cronan, The Next Challenge for the First Amendment: the Framework for an Internet Incitement Standard, „Catholic University Law Review", vol. 51 2001-2002.

[8] B.E. Jr. Nodzon, Free Speech in Digital Economy: an Analysis of How Intellectual Property Rights Have Been Elevated at the Expense of Free Speech, „The John Marshall Law Review", vol. 36 2002-2003, passim.

[9] P.S. Berman, Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to 'Private' Regulation, „University of Colorado Law Review", vol. 71 2000, passim.

[10] Z. Bauman, Gobalizacja, Warszawa 2000, s. 22.

[11] Klauzula ta stanowi część „testu obsceniczności", który został ustalony w wyroku Sądu Najwyższego USA - Miller v. California 413 U.S. 15, 24 (1974).

[12] Por. D.D. Burke, Cybersmut and the First Amendment: A Call for a New Obscenity Standard, „Harvard Journal of Law & Technology", vol. 9 nb. 1 1996, s. 108 – 113; J.S. Zanghi, „Community Standards" in Cyberspace, „Dayton Law Review", vol. 21 1995-1996, s. 108 i n.

[13] Problem ten porusza William D. Deane, uznając, że zastosowanie standardów ocennych gegraficznie wyodrębnionych społeczności do ustalenia odpowiedzialności karnej podmiotu publikującego przez Internet stanowi nadmierną ingerencję w wolność słowa - tenże, W.D. Deane, Copa and Community Standards on the Internet: Should the People of Maine and Mississippi Dictate the Obscenity Standard in Las Vegas and New York?, „Catholic University Law Review", vol. 51 2001-2002; Podobną opinię wyraża P.E. Lewis, A Brief Comment on the Application of the „Contemporary Community Standard" to the Internet, „Campbell Law Review", vol. 22 1999-2000.

[14] Sprawa Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

[15] C. Fogo-Schensul, More Than a River in Egypt: Holocaust Denial, the Internet, and International Freedom of Expression Norms, „Gonzaga Law Review", vol. 33 1997-1998.

[16] Definicja konfliktu wartości zaczerpnięta z : T. Ślipko, Zarys etyki ogólnej, WAM, Kraków 2004, s. 230.

[17] E.J. (Bert-Jaap) Koops, Law, Technology, and Shifting Power Relations, "Berkeley Technology Law Journal", Vol. 25, No. 2, 2010, s. 1029.

Przeczytaj
broszurę informacyjną

Read
information brochure

Paweł Litwiński*

Udostępnianie danych osobowych na potrzeby postępowań cywilnych

(Personal data disclosure for the purpose of conducting civil proceedings)

Cytowanie: P. Litwiński, *Udostępnianie danych osobowych na potrzeby postępowań cywilnych*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, nr 1/2013, s. 24-37.

Artykuł dotyczy problemu udostępniania danych osobowych na potrzeby postępowań cywilnych. Udostępnianie takich danych osobowych możliwe jest w polskim prawie dwutorowo: po pierwsze, na podstawie przepisów szczególnych ustawy o prawie autorskim i prawach pokrewnych, ustawy Prawo własności przemysłowej i ustawy o ochronie baz danych oraz po drugie, na podstawie ogólnych przepisów ustawy o ochronie danych osobowych.

Abstrakt

Z dokonanej analizy wyłania się sytuacja, w której przepisy ustawy o prawie autorskim i prawach pokrewnych, ustawy Prawo własności przemysłowej i ustawy o ochronie baz danych są interpretowane przez orzecznictwo sądowe i naukę prawa w ten sposób, że umożliwiają udostępnianie danych osobowych osób fizycznych, jednak tylko tych, które naruszają prawa własności intelektualnej. Wydaje się, że na podstawie tych przepisów można również udostępniać informacje objęte ochroną tajemnicy telekomunikacyjnej. Z drugiej strony, procedura oparta o ogólne przepisy ustawy o ochronie danych osobowych obejmuje swoim zakresem wszelkie sprawy cywilne, nie tylko dotyczące naruszeń praw własności intelektualnej. I mimo zmian w przepisach ustawy o ochronie danych osobowych, które – wydawałoby się – procedurę tą wyeliminują z systemu, polski organ ochrony danych osobowych w dalszym ciągu wydaje decyzje administracyjne nakazujące udostępnienie danych osobowych. Praktyka taka jest akceptowana przez część nauki prawa, przy sprzeciwie innych autorów. Orzecznictwo sądowe wydaje się tą praktykę akceptować, choć brak jest dotychczas jakiegokolwiek prawomocnego wyroku.

W tym świetle autor stawia tezę, że sytuacja dojrzała do ingerencji ze strony ustawodawcy, który powinien uporządkować zagadnienie udostępniania danych osobowych na potrzeby postępowań cywilnych. Jest to problem tym bardziej palący, że konieczność zapewnienia możliwości udostępniania danych osobowych na potrzeby postępowań cywilnych wynika wprost z międzynarodowych zobowiązań Polski, co potwierdził Europejski Trybunał Praw Człowieka w wyroku sprawie K.U. przeciwko Finlandii.

Słowa kluczowe: dane osobowe, Internet, postępowanie cywilne, udostępnienie danych osobowych, własność intelektualna

---

Cite: P. Litwiński, *Udostępnianie danych osobowych na potrzeby postępowań cywilnych*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, vol. 1/2013, p. 24-37.

This article concerns the problem of the personal data disclosure for the sole purpose of conducting civil proceedings. The access to such personal information is legitimate under Polish law in two situations; firstly, there is a specific provisions of the Copyright and Related Rights Law, Industrial Property Law, and the Database Protection Law which allows such disclosure; secondly, ther is a general provision in the Personal Data Protection Act.

Abstract

The author describes the interpretation of the provisions on personal data disclosure situated in the Copyright and Related Rights Law, the Industrial Property Law and the Database Protection Law. On one hand, the analysis of judicial decisions concerning the subject matter as well as views presented by academic scholars lead to the conclusion that theonly access to the personal data is allowed only if the individuals whose data is concerned violate intellectual property rights. What is more, it appears that under the above legislation also the information protected by the telecommunications secrecy might be accessed. On the other hand, the scope of the procedure based on the general provisions of the Personal Data Protection Act encompasses all civil cases, not only those concerning the IP rights infringements . Despite amendments of the Personal Data Protection Act, the procedure was not annulled from the Polish legal system. In consequence, the Polish Data Protection Authority has still competence to issue administrative decisions requiring the personal data disclosure. The current state of affairs is accepted only partially by academic scholars and among others it is still contro-

versial. The Polish judicature seems to notice less controversy in the issue than academic environment; however, the final verdict has not been reached yet.

In the light of the above concerns, the author argues that it is high time that the Polish legislative power intervened and sorted out the provisions on personal data disclosure.The problem is all the more urgent given the fact that the need to guarantee access to personal data for the purpose of civil proceedings is one of Poland's international obligations which was confirmed by the European Court of Human Rights in its judgment passed on the case K.U. versus Finland.This article concerns the problem of the personal data disclosure for the sole purpose of conducting civil proceedings. The access to such personal information is legitimate under Polish law in two situations; firstly, there is a specific provisions of the Copyright and Related Rights Law, Industrial Property Law, and the Database Protection Law which allows such disclosure; secondly, ther is a general provision in the Personal Data Protection Act.

The author describes the interpretation of the provisions on personal data disclosure situated in the Copyright and Related Rights Law, the Industrial Property Law and the Database Protection Law. On one hand, the analysis of judicial decisions concerning the subject matter as well as views presented by academic scholars lead to the conclusion that theonly access to the personal data is allowed only if the individuals whose data is concerned violate intellectual property rights. What is more, it appears that under the above legislation also the information protected by the telecommunications secrecy might be accessed. On the other hand, the scope of the procedure based on the general provisions of the Personal Data Protection Act encompasses all civil cases, not only those concerning the IP rights infringements . Despite amendments of the Personal Data Protection Act, the procedure was not annulled from the Polish legal system. In consequence, the Polish Data Protection Authority has still competence to issue administrative decisions requiring the personal data disclosure. The current state of affairs is accepted only partially by academic scholars and among others it is still controversial. The Polish judicature seems to notice less controversy in the issue than academic environment; however, the final verdict has not been reached yet.

In the light of the above concerns, the author argues that it is high time that the Polish legislative power intervened and sorted out the provisions on personal data disclosure.The problem is all the more urgent given the fact that the need to guarantee access to personal data for the purpose of civil proceedings is one of Poland's international obligations which was confirmed by the European Court of Human Rights in its judgment passed on the case K.U. versus Finland.

Key words

civil proceedings, intellectual property personal data, Internet, personal data disclosure

1. Wstęp

Problem udostępniania danych osobowych nabiera szczególnego znaczenia w związku z naruszeniami praw własności intelektualnej dokonywanymi z wykorzystaniem sieci Internet. Środowisko internetowe sprzyja bowiem działaniu w sposób anonimowy, bez podawania danych identyfikujących uczestnika obrotu, a często przy wykorzystaniu pseudonimów, czy wręcz z podaniem danych fałszywych. Stąd podmioty, które zamierzają dochodzić ochrony swoich praw wyłącznych w związku z domniemanymi naruszeniami, stają przed istotnym problemem praktycznym – w jaki sposób oznaczyć stronę pozwaną w piśmie inicjującym postępowanie sądowe? Zgodnie bowiem z art. 187 § 1 w zw. z art. 126 § 1 kodeksu postępowania cywilnego[1], w treści pozwu konieczne jest m.in. podanie imienia i nazwiska oraz adresu pozwanego. Wymóg ten w sposób oczywisty znajduje również zastosowanie w sprawach o naruszenie dóbr osobistych, czy autorskich praw majątkowych. Jednakże problem ma też istotnie szersze znaczenie – w jaki sposób uzyskać dane osobowe przyszłego pozwanego np. w sprawie o naruszenie dóbr osobistych, gdy przyszły powód nie dysponuje danymi osobowymi, przy pomocy których powinien oznaczyć stronę pozwaną, ponieważ sprawca posługuje się pseudonimem?

2. Udostępnianie danych osobowych

Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6 ust. 1 ustawy ochronie danych osobowych[2], dalej jako u.o.d.o.). U.o.d.o. w dalszej części art. 6 precyzuje, że osobą możli-

wą 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. Za dane osobowe należy więc uznać wszelkie informacje dotyczące osoby fizycznej, o ile możliwe jest zidentyfikowanie tej osoby na podstawie tych informacji[3]. U.o.d.o. nie zawiera przy tym katalogu (nawet otwartego) informacji mających charakter danych osobowych. Nie jest również możliwe ustalenie z góry katalogu informacji o charakterze danych osobowych[4]. Na potrzeby dalszych rozważań można jednak przyjąć z pewnością, że danymi osobowymi będą informacje identyfikujące stronę postępowania cywilnego, tj. imię i nazwisko oraz adres zamieszkania.

W przepisach ustawy o ochronie danych osobowych, jak i w innych aktach prawnych, brak jest legalnej definicji udostępniania danych osobowych. U.o.d.o. stanowi tylko w art. 7 pkt 2, że udostępnianie danych osobowych stanowi jedną z postaci przetwarzania danych. Natomiast w literaturze zwrócono uwagę, że udostępnianie danych osobowych następować będzie wówczas, gdy następuje przekazanie danych osobowych odbiorcy danych, który pełni w stosunku do tych danych rolę administratora danych, tj. podmiotu decydującego o celach i środkach przetwarzania danych osobowych[5]. W nauce prawa wskazuje się również, że z udostępnianiem danych osobowych mamy do czynienia wówczas, gdy następuje objęcie „danych w posiadanie" przez odbiorcę danych, który staje się wtedy administratorem danych osobowych[6].

Udostępnienie danych osobowych nastąpi więc wtedy, gdy administrator danych osobowych w sposób faktyczny przekaże, bądź inaczej umożliwi zapoznanie się z danymi osobowymi innej osobie lub podmiotowi, który to podmiot pełnić będzie w stosunku do tych danych osobowych rolę administratora danych. Samo „udostępnianie" danych ma przy tym charakter czynności faktycznej i może nastąpić w dowolny sposób – ważne, żeby w jej wyniku doszło albo do przekazania danych (np. kopia danych zapisana nanośniku), albo do umożliwienia zapoznania się z danymi.

Przekazanie danych osobowych domniemanego sprawcy naruszenia praw wyłącznych, w tym praw własności intelektualnej, czy też innych dóbr prawnie chronionych, podmiotowi, który zamierza wytoczyć powództwo przeciwko temuż sprawcy, winno zostać uznane za udostępnianie danych osobowych. Odbiorca takich danych sam bowiem będzie decydował o tym, w jaki sposób te dane wykorzysta (decydowanie o celach przetwarzania danych), a także jak to wykorzystanie danych nastąpi od strony technicznej (decydowanie o środkach przetwarzania danych). Tym samym podmiot taki powinien zostać uznany za administratora przekazanych mu danych osobowych (administratora danych to właśnie podmiot decydujący o celach i środkach przetwarzania danych osobowych), a cała operacja za udostępnienie danych osobowych.

3. Udostępnianie danych osobowych na potrzeby postępowań cywilnych w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej oraz Europejskiego Trybunału Praw Człowieka

Problem udostępniania danych osobowych dla potrzeb postępowań cywilnych pojawiał się wielokrotnie w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej oraz Europejskiego Trybunału Praw Człowieka.

Podstawowym problemem, przed którym stanął Trybunał Sprawiedliwości, było udzielenie odpowiedzi na pytanie, czy prawo unijne nakłada na państwa członkowskie obowiązek ujawniania danych osobowych na potrzeby postępowania cywilnego, w celu zapewnienia skutecznej ochrony praw autorskich. Na tak postawione pytanie Trybunał w sprawie Promusicae przeciwko Telefónica1 udzielił odpowiedzi negatywnej:

„Dyrektywy 2000/31 w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjne-

go, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), 2001/29 w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych [prawa autorskiego i praw pokrewnych] w społeczeństwie informacyjnym, 2004/48 w sprawie egzekwowania praw własności intelektualnej oraz 2002/58 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) nie zobowiązują państw członkowskich do ustanowienia obowiązku przekazania danych osobowych w celu zapewnienia skutecznej ochrony praw autorskich w ramach postępowania cywilnego, w sytuacji gdy stowarzyszenie niemające celu zarobkowego grupujące producentów i wydawców nagrań muzycznych oraz opracowań audiowizualnych wniosło o nakazanie, by dostawca usług w zakresie dostępu do Internetu wskazał tożsamość i adresy określonych abonentów, w celu umożliwienia mu wytoczenia następnie przeciwko tym osobom powództw cywilnych z tytułu naruszenia praw autorskich."

Jak się wydaje, pogląd ten może zostać przeniesiony również na inne przykłady roszczeń cywilnoprawnych, takie jak roszczenia o ochronę praw wyłącznych, czy roszczenia o ochronę dóbr osobistych. Co do zasady więc nie istnieje obowiązek wywodzący się z prawa Unii Europejskiej, który polegałby na konieczności ustanowienia w prawie krajowym procedury udostępniania danych osobowych na potrzeby sądowych postępowań cywilnych. Prawo wspólnotowe nie zabrania jednak ustanowienia takiego obowiązku w prawie krajowym.

Podobne stanowisko zostało zajęte przez Trybunał w sprawie LSG przeciwko Tele2[8]. W szczególności, Trybunał ponownie uznał, że właściwe dyrektywy nie wykluczają nałożenia na dostawców usług internetowych obowiązku ujawnienia danych osobowych użytkowników pozwanych o naruszenie praw autorskich. Z orzecznictwa Trybunału wynika jednak obowiązek zapewnienia równowagi pomiędzy prawem do prywatności, a ochroną własności intelektualnej. Obydwa te prawa wywodzą się bowiem z Karty Praw Podstawowych. Obowiązek zapewnienia równowagi pomiędzy prawami podstawowymi spoczywa na państwach członkowskich, które będą ustanawiać w krajowym porządku prawnym odpowiednią procedurę udostępniania danych[9].

Istotne znaczenie dla tematyki udostępniania danych osobowych może mieć również orzeczenie w sprawie Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget Aktiebolag, Storyside AB przeciwko Perfect Communication Sweden AB[10]. W sprawie tej zostało skierowane do Trybunału następujące pytanie:

„Czy dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (1), a w szczególności jej art. 3, 4, 5 i 11 wykluczają stosowanie przepisu krajowego, opartego o art. 8 dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (2), na mocy którego w postępowaniu cywilnym można, w celu zidentyfikowania określonego abonenta, nakazać dostawcy usług internetowych ujawnienie uprawnionemu z prawa autorskiego albo jego przedstawicielowi [Or. 10] informacji o abonencie, któremu dostawca usług internetowych udostępnił określony adres IP, przy użyciu którego miało zostać popełnione naruszenie? Pytanie niniejsze oparte jest o założenie, że powód uprawdopodobnił naruszenie konkretnego prawa autorskiego, a wydanie nakazu byłoby proporcjonalne."

Pytanie zostało skierowane w związku ze sprawą toczącą się w Szwecji, w której obowiązujące przepisy prawne wprost umożliwiają pozyskiwanie danych osobowych sprawców naruszeń praw własności intelektualnej od podmiotów zajmujących się dostarczaniem usług dostępu do Internetu. W sprawie tej została sporządzona opinia Rzecznika Generalnego Nilla Jaaskinena[11], zgodnie z którą:

„Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie prze-

chowywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE nie ma zastosowania do przetwarzania danych osobowych do celów innych niż wymienione w art. 1 ust. 1 tej dyrektywy. W konsekwencji wspomniana dyrektywa nie wyklucza stosowania przepisu krajowego, na mocy którego w postępowaniu cywilnym można, w celu zidentyfikowania określonego abonenta, nakazać dostawcy usług internetowych ujawnienie uprawnionemu z prawa autorskiego albo jego przedstawicielowi informacji o abonencie, któremu dostawca usług internetowych udostępnił określony adres IP, przy użyciu którego miało zostać popełnione naruszenie. Jednakże te informacje, dla ich rozpowszechnienia i wykorzystania w tym celu, powinny były być przechowywane zgodnie ze szczegółowymi krajowymi przepisami ustawodawczymi, które zostały przyjęte z poszanowaniem prawa unijnego w dziedzinie ochrony danych osobowych. W świetle odpowiedzi udzielonej na pierwsze pytanie, drugie pytanie jest bezprzedmiotowe".

Opinia Rzecznika Generalnego wydana do sprawy Bonnier w oczywisty sposób potwierdza więc możliwość udostępniania danych osobowych sprawców naruszeń praw własności intelektualnej dla celów postępowania cywilnego. Mimo braku normy wspólnotowej nakazującej państwom członkowskim wprowadzenie do prawa krajowego takiej procedury, nie ma również przepisu wyłączającego taką możliwość.

Kwestia istnienia w prawie krajowym procedury udostępniania danych osobowych na potrzeby postępowań sądowych cywilnych przedstawia się zgoła odmiennie na gruncie Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. W wyroku Europejskiego Trybunału Praw Człowieka z dnia 2 grudnia 2008 r. w sprawie K.U. przeciwko Finlandii[12], Trybunał analizował pod kątem zgodności z Konwencją stan prawny obowiązujący w Finlandii, w którym nie istniały prawne możliwości ujawnienia danych osobowych sprawcy naruszenia dóbr osobistych w Internecie. W tym świetle trybunał stwierdził naruszenie art. 8 Konwencji przez Finlandię. W ocenie Trybunału, państwo ma obowiązek zapewnienia środków prawnych dla ochrony życia prywatnego jednostki także wtedy, gdy ochrona ta ma dotyczyć relacji między jednostkami. Nie wystarczy więc powstrzymywanie się przez państwo od ingerencji w sferę życia prywatnego jednostki. Trybunał podkreślił również, że gwarancje prywatności dla użytkowników Internetu nie mogą mieć charakteru absolutnego i w pewnych sytuacjach, takich jak zapobieganie przestępczości, czy ochrona praw i wolności innych osób, gwarancje prywatności mogą podlegać ograniczeniom. Tym samym Konwencja nie tylko, że nie stoi na przeszkodzie wprowadzeniu w prawie krajowym procedury udostępniania danych osobowych na potrzeby postępowań cywilnych, ale wręcz wymaga, aby w prawie krajowym została ustanowiona skuteczna procedura identyfikacji sprawców naruszeń[13].

4. Udostępnianie danych osobowych na potrzeby postępowań cywilnych w prawie polskim

W prawie polskim nie istnieje procedura o charakterze generalnym, regulująca zasady udostępniania danych osobowych dla potrzeb postępowań cywilnych. Zamiast tego, zasady udostępniania danych osobowych na potrzeby postępowań sądowych cywilnych określone zostały w polskim prawie na dwa sposoby:
a) jako przepisy szczególne względem przepisów u.o.d.o., tj. przepisy dotyczące naruszeń praw własności intelektualnej;
b) jako zasady wynikające z przepisów u.o.d.o.

Stosunek przepisów szczególnych do przepisów u.o.d.o. w zakresie procedury udostępniania danych osobowych powinien zostać ustalony w oparciu o zasadę lex specialis derogat legi generali. W konsekwencji, przepisy szczególne znajdą zastosowanie z pierwszeństwem przed regulacją u.o.d.o. Konstrukcji tej nie stoi na przeszkodzie norma art. 5 u.o.d.o., zgodnie z którą jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

Przepis ten dotyczy bowiem wyłącznie sytuacji zwiększenia poziomu ochrony danych osobowych w odrębnych. Tymczasem w systemie prawnym mamy również do czynienia – stosunkowo rzadko – z przypadkami obniżenia poziomu ochrony danych osobowych w stosunku do poziomu wyznaczonego przez przepisy u.o.d.o. Przykładem takiego rozwiązania są właśnie przepisy przewidujące szczególny tryb udostępniania danych osobowych, tj. art. 80 ustawy o prawie autorskim i prawach pokrewnych[14] (dalej jako u.p.a.i.p.), art. 286[1][15] ustawy Prawo własności przemysłowej oraz art. 11a. ustawy o ochronie baz danych[16]. Skoro więc art. 5 u.o.d.o. dotyczy wyłącznie zwiększenia poziomu ochrony danych osobowych, przypadki obniżenia poziomu ochrony powinny być oceniane na zasadzie ogólnej reguły wyłączającej przepis ogólny w oparciu o przepis szczególny. Podkreślić jednak należy, że skutek w postaci wyłączenia stosowania przepisów u.o.d.o. wystąpi jedynie w stosunku do tych przepisów, które pozostają w bezpośredniej sprzeczności z przepisami szczególnymi. Innymi słowy, w zakresie nieuregulowanym przez przepisy szczególne dane osobowe w dalszym ciągu będą podlegały ochronie ustanowionej w przepisach u.o.d.o.

5. Udostępnianie danych osobowych na podstawie przepisów szczególnych względem u.o.d.o.

Analizując możliwość udostępniania danych osobowych na potrzeby postępowań cywilnych należy w pierwszej kolejności zwrócić uwagę na tzw. roszczenia informacyjne, tj. roszczenia opisane w art. 80 u.p.a.i.p., w art. 286[1] ustawy Prawo własności przemysłowej oraz w art. 11a ustawy o ochronie baz danych. Wszystkie te przepisy wywodzą się bowiem ze wspólnego pierwowzoru w prawie wspólnotowym, jakim jest Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (dalej jako dyrektywa Enforcement). Jeżeli inaczej nie zaznaczono, dalsze rozważania prowadzone na gruncie przepisów u.p.a.i.p. odnoszą się więc również do roszczeń informacyjnych przewidzianych w ustawie Prawo własności przemysłowej, jak i w ustawie o ochronie baz danych.

W nauce prawa jeszcze przed wprowadzeniem odpowiednich przepisów nakazujących ujawnianie informacji podnoszono, że w prawie cywilnym brak jest ogólnej podstawy do żądania informacji, a art. 189 kodeksu postępowania cywilnego i art. 460 kodeksu cywilnego zawierają niedostateczne podstawy do pozyskania niezbędnych informacji[17].

Bazując na tych samych założeniach, prawodawca wspólnotowy w art. 8 dyrektywy Enforcement ustanowił zasady udostępniania informacji związanych z dochodzeniem roszczeń z tytułu naruszenia praw własności intelektualnej. Zakres zastosowania roszczeń informacyjnych opartych o art. 8 dyrektywy Enforcement ogranicza się jednak wyłącznie do zakresu zastosowania samej dyrektywy, tj. do naruszeń praw własności intelektualnej i tym samym nie obejmuje udostępniania danych osobowych dla potrzeb dochodzenia innych roszczeń opartych o prawo cywilne.

Informacje, których można żądać w trybie art. 8 Dyrektywy Enforcement, obejmują nazwy i adresy producentów, dystrybutorów, dostawców lub innych uprzednich posiadaczy towarów lub usług, jak również ich odbiorców i sprzedawców detalicznych, informacje o ilości produkowanych, dostarczanych, otrzymanych lub zamówionych towarów lub usług oraz o cenie za nie otrzymanej. Krąg podmiotów zobowiązanych do udzielenia informacji został przy tym zakreślony niezwykle szeroko. Udzielenie informacji może zostać nakazane nie tylko naruszycielowi, ale i innej osobie, która jest w posiadaniu towarów naruszających prawo własności intelektualnej na skalę handlową bądź korzysta na skalę handlową z usług naruszających te prawa albo też świadczy na skalę handlową usługi wykorzystywane w działalności naruszycielskiej bądź została wskazana przez którąś z wyżej wymienionych osób jako włączona w produkcję, dystrybucję towarów lub dostarczanie usług[18]. Podkreślić jednak należy, że zgodnie z tezą 14 preambuły dyrektywy Enforcement, prawo do informacji ma być stosowane do naruszeń dokonywanych na skalę handlową, a więc działań nakierowanych „na uzyskiwanie bezpośredniego lub pośredniego zysku ekonomicznego lub

korzyści handlowej, ale normalnie nie obejmuje to działań prowadzonych przez działających w dobrej wierze konsumentów końcowych".

Zgodnie z art. 80 ust. 1 pkt. 3 u.p.a.i.p. sąd właściwy do rozpoznania spraw o naruszenie autorskich praw majątkowych miejsca, w którym sprawca wykonuje działalność lub w którym znajduje się jego majątek, także przed wytoczeniem powództwa rozpoznaje, wniosek mającego w tym interes prawny o zobowiązanie innej niż naruszający osoby do udzielenia informacji, które mają znaczenie dla roszczeń, określonych w art. 79 ust. 1 u.p.a.i.p., o pochodzeniu, sieciach dystrybucji, ilości i cenie towarów lub usług naruszających autorskie prawa majątkowe, m.in. jeżeli stwierdzono, że świadczy ona usługi wykorzystywane w działaniach naruszających autorskie prawa majątkowe. Usługami takimi są m.in. usługi dostępu do sieci Internet, czy usługi świadczone droga elektroniczną, pozwalające na udostępnianie treści w Internecie, takie jak usługa hostingu. Potencjalnie więc roszczenie informacyjne może zostać skierowane przeciwko podmiotom, które dostarczają infrastrukturę wykorzystywaną przy naruszaniu praw własności intelektualnej i które z tego tytułu dysponują danymi osobowymi sprawców tychże naruszeń (operator telekomunikacyjny świadczący usługę dostępu do Internetu, czy podmiot prowadzący stronę internetową, za pomocą której dochodzi do rozpowszechniania utworów w sposób naruszający autorskie prawa majątkowe).

Zakres informacji, które mogą zostać ujawnione na podstawie art. 80 ust. 1 pkt. 3 u.p.a.i.p., obejmuje informacje o pochodzeniu, sieciach dystrybucji, ilości i cenie towarów lub usług naruszających autorskie prawa majątkowe. Przepis ten nie odpowiada dokładnie swojemu pierwowzorowi z Dyrektywy 2004/48/WE, stąd zgodzić się należy ze stanowiskiem Sądu Apelacyjnego w Warszawie[19], zgodnie z którym przepis art. 80 u.p.a.i.p. należy wykładać zgodnie z postanowieniami Dyrektywy, a więc:

„informacje o sieciach dystrybucji obejmują dane o osobach, które rozpowszechniają – rozprowadzają towary lub usługi pomiędzy inne podmioty".

Tym samym, zdaniem Sądu, roszczenie informacyjne z art. 80 ust. 1 pkt. 3 u.p.a.i.p. obejmuje również dane osobowe osób fizycznych, które naruszają autorskie prawa majątkowe. Stanowisko to aprobowane jest również w nauce prawa – podkreśla się bowiem, że „inaczej sytuacja ta będzie oceniana, gdy podmiot, któremu przysługują autorskie prawa majątkowe wystąpi z wnioskiem o nakazanie ujawnienia danych osobowych w celu wniesienia powództwa przeciwko użytkownikom, którzy rozpowszechniają w systemach peer to peer utwory chronione prawem autorskim. Wydaje się, że wówczas na podstawie art. 18 ust. 6 i art. 21 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[20] (dalej jako u.ś.u.d.e.) w zw. z art. 80 ust. 1 pkt 3 lit. c pr. aut. i pr. pokr. sąd cywilny, po rozważeniu kwestii proporcjonalności takiego żądania oraz kierując się wytycznymi Trybunału Sprawiedliwości zawartych m.in. w wyroku Promusicae, powinien wydać taki nakaz"[21]. Z drugiej strony, jeszcze przed nadaniem art. 80 u.p.a.i.p. obecnej treści zwracano uwagę, że „w ramach harmonizacji z wymogami dyrektywy niezbędna jest modyfikacja regulacji prawa do informacji zarysowanego zaledwie w PrAut. Nowelizując art. 80 1 pkt 2 PrAut należy przede wszystkim rozszerzyć krąg podmiotów zobowiązanych do udzielenia informacji, wprowadzając możliwość dochodzenia tego prawa w stosunku do podmiotów innych niż naruszyciel. Niezbędne jest zarysowanie granic przedmiotowych obowiązku informacyjnego, w szczególności poprzez wskazanie, że informacja ta może obejmować również dane dotyczące osób trzecich"[22].

W świetle powyższego podmioty, które zamierzają dochodzić ochrony przysługujących im autorskich praw majątkowych, uprawnione są do żądania, aby sąd nakazał udostępnienie danych osobowych sprawców takich naruszeń tym podmiotom, które dostarczają infrastrukturę wykorzystywaną przy naruszaniu praw własności intelektualnej, i które z tego tytułu dysponują danymi osobowymi sprawców tychże naruszeń. Jednocześnie należy podkreślić, że uprawnienie do domagania się udostępnienia danych osobowych nie dotyczy działań konsumentów będących w dobrej wierze. Oznacza to, że z kręgu osób zobowiązanych do udzielania

informacji wyłączono konsumentów działających w dobrej wierze, a więc nieświadomych bezprawnego charakteru nabywanych towarów lub usług[23].

Podkreślić należy, że – zgodnie z art. 80 ust. 2 u.p.a.i.p. – sąd, dopuszczając dowód lub rozpoznając wnioski, o których mowa w ust. 1, zapewnia zachowanie tajemnicy przedsiębiorcy i innych tajemnic ustawowo chronionych. Taką inną tajemnicą ustawowo chronioną jest m.in. tajemnica telekomunikacyjna, ustanowiona w art. 159 ustawy Prawo telekomunikacyjne[24]. Z tego względu wydaje się, że roszczenia przewidziane w art. 80 u.p.a.i.p. nie stoją na przeszkodzie udostępnianiu danych osobowych objętych tajemnicą telekomunikacyjną, a więc np. danych osobowych osób korzystających z usługi dostępu do sieci Internet w celu sprzecznego z prawem rozpowszechniania utworów. W przepisach u.p.a.i.p. nie ograniczono bowiem możliwości udostępnienia danych objętych ochroną tajemnicy, a jedynie nakazano zapewnienie zachowania tej tajemnicy. Jak się wydaje, przepis powinien być więc rozumiany jako nakaz zapewnienia ochrony informacji objętych tajemnicą w toku postępowania, nie zaś jako zakaz udostępniania tych informacji. W orzecznictwie sądów polskich brak jest jednak orzecznictwa sądowego, które wprost odnosiłoby się do tej kwestii.

W świetle dokonanych wyżej ustaleń wydaje się, że art. 80 u.p.a.i.p., art. 286[1] ustawy Prawo własności przemysłowej oraz art. 11a ustawy o ochronie baz danych są interpretowane na gruncie prawa polskiego przez orzecznictwo sądowe i naukę prawa w ten sposób, że obejmują również dane osobowe osób fizycznych, które naruszają prawa własności intelektualnej. Na ich podstawie istnieje możliwość nakazania udostępnienia danych osobowych dla potrzeb postępowania cywilnego, co wymaga spełnienia warunku w postaci uprawdopodobnienia naruszenia praw wyłącznych.

6. Udostępnianie danych osobowych na podstawie u.o.d.o.

Poza omówionymi wyżej przypadkami udostępniania danych osobowych na podstawie przepisów szczególnych, możliwość udostępniania danych osobowych na potrzeby postępowań cywilnych wynika również z ogólnych przepisów u.o.d.o. Dotyczy ona przy tym wszelkich postępowań cywilnych, a więc nie tylko tych dotyczących naruszeń praw własności intelektualnej.

Udostępnianie danych osobowych regulowane było od wejścia w życie przepisów u.o.d.o. przez art. 29 i 30 ustawy. Zgodnie z art. 29 ust. 2 u.o.d.o. dane osobowe mogły być udostępniane w celach innych, niż włączenie do zbioru danych osobowych, podmiotom, które w sposób wiarygodny uzasadniły potrzebę posiadania danych i pod warunkiem, że udostępnienie danych nie będzie naruszać praw i wolności osób, których dane dotyczą. Przepis ten wraz z objęciem swoim zastosowaniem podmiotów ze sfery prawa prywatnego, co nastąpiło w 2004 r., stał się podstawą prawną dla udostępniania danych osobowych podmiotom, których prawa zostały naruszone i które poszukiwały ochrony tych praw na drodze sądowej.

W nauce prawa podkreślano, że obowiązek wiarygodnego uzasadnienia potrzeby posiadania danych nie mógł być interpretowany jako konieczność udowodnienia potrzeby posiadania danych – podnoszono mianowicie, że wystarczy, iż potrzeba ta zostanie uprawdopodobniona[25]. Należy również podkreślić, że zakres pojęcia „potrzeba posiadania danych" obejmował tak interes prawny, jak i interes faktyczny wnioskodawcy – warunkiem było jedynie, aby do urzeczywistnienia interesu koniecznym było udostępnienie danych osobowych, a jeżeli podstawą złożenia wniosku był interes faktyczny, musiał on zostać uznany za usprawiedliwiony w świetle obowiązującego prawa[26].

W tego rodzaju stanach faktycznych, Generalny Inspektor Ochrony Danych Osobowych (dalej jako GIODO) przyjmował, że konieczność wskazania w pozwie danych osobowych osoby pozwanej uzasadnia wiarygodną potrzebę posiadania danych osobowych. Jako reprezentatywną dla tej linii orzeczniczej wskazać można decyzję z dnia 9 lutego 2004 r.[27], której uzasadnienie jest niezwykle istotne dla dalszych rozważań:

„Wskazać również należy, iż w celu „zainicjowania" sądowego procesu ochrony dóbr osobistych Skarżącego, niezbędnym elementem – w przypadku dochodzenia przez niego roszczeń niemajątkowych (określonych przepisem art. 24 Kodeksu cywilnego) - jest precyzyjne określenie przez niego w pozwie osoby (osób), która dopuściła się naruszenia jego dóbr osobistych. Zgodnie bowiem z art. 187 § 1 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.), pozew powinien czynić zadość warunkom pisma procesowego, a nadto zawierać: dokładnie określone żądanie, a w sprawach o prawa majątkowe także oznaczenie wartości przedmiotu sporu, chyba że przedmiotem sprawy jest oznaczona kwota pieniężna; przytoczenie okoliczności faktycznych uzasadniających żądanie, a w miarę potrzeby uzasadniających również właściwość sądu. Natomiast, w myśl art. 126 § 1 pkt 1 Kodeksu postępowania cywilnego, każde pismo procesowe powinno zawierać m.in. oznaczenie sądu, do którego jest skierowane, imię i nazwisko lub nazwę stron, ich przedstawicieli ustawowych i pełnomocników. Z powyższego wynika zatem, iż niezbędnym elementem pozwu o naruszenie dóbr osobistych jest oznaczenie w nim osoby, przeciwko której żądanie określone w pozwie jest skierowane (tj. przyszłej strony procesowej w sporze z tytułu naruszenia dóbr osobistych). […] Z przytoczonych powyżej przepisów jednoznacznie wynika zatem, iż dla prawidłowego wszczęcia przez Skarżącego postępowania sądowego (karnego, cywilnego), przytoczone powyżej przepisy Kodeksu postępowania karnego oraz Kodeksu postępowania cywilnego, nakładają na Skarżącego obowiązek oznaczenia w pierwszym piśmie procesowym (prywatnym akcie oskarżenia, pozwie) osoby (oskarżanego, pozwanego), przeciwko której zamierza wszcząć dane postępowanie sądowe."

GIODO przyjął więc, że podmiot, który zamierza dochodzić swoich praw przed sądem, działa w warunkach prawnie usprawiedliwionego celu przetwarzania danych osobowych niezbędnych do wskazania osoby pozwanej w piśmie inicjującym postępowanie sądowe w sprawie. Tym samym podmiot taki dysponował podstawą prawną dla przetwarzania danych osobowych osoby pozwanej. Pogląd ten był również akceptowany w doktrynie – podkreślano w szczególności, że dopuszczalnym jest przetwarzanie danych osobowych na podstawie art. 23 ust. 1 pkt 5 u.o.d.o. w związku z dochodzeniem roszczeń w ogólności, nie tylko zaś roszczeń z tytułu prowadzonej działalności gospodarczej[28]. W sytuacji natomiast, w której podmiot ten nie dysponował danymi osobowymi pozwanego, konieczność wskazania w pozwie danych osobowych osoby pozwanej uzasadnia wiarygodną potrzebę posiadania danych osobowych. W konsekwencji podmiot, który takimi danymi dysponował, winien je udostępnić osobie żądającej tychże danych, na zasadzie art. 29 ust. 2 u.o.d.o.

Stanowisko GIODO podzielały również sądy administracyjne. Tytułem przykładu wskazać można wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 26 października 2009 r.[29], w którym Sąd uznał, że:

„żądane dane były niezbędne do wystąpienia przez wnioskodawcę na drogę sądową przeciwko osobom, które mogły zdaniem wnioskodawcy naruszyć jego dobra osobiste. Natomiast przyjęcie, że udostępnianie danych osób, wobec których chce się wytoczyć powództwo cywilne miałoby godzić w ich prawa i wolności prowadziłoby do nieuzasadnionej ochrony takich osób przed ewentualną odpowiedzialnością za swoje działania, zwłaszcza że mogą one w czasie takiego postępowania sądowego w pełni korzystać ze swoich praw zagwarantowanych przepisami k.p.c."

Co więcej, orzecznictwo sądów administracyjnych szło nawet o krok dalej. Naczelny Sąd Administracyjny przyjął mianowicie, że art. 29 u.o.d.o. umożliwia udostępnienie danych także wówczas, gdy dane te podlegają dalej idącej ochronie, niżby wynikała z przepisów samej u.o.d.o. Chodzi tutaj o przypadki, gdy dane osobowe chronione były tajemnicą zawodową, taką jak tajemnica telekomunikacyjna. Ma to istotne znaczenie w sytuacji, gdy podmiot praw dysponuje wyłącznie adresem IP potencjalnego naruszyciela i poszukuje jego danych osobowych w celu wytoczenia powództwa. Te dane są w posiadaniu

przedsiębiorcy telekomunikacyjnego świadczącego usługę dostępu do sieci Internet, podlegają jednak ochronie jako informacje objęte tajemnicą telekomunikacyjną, na zasadzie art. 159 ustawy Prawo telekomunikacyjne[30]. W tego rodzaju stanie faktycznym Naczelny Sąd Administracyjny w wyroku z dnia 5 lutego 2008 r.[31] wskazał, że brzmienie art. 161 ust. 1 zd. 2 ustawy Prawo telekomunikacyjne prowadzi do wniosku, iż przetwarzanie danych objętych tajemnicą telekomunikacyjną może odbywać się w oparciu o przesłanki określone w innych aktach prawnych rangi ustawowej. Zdaniem Sądu, takimi przepisami odrębnymi, które upoważniają do przetwarzania danych osobowych, są m. in. przepisy u.o.d.o., co stanowiło podstawę dla dopuszczalności udostępniania danych osobowych objętych tajemnicą telekomunikacyjną na podstawie art. 29 ust. 2 u.o.d.o. Analogiczny pogląd wyrażony został w prawomocnym wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 lutego 2010 r.1, w którym Sąd nakazał przedsiębiorcy telekomunikacyjnemu udostępnienie danych osobowych osoby korzystającej z usługi dostępu do sieci Internet. Pogląd taki aprobowany był również w nauce prawa[33].

Konsekwencją takiego stanu rzeczy była praktyka polegająca na udostępnianiu, na warunkach określonych w art. 29 ust. 2 u.o.d.o., informacji o osobach, w stosunku do których zamierzano wszcząć postępowanie cywilne o ochronę praw własności intelektualnej. Wraz z upływem czasu dostrzegalna była jednak ewolucja w podejściu GIODO oraz sądów administracyjnych do możliwości nakazania udostępniania przez GIODO danych osobowych objętych tajemnicą telekomunikacyjną. W szczególności, w wyroku z dnia 28 listopada 2011 r.[34], Wojewódzki Sąd Administracyjny w Warszawie stwierdził:

„ Zasadne jest stanowisko Generalnego Inspektora, że obowiązujący w czasie rozpoznawania sprawy art. 29 ust. 2 ustawy o ochronie danych osobowych nie jest przepisem odrębnym, o którym mowa w art. 159 ust. 2 pkt 4 i ust. 3 oraz art. 161 ust. 1 ustawy – Prawo telekomunikacyjne. Przedstawiona w uzasadnieniu zaskarżonej decyzji argumentacja nie budzi zastrzeżeń i Sąd ją podziela. Wbrew twierdzeniom skarżącego, przepis art. 29 ust. 2 ustawy o ochronie danych osobowych nie mógł mieć w niniejszej sprawie zastosowania chociażby dlatego, że nie zawiera jednoznacznych dyrektyw pozwalających na odkodowanie zakresu znaczeniowego użytego w tym przepisie zwrotu „jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych" (v. wyrok NSA z dnia 22 marca 2011 r., sygn. akt I OSK 623/10). Tymczasem, istotę wyjątku (od przestrzegania tajemnicy telekomunikacyjnej) określonego w art. 159 ust. 2 pkt 4 usatwy – Prawo telekomunikacyjne, jest właśnie dookreśloność celu, czy powodu, jak mówi ustawodawca – przewidzianego jednocześnie w przepisie szczególnym innego aktu prawnego. Tym przepisem szczególnym nie był przepis art. 29 ust. 2 u.o.d.o."

Po uchyleniu art. 29 ust. 2 u.o.d.o. Wojewódzki Sąd Administracyjny w Warszawie stanął więc na stanowisku, zgodnie z którym uchylony przepis nie stanowił podstawy prawnej dla udostępniania danych osobowych objętych tajemnicą telekomunikacyjną.

Wraz z wejściem w życie ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw[35], uchylony został art. 29 i powiązany z nim art. 30 u.o.d.o. Powstaje więc pytanie, czy po 7 marca 2011 r. (data wejścia w życie ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw) istnieją podstawy prawne dla udostępniania danych osobowych sprawców naruszeń praw własności intelektualnej w Internecie, celem wytoczenia przeciwko nim powództwa?

W literaturze zwrócono uwagę, że po uchyleniu art. 29 i 30 u.o.d.o., udostępnienie danych osobowych na wniosek podmiotu, który nie legitymuje się szczególną podstawa prawną dla udostępnienia danych osobowych (a takim podmiotem jest właśnie ten, kto zamierza wytoczyć powództwo cywilne), wymaga istnienia prawnie usprawiedliwionego celu nie tylko po stronie wnioskodawcy, ale również po stronie podmiotu udostępniającego dane. Z systemu prawnego został bowiem usunięty przepis, który umożliwiał udostępnianie danych w razie wiary-

godnego uzasadnienia potrzeby posiadania danych. Z tego względu, dopuszczalność udostępniania danych osobowych powinna być oceniana na gruncie ogólnych podstaw prawnych przetwarzania danych, tj. na podstawie art. 23 ust. 1 albo art. 27 ust. 2 u.o.d.o. Skoro więc osoba, której dane dotyczą, nie wyraziła zgody na udostępnienie jej danych osobowych, a na takie udostępnienie nie zezwala żaden szczególny przepis prawa, istotnie jedyną możliwością legalnego udostępnienia danych stanowi powołanie się na art. 23 ust. 1 pkt. 5 u.o.d.o.[36]. Przytoczony wyżej pogląd wydaje się jednak dyskusyjny, jako że w art. 23 ust. 1 pkt 5 u.o.d.o. w sposób wyraźny odwołano się do prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych. Użycie spójnika „albo" przesądza, że istnienie prawnie usprawiedliwionego celu po stronie odbiorcy danych (tutaj: podmiotu wnioskującego o udostepnienie danych) jest wystarczającym dla przyjęcia dopuszczalności przetwarzania danych osobowych na podstawie art. 23 ust. 1 pkt. 5 u.o.d.o. Skoro więc dopuszczalne jest przetwarzanie danych, to także i udostępnianie danych, jako że udostępnianie danych osobowych jest jedną z postaci przetwarzania danych. Co więcej, próba poszukiwania prawnie usprawiedliwionego celu po stronie podmiotu udostępniającego dane osobowe w celu wytoczenia powództwa przez odbiorcę danych z zasady skazana byłaby na porażkę. W tym przypadku bowiem udostępnianie i dalsze przetwarzanie danych odbywa się wyłącznie w interesie odbiorcy danych (podmiotu wnioskującego o udostępnienie danych), nie można więc mówić o istnieniu jakiegokolwiek prawnie usprawiedliwionego celu po stronie podmiotu, który dane udostępnia. Uchylenie art. 29 u.o.d.o. przesądziło również – niezależnie od zmiany linii orzeczniczej sądów administracyjnych – o braku możliwości udostępniania na jego podstawie danych osobowych objętych tajemnicą telekomunikacyjną. To właśnie na podstawie tego przepisu zapadały bowiem wyroki[37] utrzymujące w mocy decyzje GIODO nakazujące udostępnienie danych osobowych objętych tajemnicą telekomunikacyjną.

Uchylenie art. 29 i 30 u.o.d.o. skłania również do postawienia pytania o istnienie podstawy prawnej do wydania przez GIODO decyzji administracyjnej nakazującej udostępnienie danych osobowych. Artykuł 29 ustawy interpretowany był w ten sposób, że w razie odmowy udostępnienia danych osobowych przez administratora danych, wnioskodawca mógł zwrócić się do GIODO, który uprawniony był do wydania decyzji administracyjnej nakazującej udostępnienie danych[38]. Podstawą prawną wydania przez GIODO decyzji nakazującej udostępnienie danych był w tym wypadku art. 18 ust. 1 u.o.d.o., zgodnie z którym w przypadku naruszenia przepisów o ochronie danych osobowych GIODO z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem. Skoro więc nieudostępnienie danych osobowych na podstawie art. 29 ust. 2 u.o.d.o. uzasadniało władczą ingerencję GIODO, a taka władcza ingerencja możliwa była wyłącznie w przypadku naruszenia przepisów o ochronie danych osobowych, pośrednio wskazuje to więc na konstrukcję, zgodnie z którą art. 29 ust. 2 u.o.d.o. kreował obowiązek udostępnienia danych osobowych, którego wykonanie podlegało ochronie prawnej w postępowaniu przed GIODO. Tymczasem uchylenie art. 29 u.o.d.o. ten obowiązek usunęło. W stanie prawnym obowiązującym obecnie u.o.d.o. przewiduje wyłącznie uprawnienie do przetwarzania danych osobowych w celu wytoczenia powództwa o ochronę dóbr osobistych. Nie przewiduje jednak – wobec uchylenia art. 29 ust. 2 – obowiązku udostępniania danych. Z tego względu wydaje się, że GIODO nie jest obecnie uprawniony do nakazania udostępnienia danych osobowych[39]. W nauce prawa wyrażony został również pogląd odmienny, zgodnie z którym odmowa udostępnienia danych osobowych stanowi naruszenie przepisów o ochronie danych osobowych i jako taka uzasadnia władczą ingerencję ze strony GIODO[40]. Uzasadnieniem dla takiego stanowiska jest przyjęcie, że pozbawienie GIODO możliwości nakazania udostępnienia danych osobowych prowadziłoby do całkowitej dowolności w ocenie dopuszczalności udostępniania danych, a tym samym do często nieuzasadnionego odmawiania udostępniania danych.

Co ciekawe, praktyka działania GIODO wątpliwości tych zdaje się nie dostrzegać – w dalszym ciągu bowiem wydawane są decyzje administracyjne

nakazujące udostępnienie danych osobowych na potrzeby prowadzenia sądowego postępowania cywilnego. Tytułem przykładu przywołać można decyzję GIODO z dnia 13 czerwca 2011 r.[41], w której stwierdzono:

„Odnosząc się do oceny Spółki 1, że art. 23 ustawy - inaczej niż art. 29 - nie obliguje administratora do udostępnienia danych, a jedynie jest podstawą prawną dającą mu uprawnienie do dokonania takiej operacji, wskazać należy, że art. 23 ustawy nie mówi o uprawnieniu administratora danych lecz o przesłankach dopuszczalności przetwarzania danych. Zdaniem Generalnego Inspektora odmowa udostępnienia danych osobowych przez Spółkę 1 pomimo zaistnienia przesłanki określonej w art. 23 ust. 1 pkt 5 ustawy, narusza ten przepis, w związku z czym konieczne jest przywrócenie stanu zgodnego z prawem. […] Z uzasadnienia skierowanego do Generalnego Inspektora wniosku wynika, że w ocenie Wnioskodawcy doszło do naruszenia jego dóbr osobistych. Uzasadnionym jest zatem dochodzenie przez Wnioskodawcę ochrony tych dóbr poprzez wystąpienie do sądu z powództwem wobec autora wpisu na forum internetowym prowadzonym przez Spółkę 1. Niewątpliwie jest to prawnie usprawiedliwiony cel Wnioskodawcy, o którym mowa w art. 23 ust. 1 pkt 5 ustawy […]. Ponadto, przyjęcie, że przetwarzanie (udostępnienie) - w celu zainicjowania postępowania sądowego - danych osoby, wobec której zachodzi domniemanie, że to ona dokonała wpisu (mającego godzić w dobra osobiste Wnioskodawcy) miałoby naruszać jej prawa i wolności, prowadziłoby do nieuzasadnionej ochrony takiej osoby przed ewentualną odpowiedzialnością za swoje działania, zwłaszcza, że może ona w trakcie postępowania sądowego w pełni korzystać ze swoich praw zagwarantowanych przepisami Kpc. Działanie Spółki 1 polegające na nieudostępnieniu Wnioskodawcy danych osobowych, może natomiast doprowadzić do ograniczenia jego prawa do wystąpienia do sądu z powództwem w sprawie naruszenia dóbr osobistych oraz skutecznie chronić sprawcę przed odpowiedzialnością cywilnoprawną za jego działania."

Co jeszcze bardziej istotne, stanowisko GIODO dotyczące możliwości nakazania udostępnianie danych osobowych na potrzeby prowadzenia postępowania cywilnego akceptowane jest w dalszym ciągu przez sądy administracyjne. Przywołać tutaj trzeba w tym kontekście – nieprawomocny – wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 26 lipca 2012 r.[42], w którym sąd utrzymał w mocy decyzję GIODO nakazującą udostępnienie danych osobowych „niezbędnych do przeprowadzenia procesu sądowego". Odnosząc się do zarzutu dotyczącego braku podstawy prawnej dla udostępnienia danych osobowych, Sąd uznał, że:

„Skoro wnioskodawca wykazał usprawiedliwiony cel do uzyskania danych osobowych, administrator danych winien mu te dane udostępnić."

Odnosząc się natomiast do zarzutu dotyczącego braku możliwości nakazania przez GIODO udostępnienia danych osobowych, Sąd uznał, że:

„Skoro [...] Uniwersytet, pomimo zaistnienia przesłanki wymienionej w art. 23 ust 1 pkt 5 ustawy, nie udostępnił wnioskodawcy danych osobowych, to naruszył przepisy o ochronie danych osobowych i zaszła konieczność wydania decyzji określonej w pkt 2 cytowanego art. 18 ust 1."

Sąd potwierdził więc legalność i zasadność praktyki wydawania decyzji administracyjnych przez GIODO nakazujących udostępnienie danych osobowych w celu wszczęcia powództwa cywilnego.

7. Próba podsumowania

Z dokonanej wyżej analizy wyłania się sytuacja, w której roszczenia informacyjne przewidziane w art. 80 u.p.a.i.p., art. 286[1] ustawy Prawo własności przemysłowej oraz art. 11a ustawy o ochronie baz danych są interpretowane na gruncie prawa polskiego przez orzecznictwo sądowe i naukę prawa w ten sposób, że obejmują również dane osobowe osób fizycznych, które naruszają prawa własności intelektualnej. Wydaje się, że na podstawie tych przepisów można również udostępniać informacje objęte ochroną tajemnicy telekomunikacyjnej? Należy jedynie rozważyć zmianę art. 80 u.p.a.i.p. (oraz

analogicznie art. 286[1] ustawy Prawo własności przemysłowej oraz art. 11a ustawy o ochronie baz danych) w ten sposób, aby przesądzić, że informacje udostępniane na podstawie tych przepisów mogą obejmować również dane dotyczące osób trzecich.

Jednocześnie funkcjonuje procedura konkurencyjna, oparta o przepisy u.o.d.o., która swoim zakresem obejmuje wszelkie sprawy cywilne, nie tylko dotyczące naruszeń praw własności intelektualnej. W szczególności, mimo uchylenia art. 29 i 30 u.o.d.o., GIODO w dalszym ciągu wydaje decyzje administracyjne nakazujące udostępnienie danych osobowych na potrzeby prowadzenia sądowego postępowania cywilnego. Praktyka taka jest akceptowana przez część nauki prawa, przy sprzeciwie innych autorów. Orzecznictwo sądowe wydaje się tą praktykę akceptować, choć brak jest dotychczas jakiegokolwiek prawomocnego wyroku.

Wydaje się więc, że sytuacja dojrzała do ingerencji ze strony ustawodawcy. I tak, w zakresie udostępniania danych osobowych na potrzeby postępowań cywilnych w procedurze administracyjnej (decyzja administracyjna GIODO) należy albo przesądzić brak takiego uprawnienia po stronie GIODO, co stanowiłoby konsekwencję uchylenia art. 29 i 30 u.o.d.o., albo takie uprawnienie na powrót GIODO przyznać. Obecny stan prawny w tym zakresie jest wysoce niepewny i nie sprzyja realizacji postulatu pewności prawa, a rola sądownictwa administracyjnego nie powinna być aż do tego stopnia prawotwórcza.

W ocenie autora, tylko obecność takiej właśnie procedury umożliwi ustalenie sprawcy naruszenia dóbr osobistych w Internecie, jako że odpowiednie roszczenia informacyjne mogą być wykorzystywane tylko w zakresie naruszeń praw własności intelektualnej. Tylko obecność takiej procedury umożliwi również udostępnianie danych osobowych na potrzeby postępowań cywilnych nie związanych w ogóle z nowymi technologiami. Konieczność zapewnienia takiej procedury wynika też wprost z wyroku Europejskiego Trybunału Praw Człowieka w sprawie K.U. przeciwko Finlandii. W końcu, odpowiednie przepisy winny wprost dopuścić możliwość udostępniania danych osobowych objętych tajemnicą telekomunikacyjną na potrzeby postępowań cywilnych. Te wszystkie argumenty przemawiają w oczywisty sposób za wprowadzeniem do prawa polskiego procedury administracyjnej, w której GIODO zostałby wyposażony w uprawnienie do nakazania udostępniania danych osobowych, także tych objętych tajemnicą telekomunikacyjną.

Czy jednak jest to jedyne potencjalne rozwiązanie problemu? Z wyroku Europejskiego Trybunału Praw Człowieka w sprawie K.U. przeciwko Finlandii wynika obowiązek ustanowienia w prawie krajowym skutecznej procedury identyfikacji sprawców naruszeń. Procedura taka nie musi jednak koniecznie polegać na udostępnianiu przyszłemu powodowi danych osobowych osób fizycznych, przeciwko którym zamierza on wytoczyć powództwo. Wręcz przeciwnie, można spotkać opinie, zgodnie z którymi przekazywanie takich danych może „grozić daleko idącymi konsekwencjami, nie tylko dla prywatności, ale nawet dla życia lub zdrowia [..] osób [których dane dotyczą]'[43]. Nie wchodząc w tym miejscu w rozważania na temat realności tychże obaw (w opinii brak jest szerszego uzasadnienia dla prezentowanego stanowiska), wydaje się, że możliwą do wyobrażenia byłaby procedura, w której to sąd cywilny prowadziłby działania mające na celu ustalenie danych osobowych sprawcy naruszenia, a danych tych – przynajmniej w początkowym okresie postępowania – nie przekazywałby powodowi. Tego rodzaju rozwiązanie, choć teoretycznie możliwe, wymagałoby jednak głębokich zmian w procedurze cywilnej. ■

* dr Paweł Litwiński, litwinski@allerhand.pl

[1] ustawa z dnia 17 listopada 1964 r. kodeks postępowania cywilnego, Dz. U. nr 43, poz. 296, ze zm.

[2] ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst jedn. Dz. U z 2002 r. nr 101, poz. 926, ze zm.

[3] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, Warszawa 2011, str. 346.

[4] A. Mednis, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2001, s. 23.

[5] P. Litwiński, Obrót prawny bazami danych osobowych, Przegląd Prawa Handlowego nr 9/2003, str. 49.

[6] A. Mednis, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2001, s. 28.

[7] sprawa Promusicae przeciwko Telefónica, C-275/06.

[8] sprawa LSG przeciwko Tele2, C-557/07.

[9] M. Walter, S. von Lewinski (red.), European Copyright Law: A Commentary, Oxford 2010, s. 1271.

[10] sprawa Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget Aktiebolag, Storyside AB przeciwko Perfect Communication Sweden AB, C-461/10.

[11] Opinia Rzecznika Generalnego Nilla Jaaskinena przedstawiona w dniu 8 marca 2012 r., sprawa Döhler Neuenkirchen GmbH przeciwko Hauptzollamt Oldenburg, C-262/10.

[12] sprawa K.U. przeciwko Finlandii, 2872/02.

[13] podobnie K. Szymielewicz, A. Mazgal, Internet a prawa podstawowe, publikacja dostępna pod adresem http://wolnyinternet.panoptykon.org/sites/default/files/raport_na_www.pdf, s. 25.

[14] ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, tekst jedn. Dz. U. z 2006 r. nr 90, poz. 631, ze zm.

[15] ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej, tekst jedn. Dz. U. z 2003 r. nr 119, poz. 1117, ze zm.

[16] ustawa z dnia 27 lipca 2001 r. o ochronie baz danych, Dz. U. nr 128, poz. 1402, ze zm.

[17] Błeszyński w: J. Barta (red.), System Prawa Prywatnego. Prawo autorskie, Warszawa 2003, s. 585.

[18] por. M. Walter, S. von Lewinski (red.), European Copyright Law: A Commentary, Oxford 2010, s. 1267.

[19] postanowienie z dnia 30 czerwca 2010 r., VI Acz 1038/10, nie publ.

[20] ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. nr 144, poz. 1204, ze zm.

[21] por. szerzej na ten temat: A. Kuźnicka, Egzekwowanie prawa autorskiego w Internecie a ochrona danych osobowych użytkowników, Prace z Prawa Własności Intelektualnej, Rok 2010, s. 110.

[22] A. Tischner, Harmonizacja prawa polskiego z wymogami dyrektywy w sprawie egzekwowania praw własności intelektualnej- cz.I, Monitor Prawniczy 2005, nr 13.

[23] por. na gruncie analogicznych przepisów ustawy Prawo własności przemysłowej: A. Tischner w P. Kostański (red.), Prawo własności przemysłowej. Komentarz, Warszawa 2010, str. 1156.

[24] ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. nr 171, poz. 1800, ze zm.

[25] A. Szewc, Z problematyki ochrony danych osobowych. Cz. II, Radca Prawny nr 4/1999, s. 8.

[26] A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Warszawa 2004, s. 185.

[27] GI-DEC-DS.-28/04.

[28] por. A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Warszawa 2004, s. 130.

[29] wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 26 października 2009 r., II SA/Wa 1759/08, nie publ.

[30] ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. nr 171, poz. 1800, ze zm.

[31] wyrok Naczelnego Sądu Administracyjnego z dnia 5 lutego 2008r., I OSK 37/07.

[32] wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 lutego 2010 r., II SA/Wa 1598/09.

[33] por. S. Piątek, Prawo telekomunikacyjne. Komentarz, Warszawa 2005, s. 866.

[34] wyrok z dnia 28 listopada 2011 r., II SA/Wa 1875/11.

[35] ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw, Dz. U. nr 229, poz. 1497.

[36] por. na ten temat X. Konarski, Nowe zasady i tryb udostępniania danych osobowych w G. Sibiga (red.), Nowelizacja ustawy o ochronie danych osobowych 2010, dodatek do Monitora Prawniczego nr 3/2011.

[37] wyrok Naczelnego Sądu Administracyjnego z dnia 5 lutego 2008r., I OSK 37/07; wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 lutego 2010 r., II SA/Wa 1598/09.

[38] G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s. 96.

[39] por. X. Konarski, Nowe zasady i tryb udostępniania danych osobowych w G. Sibiga (red.), Nowelizacja ustawy o ochronie danych osobowych 2010, dodatek do Monitora Prawniczego nr 3/2011.

[40] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, Warszawa 2011, s. 433.

[41] DOLiS/DEC- 480/11.

[42] wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 26 lipca 2012 r., II SA/Wa 892/12.

[43] por. K. Siewicz, Opinia nt. projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną, publikacja dostępna pod adresem http://panoptykon.org/sites/default/files/opinia_nowelizacja_usude.pdf.

Maciej Kawecki*

Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej (Inspector General for the Protection of Personal Data as a central public authority net)

Cytowanie: M. Kawecki, *Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej*, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, nr 1/2013, s. 38-44.

Abstrakt: Przedmiotem artykułu jest próba określenia pozycji ustrojowej organu ochrony danych osobowych jakim jest GIODO. Ustawa o ochronie danych osobowych, wskutek braku wyraźnego przepisu, nie wskazuje jednoznacznie jego statusu prawnego. W doktrynie oraz literaturze przedmiotu pojawiła się bardzo duża liczba, często ze sobą sprzecznych poglądów w tym zakresie. Ze względu na prawną doniosłość omawianego zagadnienia, autor poprzez wnikliwą analizę zarówno stanu prawnego jak i literatury, stara się postawić jasną tezę co do analizowanego problemu. Artykuł został też wzbogacony o wnikliwą analizę poglądów doktrynalnych dotyczących innych organów państwowych, których pozycja ustrojowa jest podobna do pozycji nadanej przez ustawodawcę GIODO.

Słowa kluczowe: dane osobowe, Generalny Inspektor Ochrony Danych Osobowych, ochrona danych osobowych

Cite: M. Kawecki, Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej, Przegląd Prawa Technologii Informacyjnych. ICT Law Review, vol. 1/2013, p. 38-44.

Abstrakt: The paper is an attempt to determine the legal position of the Inspector General for the Protection of Personal Data. The Act of 29 August 1997 on the Protection of Personal Data, due to the lack of an express provision, does not clearly indicate such position of this authority. Because of the legal significance of the analyzed issues, by analyzing both the law and literature, this paper try to put a clear thesis about the analyzed problem. The article was also enriched in the evaluation of the doctrinal views concerning other state authorities, whose position is similar to the legal position given GIODO by the legislature.

Key words: Inspector General for the Personal Data, personal data, personal data protection

Na mocy przepisów ustawy o ochronie danych osobowych z 1997 roku powołano do życia organ państwowy właściwy w sprawach ochrony danych osobowych – Generalnego Inspektora Ochrony Danych Osobowych. Jednak od początku istnienia polskiego systemu ochrony danych osobowych istniały i do dzisiaj istnieją rozbieżności co do określenia miejsca GIODO w strukturze administracji publicznej. W szczególności wątpliwości dotyczą dopuszczalności uznania Generalnego Inspektora za centralny organ administracji, gdyż ustawa tego zagadnienia nie reguluje. Z tego właśnie powodu nie jest możliwym zastosowanie do Generalnego Inspektora pozytywistycznej teorii organu, wedle której organem centralnym byłby podmiot, który został za taki uznany przez wyraźny przepis prawny[1].

Generalnego Inspektora powołuje i odwołuje Sejm RP za zgodą Senatu. Ustawa nie określa wyraźnie, kto proponuje kandydata na stanowiska Generalnego Inspektora i rozstrzygnięcia w tej materii należy poszukiwać w regulaminie Sejmu[2]. Zgodnie z jego przepisami, wnioski w sprawie powołania GIODO może zgłaszać Marszałek Sejmu albo grupa co najmniej 35 posłów. Powołanie tego organu przez Sejm gwarantuje jego niezależność od organów administracji publicznej, których działanie podlega kontroli GIODO. Ustawa o ochronie danych osobowych wskazuje wymogi, jakie trzeba spełnić by pełnić funkcje Generalnego Inspektora. Osoba taka powinna: mieć obywatelstwo polskie i stałe miejsce zamieszkania na terytorium RP, wyróżniać się wysokim autorytetem moralnym, mieć wyższe wykształ-

cenie prawnicze oraz doświadczenie zawodowe i nie być karana za przestępstwo. Kadencja Generalnego Inspektora trwa 4 lata licząc od dnia złożenia ślubowania. Ta sama osoba nie może pełnić funkcji Generalnego Inspektora więcej niż przez dwie kadencje. Ustawa przewiduje możliwość wygaśnięcia kadencji oraz odwołania GIODO. Przesłankami uzasadniającymi wygaśniecie kadencji są: śmierć osoby pełniącej funkcje Generalnego Inspektora, odwołanie ze stanowiska oraz utrata obywatelstwa polskiego. Organy, które powołały Generalnego Inspektora, mogą go odwołać w przypadkach enumeratywnie określonych w przepisach ustawy. Może to nastąpić, gdy wskutek choroby stał się on trwale niezdolny do pełnienia swojej funkcji, sprzeniewierzył się ślubowaniu oraz został skazany prawomocnym wyrokiem z popełnione przestępstwo. Zgodnie z art. 12 ustawy, do zadań Generalnego Inspektora należy w szczególności kontrola zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych, wydawanie decyzji administracyjnych, rozpatrywanie skarg w sprawach wykonywania przepisów oraz prowadzenie rejestrów zbiorów danych osobowych. Swoje zadania oraz kompetencje Generalny Inspektor wykonuje przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. Organizację oraz zasady działania biura określa statut nadany w drodze rozporządzenia przez Prezydenta RP.

Dla rozstrzygnięcia kwestii dopuszczalności uznania Generalnego Inspektora za centralny organ administracji, konieczne jest wyjaśnienie pojęcia organu centralnego. Na wstępie należy wskazać, że kształt administracji centralnej wyznaczony jest przez przepisy najwyższego rzędu tj. przez Konstytucję Rzeczypospolitej Polskiej, akty rangi ustawowej oraz w zakresie rozstrzygnięć szczegółowych przez akty wykonawcze do ustaw. W doktrynie prawniczej, ale także w przepisach prawnych oraz w praktyce w obrębie kategorii centralnych organów administracji tradycyjnie wyróżnia się dwa ich rodzaje: organy naczelne oraz pozostałe organy centralne określane często zbiorczą nazwą „urzędy centralne”[3]. W ramach przyjętego więc kryterium zakresu właściwości terytorialnej, organy dzielimy na organy centralne obejmujące swoim zasięgiem obszar całego państwa oraz organy terenowe. W ramach organów centralnych w oparciu o inne przesłanki wyróżniamy natomiast organy naczelne i pozostałe organy centralne nazwane także urzędami centralnymi. Obecnie w Polsce wszystkie organy naczelne oraz urzędy centralne są jednocześnie organami centralnymi, ponieważ realizują swoje kompetencje na terytorium całego państwa[4]. Przy udzielaniu odpowiedzi na pytanie o dopuszczalność uznania Generalnego Inspektora Ochrony Danych Osobowych za centralny organ administracji należy właśnie przyjąć takie rozumienie pojęcia organu centralnego zwanego inaczej urzędem centralnym. Wyodrębnienie organów naczelnych obok organów centralnych miało swoje uzasadnienie w okresie obowiązywania Konstytucji z 1952 roku, która wyraźnie przyznawała im status organów znajdujących się na szczycie aparatu władzy. Mimo iż współczesna konstytucja nie posługuje się takim pojęciem, funkcjonuje ono w ustawodawstwie zwykłym i jest powszechnie zaakceptowane. Podstawowym kryterium odróżniającym omawiane organy naczelne od organów centralnych jest to, że kierownicy organów centralnych nie wchodzą w skład Rady Ministrów, mimo ogólnokrajowego zasięgu działania[5]. Różnic można się też dopatrzeć w zakresie ich powoływania, kompetencji a nawet ich rangi w systemie administracji. Organy naczelne zajmują bowiem w strukturze administracji nadrzędne miejsce w stosunku do innych organów tworzących administrację centralną i które są im podporządkowane[6]. Podział organów administracji publicznej na organy naczelne i organy centralne doprowadził do wielu rozbieżności terminologicznych, które trzeba mieć na uwadze, ale literatura prawa administracyjnego ostatnich lat jest już konsekwentna w sprawie odróżnienia organów naczelnych i centralnych[7].

Przechodząc do kwestii dopuszczalności uznania Generalnego Inspektora za organ centralny, należy wskazać, że w doktrynie brak jest jednoznacznej odpowiedzi na to pytanie. Część przedstawicieli nauki bezdyskusyjnie uznaje Generalnego Inspektora za urząd centralny inni traktują go jako organ administracji specjalnej porównując go z pozycją prawnoustrojową Państwowej Inspekcji Pracy. Są też tacy, którzy wskazują, iż pozycja ustrojowa

GIODO podobna jest do pozycji organów kontroli państwowej i ochrony prawa, a nawet do rzecznika praw obywatelskich[8]. Należy jeszcze wskazać, że w każdej z dotychczas powstałych w tym zakresie prac, problem uznania Generalnego Inspektora za organ centralny w rozumieniu wcześniej wskazanym jest jednak rozstrzygany marginalnie, nie jako na boku innych zagadnień dotyczących funkcjonowania tego organu i nie zostaje potraktowany wystarczająco wnikliwie. Bardzo często wskazuje się, iż GIODO jest co prawda organem centralnym, ale nie przedstawia się jakichkolwiek argumentów popierających tą tezę.

Bez wątpienia GIODO jest organem państwowym. Przepisy ustawy o ochronie danych osobowych, na podstawie których Generalny Inspektor został utworzony nadają mu charakter instytucji działającej w imieniu i na rzecz państwa w celu wykonywania nadzoru nad realizacją prawa do ochrony danych osobowych. W literaturze sporne jest natomiast czy GIODO jest organem administracji publicznej, czy nie. W moim natomiast przekonaniu, wielu autorów błędnie uznaje udzielenie pozytywnej odpowiedzi na to pytanie za wystarczające do potraktowania Generalnego Inspektora za centralny organ administracji[9]. Pojęcie organu administracji publicznej ma bowiem zdecydowanie szersze znaczenie. W omawianym kontekście jest to szczególnie widoczne w przypadku rozpatrywania dopuszczalności uznania Generalnego Inspektora za organ administracji specjalnej zwanego też organem administracji niezespolonej lub wyspecjalizowanej. Organy administracji niezespolonej to przecież terenowe organy administracji rządowej, które jako organy rządowe obok organów samorządowych tworzą podstawowy podział organów administracji publicznej. Nie jest więc możliwym utożsamianie pojęcia organu centralnego z pojęciem organu administracji publicznej. Nie mniej jednak dopuszczalność uznania GIODO za organ administracji publicznej ma bardzo ważne znaczenie z punktu widzenia możliwości uznania Generalnego Inspektora za organ centralny. W nauce prawa administracyjnego przyjmuje się wiele definicji organu administracji publicznej, według E. Ochendowskiego organ taki: jest wyodrębniony organizacyjnie, działa w imieniu i na rzecz państwa w zakresie przyznanych mu kompetencji oraz jest uprawniony do stosowania środków władczych[10]. Nieco szersze kryteria wyodrębnienia organu administracyjnego przyjmuje J. Boć, według którego oprócz wskazanych już wymogów musi on być jeszcze powołany w celu realizacji norm prawa administracyjnego w sposób i ze skutkami właściwymi temu prawu[11]. Jak już wskazuje tytuł rozdziału II u.o.d.o. zawarta w nim regulacja dotyczy wyodrębnionego organizacyjnie „organu ochrony danych osobowych", który będąc tak jak to wyżej zostało wskazane organem państwowym działa w imieniu i na rzecz państwa sprawując nadzór nad procesem przetwarzania danych osobowych. Jak przyjmuje się w literaturze przedmiotu treść art. 8 ust. 1 u.o.d.o. określa w sposób najbardziej ogólny kompetencje i zakres zadań GIODO wskazując, że obejmują one „sprawy dotyczące ochrony danych osobowych"[12]. Konkretyzacją tego przepisu jest art. 12 u.o.d.o., który wymienia podstawowe zadania i kompetencje Generalnego Inspektora przyjmując, iż głównym z nich jest prowadzenie kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Wszystkie kompetencje Generalnego Inspektora są wykonywane w prawnych formach działania administracji[13]. Spośród władczych oraz niewładczych form działania w wykonywaniu swoich kompetencji Generalny Inspektor wykorzystuje obie. Wyrazem władztwa przysługującego GIODO jest przyznanie mu prawa do wydawania decyzji administracyjnych. Uprawnienie do wydawania decyzji administracyjnych oraz fakt jego ustrojowej niezależności wyrażający się również w obejmującym Generalnego Inspektora zakazie członkostwa w partii politycznej można porównać do niezależności sądu i sędziego. Jak wskazał w jednym ze swoich wyroków Trybunał Konstytucyjny wprowadzenie tak istotnych ustawowych ograniczeń prawa zrzeszania się, jest uzasadnione właśnie „faktem przyznania Generalnemu Inspektorowi kompetencji władczych"[14]. Generalny Inspektor Ochrony Danych Osobowych posługuje się również niewładczymi formami działania, zwłaszcza podczas dokonywania czynności materialno-technicznych jakimi bez wątpienia jest prowadzenie przez niego ogólnopolskiego rejestru zgłoszonych zbiorów danych osobowych. Literatura przedmiotu bezdyskusyjnie

przyjmuje, iż regulacja ochrony danych osobowych należy do materii prawa administracyjnego, a Generalny Inspektor jako organ ochrony danych osobowych poprzez realizacje przyznanych mu uprawnień wykonuje normy tego prawa[15]. Można więc z całą pewnością stwierdzić, iż Generalny Inspektor Ochrony Danych Osobowych spełnia wszystkie powszechnie akceptowalne warunki stawiane organowi administracji publicznej, niezależnie od różnic występujących w definicjach kreowanych przez różnych przedstawicieli doktryny.

Uznanie Generalnego Inspektora za organ administracji publicznej pozwala zawęzić zakres prowadzonych rozważań do odpowiedzi na pytanie czy Generalny Inspektor Ochrony Danych Osobowych może zostać uznany za organ centralny.

Jako główny problem w tym zakresie należy uznać ciągle jeszcze istniejące w literaturze przedmiotu przekonanie, że z punktu widzenia hierarchii aparatu administracyjnego, organy centralne (urzędy centralne) tworzą szczebel bezpośrednio niższy w stosunku do organów rządowych i podlegają ich zwierzchnictwu[16]. Biorąc natomiast pod uwagę tryb powoływania i odwoływania Generalnego Inspektora oraz obowiązek składania przez GIODO corocznych sprawozdań Sejmowi, można z pewnością wskazać, iż z punktu widzenia ustrojowego podlega on wyłącznie Sejmowi. Parlament nie ma natomiast żadnych kompetencji merytorycznego wpływu na działalność Generalnego Inspektora i dlatego w tym zakresie podlega on wyłącznie ustawie. Generalny Inspektor jest więc usytuowany poza administracją rządową (i oczywiście poza administracją samorządową) i kompetencji nadzorczych ani kontrolnych w stosunku do niego nie można wywodzić z faktu, że u.o.d.o. upoważnia ministra właściwego do spraw administracji do wydawania aktów wykonawczych do tej ustawy ani tym bardziej z faktu nadawania przez Prezydenta RP statutu dla Biura Generalnego Inspektora[17]. W dzisiejszej strukturze administracji publicznej wyróżnia się natomiast dwa rodzaje administracji: rządowa i samorządowa, stąd też wyłączając możliwość odwołania się do administracji samorządowej konstrukcja organu centralnego opiera się wyłącznie na wskazaniu jego relacji względem organów administracji rządowej. Oprócz nich jednak, w strukturze administracji można dostrzec organy czy instytucje takie jak GIODO, które nie wpisują się w żadną ze wskazanych kategorii organów administracji, jako że jednej strony nie należą do administracji samorządowej, a z drugiej strony nie podlegają zwierzchnictwu Rady Ministrów (i Prezesa Rady Ministrów). Jeżeli przyjmiemy, że GIODO nie należy do administracji samorządowej i wskutek braku jego bezpośrednich bądź pośrednich powiązań z Radą Ministrów nie należy również do administracji rządowej, należy zakwalifikować go do kategorii organów administracji państwowej, ale nie rządowej[18]. W związku z powyższym należy poprzeć pogląd wyrażony przez E. Ure bądź E. Kulesze i wielu innych przedstawicieli doktryny, którzy w swoich publikacjach dokonują wyodrębnienia centralnych organów administracji państwowej, które dopiero w swoim zakresie mieszczą zarówno organy administracji rządowej jak i takie, których pozycja jest tożsama lub podobna do pozycji GIODO[19]. Krytycznie należy więc odnieść się do nazywania organów centralnych, centralnymi organami administracji rządowej[20]. Część autorów unikając niejako próby definiowania tych organów, nazywa je po prostu centralnymi organami administracji[21]. Posługiwanie się określeniem centralnego organu administracji rządowej można uznać za uzasadnione jedynie w przypadku gdy zakresem pojęciowym obejmujemy jedynie te spośród organów centralnych, które są podporządkowane rządowi, nie można natomiast używać tej nazwy jako generalnego oznaczenia wszystkich organów centralnych[22]. Ze względu na te właśnie problemy w niniejszej pracy posługiwałem się dotychczas pojęciem organów centralnych, unikając nazywania ich centralnymi organami administracji rządowej. Taka zmiana nazewnictwa wydaje się być koniecznym i jedynym możliwym rozwiązaniem pozwalającym na określenie pozycji ustrojowej nie tylko GIODO, ale również innych organów jak np. Głównego Inspektora Pracy i która to pozycja odpowiadałaby rzeczywistej roli jaką sprawują te organy w państwie. Przyjęcie takiego stanowiska rodzi jednak jeszcze problem zmiany kryterium wyodrębniania centralnych organów (urzędów centralnych) spośród innych organów administracji publicznej.

Jest bowiem oczywistym, że skoro Generalny Inspektor nie jest podległy rządowi, a ma należeć do urzędów centralnych, których podstawowym kryterium wyodrębnienia była właśnie ich podległość wobec rządu, i skoro postuluje się zmianę nazwy tych organów na organy administracji państwowej to konieczna jest zmiana kryterium ich wyodrębniania. W praktyce nie ma jednak znaczenia charakter podległości danego organu, ale jego rola i znaczenie w całym aparacie administracyjnym. Rola ta ma polegać na tym, że organy te zawiadują ze szczebla centralnego bieżącą realizacją wyznaczonych przez prawo zadań administracyjnych, w określonych dziedzinach spraw, istotnych z punktu widzenia codziennego, stabilnego funkcjonowania państwa poprzez podejmowanie rozstrzygnięć zarówno generalnych jak i indywidualnych i tym samym należą do segmentu organów wykonawczych[23]. To więc nie kryterium podporządkowania organom administracji rządowej ma być w konsekwencji jedynym decydującym wyznacznikiem konkretnego miejsca organów w aparacie administracji centralnej, ale również rola jaką sprawują w państwie. Inaczej przedstawia się pozycja organów naczelnych, które należą do drugiego segmentu administracji centralnej a mianowicie do segmentu polityczno -rządowego. Należy więc pozytywnie wypowiedzieć się co do poglądu J. Bocia, który w swoich rozważaniach na temat organów centralnych wskazuje, iż są to organy, których organami zwierzchnimi są: Sejm, Rada Ministrów, Prezes Rady Ministrów i poszczególni ministrowie, którym też przysługują uprawnienia nadzorcze[24]. Za przedstawionym powyżej rozwiązaniem przemawia również fakt, iż tryb wyboru organu ochrony danych osobowych przez parlament jest normą przyjętą w ustawodawstwach państw europejskich gdyż stanowi gwarancję jego demokratycznej legalizacji i zapewnia bezpieczny dystans w stosunku do innych organów administracji publicznej, które mogę przecież podlegać jego kontroli[25]. Przyjęcie takiego rozwiązania nie stanowi bowiem próby wydzielenia tego organu spośród innych organów centralnych ale ma charakter ogólnoustrojowy i służy podkreśleniu prestiżu i rangi Generalnego Inspektora jako jedynego organu stojącego na straży praworządności w kontekście ochrony danych osobowych. Jedyny mankament przyjętego rozwiązania może wiązać się z tym, iż obecna forma wyboru Generalnego Inspektora ma charakter polityczny, a więc jest w znacznym stopniu uzależniona od układu sił politycznych w parlamencie. Nie zmienia to jednak faktu, że Generalny Inspektor jest organem w pełni niezależnym w wykonywaniu swojej funkcji i tak jak zostało to już wyżej zaakcentowane w tym zakresie podlega wyłącznie ustawie.

Za uznaniem Generalnego Inspektora za centralny organ administracji państwowej przemawia nie tylko rola jaką organ ten pełni w aparacie administracji centralnej, ale również obszar jego działania. Jak już wyżej zostało wskazane jest on bowiem jedynym organem, który w skali całego kraju sprawuje nadzór nad realizacją prawa do ochrony danych osobowych. Status organów centralnych w żadnym wypadku nie może natomiast przysługiwać Inspektorom podlegającym Generalnemu Inspektorowi. Podobnie też jak zdecydowana większość organów centralnych, Generalny Inspektor jest organem o charakterze jednoosobowym. Spośród tych organów, najbardziej charakterystyczną grupą są organy w postaci kierowników urzędów, przy pomocy których realizują oni swoje kompetencje. Taki też status można przypisać Generalnemu Inspektorowi Ochrony Danych Osobowych, który stoi na czele swojego biura. Generalny Inspektor Ochrony Danych Osobowych został ustanowiony na podstawie ustawy podobnie jak zdecydowana większość inny organów centralnych. Od każdej z wymieniony przeze mnie powyżej cech organu centralnego, występują jednak odstępstwa. Dla przykładu można wskazać organy, w ramach których to urząd, a nie jednostka (prezes, kierownik itd.) jest uznawany za centralny organ administracji państwowej (np. Urząd Patentowy RP). Nie jest również zasadnym posługiwanie się argumentem, iż za organ centralny administracji państwowej można uznać tylko taki organ, któremu taki status został nadany wyraźnie przez przepisy prawne. Jako przykład można wskazać tutaj Głównego Inspektora Pracy, który w literaturze przedmiotu również jest uznany za centralny organ administracji państwowej, a brak jest wyraźnej podstawy prawnej nadającej mu taką pozycję ustrojową[26].

Bez wątpienia część przedstawicieli doktryny słusznie zauważa, iż pozycja ustrojowa Generalnego Inspektora jest podobna do pozycji organów kontroli państwowej i ochrony prawa, wskazanych w Rozdziale IX Konstytucji RP. Zbieżności upatruje się zwłaszcza w przyznanych mu uprawnieniach kontrolnych, a w stosunku do Rzecznika Praw Obywatelskich w sposobie powoływania i dowoływania GIODO przez sejm oraz w przyznanej mu gwarancji niezależności od innych organów. Jednak określony w Konstytucji RP katalog organów kontroli państwowej i ochrony prawa ma charakter zamknięty i obejmuje swoim zakresem Najwyższą Izbę Kontroli, KRRiT oraz Rzecznika Praw Obywatelskich (dalej RPO). Pozycja tych organów ze względu na fakt ich umieszczenia w Konstytucji RP jest znacznie silniejsza niż GIODO. Dodatkowo możliwość utożsamiania pozycji GIODO z pozycją Rzecznika Praw Obywatelskich wyłącza przyznanie temu pierwszemu uprawnień do wydawania rozstrzygnięć indywidualnych w formie decyzji administracyjnych, jakich to uprawnień nie posiada RPO[27].

Ustanowienie przez polskiego ustawodawcę wyspecjalizowanego organu ochrony danych osobowych jakim bez wątpienia jest GIODO w moim przekonaniu nie uprawnia jeszcze do uznania go za organ administracji specjalnej. Pogląd taki w jednej ze swoich prac wyraził J. Niczyporuk, który wskazuje, iż GIODO należy traktować jako organ administracji specjalnej, czy też innymi słowy administracji niezespolonej lub wyspecjalizowanej[28]. Podążając za poglądami wskazanymi przez M. Jełowickiego organy administracji specjalnej są usytuowane w scentralizowanych systemach hierarchicznych i podporządkowane jednemu z naczelnych lub centralnych organów administracji państwowej[29]. Pozycja ustrojowa Generalnego Inspektora w żaden sposób nie wpisuje się więc w pozycje organów specjalnych przedstawioną w powyższej definicji. Jeżeli natomiast przyjmiemy, iż decydującym kryterium nie jest tutaj pozycja organu administracji specjalnej względem organów naczelnych bądź centralnych, ale rola jaką pełni w systemie administracji publicznej, to też pojawia się problem. Takie myślenie doprowadziłoby bowiem to wniosku, iż pozycja takich organów administracji niezespolonej jak dyrektorzy izb celnych, naczelnicy urzędów celnych czy dyrektorzy izb skarbowych jest tożsama z pozycją Generalnego Inspektora Ochrony Danych Osobowych. Takie myślenie jest niedopuszczalne choćby ze względu na fakt, iż Generalny Inspektor jest jedynym w Polsce organem stojącym na straży realizacji prawa do ochrony danych osobowych i nie jest związany z jakimkolwiek podziałem terytorialnym.

W moim przekonaniu nie ulega wątpliwości, że Generalny Inspektor jest centralnym organem administracji w rozumieniu kpa. Wydawane przez niego decyzje mają charakter ostateczny w administracyjnym toku instancji i nie przysługuje od nich odwołanie. Uprawnienie do wystąpienia ze skargą do sądu administracyjnego powstaje natomiast dopiero po wydaniu przez Generalnego Inspektora ponownej decyzji wskutek wniesienia do niego wniosku o ponowne rozpatrzenie sprawy[30].

Przedstawione powyżej poglądy doktryny jak i analiza materiału normatywnego prowadzi do wniosku, iż pozycja ustrojowa Generalnego Inspektora Ochrony Danych Osobowych została ukształtowana w sposób niedokładny i może rodzić wiele wątpliwości. Jako organ państwowy, jego kompetencje jak i charakter odpowiadają częściowo pozycji nadanej przez ustawodawcę innym organom państwowym, różniąc się jednocześnie od nich na tyle, że nie jest możliwe porównanie go w pełni do żadnego z innych organów. Mimo iż, tak jak to wykazałem, nie powinien budzić wątpliwości fakt uznania Generalnego Inspektora za centralny organ administracji państwowej, postuluje się by ustawodawca przy najbliższej nowelizacji ustawy, wprost określił, że Generalny Inspektor jest centralnym organem administracji państwowej. Problem zakwalifikowania tego krajowego organu ochrony danych osobowych do jednej z kategorii organów administracji publicznej ma znaczenie nie tylko ze względów czysto ustrojowych, ale również praktycznych. Utrzymanie takiego stanu niepewności poddaje pod wątpliwość nie tylko dopuszczalność stosowania do tego organu przepisów prawa formalnego adresowanych do organów centralnych. Chodzi głównie o problem dopuszczalności stosowania do rozważań dotyczących GIODO poglądów doktrynalnych, orzecznictwa,

literatury dotyczących innych centralnych organów przez analogię. Jasne opowiedzenie się za uznaniem Generalnego Inspektora za organ centralny, pozwala więc uniknąć wielu wątpliwości interpretacyjnych, bez wątpienia wpływających pozytywnie na większą skuteczność działania organu. ■

* Maciej Kawecki, doktorant w Katedrze Postępowania Administracyjnego na WPiA Uniwersytetu Jagiellońskiego w Krakowie, student European Academy of Diplomacy oraz stypendysta Fundacji im. K. Pułaskiego w Warszawie. Absolwent Uniwersytetu Jagiellońskiego oraz Uniwersytetu w Sztokholmie. Autor wielu artykułów naukowych z zakresu prawa nowych technologii oraz prawa autorskiego.

[1] Cz. Martysz, Pozycja prawnoustrojowa Generalnego Inspektora Ochrony Danych Osobowych, [w:] Ochrona danych osobowych. Skuteczność regulacji, pod red. G. Szpor, Warszawa 2009, s. 67.

[2] M. P. nr 5 poz. 47, z późn. zm.

[3] M. Wierzbowski, Prawo administracyjne, Warszawa 2007, s. 140.

[4] E. Ochendowski, Prawo administracyjne, Toruń 2005, s. 231.

[5] E. Ura, Prawo administracyjne, Warszawa 2009, s. 151.

[6] M. Wierzbowski, Prawo..., s. 140.

[7] J. Boć, Prawo administracyjne, Wrocław 2002, s. 152.

[8] Zob. P. Barta, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2009, s.150; J. Niczyporuk, Administracja ochrony danych osobowych , [w:] Prawa jednostki w społeczeństwie informatycznym, pod red. M. Grzybowskiego , Rzeszów 1999, s. 32; E. Ura, Prawo..., Warszawa 2009, s. 153.

[9] Por. P. Fajgielski, Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne, Lublin 2008, s. 227; E. Kulesza, Pozycja i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych w świetle ustawy o ochronie danych osobowych. Uwagi de lege lata i de lege ferenda „Przegląd Sejmowy" 1999, nr 6, s.9.

[10] E. Ochendowski, Prawo administracyjne... s. 224 i n.

[11] J. Boć, Prawo..., s. 133.

[12] J. Barta, Ochrona danych osobowych. Komentarz, Warszawa 2011, s. 390.

[13] J. Niczyporuk, Prawa jednostki w społeczeństwie..., s. 34 i n.

[14] Wyrok TK z dnia 10 kwietnia 2002 r., sygn. Akt K 26/00.

[15] Zob. Z. Leoński, Materialne prawo administracyjne, Warszawa 2003, s. 42 i n. ; Niczyporuk, Prawa jednostki w społeczeństwie..., s. 35.

[16] M. Wierzbowski, Prawo..., s. 182.

[17] M. Sakowska, Pozycja ustrojowa i zadania Generalnego Inspektora Ochrony Danych Osobowych, „Przegląd Sejmowy" 2006, nr 2, s.85.

[18] Por. M. Gersdorf, Komentarz do ustawy o Państwowej Inspekcji Pracy, Warszawa 2008, s. 19 i n.

[19] E. Ura, Prawo..., s. 151 i n.; Zob. E. Kulesza, Pozycja... s. 10 i n.

[20] Zob. Z. Niewiadomski, Prawo administracyjne, Warszawa 2009, s. 196 i n.; M. Domagała, Encyklopedia Prawa Administracyjnego, Warszawa 2010, s. 43.

[21] M. Wierzbowski, Prawo..., s. 177 i n.

[22] Zob. Tytuł ustawy z 1 marca 2002 r. o zmianach w organizacji i funkcjonowaniu centralnych organów administracji rządowej i jednostek im podporządkowanych... (Dz. U. Nr 25, poz. 253 ze zm.).

[23] M. Wierzbowski, Prawo..., s. 185.

[24] J. Boć, Prawo..., s. 158.

[25] Zob. E. Kulesza, Pozycja... s. 11 i podana tam literatura.

[26] E. Ura, Prawo..., s. 155; J. Boć, Prawo..., s. 159; Cz. Martysz ,Ochrona danych ...s. 71.

[27] M. Sakowska, Pozycja ustrojowa..., s.83; G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s. 117.

[28] J. Niczyporuk, Prawa jednostki w społeczeństwie..., s. 34 i n.

[29] M. Jełowicki, Organy administracji specjalnej, Warszawa 1990, s. 31.

[30] Zob. art. 5§2 pkt 4 i art. 127§ 3 ustawy z dnia 14 czerwca 1960r.-Kodeks postępowania administracyjnego (Dz. U. Nr 98, poz. 1071 ze zm.) oraz art. 21 ust. 1 ustawy z dnia 29 sierpnia 1997r. -o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883).

Arkadiusz Pietrzak*

Spam - niechciana poczta elektroniczna (Spam - unwated e-mails)

Koniec XX wieku, a dokładniej ostatnia jego dekada przyniosły zaskakujący rozwój Internetu. Nowinki techniczne umożliwiły rewolucje w dziedzinie szeroko rozumianej komunikacji. Nie ma w tym nic złego, jednakże każdy kij ma dwa końce. Wraz z nowymi możliwościami porozumiewania się pojawiła się kusząca możliwość zarobienia na tym pieniędzy, dużych pieniędzy. Dostrzeżono, że korespondencja elektroniczna może być znakomicie wykorzystywana do działań marketingowych. Zapewnia indywidualny kontakt reklamodawcy z odbiorcą, który jest niemalże natychmiastowy. Niewątpliwą zaletą są oczywiście niskie koszty przesyłu informacji. Jedyne co pozostaje to zdobyć odpowiednio zdefiniowaną bazę danych z adresami e-mail. I tu często pojawia się problem legalności pozyskiwania takich baz danych oraz ich późniejszego przetwarzania, zwłaszcza gdy adresy e-mail stanowią dane osobowe.

Wiele narzędzi internetowych śledzących aktywność użytkownika w sieci dodatkowo buduje profil odbiorcy (przeszukuje Internet w poszukiwaniu informacji co dany adresat wiadomości e-mail lubi, czym się interesuje, jakie miejsca w sieci i poza nią potencjalnie odwiedza). Pomaga to bardzo w dopasowaniu odpowiedniej oferty i jest legalne. A na czym polega spam ? Aby na to pytanie odpowiedzieć warto posłużyć się kilkoma podstawowymi informacjami o znaczeniu historycznym. Spam jest słowem pochodzenia angielskiego i oznacza dosłownie konserwy mięsne[1]. Na świecie określenie to weszło w krew za sprawą II wojny światowej (owe konserwy były podstawą wyżywienia armii alianckiej). Z kolei w latach 60. XX wieku angielska grupa komików Monty Python użyła tego określenia dla niezbyt smacznej potrawy, która stale była dostępna w menu restauracji[2]. Dlatego też trafnym okazało się przejęcie tego słowa do języka Internetu. Tutaj również oznacza rzecz niechcianą i bezużyteczną z punktu widzenia odbiorcy. O tym jak bardzo owe słowo „spam" stało się powszechne w użyciu świadczyć może wydana przez OHIM (*The Office for Harmonization in the Internal Market*) w 2006r. decyzja odmowna w przedmiocie rejestracji znaku towarowego mielonki firmy Hormel Foods Corporation o zarejestrowanie tej nazwy jako znaku towarowego owej mielonki[3]. Decyzję uzasadniono tym, że dla konsumenta słowo spam nie oznacza mielonki, ale niechcianą pocztę elektroniczną.

Spam można podzielić na spam *sensu stricto* (komercyjny) i *sensu largo* (niekomercyjny, towarzyski itd.)[4]. Istnieje również spam mobilny (m-spam), który jest rozsyłany na telefony komórkowe poprzez krótkie wiadomości tekstowe (sms)[5].

Pierwsze orzeczenia i akty prawne w materii spamu *sensu stricto* (komercyjnego) zostały wydane w Stanach Zjednoczonych Ameryki Północnej (dalej USA). Zarzuty podnoszone w tych orzeczeniach to najczęściej „fałszerstwa (ang. *forgery*), oszustwa (ang. *fraud*), naruszenia znaku towarowego (ang. *trademark infringement*), zajęcie ruchomości (ang. *tresspass to chatteles*), naruszenia postanowień umownych (ang. *breach of contract*) oraz przestępstwa komputerowe"[6]. W 2003 r. po kliku inicjatywach ustawodawczych została przyjęta na poziomie federalnym ustawa określana skrótem „CAN-Spam Act 2003". Do końca 2004 r. podobne akty zostały przyjęte również na poziomie stanowym (38 stanów). Unia Europejska również nie pozostała bierna i wydała szereg przepisów prawnych w tym zakresie[7]. Ustawodawstwa krajów europejskich przedstawiają się różnie. Dla przykładu Holandia posiada liberalny system *soft opt-in*. Niemcy, Szwecja, Finlandia, Włochy czy Belgia natomiast przyjęły system *opt-in*[8] (legalność wysyłanej wiadomości zależy od uprzednio wyrażonej zgody). Drugi system stosowany na świecie to *opt-out*. Pozostawia on użytkownikowi opcję wycofania się z otrzymywania wiadomości e-mail (wyrażenia sprzeciwu) np. poprzez kliknięcie w odpowiedni odnośnik podany w wiadomości. W tym systemie uprzednia zgoda na wejście do systemu nie jest brana pod uwagę.

Zwracając uwagę na polskie przepisy odnoszące się do przesyłania wiadomości typu spam na-

leży powołać się na ustawę z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną, a dokładniej art. 10 ust. 1 tejże ustawy oraz art. 24 i 25 (Dz. U. z 2002r. Nr 144 poz. 1204 z późń. zm.). Rozsyłanie niezamówionej informacji handlowej stanowi wykroczenie, jest ścigane na wniosek pokrzywdzonego (nowelizacja, która weszła w życie 21 stycznia 2013r. uściśliła, że chodzi o osobę fizyczną) i zagrożone jest karą grzywny. Ważnym aktem jest także ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153 poz. 1503). Ma ona zastosowanie przy tzw. reklamie uciążliwej, gdy zostanie naruszony art. 16 ust. 1 pkt 5 tejże ustawy. W tym przypadku przesyłanie niezamawianej reklamy gospodarczej przez pocztę elektroniczną będzie stanowiło delikt.

Podzielam stanowisko *Mail Abuse Prevention System*, że muszą być spełnione kumulatywnie trzy przesłanki, aby wiadomość można było określić mianem spamu:
1. Treść wiadomości jest niezależna od tożsamości odbiorcy;
2. Odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymywanie tej wiadomości;
3. Treść wiadomości daje podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy[9].

Spam to niechciane wiadomości i warto o tym pamiętać, że są one źle odbierane przez odbiorców. Jak reagujemy na niechcianą wiadomość e-mail? 55.8% osób usuwa je od razu gdy zorientuje się, że ich nie interesuje, 38% użytkowników przegląda z grubsza by zorientować się o co w nich chodzi a jedynie 3.9% czyta je dokładnie. Najbardziej uciążliwe są przesyłki e-mail zawierające ofertę zakupu produktów (wg 45.5%), na drugim miejscu są banery (wg 27.7%) i na trzecim przesyłki e-mail zachęcające do odwiedzenia stron WWW (wg 17%)[10]. Niechęć jest zrozumiała. Spam zabiera czas użytkowników, narusza ich prywatność i bezpieczeństwo (niejednokrotnie w treści wiadomości znajdują się złośliwe linki lub dołączane są załączniki zawierające złośliwe oprogramowanie). Wszystko to powoduje zmniejszenie zaufania do poczty elektronicznej. Najwięcej spamu w grudniu 2011 r. pochodziło z Indii (12.4%), Indonezji (11.0 %) i Brazylii (9.7%). Z Polski było to tylko 3.2% co plasowało ją na ósmym miejscu[11]. Natomiast w III kwartale 2012r. najwięcej spamu pochodziło z USA(26,7%) i Chin (25,5%). Na trzecim miejscu uplasowały się Indie (9,8%). Polska nie znalazła się w rankingu 20 krajów[12]. Według innego raportu Kaspersky Lab w maju 2011 r. ilość spamu w ruchu pocztowym w stosunku do wszystkich wysłanych w tym czasie wiadomości e-mail wyniosła średnio 80.8%[13]. Zaskakujące jest to, że od pewnego czasu poziom spamu spada. Dla przykładu w listopadzie 2012r. ilość spamu w ruchu pocztowym stanowił 62,9%[14]. Czy to dobrze? To na co warto zwrócić uwagę to twierdzenia analityków ds. bezpieczeństwa, że pomimo tego, iż spamu jest mniej to stanowi on jednak większe zagrożenie[15].

Jeżeli spojrzymy z punktu widzenia pracodawcy spam jest zjawiskiem negatywnym ponieważ spada produktywność pracownika przeglądającego tego typu wiadomości e-mail.

Spam w praktykach reklamowych skazany jest na porażkę. Jak wynika z praktyki pomimo tego, że jest on źle odbierany przez odbiorców mamy z nim do czynienia. Pozostaje otwarte pytanie: jak skutecznie walczyć z tym patologicznym zjawiskiem? Czy wystarczy egzekwowanie istniejących już przepisów czy może należy ustanowić nowe rozwiązania? Moim zdaniem wystarczy elastycznie reagować na zachodzące zmiany. Nie widzę potrzeby rewolucji pod względem prawnym czy nawet dokonywania poważniejszych zmian w istniejącym stanie prawnym. Jestem zdania, że decydującą rolę w zwalczaniu tego typu praktyk odgrywa i odgrywać będzie większa świadomość społeczeństwa. Uważam, że to w gruncie rzeczy przyczyni się do zmiany mentalności i kultury przesyłania informacji handlowych drogą elektroniczną. ■

* Arkadiusz Pietrzak, aplikant adwokacki. Absolwent prawa na Wydziale Prawa i Administracji UMK w Toruniu

[1] English-polish DICTIONARY by K. Bulas F.J. Whitfield, Mouton & Co, The Hague, tłum. polskie PWN 1961, s. 880.

[2] W skeczu tym Wikingowie siedzący w restauracji nie mogą zamówić nic innego poza spamem. Poprzez wielokrotne użycie tego słowa zostało ono ośmieszone.

[3] decyzja OHIM z dnia 19.06.2006r., http://oami.europa.eu/LegalDocs/BoA/2006/en/R0450_2006-2.pdf

[4] D. Kasprzycki: *Spam, czyli niezamawiana komercyjna poczta elektroniczna*, Kraków 2005, s. 58.

[5] http://www.wisegeek.com/what-is-mobile-phone-spam.htm, Wskazówki jak sobie z tym radzić oraz opis zagrożeń znajduje się również na stronie http://www.t-mobile.co.uk/help-and-advice/advice-for-parents/spam/;

[6] D. Kasprzycki: *Spam, czyli niezamawiana komercyjna poczta elektroniczna*, Kraków 2005, s. 71;

[7] Dyrektywa 95/46/WE dotycząca przetwarzania danych osobowych (Dz.U. L 281 z 23.11.1995, s. 31—50);
Dyrektywa 97/66/WE dotycząca ochrony danych osobowych i prywatności w sektorze telekomunikacyjnym (DzU. WE L 24, 30.01.1998, s. 1–8);
Dyrektywa 97/7/WE w sprawie ochrony konsumentów w umowach zawieranych na odległość (Dz.U. L 144 z 4.6.1997, s. 19—27);
Dyrektywa 2000/31/WE w sprawie niektórych prawnych aspektów usług społeczeństwa informacyjnego, w szczególności we Wspólnym Rynku (Dz.U. L 178 z 17.7.2000, s. 1—16);
Dyrektywa 2002/58/WE w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej (Dz.U. L 201 z 31.7.2002, s. 37—47);
Dyrektywa 2002/65/WE w sprawie marketingu prowadzonego na odległość w ramach konsumenckich usług finansowych (Dz.U. L 271 z 9.10.2002, s. 16—24);
Dyrektywa 2005/29/WE w sprawie nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym (Dz.U. L 149 z 11.6.2005, s. 22—39).

[8] D. Kasprzycki: Spam, czyli niezamawiana komercyjna poczta elektroniczna, Kraków 2005, s. 112-113,116, 124, 127, 129, 134, 135.

[9] http://www.mail-abuse.org/spam_def.html

[10] Badanie polskich użytkowników sieci Internet, Katedra Marketingu, Akademia Ekonomiczna w Krakowie, http://badanie.ae.krakow.pl

[11] Raport Kaspersky Lab, http://www.viruslist.pl/analysis.html?newsid=693#4

[12] Źródła spamu, Kaspersky Lab, http://www.kaspersky.pl/images/viruslist/q3spam2012_pic19.png

[13] Raport Kaspersky Lab, http://www.egospodarka.pl/67514,Spam-w-V-2011-r,1,12,1.html

[14] Raport Kaspersky Lab, http://www.kaspersky.pl/about.html?s=news&newsid=1847

[15] Przegląd Kaspersky Lab, http://www.kaspersky.pl/about.html?s=news_reviews&cat=3&newsid=1823

Daria Gęsicka

Sprawozdanie z konferencji „CopyCamp"

(The report on 'Copy Camp' conference)

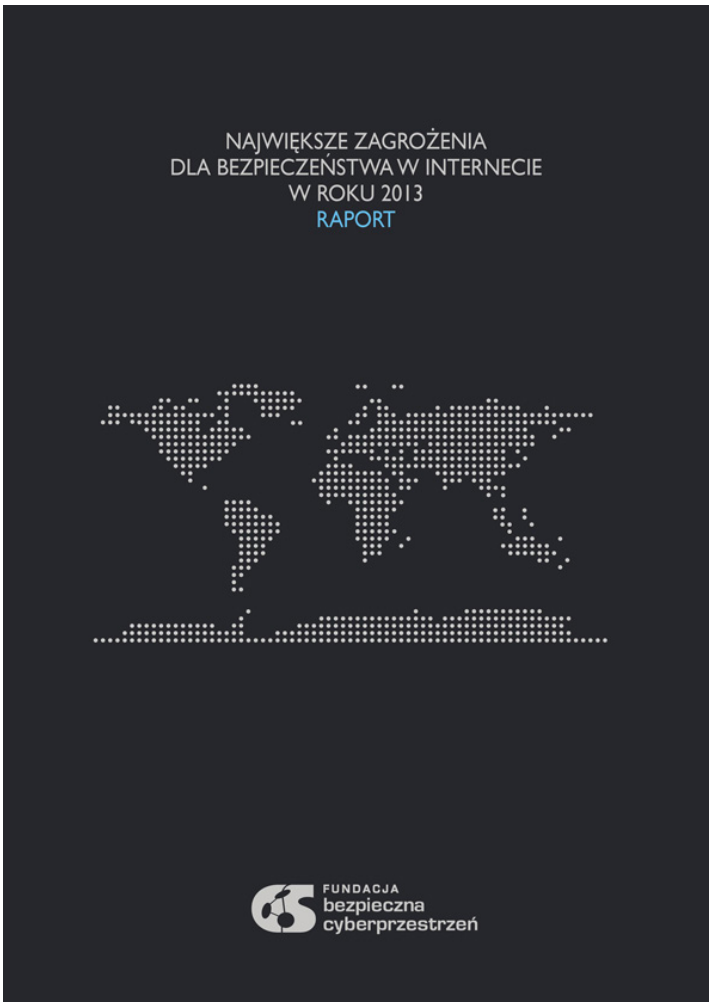
W dniu 26 listopada 2012 r. w Kinie Kultura w Warszawie odbyła się konferencja poświęcona przyszłości prawa autorskiego zorganizowana przez Fundację Nowoczesna Polska oraz Prawo Kultury. W konferencji udział wzięli reprezentanci środowisk naukowych, twórczych a także działacze społeczni oraz politycy. Spotkanie przeprowadzono w formule „campu", czyli równolegle toczących się dyskusji w dwu salach, pomiędzy którymi uczestnicy mogli się przemieszczać. Całość wystąpień zwieńczona została uroczystym bankietem stanowiącym doskonałą okazję do prowadzenia ożywionych dyskusji. Liczba uczestników spotkania (ok. 200 osób) świadczy o tym, że przyszłość prawa autorskiego jest tematem wymagającym dyskusji i mimo wielu wydarzeń o tej tematyce zorganizowanych w bieżącym roku ilość problemów oraz ścierających się interesów jest tak duża, że nadal dialog pomiędzy poszczególnymi środowiskami nie ustaje.

Po uroczystym otwarciu konferencji przez organizatorów oraz partnerów strategicznych głos zabrała Nina Paley – autorka komiksów, grafik oraz animacji a także działaczka społeczna na rzecz uwolnienia kultury. Wystąpienie gościa specjalnego dotyczyło przede wszystkim tych przepisów prawa autorskiego, które spowalniają lub uniemożliwiają swobodny obieg kultury.

Wśród licznych wstąpień w trakcie pierwszego panelu wyróżnić należy stanowisko prof. Jana Błeszyńskiego, który zwrócił uwagę na fakt, że zaniedbanie polskiego ustawodawcy w postaci wadliwej implementacji dyrektywy enforcement do polskiego porządku prawnego nadal nie zostało skorygowane. Prof. Elżbieta Traple w trakcie swojej wypowiedzi podkreśliła konieczność dalszej harmonizacji przepisów prawa autorskiego a także precyzyjnego formułowania przepisów prawa z uwzględnieniem rozwoju nowych technologii. Prof. E.Traple wskazała także, że nie zawsze obowiązujące przepisy prawa są skutecznie egzekwowane. Przykładem przywołanym przez prof. E.Traple jest sprawa portali NewzBin i NewzBin2. Co istotne, prof. E.Traple przypomniała o roli prawa autorskiego, bez którego prawdopodobnie utwory przestałyby istnieć. Mec. Helena Rymar z Centrum Cyfrowego Projekt:Polska zaprezentowała główne założenia idei swobodnego dostępu do dziedzictwa kulturowego oraz naukowego. Następnie Radosław Czajka przedstawił koncepcję fetyszyzacji egzemplarza argumentując, że swobodny obieg kultury nie stanowi straty, ale ogólny zysk dla społeczeństwa i cywilizacji. Hirek Wrona zarysował założenia programu „Bądź świadomy" adresowanego do młodzieży szkolnej mającego na celu uwrażliwienie tej grupy społecznej na problemy prawa autorskiego, zwłaszcza w kontekście wymiany plikami w sieciach peer-to-peer oraz korzystania z nielegalnych źródeł utworów muzycznych, audiowizualnych czy programów komputerowych. H.Wrona podkreślił, że program ten jest jednym z wielu tego typu działań mających na celu szerzenia wiedzy o własności intelektualnej wśród młodzieży. W drugim panelu Alicja Wacławik-Wejman reprezentująca Google Poland Sp. z o.o. przedstawiła uczestnikom korzyści, jakie mogą odnieść twórcy, dzięki obiegowi utworów w Internecie. Ponadto, prelegentka omówiła funkcjonowanie technologii Content ID umożliwiającej analizowanie materiałów umieszczanych przez użytkowników w należącym do spółki serwisie YouTube pod kątem ewentualnych naruszeń a także zalety systemu fonetyzacji. Uczestnicy dowiedzieć się mogli także, jakie są zasady zorganizowanego przez Google Poland Sp. z o.o. konkursu „Next Up", w którym jedną z głównych nagród jest szkolenie dotyczące praw autorskich. Grzegorz Gauden, dyrektor Instytutu Książki, przedstawił inicjatywy oraz działania podejmowane przez agendę rządową Ministerstwa Kultury i Dziedzictwa Narodowego mające na celu wspieranie czytelnictwa oraz promowania polskiej literatury za granicą a także działania podejmowane w ramach zarządu prawami autorskimi Janusza Korczaka.

Każdy z prelegentów miał na przedstawienie swojego stanowiska jedynie 10 minut z uwagi na fakt, że najważniejszym elementem CopyCampu były ożywione dyskusje kuluarowe. Idea organizacji spotkań, w których biorą udział przedstawiciele różnych środowisk reprezentujących często sprzeczne interesy, jest unikalną szansą dla możliwości osiągnięcia kompromisu. Przede wszystkim zaś podkreślenia wymaga fakt, że pierwszym krokiem do jakiegokolwiek kompromisu jest zrozumienie drugiej strony. CopyCamp jest wydarzeniem, podczas którego rodzi się to zrozumienie, dlatego też organizatorzy zapowiedzieli ponowną organizację campu w przyszłym roku.

Informacje o wydarzeniu znajdują się na podanej poniżej stronie internetowej: http://copycamp.pl/



Beata Marek

Rozmowa z dr Wojciechem Wiewiórowskim Generalnym Inspektorem Ochrony Danych Osobowych (Conversation with Polish Inspector General for the Protection of Personal Data)

Beata Marek: Zacznijmy od „ciasteczek". Otóż jednym z argumentów powoływanych przez ich przeciwników jest twierdzenie, że mechanizm ten działa poza wiedzą i zgodą użytkowników końcowych, a tym samym narusza ich prywatność. Czy zrewidowany art. 5 (3) dyrektywy 2002/58/WE e-privacy wpłynie na to, że te obawy nie będą już podnoszone?

Generalny Inspektor Ochrony Danych Osobowych: „Ciasteczka" są rzeczywiście problemem. Już na poziomie dyrektywy o prywatności i łączności elektronicznej tak naprawdę mamy do czynienia z pewnym błędem w założeniach. Przyjmuje się, że cookies to jednolite rozwiązanie czy też jedna grupa rozwiązań. Tymczasem cookies bardzo się od siebie różnią. O ile zarzuty dotyczące ochrony danych osobowych i ochrony prywatności rzeczywiście mają duży sens przy tzw. tracking cookies, o tyle przy innego rodzaju „ciasteczkach", które są dołączane do różnego rodzaju stron czy serwisów internetowych, te obawy nie są wystarczająco uargumentowane. To spowodowało swego rodzaju rozdarcie GIODO przy pracach nad nowelizacją Prawa telekomunikacyjnego, którą kwestie *cookies* były objęte. Gdybyśmy bowiem, z jednej strony, chcieli stosować literalne brzmienie przepisów dyrektywy, to nowe rozwiązania trzeba byłoby odnieść do wszystkich rodzajów cookies i jedynie rozwiązania typu *opt-in* uznać jako jedyne możliwe do zastosowania. Jednak z drugiej strony, spowodowałoby to konieczność wielokrotnego wyrażania zgody na ich stosowanie w serwisach internetowych. Moglibyśmy doprowadzić do sytuacji, w której literalne wdrożenie zapisów dyrektywy tak naprawdę działałoby przeciwko ochronie prywatności, ponieważ użytkownik ciągle pytany o zgodę dotyczącą cookies albo wyrażałby ją bez zastanowienia i godził się na wszystko, albo w ogóle zniechęciłby się do idei prywatności, gdyby miała prowadzić do stosowania tego typu rozwiązań.

Biorąc pod uwagę interpretacje ze strony Komisji i dyskusje, które toczyły się w innych krajach, zdecydowaliśmy się nie protestować przeciwko ostatecznemu rozwiązaniu, które pojawiło się w polskim Prawie telekomunikacyjnym, uznając je za akceptowalne. Aczkolwiek to określenie – akceptowalne - jest chyba jedynym, którego jestem w stanie użyć w stosunku do nowego brzmienia przepisu. Faktycznie powoduje on powstanie systemu opt-out, który jest pewnego rodzaju wyjątkiem od rozwiązań, które do tej pory były stosowane w polskim prawie. Można więc powiedzieć, że zaakceptowaliśmy propozycję kompromisową, zdając sobie sprawę z tego, że jako GIODO narażamy się na zarzuty niewystarczająco silnej ochrony prywatności, co było założeniem dyrektywy o prywatności i łączności elektronicznej. Aczkolwiek podkreślam, że patrząc na wypowiedzi przedstawicieli Komisji Europejskiej dotyczące interpretacji projektu, jestem zdania, że jest to uzasadnione odstępstwo od takiego literalnego brzmienia przepisów. Jak one będą działały w praktyce, również w odniesieniu np. do strony internetowej GIODO, to wciąż otwarte pytanie.

BM: Nawiązując do opinii Europejskiego Inspektora Ochrony Danych Osobowych w sprawie neutralności sieci, zarządzania ruchem oraz ochrony prywatności i danych osobowych (Dziennik Urzędowy C 034 , 08/02/2012 P. 0001 - 0017), w której dostrzeżono problem stosowania przez dostawców usług internetowych „polityki zarządzania ruchem" jestem ciekawa czy zdaniem dra w prawie należy bardziej szczegółowo określić obowiązki nakładane na providerów związane z neutralnością sieci?

GIODO: Jestem przeciwnikiem wprowadzania re-

gulacji prawnych dotyczących neutralności sieci. Uważam, że to powinna być część rozwiązań, które są najpierw sprawdzone na rynku, a dopiero potem ewentualnie podejmowane są jakiekolwiek decyzje prawne w tym zakresie. Z drugiej strony jestem przeciwny rozwiązaniom, które miałyby prowadzić do nadzoru i blokowania treści, które pojawiają się w Internecie.

BM: A czy dr zgadza się z twierdzeniem, że polskie przepisy dotyczące retencji danych pozwalają na zbyt łatwy dostęp do danych organom ścigania? Jak dostęp ten powinien być uregulowany w zgodzie z ochroną danych osobowych obywateli?

GIODO: Zdecydowanie zgadzam się z opinią, że polskie przepisy dotyczące retencji danych telekomunikacyjnych wciąż nie są zadowalające. O tym, że to dla GIODO bardzo istotny problem, świadczy m.in. fakt, że już 2 lata temu tematem przewodnim Dnia Ochrony Danych Osobowych (28 stycznia 2011 r.) była właśnie ta kwestia. Uważaliśmy już wtedy, że korekta przepisów w tym zakresie jest absolutnie niezbędna. Niestety, wciąż jej nie ma, bo trudno za sukces uznać kosmetyczne zmiany przy ostatniej nowelizacji Prawa telekomunikacyjnego.

Uważam też, że dyrektywa jest napisana źle, przez co jest narzędziem nieadekwatnym i, co więcej, kompletnie nieskutecznym. Przypominam, że pojawiła się jako rozwiązanie z zakresu prawa ochrony konkurencji i miała doprowadzić do tego, by operatorzy na rynku europejskim mieli mniej więcej takie same obowiązki, niezależnie od tego, czy działają w Niemczech, Francji, Austrii czy w Estonii. Jednak kilka krajów Unii Europejskiej w ogóle jej nie wdrożyło, a te, które wprowadziły rozwiązania w tym zakresie, zastosowały je w sposób na tyle różny i na tyle różnie odnoszący się do obowiązków operatorów telekomunikacyjnych, że nawet z punktu widzenia ochrony konkurencji zakładany cel zupełnie nie został osiągnięty. Natomiast niektóre państwa zaczęły wykorzystywać ją jako narzędzie z zakresu bezpieczeństwa. Niemniej implementacja rozwiązań dotyczących retencji danych w wielu krajach wywołała burzliwe spory, jak np. w Bułgarii, Rumunii, Czechach, Szwecji, Austrii i na Węgrzech, a Niemcy nawet wycofali się z ich wdrożenia.

To powoduje, że jestem wielkim zwolennikiem zmiany dyrektywy, a tym samym jestem mocno niezadowolony z tego, że prace, które są w tym zakresie prowadzone, trwają tak długo i nie przynoszą żadnych realnych efektów.

Wracając do oceny rozwiązań, które przyjęto w Polsce, trzeba podkreślić, że były one najdalej idącymi z możliwych. Niemniej kwestia okresu obowiązkowej retencji danych jest tu, oczywiście, sprawą najmniej istotną. To, że wcześniej okres ten wynosił 24 miesiące, a po zmianie Prawa telekomunikacyjnego wynosi 12 miesięcy, nie oznacza, że sytuacja poprawiła się dwukrotnie czy też, że mamy o 50% lepsze rozwiązania niż wcześniej. W odniesieniu do rynku internetowego, problemem jest to, jakiego rodzaju dane mogą być zbierane. To nie jest określone wprost w przepisach polskich, toteż uznać można, że Polska nie dokonała wdrożenia dyrektywy w odpowiedni sposób.

Jeśli zaś chodzi o rynek telekomunikacyjny, to najpoważniejszym problemem jest kwestia dostępu do danych retencyjnych. Wątpliwości GIODO budzi przyjęte w Polsce rozwiązanie, które umożliwia niektórym służbom dostęp do danych telekomunikacyjnych przy pomocy specjalnego interfejsu. Nie przekonują mnie tłumaczenia, że ograniczono liczbę policjantów, którzy mają dostęp do tych danych, że istnieje śladowanie, które pozwala zweryfikować, który policjant, do których danych miał dostęp. O ile bowiem faktycznie takie rozwiązania wprowadzono w praktyce, o tyle nie przewidują ich polskie przepisy. Poza tym uważam, że jest to zbyt duży dostęp, do zbyt dużego zakresu danych, przy zbyt dużej liczbie zdarzeń, o które może chodzić. Niech świadczy o tym fakt, że kiedy GIODO zapytał się policji i służb, jakie przestępstwa uważają za poważne (ustawa ich nie wymienia, a zarazem dostęp do danych możliwy jest przy „przestępstwach poważnych"), to otrzymaliśmy bardzo różne odpowiedzi. Jedna ze służb wskazała, że wszystkie przestępstwa, którymi się zajmuje, są poważne. Druga przekazała informację, że „właśnie czeka na wytyczne GIODO dotyczące tego, co jest poważnym przestępstwem".

Od innych służb, które odpowiedziały na nasze pytanie, oraz od policji, otrzymaliśmy wewnętrzne instrukcje mówiące o tym, które przestępstwa należy traktować jako poważne. Abstrahując od faktu, że ten bardzo ważny element regulowany jest na poziomie aktów wewnętrznych, co jest sprzeczne z prawem, w tym z Konstytucją RP – powinno być to bowiem uregulowane w ustawie i rozwinięte w przepisach rozporządzenia - to te instrukcje były różne. Inną instrukcją posługuje się Policja, a innymi służby specjalne. To wyraźnie pokazuje, że jest konieczność ujednolicenia choćby rozumienia definicji poważnego przestępstwa. Inna sprawa, że przez nieprawidłową implementację dyrektywy doprowadziliśmy do tego, że dane te mogą być wykorzystywane w postępowaniach cywilnych, przede wszystkim w sprawach rozwodowych. Nie jest to z pewnością walka z terroryzmem, a więc kwestia zapewnienia bezpieczeństwa.

BM: Pozostając jeszcze na chwilę w temacie retencji danych chciałabym się spytać dra czy mrożenie danych ma szansę zastąpić retencję danych? Jeśli tak to w czym jest lepszy ten model archiwizacji danych?

GIODO: Retencja jako zjawisko i tak będzie istniała. To nie jest tak, że jestem przeciwny rozwiązaniu, jakim jest retencja danych. Jest ona potrzebna choćby dla rozpatrywania reklamacji klientów. Co do mrożenia to jest oczywiście idea, którą bardzo popiera np. Panoptykon. Natomiast ja przyznaję, że wciąż nie do końca rozumiem, czym różni się proponowane mrożenie od rozwiązań, które istnieją dzisiaj i które też powodują, że pewien zestaw danych, o który wnioskowała policja miałby zostać zachowany na jej potrzeby.

Oczywiście rozumiem, że w przypadku mrożenia danych pozostawałyby one po stronie operatora, a policja mogłaby do nich tylko ewentualnie sięgać, a w przypadku dzisiejszych rozwiązań dane te są transportowane do policji i tam przetwarzane. Jeżeli tylko o to chodzi, to mrożenie podoba mi się bardziej, choć nakłada na operatorów telekomunikacyjnych dodatkowe obowiązki. Powstaje w związku z tym pytanie, czy można nakazać operatorom telekomunikacyjnym przechowywanie danych, które tak naprawdę są potrzebne policji. Być może jest to ciekawe i dobre rozwiązanie. Nie jestem jednak przekonany, czy ono tak naprawdę wiele zmienia. Dla mnie najbardziej istotną kwestią jest to, w jakich sprawach można sięgać do danych oraz czy można to robić bez żadnej kontroli zewnętrznej, choćby *post factum*. Tu jest bardzo poważny problem dodatkowy, który trzeba byłoby rozważyć. Rozumiem zastrzeżenia ze strony policji i służb, że dane z retencji niekiedy potrzebne są natychmiast, w tym znaczeniu, że nie ma czasu na przeprowadzenie procedury, która miałaby zezwalać na dostęp do tych danych, że przeprowadzenie tego typu procedury byłoby de facto fikcją. Być może więc pomysłem jest dokonywanie oceny *post factum*, czyli oceny, w jakich sytuacjach i celach dane retencyjne zostały wykorzystane. Gdyby wówczas okazało się, że zostały one pozyskane lub wykorzystane nieprawidłowo, można byłoby nakazać ich zniszczenie. To rozwiązanie jest jednak bardzo niewygodne dla policji, ponieważ każda kontrola post factum zakłada, że w momencie kiedy okaże się, że funkcjonariusz zażądał danych, które nie były potrzebne albo nie było żadnych podstaw do ich uzyskania, to powinna pojawić się kara. Jest to zatem dla policji i służb niewątpliwie temat trudny, ponieważ mogący wpływać na ograniczanie działań tam, gdzie one faktycznie byłby potrzebne.

BM: Nie ulega wątpliwości, że podniesione przez dra postulaty zarówno w odniesieniu do frywolnej interpretacji „poważnego przestępstwa" oraz zakresu i sposobu pozyskiwanych danych są bardzo ważne i wymagają podjęcia konkretnych działań na drodze legislacyjnej. Mam nadzieję, że wydarzy się to w niedalekiej przyszłości.

W kolejnym pytaniu chciałabym się odnieść do zyskującej na znaczeniu chmury. W czasie kryzysu każdy podmiot szuka oszczędności i m.in. dlatego od pewnego czasu obserwujemy tzw. „boom" na usługi w chmurze. Martwi mnie jednak fakt, że wielu przedsiębiorców wciąż jeszcze nie zdaje sobie sprawy z zagrożeń chmury oraz obowiązków wynikających z przepisów o ochronie danych osobowych. Pomimo swej niewiedzy decyduje się na

outsourcing w chmurze – co może wywołać przysłowiowe gradobicie (np. nie są zawierane umowy powierzania albo outsourcowane są dane osobowe poza Europejski Obszar Gospodarczy sprzecznie z przepisami ustawy). Jakie zdaniem dra są największe zagrożenia związane z chmurą i co jest absolutnym „must have" przy przejściu do tego modelu biznesowego?

GIODO: W odniesieniu do chmury często używam motta (które powinni stosować Ci, którzy chcieliby z usług chmurowych korzystać) mojego rodzinnego miasta czyli Gdańska – nec temere nec temide (pol. bez strachu, ale z rozwagą). Tak dokładnie trzeba podchodzić do usług chmurowych. Jest oczywiste, że ten model biznesowy będzie coraz częściej stosowany przy różnego rodzaju usługach. Nie można też twierdzić, że w ogóle nie należy z chmury korzystać, bo ona jest niebezpieczna. Trzeba korzystać, ale z rozsądnym spojrzeniem na to, co się dzieje. W 2012 roku unijni rzecznicy ochrony danych osobowych opublikowali dwa zestawy wskazań dotyczących tego, jak podchodzić do usług chmurowych. Pierwsze to memorandum sopockie, które zostało wydane przez tzw. Grupę Berlińską (grupę do spraw ochrony prywatności w telekomunikacji). Drugie to opinia Grupy Roboczej Art. 29 (zrzeszającej odpowiedników GIODO z wszystkich państw UE) przyjęta w lipcu 2012 r. Dokumenty te zwracają uwagę na najważniejsze kwestie, które przy stosowaniu *cloud computing*u powinny być brane pod uwagę. Uwzględnić trzeba m.in. to, że czym innym jest ochrona danych osobowych w chmurze, a czym innym ochrona tajemnic prawnie chronionych. Umieszczanie w chmurach danych, które są objęte tajemnicą lekarską, adwokacką czy radcowską lub innymi rodzajami tajemnic prawnie chronionych albo informacji, które są informacjami niejawnymi w rozumieniu ustawy o ochronie informacji niejawnych może powodować problem z punktu widzenia tych przepisów. Najprostszym przykładem jest niemożność umieszczania w chmurze, która znajduje się poza Polską, informacji niejawnej, która ze względu na bezpieczeństwo państwa chroniona jest odpowiednią klauzulą.

Z punktu widzenia ochrony danych osobowych jest dla mnie oczywiste, że podmiot, który decyduje się na skorzystanie z usługi albo infrastruktury chmurowej, powinien rozważyć, czy musi zastosować art. 31 ustawy o ochronie danych osobowych odnoszący się do powierzania przetwarzania danych. W niektórych sytuacjach należy bowiem zawrzeć umowę w tym zakresie, a w niektórych nie trzeba. Gdy mamy do czynienia z danymi tzw. zwykłymi i są one szyfrowane i w tej postaci przenoszone do infrastruktury chmurowej, to można się zastanawiać, czy po stronie dostarczyciela chmury w ogóle dochodzi do przetwarzania danych, czy jest on tylko hosterem. Niemniej jeżeli mówimy o rozwiązaniu typu SaaS, jest to już znacznie mniej prawdopodobne. Nawet jeżeli umieścimy zaszyfrowaną informację, to i tak będzie ona odszyfrowana przez oprogramowanie, które będzie działało w chmurze, po to, by mogła zostać przetworzona. A to już oznacza, że ktoś przynajmniej teoretycznie może do tej informacji mieć dostęp.

Zwracam więc uwagę na konieczność przeprowadzenia analizy każdego z rozwiązań chmurowych, które ma być zastosowane oraz z zasady unikania umów adhezyjnych (umów, których nie negocjujemy). Warto pamiętać jednocześnie, że możliwość negocjowania umowy spoczywa na administratorze danych osobowych (dalej ADO). ADO, przekazując dane przetwarzającemu – procesorowi, nie gubi odpowiedzialności za te dane, w stosunku do których decyduje o celach i środkach ich przetwarzania. Cały czas ta odpowiedzialność zarówno za dane, jak i sposób ich przetwarzania spoczywa na nim. W związku z tym ADO musi sobie zapewnić kontrolę nad tym, w jaki sposób dane są przetwarzane przez podmiot, któremu zostały powierzone. I tu ciekawostka. Z reguły umowy, które trafiają do ADO zamierzających skorzystać z usług chmurowych, nie zawierają żadnych klauzul dotyczących możliwości przeprowadzenia kontroli. Natomiast gdy ADO wskaże, że taką kontrolę chciałby sobie zapewnić, to okazuje się, że istnieje również druga wersja umowy, która już zawiera rozwiązania dotyczące kontroli. Zatem to, że w umowie, którą nam przedstawiono, nie znajdują się takie rozwiązania, a nam wydaje się, że niemożliwe jest przeprowadzenie zewnętrznej kontroli, nie wyłącza wcale naszej

odpowiedzialności za to, że zrezygnujemy z jednego z podstawowych obowiązków, które leżą po stronie ADO.

BM: No właśnie. W praktyce widać, że nie ma jednolitej polityki po stronie providerów w zakresie podejścia do klienta oraz informowania go.

GIODO: I dobrze. Rynek konkurencji polega na tym, że różne podmioty mają różną politykę. Wręcz niepokoiłaby mnie sytuacja gdyby powstał kartel. Dlatego polityki są różne. Dobrze żeby były dobre.

BM: Nie miałam na myśli stworzenia kartelu. Mi chodziło o obecną sytuację gdzie jest skrajnie różna polityka informacyjna po stronie providerów. Moim zdaniem powinny być pewne obowiązki informacyjne nałożone na wszystkich usługodawców takie same. Np. informowania o tym, że provider nie posiada własnej infrastruktury informatycznej tylko „dzierżawi ją". Miałam taki przypadek, że zwrócił się do mnie podmiot, któr miał problem z providerem oferującym usługę chata w modelu SaaS. Usługodawca nie wyrażał zgody na podpisanie umowy powierzania zasłaniając się twierdzeniem „jesteśmy zarejestrowani w GIODO, a zatem nie ma potrzeby takiej umowy zawierać". Dodam, że działał w IaaS co zatajał przed potencjalnym klientem (odpowiednia umowa podpowierzania także nie zostałaby zawarta). Dodatkowo dane były przetwarzane poza Europejskim Obszarem Gospodarczym o czym potencjalny klient nie został poinformowany (to wykazał przeprowadzony przeze mnie audyt).

GIODO: Oczywiście taki przypadek jest karygodny. To, że ktoś zarejestrował swój zbiór w rejestrze prowadzonym przez GIODO, po pierwsze, nie oznacza, że na pewno wypełnia obowiązki wynikające z ustawy, po drugie ten usługodawca wyraźnie wskazał, że jego zbiór został zarejestrowany, co oznacza, że nasze dane osobowe chce dołączyć do swojego zbioru. Innymi słowy on będzie ADO, a więc podmiotem, który będzie decydował o celach i środkach przetwarzania danych. Jeżeli więc ktoś nam mówi, że ma już przecież zgłoszoną bazę, to oznacza to, że nie traktuje nas jak ADO, tylko uważa, że to on nim będzie. Z pewnością w tym momencie powinno zapalić się nam już nie żółte, ale czerwone światełko. Natomiast dotknęła Pani innego problemu, który może się pojawić, i z którym bardzo trudno sobie radzić. To jest sytuacja, w której tym providerem usług chmurowych nie jest tak naprawdę dostarczyciel chmury. On zaś jest tylko pośrednikiem w kontakcie z tymi, którzy chmurę „posiadają". Dostarcza usługę, którą stworzył, ale nie na swoich zasobach. Taka sytuacja jest niekiedy nazywana stosem chmur. Polega na tym, że my tak naprawdę kontaktujemy się z obłoczkiem, a ten obłoczek będzie nasze dane przetwarzał w chmurach, których sam nie jest właścicielem. I to jest bardzo skomplikowana sytuacja. Musimy zdawać sobie sprawę z tego, jakie umowy i z jakimi podmiotami ma zawarte usługodawca, z którym chcemy zawrzeć umowę. Może się okazać, że tylko on działa na terenie Polski, a chmury umieszczone są poza obszarem EOG.

BM: Dokładnie. Projekt rozporządzenia unijnego zaprezentowanego w styczniu 2012r., które ma zastąpić unijną dyrektywę z 1995 r. jest uważany za dość rewolucyjny. Czy faktycznie tak jest?

GIODO: Moim zdaniem, projekt nie jest nadzwyczaj rewolucyjny, choć pojawiają się w nim pewne nowe zasady. Swego rodzaju rewolucją jest zapewne to, że zniknie 27 ustaw krajowych, a zamiast nich pojawi się jeden akt prawny na poziomie europejskim. To, oczywiście, jest uproszczenie, bo ustawy odnoszące się do ochrony danych osobowych w poszczególnych krajach będą musiały istnieć. Rozporządzenie nie reguluje bowiem sposobu ukształtowania organu ds. ochrony danych osobowych ani kwestii kontroli sądowej. Natomiast pojawia się wiele rozwiązań nowych, bardzo dobrych – np. wiążące reguły korporacyjne. Mi, jako GIODO, bardzo ich brakuje. Obecnie ani polskie, ani europejskie prawo nie przewiduje bowiem istnienia BCR, więc pojawienie się ich w rozporządzeniu jest bardzo dobrym rozwiązaniem. Z drugiej jednak strony niektóre z zasad, które przewidziano rozporządzeniu jako nowe, są albo rozwinięciem zasad już istniejących, albo próbą doprecyzowania pewnych filozoficznych pomysłów, które do tej pory były wyrażane w doktrynie. Za takie przypadki uważam zasadę przenaszalności danych (ang. portability),

prawo do bycia zapomnianym, privacy by design i privacy by default. W tym zakresie niewątpliwie pojawiają się nowe rozwiązania . Wielokrotnie jest to uszczegółowienie i odniesienie do nowych rozwiązań technologicznych, co czasem powoduje problem, np. przy zasadzie przenaszalności danych. O ile jest ona zrozumiała, oczywiście przy wszystkich zastrzeżeniach, w przypadku przenoszenia pomiędzy portalami społecznościowymi, o tyle nie bardzo wiem, jak miałaby funkcjonować, jeżeli dotyczyłaby np. ubezpieczycieli. Czy to oznacza, że wszystkie informacje, które posiada o mnie ubezpieczyciel A mogę od niego zabrać i przekazać darmowo ubezpieczycielowi B? Są sytuacje, w których możemy mieć co do tego wątpliwości. Przykładowo jeżeli oferta, która została mi przedstawiona, bazuje na badaniach lekarskich, za które zapłacił ubezpieczyciel A, to mimo iż są to dane o mnie, czyli powinienem mieć do nich dostęp. Natomiast wcale nie jest takie oczywiste, czy mogę je zabrać ubezpieczycielowi A i przedstawić ubezpieczycielowi B.

Jestem generalnie zwolennikiem tego rozporządzenia. Uważam, że to dobry pomysł, również od strony formalnej. Czeka nas jednak jeszcze poważna dyskusja co do ostatecznego kształtu przepisów. Ta dyskusja już się toczy i my jako Biuro GIODO uczestniczymy w niej jako eksperci po stronie polskiej, biorąc udział m.in. w spotkaniach Grupy Roboczej ds. wymiany informacji i ochrony danych DAPIX. Bierzemy także aktywny udział w pracach Parlamentu Europejskiego. Podczas dwudniowej konferencji PE z 27 parlamentami krajowymi, miałem zaszczyt wygłosić wykład na temat dyrektywy, czyli drugiego aktu, który jest dołączony do pakietu proponowanych zmian. Uważam, że jest to regulacja, która jest w Polsce niezbędna. Oczywiście wiem o wszystkich zastrzeżeniach, które zgłaszają inne kraje członkowskie, ale wszystko, co proponuje dyrektywa, jest lepsze niż przepisy obecnie obowiązujące w Polsce. W związku z tym jestem absolutnym zwolennikiem rozwiązań, które tam zaproponowano.

BM: A co dr sądzi o projektach typu Google Glass oraz Facedeals?

GIODO: Są to bardzo ciekawe projekty. Szczerze mówiąc, w jakimś stopniu brakuje mi tego typu rozwiązań technicznych na rynku. Rozwiązań, dzięki którym miałbym taką rozszerzoną rzeczywistość, która umożliwiałaby natychmiastowy dostęp do Wikipedii czy innego rodzaju serwisów, dotyczących np. każdego kościółka czy komina, które znajdują przy drodze, którą jadę. Jestem osobą, która dużo podróżuje i szukam czasem informacji o miejscowościach – czasem nawet bardzo małych – przez które przejeżdżam. Np. niedawno, podczas jednej z podróży, zastanowił mnie ogromny komin stojący w polu pod Pruszkowem. Okazało się, że istnieje blog poświęcony kominom w Polsce. Można było znaleźć tam dokładne informacje o tym kominie i o tym, że powstał w związku z planowaną budową elektrociepłowni, która, jak się okazało, w efekcie nigdy nie powstała. No, ale domyślam się, że nie chce mnie Pani pytać o kominy ani informacje o XVII-wiecznych kościołach, tylko o te dane, które są danymi osobowymi. O dane, które przy pomocy Google Glass miałyby być dostępne. No i to już jest problem poważny. Z jednej strony, oczywiście, możemy powiedzieć, że każdy musi się samodzielnie zgodzić na to, żeby jego dane były możliwe do wyszukiwania przy pomocy różnego rodzaju aplikacji robionych na potrzeby takich rozwiązań.

Problem polega nawet nie na dobrowolności, lecz na tym, na ile jesteśmy poinformowani o tym, na co tak naprawdę się godzimy. Nie neguję rozwiązania jako takiego. Rozumiem jego przydatność. Sam pewnie chętnie bym z niego skorzystał, aczkolwiek bardzo ostrożnie i rozważnie. Pamiętajmy, że serwis typu Google Glass nie różni się aż tak bardzo od tego, co możemy znaleźć w Internecie. Przy pomocy tej usługi zostaną wyszukane informacje, które już dzisiaj umieszczamy w Internecie i są wyszukiwane choćby na potrzeby reklamy behawioralnej. Cały czas przypomina mi się sytuacja, z którą miałem do czynienia kilka miesięcy temu, kiedy w Internecie przypadkowo trafiłem na informację o książce, którą czytałem w dzieciństwie - „Feniks i dywan". Przez kilka minut przeszukiwałem Internet, by znaleźć informacje o niej, bo chciałem ją przeczytać swojej córce. Znalazłem wszystkie wydania, które ukazały się na rynku. Jakież było moje zdziwienie, gdy

przez następną godzinę, gdy korzystałem z zupełnie innych tematycznie serwisów, wszystkie reklamy behawioralne odnosiły się do pobliskich salonów z dywanami. Okazało się, że zostałem zgeolokalizowany i to w dodatku jako osoba szukająca dywanów. Dobrze, że nie pokazano mi, gdzie można kupić feniksy. Sądzę, że informacja, która trafiła na potrzeby reklamy behawioralnej, była zbliżona do tego, co otrzymałbym w serwisie Google Glass. W tym przypadku wyszedłbym na ulicę, a serwis pamiętałby, że niedawno szukałem feniksów i dywanów w związku z czym należy mnie poinformować, w którą stronę należy się udać, żeby owe dywany znaleźć. Oczywiście, należy pamiętać, że gdzieś odkłada się informacja dotycząca tego, czego posiadacz tych konkretnych okularów szukał w ostatnim czasie.

BM: W jaki sposób kontrolować podmioty, które zbierają aż tyle informacji na rynku europejskim? Czy jest to realnie możliwe?

GIODO: Jest to możliwe. Z jednej strony ze względu na fakt, że każdy z nas może wystąpić o to, aby dostać komplet informacji o sobie, które znajdują się w posiadaniu danej firmy. O ile jeszcze 3 czy 4 lata temu osoby, które ubiegały się o takie informacje, były wyśmiewane, o tyle obecnie firmy zdają sobie sprawę z tego, że obowiązek udzielenia informacji istnieje i są zobowiązane go respektować. Z drugiej strony większość firm ma swoje przedstawicielstwo europejskie, a GIODO poprzez współpracę z swoimi odpowiednikami w UE, a czasami poza Unią (równie dobrze współpraca wygląda jeżeli chodzi o Kanadę, Australię czy Nową Zelandię, coraz lepiej w przypadku Stanów Zjednoczonych gdzie Federal Trade Commision jest coraz bardziej aktywna na rynku prywatnym) ma możliwość wpłynięcia na to jak wyglądają polityki prywatności tego typu serwisów. Oczywiście w tym momencie przytaczam przykłady dotyczące dużych serwisów. Gorzej jest w przypadku serwisów, które oferują gry online czy wirtualne światy (część gier tworzy de facto takie światy, społeczności przywiązane do określonej gry), a których właścicielami są firmy mające siedziby w bardzo egzotycznych miejscach na świecie.

BM: Czy zgadza się dr z twierdzeniem, że prawo do bycia zapomnianym może prowadzić do ograniczenia wolności słowa w Internecie?

GIODO: Tak, zgadzam się z takim twierdzeniem. Uważam, że powinniśmy bardzo ostrożnie podchodzić do tego zagadnienia. W ostatnim czasie miałem dwa duże wystąpienia na ten temat. Pierwsze na konferencji zorganizowanej przez Agencję Praw Podstawowych w Wiedniu, drugie podczas dnia otwartego biura GIODO w Dąbrowie Górniczej gdzie zwracałem uwagę na tę kolizję, która występuje pomiędzy prawem do bycia zapomnianym, a wolnością wypowiedzi, pamiętając przede wszystkim, że nasz przepis konstytucyjny dotyczący swobody wypowiedzi jest tym samym przepisem, w którym zapisane jest prawo do przetwarzania informacji. W związku z tym to jest nie tylko wolność słowa, ale również wolność przetwarzania informacji. Na czym polega problem? Poprzez wycofanie informacji o sobie (mówię teraz tylko o informacji legalnie umieszczonej w sieci) możemy tak naprawdę wpływać na to, jak wygląda pamięć historyczna. Dwa przykłady, które dobrze to ilustrują. Po pierwsze przypadek, gdzie zabójca aktora Waltera Sedlmayra zażądał od Wikipedii usunięcia informacji o tym, że jest mordercą (tłumacząc to tym, że ma on problem z powrotem do społeczeństwa, gdyż jego nazwisko jest ciągle łączone z przestępstwem dokonanym wiele lat wcześniej). Co ciekawe, niemiecka Wikipedia wycofała dane osobowe zabójcy, ale bez trudu można znaleźć te dane w angielskiej wersji Wikipedii oraz w archiwach gazetowych. Drugi przykład dotyczy wspomnianego przeze mnie wcześniej blogu o kominach. Jest tam także napisane, kto nie wybudował elektrociepłowni i kto podejmował decyzje, skutkujące różnymi opisanymi w blogu konsekwencjami. Zapewne te osoby również mogłyby wystąpić, w ramach prawa do bycia zapomnianym o to, żeby ich dane zostały usunięte z Internetu.

Jeszcze może dodam, że w tej chwili toczy się postępowanie dotyczące z jednej strony neutralności sieci, a z drugiej strony prawa do bycia zapomnianym. Dotyczy ono Maxa Mosleya (jest to dobrze znane nazwisko wszystkim osobom, które interesują się wyścigami samochodowymi, jako że był on szefem Formuły 1). W pewnym momencie w sieci

pojawiły się zdjęcia oraz nagrania dotyczące sfery prywatnej Maxa Mosleya. Wytoczył on sprawę, w której zażądał odszkodowania oraz usunięcia materiałów z serwisów należących do gazety i wygrał ją. Ale informacja się klonuje. Max Mosley od kilku lat dąży do usuwania tych materiałów z różnych miejsc w sieci i skutecznie w jakimś stopniu je usuwa. Ta informacja jednak w dalszym ciągu się klonuje i pojawia w nowych miejscach. Jaki jest nowy pomysł Maxa Mosleya? Pozwał Google. Uznał, że ten podmiot powinien doprowadzić do sytuacji, gdy w wynikach wyszukiwania nie będą znajdowały się informacje dotyczące zdarzenia, które niewątpliwie narusza prywatność Maxa Mosleya. Google odpowiada, że może nawet by się na to zgodził w przypadku Maxa Mosleya, natomiast co stanie się, jeżeli pozostałe 6 mld ludzi na Ziemi zgłosi zastrzeżenia co do informacji, które na ich temat pojawiają się w różnych miejscach w sieci. Czy też mają być filtrowane z wyników wyszukiwania?

W związku z tym próba wpłynięcia na usunięcie danych z Internetu nie dość, że jest nieskuteczna, to może wywołać efekt przeciwny – tzw. efekt Barbry Streisand, polegający na tym, że jak coś bardzo chce się ukryć, to ukrywana treść staje się bardziej widoczna. Barbra Streisand zaprotestowała kiedyś przeciwko albumowi zdjęć wybrzeża Kalifornii, gdzie znajdowało się zdjęcie jej posiadłości. Ten album nie był specjalnie popularny do czasu, kiedy Barbra Streisand zaprotestowała. Wtedy wszyscy zainteresowali się przede wszystkim tym, czegóż to ona nie chciała pokazać.

BM: Niewątpliwie potęga Google tkwi w ilości i różnorodności informacji oraz m.in. skali ich odbioru. Z powodzeniem można powiedzieć, że na Google spoczywa też swego rodzaju odpowiedzialność w zakresie dostarczania tychże informacji. Ingerowanie w treści znajdujące się w Internecie jest sprawą bardzo delikatną i powinno mieć moim zdaniem zawsze incydentalny charakter.

Na koniec przenieśmy się na chwilę myślami do przyszłości. Czy zdaniem dra e-administracja będzie opierała się wyłącznie na biometrycznych systemach uwierzytelniania znanych z filmów *science fiction*? Przykładowo będzie liczył się odcisk palca, skan siatkówki oka, a nie posiadany dowód osobisty czy złożony podpis na dokumencie.

GIODO: Mam nadzieję, że nie. Mam nadzieję, że biometria będzie jedną z opcji, którą będzie można stosować. Natomiast nie będzie się przymuszało do tego, aby wszystkie dane biometryczne i to wszystkich obywateli były przetwarzane w systemach. Ja, oczywiście, nie chcę się wypowiadać na temat tego, czy skan siatkówki oka może być niebezpieczny ze względu na stan pseudo-nauki, jaką jest irydologia. Tak czy inaczej nie wiemy, jak te dane biometryczne mogą być wykorzystane w przyszłości.

Pamiętajmy, że niektóre z danych biometrycznych, a szczególnie dane genetyczne, w jeden zasadniczy sposób różnią się od jakichkolwiek danych osobowych. Są naprawdę niezmienne. Nawet imię i nazwisko, nr PESEL, nr NIP można zmienić w ekstremalnych sytuacjach w życiu. Natomiast genomu nie zmienimy. W związku z tym, jeżeli raz skompromitujemy genom czy pewne rodzaje informacji biometrycznych, to nigdy więcej nie będziemy mogli ich odtworzyć w sposób neutralny na nowo. Tym samym zalecałbym dużą ostrożność w przypadku biometrii.

Trudno jest też dobrze zdefiniować dane biometryczne. W niektórych przypadkach jesteśmy pewni, że mamy do czynienia z danymi biometrycznymi, a w niektórych nie. Przykładowo kartka z odręcznym pismem zawiera dane biometryczne. Można pismo ocenić grafologicznie. Można też zmierzyć np. nacisk na kartkę. Ale czy skan lub kserokopia takiego dokumentu zawierają w dalszym ciągu dane biometryczne? A w końcu czy to oznacza, że każdy własnoręcznie podpisany dokument zawiera dane biometryczne? Zalecałbym dużą ostrożność. Tam gdzie biometria miałaby służyć do identyfikacji osoby i w szczególności do uwierzytelniania się w systemach należałoby zachować dużą ostrożność i dać możliwość wyboru. Już dzisiaj pojawiają się np. bankomaty biometryczne w Polsce, ale są bardzo rozsądnie wprowadzane. Można pozostać przy zwykłej karcie bankomatowej, a można zrezygnować z karty i posługiwać się danymi biometrycznymi. Do

momentu, w którym nie ma preferencji w stosunku do danych biometrycznych, czyli np. nie dostaje się lepszej oferty, jeżeli stosuje się dane biometryczne, to można mówić, że jest to dobrowolnie wyrażona zgoda osoby.

BM: Dziękuję za rozmowę.

GIODO: Również dziękuję za rozmowę.

PATRONAT MEDIALNY

Z przyjemnością zapraszamy Państwa na wyjątkowe wydarzenie jakim jest debata:

Prywatność w nowych technologiach

20 marca 2013r.
Collegium Iuridicum II
Biblioteka Uniwersytetu Warszawskiego (ul. Lipowa 4)
WSTĘP NIEODPŁATNY

Debata zostanie poprzedzona wykładem wprowadzającym Ministra Wojciecha Wiewiórowskiego (Generalnego Inspektora Ochrony Danych Osobowych)

Formuła wydarzenia zakłada przedstawianie dwóch odmiennych poglądów na dany temat z zakresu ochrony prywatności w obliczu nowych technologii. W roli adwersarzy wystąpią znawcy tematu:

1. Arwid Mednis (Wierzbowski/Eversheds), adwersarz - Katarzyna Szymielewicz (Fundacja Panoptykon) – ochrona przed naruszeniami a prawo do prywatności;
2. Xawery Konarski (Traple, Konarski, Podrecki), adwersarz - Igor Ostrowski (Salans) – prywatność a reklama behawioralna;
3. Tomasz Grzegory (Google), adwersarz - Mariusz Grzesiuk (Onet.pl) – prywatność w usługach świadczonych drogą elektroniczną;
4. Grzegorz Wanio (Olesiński i Wspólnicy), adwersarz - Maciej Kołodziej (naszaklasa.pl) – prywatność w serwisach społecznościowych.

PATRONAT HONOROWY:

Generalny Inspektor Ochrony Danych Osobowych - dr Wojciech Wiewiórowski
Dziekan WPiA UW - prof. dr hab. Krzysztof Rączka
Polska Izba Informatyki i Telekomunikacji

Organizatorem wydarzenia jest fundacja Bezpieczna Cyberprzestrzeń oraz interdyscyplinarne koło naukowe badań nad Internetem i nowoczesnymi technologiami „Cyberlaw". Koordynatorem projektu jest radca prawny Artur Piechocki.

Zasady Czasopisma

Rada Naukowa
Redakcja
Zakres tematyczny i struktura
Zasady publikacji
Wymogi edytorskie
Postanowienia licencyjne

Harmonogram pracy Redakcji

How do we function?

Who is the member of the Scientific Council?
Who is the member of our Editorial Team?
What are we going to write about?
and how will our quarterly look like?
What is important for you as an Author?
How to edit your article?
What are the licence provisions?

Our work schedule