Dny práva – 2009 – Days of Law: the Conference Proceedings, 1. edition.
Brno : Masaryk University, 2009, ISBN 978-80-210-4990-1

PERSONAL DATA PROTECTION AS TOPICAL EU LAW PROBLEM

DANIEL NOVÁK

Department of International and European Law - Faculty of Law – Masaryk University - Czech Republic

Abstract in original language
V minulosti převážně platilo, že právo duševního vlastnictví podporuje ochranu soukromí. Kupříkladu autorské právo chrání soukromí autora a skutečných osob, které jsou rozpoznatelné v literárním příběhu, tím, že zamezuje volné distribuci díla. V současnosti můžeme vidět změny v tomto vztahu. Běžně ochrana soukromí omezuje svobodu projevu. V našich souvislostech je ale určující, že příliš snadný přístup ke komunikačním údajům týkajícím se připojení k internetu, může znamenat ohrožení svobody projevu.

Key words in original language
Ochrana soukromí, ochrana osobních údajů, ochrana duševního vlastnictví, Listina základních práv Evropské unie, Úmluva o ochraně lidských práv a základních svobod, směrnice 2006/24/ES, uchovávání údajů, Malone v. Spojené království, Klass v. Spolková republika Německo, Promusicae, LSG.

Abstract
In the past, it was predominantly true that the intellectual property laws were supporting the protection of privacy. For example, copyright protects the privacy of the author and the actual people who are recognizable in the literary story by preventing the free distribution of works. Nowadays, we can see changes in this relation. Normally, the protection of privacy interferes with the freedom of expression. But in our context, the too easy access to Internet traffic data could mean a threat to the freedom of expression.

Key words
Privacy protection, personal data protection, protection of intellectual property, Charter of Fundamental Rights of the European Union, Convention for the Protection of Human Rights and Fundamental Freedoms, Directive 2006/24/EC, data retention, Malone v United Kingdom, Klass v Federal Republic of Germany, Promusicae, LSG.

1. INTRODUCTION

In the past, it was predominantly true that the intellectual property laws were supporting the protection of privacy. For example, copyright protects the privacy of the author and the actual people who are recognizable in the literary story by preventing the free distribution of works.

Nowadays, we can see changes in this relation.

James Whitman said: "American privacy protections are at their conceptual core, protections against the state, while European privacy protections are, at their conceptual core, protections against the media and the general public."[1]

We do not leave out the efforts of States to intensify control over their citizens which is justified by the fight against the phenomena such as terrorism and organized crime, or unwelcomed media attention to celebrities.

But we have to stress that the most active private players in the field of attempts to gain access to personal data are those associated with the issue of intellectual property rights. These various organizations fight in particular against illegal software copying and distribution or infringement of copyright in musical works (hereinafter referred to as "representatives of right holders").

This is because the electronic data can be easily spread around the world and – even if the unit price of illegally used intellectual property rights can be small – the sum at stake is substantial.

Nowadays, there is a tension between the intellectual property rights and the personal data protection. Owners of the intellectual property go by the Francis Bacon's paraphrased statement: Knowledge is wealth. Personal data protection makes it more difficult.

Organized interests of the owners of intellectual property rights are clearly visible at all levels of decision-making: the sectoral organization WIPO, the WTO, the European Union institutions, even national legislative processes. Every day we see their more or less open presence in the media space.

They also use the court proceedings with the growing vehemence.[2]

---

[1] *Whitman, J. Q. Human dignity in Europe and the United States: the social foundations, p. 121. In: Nolte, G. (ed.) European and US Constitutionalism. Cambridge: Cambridge University Press, 2005.*

[2] *See Virgin Records America, Inc v. Thomas, Available Case Documents. On line http://news.justia.com/cases/featured/minnesota/mndce/0:2006cv01497/82850/*

2. INTELLECTUAL PROPERTY RIGHTS PROTECTION THROUGH CRIMINAL JUSTICE AND DATA RETENTION DIRECTIVE

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 (hereinafter referred to as the "DRD") is one of the most controversial parts of EU law, precisely in view of its attachment to privacy.

This directive wants to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (Art. 1, paragraph 1 DRD).

It shall not apply to the content of electronic communications, including information consulted using an electronic communications network. (Article 1, paragraph 2 DRD).

The DRD is applicable in the field of protection of intellectual property if the (perceived or real) offense has a criminal dimension.

This criticized directive refers to Article 95 of the Treaty establishing the European Community. Ireland submitted that the choice of Article 95 TEC as the legal basis for the Directive is fundamentally flawed.

The Irish government filed its case in the European Court of Justice on 6 July 2006 as C-301/06.

On 2nd February 2009 The European Court of Justice in issued that the DRD: "regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonizes neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive, as is stated, in particular, in recital 25 in the preamble to, and Article 4 of, Directive 2006/24/EC."

The Court summarized that in light of its substantive content, Directive 2006/24/EC relates predominantly to the functioning of the internal market.

In other words, the European Court of Justice gave emphasis on the fact that the addressee of the obligations, market participants, i.e. "service providers", and it put into the background that the data are intended for security forces.

But this is in terms of the standard scheme of regulation rather controversial. For example the obligation of a company to release proof to the court (which is comparable) in criminal proceedings, is ranked in the criminal procedure and not in the company law or the public economic law.

The decision does not consider whether the DRD is in breach of fundamental rights.

As the European Court of Human Rights stated in Malone v United Kingdom, the records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8.[3]

The Lisbon Treaty has acknowledged the Charter of Fundamental Rights and the Convention for the Protection of Human Rights and Fundamental Freedoms as a reference framework.

Sometimes it appears that the Convention No. 108 for the Protection of Individuals with regard to automatic processing of personal data should be applied by the European Court of Human Rights. Rolv Ryssdal, former President of the European Court of Human Rights, advocated that the Court should not ignore the fundamental principles of Convention No. 108. They constitute a sectoral implementation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms in the context of automatic processing of personal data and they can help with the interpretation of those obligations.[4]

Therefore the DRD has to succeed in the test of proportionality, which consists of the criteria of suitability, necessity and importance of the conflicting rights.

The DRD refers to constitutional values (values of primary EU Law), i.e. public order and safety. According to case law on the fundamental freedoms the argumentation by the public order and safety can be applied only if there is a genuine and sufficiently serious threat affecting one of the fundamental interests of society. See, for example, Case of 29 April 2004 Orfanopoulos and Oliveri (C-482/01 and C-493/01, ECR I 5257, paragraph

---

[3] *See Malone v United Kingdom (Application No 8691/79) ((1984) 7 EHRR 14; Series A No 82, paragraph 84).*

[4] *Ryssdal, R. Data Protection and the European Convention on Human Rights, in Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2–4 October 1991 in Strasbourg, Strasbourg: CoE, 1992, p. 42.*

66), to the free movement of persons and of 14 March 2000, Eglise de Scientology (C-54/99, ECR I 1335, paragraph 17), to the free movement of capital.

The DRD is suitable for its purpose since there is no doubt that electronic communications are eligible to be a tool for criminal activities. But this does not mean that it can not be circumvented, and quite easily.

The DRD may be considered necessary if its purpose can be achieved by alternative means of regulation which limit the constitutionally protected values in smaller extent. This legislative solution is sustainable, because data can not be effectively required later without retention.

With regard to the proportionality in the strict sense, it is necessary to state that there were some critical calculations:

„Suppose there will be an obligation to retain all traffic data for 36 (in fact most 24) months, while an evaluation shows that only 2% of these data are being demanded for inquiries in criminal cases. Of that 2%, it turns out, only 10% proves to be really necessary as proof in the case, be it as direct evidence, or as a trace to such evidence. In that case, only 0.2% of all stored data are necessary for law enforcement. In that case, 99.8% of all these data would be stored on behalf of the useful 0.2%. Let us, for the sake of this example, continue to suppose that half of the 2% of data would be requested within the first week, and 9/10 within the first month. In that case during 35 (in fact most 23) months data would be stored on behalf of the 0.02% that would be useful in a criminal court case.“[5]

The statistics held in accordance with article 10 of the DRD could allow a verification of these considerations.

The fact that the proportion of usable data will be near to zero, of course, suggests that the proportionality test is not fulfilled. On the other hand, we can shorten a retention time but other adjustments go against the principle of non-interception of the content of communication (Article 1, paragraph 2 DRD).

The content remains inaccessible only in certain cases. If the requiring authority lawfully found the content of communications, provision incorporated in the article 1 paragraph 2, has not practical implications.

---

[5] *Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention. On line www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html*

But it is already comparable to the wiretapping (and not only the metering).

The DRD does not address the question of how the communication party learns that the data were transmitted to the police. This can not be harmonized on the basis of Article 95 EC.

In connection with the wiretapping, there is a general obligation to provide information (with exceptions for particularly serious situations) based on the case law of the European Court of Human Rights, specifically the judgement of Klass v Federal Republic of Germany, which states: The Court points out that where a State institutes secret surveillance of the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 (art. 8), or even to be deprived of the right granted by that Article (art. 8), without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions.[6]

Some member states have experienced delays in transposition of the DRD (Austria, Greece, Ireland, the Netherlands, Poland and Sweden). In relation to the procedures of the European Commission and the European Court of Justice, there will be the possibility to evaluate this directive from the perspectives of the protection and promotion of European human rights standards.

The European Court of Human Rights is self-restrained to the legal acts of the European Union. His criticism of procedures under the DRD would oblige Member States to choose between the breach of the DRD and the Convention. But it might later lead to a change of the DRD.

The mere availability of data raises other people's (which are unauthorized according to the original intention of the legislature) efforts to gain access to them.

3. CIVIL PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

In the recent past, under the preliminary ruling procedure the European Court of Justice issued two decisions, which interpret the obligation to surrender internet traffic data to representatives of right holders: judgement of 29 January 2008 Promusicae (C-275/06, no. ECR. I p.

---

[6] *Klass v Federal Republic of Germany (Application No 5029/71) ((1979-80) 2 EHRR 214, paragraph 36).*

271) and judgement of 19 February 2009 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH (C-557/07).

In the main proceedings Productores de Música de España (Promusicae), a non-profit-making organization of producers and publishers of musical and audiovisual recordings, requested against Telefónica de España SAU, the disclosure of informations identifying the users who have allegedly violated copyright by "providing access in shared files of personal computers to phonograms in which the members of Promusicae held the exploitation rights". Promusicae wanted to bring civil proceedings against these users.

Telefónica refused to release such data with reference to Article 12 of Law 34/2002 on information society services and electronic commerce which stated: "The data shall be retained for use in the context of a criminal investigation or to safeguard public security and national defense, and shall be made available to the courts or the public prosecutor at their request."

The national court found that in Spain the copyright infringement was a crime only if it was committed for profit.

In accordance with the Advocate General's opinion the European Court of Justice ruled that:

European directives "do not require the Member States to lay down an obligation to communicate personal data in order to Ensure effective protection of copyright in the context of civil proceedings, in a situation in which a non-profit-making organization of producers and publishers of musical and audiovisual recordings has brought proceedings seeking an order that a provider of internet access services to the organization disclose the identities and physical addresses of certain subscribers, so as to enable civil proceedings to be brought for infringement of copyright."

Similarly, as to Articles 41, 42 and 47 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) ... "do not contain provisions which require those directives to be interpreted as compelling the Member States to lay down an obligation to communicate personal data in the context of civil proceedings".

The European Court of Justice emphasized that "However, Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the

other general principles of Community law, such as the principle of proportionality." (see paragraphs 60, 70, operative part)

The European Court of Justice dealt with the legal framework before the transposition of the DRD and it did not comment the Advocate General's opinion which stated that: "It is already doubtful whether that exception (incorporated in the article 6(2) of Directive 2002/58) allows any storage at all of particulars concerning the persons to whom and times when a dynamic IP address was assigned. That information is not normally needed for the purpose of billing the access provider's charges."[7]

States have been allowed a relatively wide margin of appreciation with respect to the formulation of criteria which are relevant for determining when the internet traffic data can be disclosed and the privacy protection will not be infringed. There should be included among others for example: the amount of damages, the profitability of infringement of intellectual property, its organization and length of duration, respectively the degree of probability that the infringement occurred.

As long as the representative of right holders does not identify the alleged offenders, he can not determine the total amount of damage caused by a single offender's repeated violations of intellectual property rights. If dynamic IP addresses are used, the access provider assigns randomly to its customers an address from its quota of addresses every time they access the Internet.

The focus of this examination would remain on the service providers (the telecommunications companies). They are at risk to make a mistake in this fragmented field and suffer the consequences. There is a topic for discussion, whether the national authorities for the protection of personal data should decide on the uncovering of the data.

The order of 19 February 2009 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, (C-557/07) is based on similar factual and legal circumstances.

LSG is a collecting society which "enforces as trustee the rights of recorded music producers in their worldwide recordings and the rights of the recording artists in respect of the exploitation of those recordings in Austria". Tele2 is an Internet access provider which assigns to its clients (dynamic) IP addresses.

---

[7] *Opinion of Advocate General delivered on 18 July 2007. Productores de Música de España (Promusicae) v Telefónica de España SAU. Case C-275/06. On line http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT*

Tele2 refused to disclose the requested informations about its clients.

Tele2 claimed that it is not an intermediary within the meaning of Paragraph 81(1a) of the Austrian Federal Law on Copyright or Article 8(3) of Directive 2001/29, because "as Internet access provider, it indeed enables the user to access the Internet, but it exercises no control, whether de iure or de facto, over the services which the user makes use of". It also stressed that the personal data protection should prevail over the right to information and the copyright.

The European Court of Justice referred in respect of the balancing conflicting rights to the judgement Promusicae.

Furthermore, the European Court of Justice established that "Access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether de iure or de facto, over the services which users make use of, must be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29".

These conclusions do not harm the service providers, since they will not be held responsible for infractions of the rules by its clients.

4. CONCLUSIONS

The requirements of representatives of right holders are partially contradictory. They seek the enforcement of privacy rights in favor of people from the entertainment industry which they represent and who are dependent on publicity. At the same time they want the public to give up the right to privacy for their economic interests.

If there is consensus that intellectual property rights should be protected legally (although they refer to trivial content), procedural mechanisms to enable their enforcement must be created.

If the presumed infringement of intellectual property rights has a specified criminal dimension, the DRD will be applicable. This act is widely criticized. So far it has not been verified for compliance with the standards of human rights laid down in the documents of the Council of Europe and the European Union.

Representatives of right holders are in more difficult situations where the offense is civil and not criminal. In these cases, the law of a Member State can exclude an obligation of the service provider to disclose Internet traffic data for use in court proceedings.

If the law of a Member State authorizes the disclosure of those data, the personal data protection (within the meaning of the Charter of

Fundamental Rights of the European Union and the Convention for the Protection of Human Rights and Fundamental Freedoms) has to be respected.

Representatives of right holders are seeking more effective ways to support their interests. A proposal of the incorporation of the right to cut off users from the Internet without judicial involvement was rejected in France. Later it was promoted into the forthcoming Telecoms Reform Package. This legislative idea was also withdrawn from it.

To some extent the DRD is based on the presumption of guilt too. But here it is important that the procedures referring to the DRD is not out of the full judicial review. The European Court of Justice has left a relatively large space for the theoretical, legislative and judicial considerations regarding the conflict of intellectual property rights and the personal data protection.

Normally, the protection of privacy interferes with the freedom of expression. But in our context, the too easy access to Internet traffic data could mean a threat to the freedom of expression.

Literature:

A Bowrey, K.: Law and Internet Cultures, Cambridge: Cambridge University Press, 2005. 250 pages, ISBN-10: 0521600480.

Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention. On line www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html

Klass v Federal Republic of Germany (Application No 5029/71) ((1979-80) 2 EHRR 214).

Malone v United Kingdom (Application No 8691/79) ((1984) 7 EHRR 14; Series A No 82).

Markesinis, B. S. (ed.): Protecting Privacy, Oxford: Oxford University Press, 1999. 264 pages, ISBN-10: 0198268858.

Mathiesen, T.: On Globalization of Control: Towards an Integrated Surveillance System in Europe, On line http://www.nsfk.org/downloads/seminarreports/researchsem_no43.pdf

McKee, A.: The Public Sphere: An Introduction, Cambridge: Cambridge University Press, 2005. 265 pages, ISBN-10: 0521549906.

Opinion of Advocate General delivered on 18 July 2007. Productores de Música de España (Promusicae) v Telefónica de España SAU. Case C-275/06. On line http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT

Ryssdal, R. Data Protection and the European Convention on Human Rights, in Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2–4 October 1991 in Strasbourg, Strasbourg: CoE, 1992.

Virgin Records America, Inc v. Thomas, Available Case Documents. On line
http://news.justia.com/cases/featured/minnesota/mndce/0:2006cv01497/82850/

Whitman, J. Q. Human dignity in Europe and the United States: the social foundations, In: Nolte, G. (ed.) European and US Constitutionalism. Cambridge: Cambridge University Press, 2005. 312 pages, ISBN-10: 0521854016.

Contact – email

52154@mail.muni.cz