CONSTITUTIONAL ASPECTS OF TOPICAL RISKS TO PERSONAL DATA PROTECTION

by

DANIEL NOVÁK

Introduction [1]

The last decades are in the sign of the growth of the interest in problems of the privacy protection, especially in connection with the development of the modern information and communication technologies. This interest rises from the academic discourse community and gradually, it spread into politics and acquired the form of the law. These debates started in the 1960s in the USA.[1]

Nowadays, the privacy protection is subordinated under the term "autonomy". The privacy refers to an individual's right to conduct his affairs without being compelled to reveal information he doesn't want to reveal. Even thought we accept the dictum of the indivisibility of human rights, it is necessary to state that privacy and personal data protection doesn't fall within the untouchable rights that invoke absolute obligations of states.[2] The justification for the limitation of the right which is related to the protection of the personal integrity has to be based on especially relevant reasons and requirements.

Recently, there is an enormous amount of effort devoted to the increase of police and security services´ "not sufficient" powers. This political pressure is invoked in the name of national and international security. Nevertheless, there are as well positive economic incentives against the personal data protection.

[1] Westin, A.F. (1970): Privacy and Freedom. New York, Atheneum. Miller, A. (1971): The Assault on Privacy: Computers, Data Banks and Dossiers. Ann Arbor, University of Michigan Press.

[2] Sudre, F. (1997): Mezinárodní a evropské právo lidských práv. Brno, MU Brno-EIS UK, p. 133

The Security Realm [2]

"Essential Liberty" and "Temporary Safety" [2.1]

The personal data protection invokes suspicions, because it points to the anonymity which facilitates many forms of crime. We have to incorporate the Philippics of James Otis against writs of assistance – despite he considered himself a loyal British citizen – in the context of the development preceding the American War of Independence. A Benjamin Franklin's famous quote, "Those who would give up Essential Liberty, to purchase a little Temporary Safety, deserve neither Liberty nor Safety", can be opposed (but not invalidated) from the perspective of the growing availability of modern destructive technologies. The phenomenon known as "group polarization" is catalyzed by the cyber technology developments.[3] We can find the logics in that argumentation, but almost every human right violation is legitimized by lofty ideals. Nevertheless, this argumentation often falls on fertile ground amongst certain parts of the electorate.

In the European Union, these tendencies are represented by the creation of the databases oriented on the information exploitable for security purposes and the enlargement of the existing databases to include biometric data. A sui generis problem involves the blanket retention of communications data.

The Biometric Data Processing [2.2]

Nowadays, in the EU, there is the Schengen Information System which works by holding a number of specific alerts on people, vehicles and property. The SIS (existing from 1995) is a secure governmental database system used for the purpose of maintaining and distributing information related to border security and law enforcement. The SIS is composed of a central database called "the Central Schengen Information System" (CS-SIS), access points defined by each Member State (NI-SIS) and a communication infrastructure. The effective execution of the control of 15 million items in the SIS is made more difficult by the fact that there is a high number of the mentioned access points.[4]

[3] Einstein, C. (2002): "The Law of Group Polarization". The Journal of Political Philosophy. No. 2, pp. 175-195

[4] Second generation Schengen Information System (SIS II). Retrieved November 14, 2006, from http://www.europarl.europa.eu/eplive/expert/shotlist_pa ge/20061023SHL12011/default_en.htm.

Complementary information can be exchanged via the Sirene bureaux. Sirene is the French acronym for "Computer System for the Register of Enterprises and their Local Units." Sirene is viewed as a threat to the rights of the individual. Sirene is not de jure part of the Schengen convention, but was established by the Schengen Executive Committee and for example Pikna rates Sirene to be the third component of the SIS and he infers that this system was established on the basis of Article 108 of the Convention Implementing the Schengen Agreement.[5]

The Schengen Information System II (SIS II) is at the stage of preparation. The start of the SIS II is scheduled for March 2007 but the last course of events indicates that this deadline won't be kept. This system includes innovations dangerous to the personal data protection. New SIS II will store photos and biometric data (e.g. digital portraits and fingerprints) among all members and will answer police queries within 5 seconds.

Council regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention plays an important role in the asylum politics. A central unit of the Eurodac is managed by the European Commission. Visa Information System will store the biometric data too.

The Europol Convention states that Europol shall establish and maintain a computerised system to allow the input, access and analysis of data. The Europol Computer System (TECS) has three principal components: an information system (EIS - Europol Information System), an analysis system (AWF - Analytical Work Files), and an index system (IIS - Interim Information System).

The information system may be used to store, modify and utilise only such data as are necessary for the performance of Europol's tasks. The data concern persons who, under the national law of a Member State, are suspected of having committed or having taken part in a criminal offence for which Europol is competent or who have been convicted of such an offence. The system also contains data concerning persons where there are serious grounds under national law for believing will commit criminal

[5] Pikna, B. (2003): Evropská unie - vnitřní a vnější bezpečnost a ochrana základních práv. Praha, Linde, pp. 251-252

offences for which Europol is competent. Europol collects, stores and manipulates data in analytical work files for the purposes of developing intelligence to guide law enforcement investigations.

It this matter, we stand on opinion that the weakness of the personal data protection is the width of the administrative discretion limited by formulations as, for example "the data necessary for the performance of Europol's tasks", "the protection of security and public order" or "protection of the rights of individuals". Such wide discretion is questionable without the sufficient and effective justice control.

The Blanket Retention of Communications Data [2.3]

Directive 2006/24/EC of the European Parliament and 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 entered into force on 3rd May 2006.

Member States shall ensure that the specified data (data necessary to trace and identify the source, destination, date, time and duration, and type of a communication, data necessary to identify users´ communication equipment or what purports to be their equipment and the location of mobile communication equipment) are retained for periods of not less than six months and not more than two years from the date of the communication.

Pursuant to Article 15(3) of the Directive, the Czech Republic hereby declared that it was postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

Although, no data revealing the content of the communication may be retained pursuant to this Directive. There is an open question, whether the stored data represents an integral and indivisible part of the communication which merits the protection of article 8(1) of the European Convention on Human Rights. Critics of the directive could refer to the judgement of the European Court of Human Rights of 2 August 1984 in the case of Malone against the United Kingdom.[6]

[6] Malone v. the United Kingdom – 8691/79 [1984] ECHR 10 (2 August 1984).

Further objections could be raised in connection with the proportionality test. We presume that only 0,2 percent of this data will be demanded by the police. About 90 percent of the data will be requested during the first month after the creation of an information.[7] The remaining 99,98 percent of the data would be stored useless and with the risk of the misuse during a 5-23 months period.

We can argue in the defence of this suspicious approach that the consequences of the realization of the corresponding criminal and terrorist threats are extreme too.

This criticized directive refers to Article 95 of the Treaty establishing the European Community. Ireland submits that the choice of Article 95 TEC as the legal basis for the Directive is fundamentally flawed. The Irish government has filed its case in the European Court of Justice on 6 July 2006 (Case C-301/06).

Since 5 March 2003 airline companies operating in Europe found themselves caught in a dilemma where on the one hand they are obliged to observe the EU legislation on data protection (principally Directive 95/46/EC) while on the other hand US legislation obliges them to allow the US Customs and Border Protection to have unrestricted access to the personal data of passengers travelling to or via the USA.

The European Parliament brought on 27 July 2004 the actions against the Council of the European Union (Case C-317/04) and the Commission of the European Communities (Case C-318/04). The European Parliament claimed that the Court should annul Council Decision 2004/496/EC of 17 May 2004 annul under Article 230 EC Commission Decision 2004/535/EC of 14 May 2004. The European Parliament emphasized the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith.

In case C-318/04 the Court agreed that the decision was adopted ultra vires. The Commission's decision did not fall within the scope of the Directive. In case C-317/04 the Court agreed that Article 95 EC could not be used as legal basis for adopting the Decision. Therefore, the Court could not

[7] Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention. Retrieved November 14, 2006, from http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html.

clarified the human rights aspects of these criticized acts. In the theory of international and European law, the EU Law which was enacted ultra vires would not be binding in Member states. The ECJ judgment is not necessary. We think such a scenario is not realistic in the practice.

The Economic Realm [3]

The Crucial argument for the liberalisation as well as for the regulation is the impact on the economic situation of data subjects. In a fully deregulated system, the holders of genetic information will assess who will pay lower mortgage rates, lower credit card rates, lower college loan rates, lower car payment rates and who will lose access to the health insurance.

The European conception of the personal data protection which is derived from the personal integrity associates the idea of intransmittable human rights. However, intransmissibility doesn't correspond with practical requirements of economic activities. Although the opinions of Advocates General of the European Court of Justice are enthralled by the radicalism, herein an other point of view is preferred. In concrete terms, Antonio Tizzano handed down an opinion arguing the absence of the connection with the Single Market.[8]

In the USA, critics of informational privacy laws often raise the First Amendment argument. Their argument is that the guarantee of free speech in the First Amendment is an explicit constitutional right and is a superior right to an implicit constitutional right to privacy, and any legislative information privacy rights granted to individuals.[9]

The Personal data protection doesn't come out victoriously in the conflicts with the protection of the property in the Czech legal literature.[10]

We can admit that the reasons for the harmonization of the personal data privacy laws was notably pragmatic. Germany was reluctant to accept any measure reducing the high level of protection afforded its citizens in the Single market. This connection with the economic system and the commerce

[8] Opinion of Advocate General Tizzano in case C-101/01 Bodil Lindqvist v Åklagarkammaren Jönköping and in case C-465/00 Rechnungshof v. Österreichischer Rundfunk.

[9] Charlesworth, A. (2000): Clash of the Data Titans? US and EU Data Privacy Regulation. European Public Law. No. 2, p. 261

[10] Bejček, J. (2003): Muže být účelem zákona samoúčel? Právní rozhledy. No. 11, p. 539

gives reasons for the subordination of personal data protection to the property protection regime. Likewise the domain names.

The reinterpretation of terms with the impacts on the human rights is not exceptional. For example in the Czech law, there was a redefinition of the concept of the things realised by the Act No. 370/2000.[11]

This reinterpretation could increase the vigilance of data subjects to the consideration (quid pro quo).

We stand on opinion that this conception is compatible with administrative interferences in the personal data protection.

The abundance of relatively uncertain terms reduces the effectiveness of the regulation. This problem can be demonstrated by the category of the sensitive personal data. In the Czech Republic, the security camera monitoring is conditional on the notice in the monitored room.[12] For sensitive data, the explicit consent of data subjects must be obtained. Is the face of an individual, revealing ethnic identity, to be treated as sensitive data? The same question applies to other biometric data. Voice recordings, iris scanning or even fingerprints may reveal race or health status. We can object that the purpose of the data processing is different. But the substantial identity of the information could not be disguised in spite of a different context. The complexity of the problem increases in virtue of the combination and the typification of the personal data. The foreseeability of the law was not reinforced by the judgment of the European Court of Justice in case Kühne & Heitz (C-453/00), and in particular by the judgment in case Kapferer (C-234/04), which is not unequivocal and requires careful interpretation.[13]

Conclusion [4]

Each free society has to protect, by force, the rights of some individuals to oppose that force. It is the paradox of a free society. Our technological progress is on the verge of giving ordinary citizens the destructive means

[11] Pelikánová, I. (2001): Problém převodu a přechodu práv, Právní rozhledy. No. 4, p. 143

[12] Stanovisko ÚOOÚ č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Retrieved November 14, 2006, from http://www.uoou.cz/stanovisko_2006_1.pdf .

[13] C-453/00 Judgement of 13/01/2004, Kühne & Heitz (Rec. 2004, p. I-837), C-234/04 Judgement of 16/03/2006, Kapferer (Rec. 2006, p. I-2585).

comparable with weapons of mass destruction held by Great Powers in the Nuclear Age. These tendencies (multiplied by the cyber technologies) can legitimize a radical extension of powers to police and security services.

Nevertheless, that objections aren't able to refute the necessity of the effective personal data protection.

Numerous references to the proportionality principle in the personal data protection law are related to the necessity of the stabilization of the regulation and its independence from technological evolutions. There is no possibility for the successful standardization of concrete situations. This conception takes its inspiration from the constitutional law. Differences between the argumentation by principles in constitutional law and the so-called "simple" law have its importance. Our contemporary practice doesn't provide an empirical basis for the conclusion about differences. In according with the Forsthoff's thesis they will be in quantitative (not qualitative) terms.

References

[1] BEJČEK, J. (2003): *Muže být účelem zákona samoúčel?* Právní rozhledy. No. 11, pp. 533 - 542. *Bezpečnostní opatření při cestě do Spojených států.* Retrieved 14 November, 2006, from www.uoou.cz/index.php?l=cz&m=left&mid=09:01:10.

[2] DWORKIN, R. (2001): *Když se práva berou vážně.* Praha, Oikoymenh.

[3] C-453/00 Judgement of 13/01/2004, *Kühne & Heitz* (Rec. 2004, p. I-837).

[4] C-234/04 Judgement of 16/03/2006, *Kapferer* (Rec. 2006, p. I-2585).

[5] CHARLESWORTH, A. (2000): *Clash of the Data Titans? US and EU Data Privacy Regulation.* European Public Law. No. 2, pp. 253 - 274.

[6 *Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention.* Retrieved 14 November, 2006, from http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html.

[7] *JAP: anonymita a soukromí na Internetu.* Retrieved 14 November, 2006, from http://www.eff.org/legal/cases/RIAA_v_Verizon/

[8] *Malone v. the United Kingdom* – 8691/79 [1984] ECHR 10 (2 August 1984).

[9] MILLER, A. (1971): *The Assault on Privacy: Computers, Data Banks and Dossiers.* Ann Arbor, University of Michigan Press.

[10] PELIKÁNOVÁ, I. (2001): *Problém převodu a přechodu práv*. Právní rozhledy, No. 4, pp. 141-151.

[11] PIKNA, B. (2003): *Evropská unie - vnitřní a vnější bezpečnost a ochrana základních práv.* Praha, Linde.

[12] *RIAA v. Verizon Case Archive.* Retrieved 14 November, 2006, from http://www.eff.org/legal/cases/RIAA_v_Verizon/.

[13] *Second generation Schengen Information System (SIS II).* Retrieved 14 November, 2006, from http://www.europarl.europa.eu/eplive/expert/shotlist_page/20061023SHL12011/default_en.htm.

[14] *Schengen Information System II*. Retrieved 14 November, 2006, from http://europa.eu/scadplus/leg/en/lvb/l33183.htm.

[15] *Stanovisko ÚOOÚ č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů.* Retrieved 14 November, 2006, from http://www.uoou.cz/stanovisko_2006_1.pdf.

[16] *Opinion of Advocate General Tizzano in case C-101/01 Bodil Lindqvist v. Åklagarkammaren Jönköping.*

[17] *Opinion of Advocate General Tizzano in case C-465/00 Rechnungshof v. Österreichischer Rundfunk.*

[18] SUDRE, F. (1997): *Mezinárodní a evropské právo lidských práv.* Brno, MU Brno-EIS UK.

[19] SUNSTEIN, C. (2002): *"The Law of Group Polarization"*. The Journal of Political Philosophy. No. 2, pp. 175-195.

[20] *USA and Europol join forces in fighting terrorism!* Retrieved 14 November, 2006, from http://www.europol.europa.eu/index.asp?page=news&news=pr011211.htm.

[21] *USA and Europol sign a full co-operation agreement.* Retrieved 14 November, 2006, from http://www.europol.eu.int/index.asp?page=news&news=pr021220.htm.

[22] WESTIN, A. F. (1970): *Privacy and Freedom.* New York, Atheneum.