Tilburg University

Private law solutions in European data protection

Purtova, N.N.

Published in:
Netherlands Quarterly of Human Rights

Publication date:
2010

Document Version
Peer reviewed version

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
Purtova, N. N. (2010). Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights. *Netherlands Quarterly of Human Rights*, 28(2), 179-198.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

PRIVATE LAW SOLUTIONS IN EUROPEAN DATA PROTECTION: RELATIONSHIP TO PRIVACY, AND WAIVER OF DATA PROTECTION RIGHTS

NADEZHDA PURTOVA *

Key words

Affirmative state obligations
Convention for the Protection of Human Rights and Fundamental Freedoms
Data protection
Horizontal effect
Negative rights
Positive state obligations
Privacy
Property rights in personal data
Waiver of fundamental rights

Abstract

This paper considers a possibility of a private law approach to data protection. The main thesis of the contribution is that the European legal order allows only a limited scope of contractual and property rights with regard to personal data, restricted by the consideration to preserve human rights. The piece first proves that in the system of the ECHR data protection interests are treated under the umbrella of Art. 8 right to privacy. As a result, the author concludes that Art. 8 right to privacy does not imply a right to waive data protection but provides a legitimate ground to restrict freedom of contract in that area.

1. INTRODUCTION

This paper focuses on the possibility of private law solutions of the data protection problem in Europe and on the issue of waiver of data protection rights as a foundation of such a possibility.¹ The interest in the issue of waiver is well-timed given the recent *I. v. Finland* decision² of the European Court of Human Rights.

* Doctoral candidate at TILT (Tilburg Institute for Law, Technology, and Society), Tilburg University, The Netherlands www.uvt.nl/tilt; the author can be contacted via e-mail n.purtova@uvt.nl.

¹ Art. 8 of the Charter of Fundamental Rights of the EU defines the right to protection of personal data as follows:

“Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.”

² ECHR 17 July 2008, *I. v. Finland*, application no. 20511/03.

This decision strikes to the core of the pro-waiver arguments, i.e. it prevents further attempts to withdraw data protection from the legal protection of Art. 8 ECHR right to privacy.³

The possibility to waive data protection guarantees on market conditions in exchange for money, goods, or services is a corner-stone of many proposals that reconsider the current European approach to data protection.⁴ Some of these proposals seek to substitute or complement existing data protection mechanisms by private law tools like contractual and property instruments.⁵ Some contend that data protection interests are not to be considered as part of a fundamental human right to privacy: privacy is portrayed as a purely defensive mechanism against intervention into some secluded personal sphere. Privacy protection mechanisms, according to those claims, are unable to take care of personal data protection which requires more 'offensive' approach – not prohibiting but channelling processing of personal information. For that reason, they argue, data protection considerations are not powerful enough to serve as a ground for legitimate restrictions of freedom of contract. The latter, when balanced against data protection interests, has precedence, and data protection rules can be contracted around freely.⁶ This paper argues to the contrary, namely, that the human rights issues cannot be avoided in the data protection debate. Although the language of the European Convention on Human Rights is silent on the matter, the recent case-law confirms that Art. 8 right to privacy fulfils the function of channelling government information practices as well as in the private sector by imposing positive obligations to create and enforce an effective system of data protection. Therefore, when considering the possibility to waive data protection, one should also take its human rights dimension into account. For that reason, although the text of the Convention is not explicit on the matter, this paper concludes that private law solutions with regard to data protection are possible in the European legal order but only within the scope limited by human rights.

The argument will be structured as follows. Part 2 will focus on the European model of the relationship between data protection and privacy. Section 2.1 will briefly outline the debate and provide a roadmap for further analysis of the data protection – privacy relationship, making a distinction between a theoretical discourse and actual legal practice. It will be clarified that the instant analysis refers to the legal rules and their application rather than philosophical definitions. The subsequent sections will review the relevant European law (section 2.2) and Art. 8

³ In that judgement the Court not only imposed on a state party to the Convention a positive obligation to create and enforce an effective system of data protection, but also found the state liable for data protection violations by private parties. The latter confirmed a wide scope of the protected privacy rights and prepared a ground to include the entire body of data protection rules into privacy interests protected by Art. 8 ECHR.

⁴ For recent evaluation and proposals of improvement of the 1995 Data protection directive see, e.g. Neil Robinson, H. G., Maarten Botterman, Lorenzo Valeri (2009). Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office. Santa Monica, RAND.

⁵ For the arguments in favor and against private law approach to personal data see, *inter alia*, Cuijpers, C. (2007). "A private law approach to privacy; mandatory law obliged? ." SCRIPT-ed 4(4): 304-318.; Blok, P. (2002). Recht op Privacy, Boom.; Prins, J. E. J. (2006). "When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?" SCRIPT-ed 3(4): 270.; Rouvroy, A., Pouillet, Yves (2009). The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. Reinventing Data Protection? S. Gutwirth, et al. Berlin, Springer: 45-77. etc.

⁶ Blok. and Cuijpers.

ECHR case-law and show that the scope of the right to privacy goes beyond protection of secret personal information and also regulates the use of collected data (2.3). Also, Art. 8 ECHR jurisprudence imposes positive obligations on the governments to create and enforce an effective system of data protection and has effect on the data practices of the private parties (2.4). Therefore, it is argued that data protection is an integral part of the legal right to privacy as protected by the Convention. As such, it cannot be contracted around (or waived) freely, and the scope of permitted contractual or property rights is limited by the existing ‘floor’ of data protection rules, e.g. the 1995 Data protection directive (Part 3).

2. EUROPEAN MODEL OF THE RELATIONSHIP BETWEEN PRIVACY AND DATA PROTECTION

2.1. THEORETICAL DEBATE AND LEGAL PRACTICE

Despite a vast amount of attention that has been devoted to the problem of data protection since 1960s, there is still no agreement on the relationship between data protection and privacy. As the introduction has already stated, this paper argues that in the European legal order there is conclusive evidence in favour of treating data protection interests as an integral part of a more general right to privacy. Therefore, data protection interests ought to enjoy the full scope of a fundamental right status. However, there have been arguments made in favour of distinguishing the two.

For a better understanding of the debate, the reader should be aware that the discussion on a relationship between privacy and data protection has been taking place in two forums: (1) *theoretical* and (2) the forum of *legal practice* (or legal rules in practice). Surely, a purely theoretical debate is a search for the ‘ultimately true’ definition of privacy and data protection, privacy as a sort of an ideal type which is useful as a reference point in a discourse but not necessarily close to an actual meaning of real-life legal norms. Privacy in the current *theoretical* debate means everything and nothing. It encompasses the whole range of interests – roughly – of personal autonomy, democratic participation, bodily integrity, family life, sanctity of the home, etc. Arguably, bringing data protection in further obscures ‘the meaning’ of privacy. Indeed, there are many opinions on the privacy – data protection relationship. The theoretical standpoints on the matter are either in favour of treating data protection as consumed by or largely intersecting with privacy, or, alternatively, treat the two categories as absolutely distinct. The approaches rest on different ways of conceptualizing privacy. Seeing data protection as a part of privacy is consistent with understanding privacy as secrecy, or a right against disclosure of concealed information, or a right to limit access to the self, or control of information pertaining to oneself. Among those, Daniel Solove submits that the meaning of the words ought to be understood from how they are actually used.⁷ Hence the relationship between privacy and data protection is better understood in terms of “family resemblance” rather than some core characteristics shared by each.⁸

It seems so far that the theoretical debate on the meaning of privacy and its relation to data protection is unlikely to end soon. Therefore, this article focuses on the actual legal rules in practice. In this respect, two points of view are of special

⁷Solove, D. J. (2002). "Conceptualizing Privacy." *Cal. L. Rev.* **90**: 1087. 1126.

⁸*Ibid.* 1126.

interest here: one developed by Paul De Hert and Serge Gutwirth,⁹ and another offered by Peter Blok and supported by Colette Cuijpers. Both concern the scope of protection of Art. 8 ECHR and argue that it does not include data protection.

Peter Blok submits that the core element of the breach of Art. 8 right to privacy is an intrusion into one's private sphere. In the framework of information privacy, only secret personal information is protected by privacy rules.

*The individual right to privacy both safeguards an undisturbed private life and offers the individual control over intrusions into his private sphere. Given this definition, the boundaries of the private sphere are central to the meaning of privacy. The right to privacy guarantees individual freedom within the home, within the intimate sphere of family life, and within confidential communication channels. In combination with physical integrity, these 'privacies' form the core of the legally protected private sphere.*¹⁰

Colette Cuijpers agrees and continues that "as the protection of the individual with regard to the processing of personal data is in no way restricted to data concerning the private sphere of the individual, [...] the choice to link data protection to the right to privacy is unjustly made."¹¹ Put differently, not all aspects of data protection are covered by the scope of privacy protection. As a result, in the part which is left out, data protection does not enjoy the status of a fundamental right. One of the consequences is that data protection considerations are not powerful enough to serve as grounds for legitimate restrictions of freedom of contract; hence, the latter, when balanced against data protection interests, has precedence. In other words, in a contract one is free not to abide by data protection requirements.¹²

The general feeling one gets after reading Blok's argument is that the Art. 8 ECHR jurisprudence should not have gone so far to extend the right to privacy beyond the text of the Convention and thus diminishing the importance of the right that was originally meant to be protected. That is in essence a normative statement pointing at the way the jurisprudence *should* have gone. De Hert and Gutwirth's approach is more structural and aims at making sense of conceptual disorder ruling privacy – data protection debate. It is based on the understanding that privacy and data protection are tools too different in nature to be treated together. This account of the relationship between privacy and data protection is offered by Paul De Hert and Serge Gutwirth.¹³ They consider the two categories against a background of a democratic constitutional state, as two distinct tools to control state power.¹⁴ They come to the conclusion that privacy limits state power by creating a sphere of individual autonomy and self-determination free from state intervention.¹⁵ Privacy labelled as an opacity tool is therefore a negative right which empowers an individual to prevent the state from intervening in his affairs, but not to require the

⁹ De Hert, P., Gutwirth, Serge (2003). "Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies." Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview.

¹⁰ Blok. 323.

¹¹ Cuijpers.

¹² Ibid. 312-315.

¹³ De Hert.

¹⁴ Ibid. 134.

¹⁵ Ibid. 134.

state to take any positive steps.¹⁶ Data protection, on the other side, is a transparency tool. It does not prohibit the state intervention, but rather channels and controls it by giving an individual positive rights and imposing on the state affirmative obligations.¹⁷ The distinction between the two should not blur.¹⁸

Despite a more normative character of Blok's argument and more conceptual nature of De Hert and Gutwirth's, they may be reduced to one core: protection of the private sphere, whatever that means, from intervention is an opacity tool, and the right to privacy is a negative right. Data protection is a transparency tool implying positive obligations and therefore cannot be taken care of by the means of privacy protection.

The following analysis will use the 'opacity-transparency tools' dichotomy as a road-map of analysis and will show that, whatever the arguments of Blok, Cuijpers, De Hert and Gutwirth are, when it comes to actual application of law, the European Court of Human Rights in Strasbourg does not limit the scope of Art. 8 ECHR to private sphere only, and the provision on privacy protection has been applied as giving individuals positive rights and imposing on the states affirmative obligations. Consequently, in legal practice there is no ground to treat data protection distinctly from privacy rights.

2.2. RELEVANT LAW

To start with, let us determine the range of the relevant legal norms. The European legal context of privacy and data protection is composed of the EC data protection regime and relevant law of the Council of Europe. The EC regime comprises four directives, one regulation, and Art. 7 and 8 of the EU Charter.¹⁹ The EU Charter, although an influential document, has not yet entered into force, Regulation (EC) 45/2001 binds only the EC institutions, and the directives on privacy and electronic communications, retention of data, and privacy in telecommunication are pieces of sectoral legislation and conform to the general principles of the Directive 95/46/EC. The latter is the key Community law instrument of personal data protection.²⁰ Besides, Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is of relevance since the institutions of the European Union declared their adherent to the

¹⁶ Ibid. 138.

¹⁷ Ibid. 144.

¹⁸ Ibid. 146.

¹⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);

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;

Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector;

EU Charter of Fundamental Rights of 7 December 2000.

²⁰ With important reservations as to the scope of the application of the Directive under Art. 3.

protection of the fundamental rights.²¹ In determining the scope of protection of the fundamental rights the European Court of Justice (ECJ) ruled itself bound by the ECHR and the jurisprudence of the Strasbourg Court.²²

The EU law concerning data protection leaves some doubt as to whether data protection is a part of the right to privacy or not. Art. 1 (1) of the 1995 Directive suggests that data protection is a building block of privacy since the objective of the data protection is “to protect the fundamental rights and freedoms..., and in particular ... right to privacy.” To be sure, the EU Charter of Fundamental Rights does distinguish a right for respect for private and family life (Art.7) and a right to data protection (Art.8). However, so it does to equality between men and women (Art. 23) and a right to non-discrimination (Art. 21), whereas the European Convention deals with those two in a single provision - Art. 14 (“Prohibition of discrimination”). The analogy allows a simple speculation that it is merely a chosen technique of the Charter to deal with special instances of more general rights separately in order to ensure their more adequate protection by customized norms. In any case, separation of a right for respect for private and family life (Art.7) and a right to data protection (Art.8) in the Charter does not exclude interpretation of data protection as a part of a general right to privacy.

To resolve the confusion let us turn to Art. 8 ECHR for guidance. As the first step of the analysis one should acknowledge that the protection of personal data provided by Art. 8 ECHR is not as complete as, for instance, protection offered in the 1995 EC Directive. Art. 8 ECHR alone is not sufficient to face challenges of protection of individuals in the information society. For instance, the study of the Committee of Ministers performed in 1968 showed that ECHR offered insufficient protection to individual privacy as well as other rights and interests of individuals with regard to automated data banks.²³ The major shortcomings of Art. 8 ECHR were that 1) the ECHR including Art. 8 does not directly apply to the private sector; 2) the right to a private life would not necessarily include all personal data but only those regarded private; 3) Art. 8 ECHR did not directly provide for a right of access to personal data.²⁴ To address those shortcomings, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was adopted in 1981.²⁵ De Hert and Gutwirth conclude that “the ECHR had a defensive approach to privacy and more positive action was necessary.”²⁶

When combined with De Hert and Gutwirth’s approach to the functions of privacy and data protection in a democratic constitutional state, one could argue that data protection may be viewed outside of the scope of Art. 8 ECHR. There are two

²¹ e.g. paragraphs 1 and 2 of Article 6 (ex Article F) of the consolidated text of the Treaty on European Union.

²² Initially in the *Nold* case (ECJ 14 May 1974, *J. Nold Kohlen- und Baustoffgroßhandlung v. Commission*, case 4/73 [1974] ECR 491, paragraphs 13 and 14) .

²³ Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

²⁴ De Hert. 119; for an updated position of De Hert and Gutwirth on the role of ECHR in data protection see De Hert, P., Gutwirth, Serge (2009). *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action. Reinventing Data Protection?* S. Gutwirth, et al. Berlin, Springer: 3-45. In comparison to their 2003 article, in this piece De Hert and Gutwirth also observe that the European Court rapidly brings data protection into the scope of the right to privacy.

²⁵ The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in 1981.

²⁶ De Hert "Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies." 119.

possible reasons supporting this claim. The first relates to the substance of protection, namely, Art. 8 ECHR protects only privacy as secrecy, i.e. concerns only concealed personal information, and prevents collection but not other information practices. The latter sees to the mode of protection; that is, Art. 8 ECHR does not apply to private parties and does not contain affirmative obligations. The following sections argue against both these reasonings.

2.3. ART. 8 ECHR: BEYOND PRIVACY AS SECRECY OF INFORMATION

In 1950s, when the Convention was adopted, or in 1968 when its applicability to data protection was evaluated, respect for private and family life as enshrined in Art. 8 ECHR might have contained only a negative right protecting an individual's private sphere from state intervention. However, at present an alternative interpretation of the article is well possible. This extensive application of the Convention is based on the understanding of its dynamic nature and on the assumption that "the Contracting Parties signed in full knowledge that ideas and morals [behind the Convention's interpretation]²⁷ would change and that the meaning of the Convention would keep pace."²⁸

Several pieces of evidence support the conclusion that the protection of Art. 8 ECHR goes beyond concealed personal information. The core of this interpretation is similar to the approach taken in the German human rights jurisprudence. In particular, De Schutter argues that Art. 8 case-law – similar to the interpretation of Art. 2 (1) of the German Basic Law – may expand to protect a broader right to free development of personality.²⁹ In German constitutional law, this is that right which is a legal basis for the right to information self-determination – the German equivalent of data protection, empowering an individual to control the disclosure and use of his/her personal data.³⁰ The ECHR jurisprudence already recognizes that the right to respect for "private life" does not end on protecting secluded information, but comprises also, "to a certain degree, the right to establish and develop relationships with other human beings especially in the emotional field, for the development and fulfilment of one's own personality."³¹ Literature supports this broad interpretation. In 1994 Beddard wrote that although the European Convention "does not talk of the right of personality, ... particularly within Articles 8 to 11 are found the rights which go towards the fulfilment of personal hopes, aspirations, and ideals."³² Since the mid-1990s the ECHR case-law has been following the idea of privacy as encompassing more than just secrecy but also personality rights. For instance, in 2009 in the case of *Reklos and Davouris v. Greece*³³ the Court affirmed:

²⁷ Text in square brackets is added.

²⁸ Beddard, R. (1994). *Human Rights and Europe*, Cambridge University Press. 96.

²⁹ De Schutter, O. (2000). "Waiver of Rights and State Paternalism under the European Convention on Human Rights." *N. Ir. Legal Q.* 51: 487. at 498

³⁰ 1983 census decision: BVerfGE 65, 1: "This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data."

³¹ Commission Report *X. v. Iceland* (Application No. 6825/74) of 18 May 1976 in Decisions and Reports, Vol 5 at p 87; Donna Gomien, D. H., Leo Zwaak (1996). *Law and practice of the European Convention on Human Rights and the European Social Charter*. Strasbourg, Council of Europe Publishing. 231; *Oosterwijck v. Belgium*, Comm. Report 1.3.79, para. 51 p. 36.

³² Beddard. 95.

³³ ECHR, 15 April 2009, *Reklos and Davourlis v. Greece*, Application no. 1234/05

... [A]ccording to its case-law “private life” is a broad concept not susceptible to exhaustive definition. The notion encompasses the right to identity (see *Wisse v. France*, no. 71611/01, § 24, 20 December 2005) and the right to personal development, whether in terms of personality (see *Christine Goodwin v. the United Kingdom [GC]*, no. 28957/95, § 90, ECHR 2002-VI) or of personal autonomy, which is an important principle underlying the interpretation of the Article 8 guarantees (see *Evans v. the United Kingdom [GC]*, no. 6339/05, § 71, ECHR 2007-..., and *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III)³⁴

Another factor in favour of this extended interpretation of Art. 8 ECHR is that the jurisprudence of the European Court of Human Rights not only limits the collection of information, but to some degree also regulates its use. For instance, in the *Leander* case³⁵ the applicant was dismissed from employment as a museum technician at a naval museum on the basis of the results of security evaluation qualifying him as a security risk. The Court found that not only storing and release of such information constituted infringement on the protected right to privacy, but also a refusal to allow Mr. Leander an opportunity to refute it.³⁶

2.4. AFFIRMATIVE OBLIGATIONS AND POSSIBILITY OF HORIZONTAL EFFECT OF ART. 8 ECHR

Another evidence against qualification of Art. 8 ECHR right to privacy as an exclusively negative right that merely prevents collection by the state of concealed personal information is that its protection also implies affirmative, or positive, obligations of a state with regard to personal data. Moreover, by means of the ‘affirmative obligations’ reasoning the effect of the Convention may also be extended to the violations by the private parties (*i.e.* horizontal effect of Art. 8 ECHR).

One may observe development of the ECHR case-law on affirmative state obligations in general, and with regard to privacy in particular, leading to recognition of the state positive obligations. In the early years of this process, when applying Art. 8 (1) ECHR, the Convention organs interpreted the right in conjunction with Art. 8 (2) ECHR, which reads “there shall be no interference by a public authority with the exercise of this right.” Indeed, the doctrine of state non-intervention used to be dominant in understanding the substance of the right to privacy under Art. 8 (1) of the European Convention,³⁷ and is consistent with the literal meaning of para. 2 of Art. 8 and classical conception of fundamental rights as negative. However, subsequent application of the Convention was clearly based on the understanding that an entirely negative approach to state responsibility is “inadequate to secure the effective exercise of the individual’s freedoms.”³⁸ This is a principle of *effective* protection that the Convention grants - as opposed to

³⁴ *Reklos*, para. 39

³⁵ ECHR, 26 March 1987, *Leander v. Sweden*, Application no. 9248/81

³⁶ *Leander*, para.48 (albeit, it should be mentioned that the infringement was found justified and did not constitute a violation).

³⁷ Gomien, D., Harris, David, Zwaak, Leo (1996). Law and Practice of the European convention on human rights. Strasbourg, Council of Europe Publishing. 231.

³⁸ David Harris, M. O. B., Edward Bates and Carla Buckley (1995). Harris, O’Boyle & Warbrick: Law of the European Convention on Human Rights, Butterworths Tolley. 1995), p. 284.

theoretical enjoyment of rights - first set out in *Golder v. UK*³⁹ and *Airey v. Ireland*.⁴⁰

Based on the principle of effective enjoyment of rights, Art. 8 ECHR jurisprudence has further evolved to show signs of recognition that the positive obligations of the state under the Convention are possible. ECHR case-law has acknowledged 1) the obligation of the state to take steps to make sure that the enjoyment of the right is effective (*Gaskin v. UK*⁴¹); 2) the obligation to ensure that the right is not interfered with in the sphere of the relations of individuals between themselves, *i.e.* respected by private persons (e.g. in *Young, James, and Webster v. UK*⁴² paras 55-56 (1981)); and, 3) the obligation of the state not only to keep private individuals from violating Art. 8 protected right but to do so in a way reflecting the ECHR standards (e.g. *X v. UK*).⁴³ The latter line of case-law in the data protection context may be interpreted as calling for creation by the states-signatories of comprehensive data protection systems which adhere to the ECHR principles and, as a result, bind private parties with the ECHR rules.

Let us revisit the three lines of cases in their order of appearance. *Gaskin v. UK* is an example of the affirmative obligation of the first type, *i.e.* of a state to ensure effective enjoyment of fundamental rights. The case involved accumulated records of Mr Gaskin's childhood in care. The authorities refused to disclose the records to protect confidentiality of contributors of the information. Commission found that respect for private life "requires that everyone should be able to establish details of their identity as individual human beings," and the Court decided that the failure of the state to develop procedures whereby the files could be available to the applicant constituted a violation of a positive obligation of the state under Article 8.

In *Klass*⁴⁴ the Court found a positive obligation of the state to protect personal data from being abused. The applicants challenged the 1968 legislation authorizing surveillance, in certain circumstances, without the need for informing the person concerned. The court found such a procedure contrary to Art. 8 ECHR. And although, in view of the threat posed to democracy nowadays by highly sophisticated forms of espionage and by terrorism the interference was found necessary in a democratic society, the Court made sure to note that adequate and effective guarantees against abuse must exist:

49. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. [...]

Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.

³⁹ ECHR 21 February 1975, *Golder v. UK* Application No. 4451/70.

⁴⁰ ECHR 09 October 1979, *Airey v. Ireland*, Application No. 6289/73.

⁴¹ ECHR 07 July 1979, *Gaskin v. UK*, Application No. 10454/83.

⁴² ECHR 13 August 1981, *Young, James, and Webster v. UK* Application No. 7601/76 ; 7806/77.

⁴³ ECHR 05 November 1981, *X v. UK*, Application No. 4515/75, cited in Gomien. 284.

⁴⁴ ECHR 06 September 1978, *Klass and Others v. Germany*, Application No. 5029/71.

50. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.

The last two lines of the case-law on the affirmative obligations are of special interest here since they bring data processing in private sector into the scope of Art. 8 ECHR. The decisions in the second line of case-law have been interpreted to support a claim that a state is obliged to make sure that private persons do not violate privacy as protected by Art. 8 ECHR. One of the first example cases is *X and Y v. the Netherlands*.⁴⁵ A mentally handicapped girl and her father complained that it was impossible for either of them to start criminal proceedings against a man who had sexually assaulted her. The Court found the girl's right to privacy under Article 8 being violated and agreed that the state had a positive obligation to ensure that all individuals have effective means to *vindicate* their right to privacy, in this case, violated by a private person.

*"The Court recalls that although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the Airey judgment of 9 October 1979, Series A no. 32, p. 17, para. 32) These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves."*⁴⁶

The cases like *X and Y v. the Netherlands* have revolutionized the ECHR privacy jurisprudence. However, the cases of the third type – *inter alia*, *I. v. Finland*⁴⁷ of 17 July 2008 – were a real death stroke to the idea of purely negative nature of Art. 8 ECHR right to privacy and absence of affirmative state obligations under the Convention in general. The *X and Y v. the Netherlands* decision has already been labelled as "landmark," and highlighting "the importance of security measures in the protection of personal data in a manner that ought not to leave any uncertainties at least for the governmental actors."⁴⁸

The applicant, a Finnish citizen, worked as a nurse in an eye clinic in the period between 1989 and 1994. During her employment, being diagnosed HIV-positive, she was regularly visiting another clinic of the same hospital. In 1992 she became suspicious of her colleagues knowing of her condition and that someone in the hospital unlawfully had access to her medical file in a hospital database. The managing system of the database allowed free access to the patients files to all hospital staff. After her complaint, the system was changed. She has also received a new patient record under a false name. When the term of her employment expired, the applicant requested an administrative body in the field of social and healthcare services to investigate who had access to her file. Due to technical limitations of the managing system of the database it turned out to be impossible. The system only kept record of the last five log-ins, and contained no reference to the names of

⁴⁵ ECHR 26 March 1985, *X. and Y. v. The Netherlands*, Application no. 8978/80.

⁴⁶ Ibid. para. 23

⁴⁷ ECHR 17 July 2008, *I v. Finland*, Application no. 20511/03.

⁴⁸ Răman, J. (2008). "European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – *I v. Finland*, no. 20511/03, 17 July 2008." *Computer Law & Security Report* 24: 5 6 2 – 5 6 4. 562.

individuals, but only their departments. After the file was returned to the archive all access record was cleared. The system was altered after the state body drew the attention of the hospital to that fact. The applicant initiated civil proceedings against the hospital and claimed damages. The claim was not satisfied since the national court did not find conclusive evidence of unauthorized access to I's medical file. On exhaustion on national measures, I filed a complaint to the European Court of Human Rights.

The applicant claimed breach of Art. 8 ECHR on the ground that the district health authority "had failed in its duties to establish a register from which her confidential patient information could not be disclosed"⁴⁹ and that "the measures taken by the domestic authorities to safeguard her right to respect for her private life had not been sufficient."⁵⁰ The premise of the claim was that Art. 8 ECHR not only protects privacy from state intervention, but also imposes on the state certain positive duties to prevent such intervention by others. The Government contended that there was no violation within the meaning of Article 8 at the time there was national legislation in place which "guaranteed the secrecy of a person's health information and, in principle, all patient information was kept secret. Only those participating in the patient's treatment were entitled to process data concerning him or her. [...] A hospital's system for recording and retrieving patient information could only be based on detailed instructions and their observance, the high moral standards of the personnel, and a statutory secrecy obligation."⁵¹

The Court disagreed with the Government's objection and supported the applicant's claim:

Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see Airey v. Ireland, judgment of 9 October 1979, Series A no. 32, p. 17, § 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (see X and Y v. the Netherlands, judgment of 26 March 1985, Series A no. 91, p. 11, § 23; Odièvre v. France [GC], no. 42326/98, ECHR 2003-III).⁵²

Thus, a cumulative reading of the aforementioned cases in general and of the decision in *I. v. Finland* in particular leaves no doubt that the right to privacy as protected by Art. 8 ECHR also implies positive state obligations, and therefore incorporates data protection interests.

Besides its vast significance for acknowledgement of the doctrine of the positive state obligations in Art. 8 jurisprudence, *I. v. Finland* has opened another door to reading data protection into Art. 8 ECHR right to privacy a little bit wider. Via the positive obligations reasoning it made one more step towards creating horizontal effect of Art. 8 ECHR protection, *i.e.* towards making its provisions relevant for private sector.

I. v. Finland first affirmed the existing second line of the case-law with regard to positive obligations:

⁴⁹ *I. v. Finland*, Para. 26.

⁵⁰ *I. v. Finland*, Para. 29.

⁵¹ *I. v. Finland*, Paras. 31, 34.

⁵² *I. v. Finland*, para. 36.

*In addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life ... These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.*⁵³

But after citing existing case-law, the Court went further:

*[T]he mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place.*⁵⁴

In other words, although in time of the violation there was a national law in place making unauthorized access to medical files unlawful, and the violation of that law in fact led to violation of Art. 8, the mere existence of general data protection rules is insufficient to fulfil the positive state duty. The state is also obliged to create an effective system of data security make sure that other (also private) actors do not violate privacy protected by Art. 8 ECHR. Thereby, first, *I. v. Finland* judgement may be interpreted to call if not for more detailed state regulation of data processing, surely for its better enforcement. However, most importantly, it may be considered as a call for the application by state parties of the ECHR principles of privacy protection (including data protection) applicable to the state actors, to the private sector. Such an effect provisionally may be called horizontal effect. As a result of the *I. v. Finland* judgement, states signatories to the Convention may be found liable for failing to ensure that private parties take positive steps to prevent privacy violations by other private parties. Therefore the decision at hand lays ground for transfer of the ECHR privacy principles into the national systems of data protection preventing such violations.

The case of *K.U. v. Finland*⁵⁵ is another example of the ECHR influence on the content of the state positive obligations under Art. 8, hence also on the content of the data protection rules and private parties' obligations. In the 2008 *K.U. v. Finland*, the ECHR court seems to have made explicit use of the possibility opened in *I. v. Finland*. Namely, not only did it clarify the content of the state positive obligations to protect privacy in general by criminalizing interference with children's privacy. It also, *albeit* through the back door of an interest counterbalancing vindication of privacy, gave guidelines the parties to the Convention as to the content of their data protection obligations regarding anonymity on the Internet.

K.U. was a boy of 12 years old when the events in question occurred. In 1999 an unknown person without the applicant's knowledge placed an ad on the dating web-site containing the applicant's personal details. The advertisement claimed that the applicant was seeking an intimate relationship with a boy of his age or older "to show him the way."⁵⁶ The boy found out about the ad after receiving an e-mail from a man inviting to meet. The applicant's father requested the police to identify who the man was. However, the service provider refused to disclose the IP address of the offender due to a statutory obligation of confidentiality. The police failed to secure a court warrant to obligate the provider to disclose the needed

⁵³ Ibid., para. 36.

⁵⁴ Para. 47.

⁵⁵ ECHR 2 December 2008, *K.U. v. Finland*, Application no. 2872/02

⁵⁶ *K.U. v. Finland*, para. 7

information, since malicious misrepresentation – as the offence in question was qualified in the national law – was not among the offences giving ground for exceptions from the confidentiality duty. The man who answered the ad was identified based on his e-mail address and criminally charged. However, the managing director of the service provider could not be criminally charged since his alleged offence became time-barred (seeking civil redress was still possible). The director allegedly was guilty of a violation of the provision of the national Personal Data Act requiring a service provider verify identity of the sender publishing a defamatory announcement. At the time, processing and publishing sensitive personal data concerning sexual behaviour on an Internet server without the subject's consent was a criminal offence.⁵⁷ The applicant claimed that failure of the state to impose criminal liability for the violation of privacy was in breach of Art. 8 ECHR. Namely, the Government failed to ensure the consistency of the provisions of the national law requiring consent of the data subject for processing of data referring to his sexual behaviour and making it a criminal offence not to verify the sender of such data on the one hand, but not including malicious misrepresentation into the list of exceptions to the duty of confidentiality on the other hand. As a result, the balance between anonymity of the Internet users and privacy was erroneously struck in favour of the offenders.⁵⁸

The Court reaffirmed the existence of state positive obligations under Art. 8,⁵⁹ and that “these obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves.”⁶⁰ The Court continued that, although the choice of means to fulfil positive obligations is in principle within the state's margin of appreciation, state's discretion is limited by the Convention's provisions.⁶¹ However, the Court analysis proceeded that although the states have a margin of appreciation in how exactly they exercise those positive obligations, the states' discretion is limited by the Convention. Namely, the Convention as a human rights instrument and for the sake of “effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, [requires] efficient criminal-law provisions,”⁶² reinforced “through effective investigation and prosecution.”⁶³ Especially welfare of children and other vulnerable individuals necessitates criminal law protection.⁶⁴

The Court acknowledged that the state positive obligations must not impose “an impossible or disproportionate burden on the authorities,”⁶⁵ and other counterbalancing interests should be taken into account, i.e. guarantees of Art. 8 and 10 ECHR.⁶⁶ Indeed, in the case at hand effective criminal prosecution of the breach of child's privacy was in conflict with the interest of confidentiality of the Internet users. However, such an interest cannot be absolute and is outweighed by the interest of effective criminal prosecution.⁶⁷

⁵⁷ *K.U. v. Finland*, paras. 7-19

⁵⁸ *K.U. v. Finland*, paras. 36-39

⁵⁹ *K.U. v. Finland*, para. 43 (“These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.”)

⁶⁰ *Ibid.*

⁶¹ *Ibid.* para. 44

⁶² *Ibid.* para. 46

⁶³ *Ibid.*, para. 46

⁶⁴ *Ibid.*, para. 46

⁶⁵ *Ibid.*, para. 48

⁶⁶ *Ibid.*, para. 48

⁶⁷ *Ibid.*, para. 49

The Court concluded that although it is the task for the national legislator to create a regulatory framework reconciling those competing claims, it had to be done in a different way. Namely, failure of the state to provide for consistent rules of criminal investigation and duties of confidentiality favouring anonymity of the Internet users rather than child welfare hindered criminal prosecution of one of the offenders.⁶⁸ Therefore, Finland was found in violation of Art. 8 right to respect for private life.

In *K.U. v. Finland* the Strasbourg Court not simply reaffirmed existence of state positive obligations under Art. 8 ECHR, but did it in a way that essentially amounts to giving the Convention state parties guidelines as to the content of data protection rights and obligations of private parties, in the case at hand – as to the user anonymity on the Internet.

Of course, there is only that much one could expect from an international treaty like the ECHR directly binding only state parties, in regulating private behaviour and holding private parties accountable. Indeed, under the standing law one cannot say that the ECHR imposes obligations on the private parties.

However, the case-law of the ECHR certainly suggests that Art. 8 of the Convention not only prevents the state itself from bad information practices, but also implies creation by the state of a system of rules governing information practices both of the state *and* private parties (i.e., system of data protection). The states signatories are found in violation of the Convention not for the violations by the private parties but for the failure to channel those private parties' behaviour. This system implies creation of the private parties' – also positive – obligations, which, have to be of a certain quality consistent with the Convention, i.e. adequate enough and properly reconciling Art. 8 interests with conflicting claims. The position of this paper is that this way Art. 8 of the ECHR provides for data protection, at least in as much as, and after *I. v. Finland*, and *K.U. v. Finland*, possibly a bit more than, an international treaty can go.

3. WAIVER OF THE RIGHT TO DATA PROTECTION: LIMITED SCOPE OF PRIVATE LAW SOLUTIONS WITH REGARD TO DATA PROTECTION

As already mentioned, the proposals to reconsider current data protection mechanism in Europe and substitute or complement it with private law tools – contract and property – have received considerable attention in the European data protection literature.⁶⁹ The corner-stone of such proposals is the possibility for an individual to trade data pertaining to him/her for money or services, or waive his/her data protection rights on market conditions. The position of this paper is that waiver of (and, hence, unlimited private law approach to) data protection is only possible if deprived of the protection of a fundamental right to privacy. This paper, however, has shown, that privacy as protected by Art. 8 ECHR is a much wider right, which extends beyond a negative interest in protecting secret information, to a positive right of personal development (and possibly even information self-determination) and affirmative obligations of a state to secure data protection interests effectively.

⁶⁸ Ibid., para. 49

⁶⁹ For the arguments in favor and against private law approach to personal data see, *inter alia* Blok, Cuijpers.; Rouvroy. etc.

This section challenges the claim made by some authors that since data protection is not a fundamental right, freedom of contract has precedence over the rules of the 1995 Data Protection Directive and the right to data protection may be waived or contracted around.⁷⁰ It has already been argued earlier in this paper that there is no sufficient ground to divorce the legal right to data protection from Art. 8 ECHR privacy. The next step in reasoning is to show that the Convention does not contain a right, in fulfilment of freedom of contract, to waive data protection interests for remuneration.

To start with, it has to be acknowledged that, although not mentioned in the text of the Convention, the phenomenon of waiver of rights is known to the system of the ECHR. In fact, there are two lines of jurisprudence on this matter. First, Art. 6 ECHR (right to fair trial) case-law confirms that, in their defence, Contracting States may rely on the waiver by applicants of their rights guaranteed by the Convention, provided the waiver was well-informed, unequivocal, and given freely, and not contradicting to public interest.⁷¹ However, whether individuals may seek Convention's protection when a State interferes in market transaction involving the waiver of a protected right is an entirely different matter, and, it is argued here, should be answered negatively. The latter issue is addressed by the Court in the second line of its case-law on the application of Art. 1 of the First Protocol to the Convention.⁷² This is this line of case-law the following passage will focus on.

The first step in the argument is that the Convention in general does not guarantee freedom of contract or any other economic freedom, except property.⁷³ What is more, contrary to some authors, De Schutter asserts that the right to peaceful enjoyment of possessions protected by Art. 1 Protocol 1 does not implicitly guarantee freedom of contract.⁷⁴ De Schutter bases his conclusion on *Mellacher* judgement.⁷⁵ As to the facts of the case, the Mellachers and others filed a complaint against Austria. The applicants all were owners of apartments which they rented out. In 1981 the state of Austria introduced a law limiting maximum rent of apartments based on their quality. As a result, the amount of rent the applicants received was dramatically reduced. The Mellachers and others claimed that the state intervention amounted to deprivation of their possessions or at least a violation of the right to receive payment of the agreed rent in violation of Art. 1 Protocol 1. The Court disagreed:

⁷⁰ Cuijpers.

⁷¹ For more detailed analysis of the ECHR case-law on waiver see De Schutter. referring, *inter alia*, to *Bulut v. Austria*, Application No. 17358/90, Judgement of 22 February 1996, para. 30, *Deewer v. Belgium*, Judgement of 27 February 1980 published in Ser. A, Vol. 35, p. 56, etc.

⁷² Article 1 of the Protocol – Protection of property – reads as follows:

“Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.”

⁷³ Wegener, B. (2007). Economic Fundamental Rights. European Fundamental Rights and Freedoms. D. Ehlers. Berlin, De Gruyter Recht: 130-151. 148.

⁷⁴ De Schutter. 505.

⁷⁵ ECHR 19 December 1989, *Mellacher and Others v. Austria*, Application No. 10522/83 ; 11011/84 ; 11070/84.

The Court finds that the measures taken did not amount either to a formal or to a de facto expropriation. There was no transfer of the applicants' property nor were they deprived of their right to use, let or sell it. The contested measures which, admittedly, deprived them of part of their income from the property amounted in the circumstances merely to a control of the use of property.

*The fact that the original rents were agreed upon and corresponded to the then prevailing market conditions does not mean that the legislature could not reasonably decide as a matter of policy that they were unacceptable from the point of view of social justice.*⁷⁶

De Schutter correctly interprets the Mellacher decision as meaning that "the protection afforded by the Convention to the property [...] does not extend to the right to exchange that property against some other advantage, under the conditions reigning in the market."⁷⁷ Same, he claims, holds for other rights and freedoms guaranteed by the Convention, also for Art. 8 right to privacy:

*[T]he right one has to freedom of expression or to respect for private life does not extend to the right to obtain, under the mechanisms of the market, a remuneration for the sacrifice of that right, or even for agreeing to that right being limited in some less complete way.*⁷⁸

To sum up, both case-law and doctrine suggest that the ECHR does not protect an individual's right to obtain remuneration for forgoing his/her fundamental right. That means that, although a state respondent in its defence may rely on the fact that an applicant waived a right in question, an individual him/herself cannot claim that his/her right was violated when the state prevents him, e.g. via regulation, from waiving a fundamental right.⁷⁹

An important remark has to be made here. This paper *does not* argue that contractual arrangements concerning personal data or propertization of personal data are altogether impossible under the Convention. However, this paper *does* argue that the consequence of classification of data protection as a fundamental right protected under Art. 8 ECHR limits the scope of the allowed contractual arrangements and possible property rights. To understand this point better one has to think of the content of the right discussed here. Data protection does not mean non-disclosure and total secrecy of personal information. As Gutwirth and De Hert explained in the piece mentioned earlier, data protection is not a defensive but transparency tool. It does not prohibit state (or other) collection of information, but rather channels and controls it by giving an individual positive rights and imposing on the state affirmative obligations.⁸⁰ Only one example of such a tool of channelling information practices in the 1995 Data Protection Directive is a requirement of consent of a data subject. The ban on waiver of data protection rights means not a ban of voluntary exchange of personal information for money, goods, or services, but prohibition of giving away for remuneration of, among others, the right to consent. Therefore, commercial exchange of personal data is not, in principle, outlawed. However, treating data protection as anything less than a

⁷⁶ *Mellacher*, paras. 44, 56.

⁷⁷ De Schutter. 506.

⁷⁸ *Ibid.* 506.

⁷⁹ *Ibid.* 506.

⁸⁰ De Hert "Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies." 144.

fundamental right under Art. 8 ECHR will lift restrictions following from the fundamental right status and allow full waiver thus opening the door for a dramatic change in approach to data protection. It is a totally different question whether personal data protection will become better in any way if a market approach to personal data protection (by contract or propertization of personal information) is adopted.

4. CONCLUSION

This paper seeks to define how the *legal* categories of privacy and data protection correlate in the European legal system, and what the effects such a correlation has on the mode of data protection. Since the norms of the EC data protection law did not provide a conclusive answer, this paper turned to the ECHR for guidance. As a roadmap of analysis this paper picked the dichotomy between privacy and data protection based on the negative rights and positive obligations explained by De Hert and Gutwirth. The analysis of Art. 8 ECHR case-law led to the conclusion that the European Court of Human Rights does not limit the application of Art. 8 ECHR to private sphere only, and the provision on privacy protection has been applied as giving individuals positive rights (for instance, to refute false information about oneself) and imposing on the states affirmative obligations to create and ensure functioning of an effective system of data protection. The conclusion has been reached that European legal order treats data protection as a privacy interest.

Besides, it has been shown that legal recognition of such a close relationship is much more than just a matter of conviction on the philosophical meaning of privacy. Data protection benefits significantly from enjoying protection of a fundamental right status. Removal of data protection from the scope of privacy rights is not necessary and not desirable. First, development of the ECHR case-law expands privacy protection beyond negative right against state intervention to include affirmative obligations of a state to create a data protection system. Second, treating data protection as anything less than a fundamental right under Art. 8 ECHR will allow its waiver and thereby open the door for a dramatic change in approach to data protection.

REFERENCES

Case-law

ECHR:

Leander v. Sweden, Application no. 9248/81, Judgement of 26 March 1987

Oosterwijck v. Belgium, Commission Report of 1 March 1979

X. v. Iceland, Application No. 6825/74, Commission Report of 18 May 1976

Golder v. UK Application No. 4451/70, Judgement of 21 February 1975

Airey v. Ireland, Application No. 6289/73, Judgement of 09 October 1979

Gaskin v. UK, Application No. 10454/83, Judgement of 07 July 1979

Young, James, and Webster v. UK Application No. 7601/76 ; 7806/77, Judgement of 13 August 1981

X v. UK, Application No. 4515/75, Judgement of 05 November 1981

Klass and Others v. Germany, Application No. 5029/71, Judgement of 06 September 1978

I v. Finland, Application no. 20511/03, Judgement of 17 July 2008

Bulut v. Austria, Application No. 17358/90, Judgement of 22 February 1996

Deewer v. Belgium, Judgement of 27 February 1980 published in Ser. A, Vol. 35, p. 56

Mellacher and Others v. Austria, Application No. 10522/83 ; 11011/84 ; 11070/84, Judgement of 19/12/1989

ECJ

Judgement of the European Court of Justice *J. Nold Kohlen- und Baustoffgroßhandlung v. Commission*, case 4/73 [1974] ECR 491

Germany

BVerfGe 65 (the 1983 census decision)

Books and Articles

Beddard, R. (1994). Human Rights and Europe, Cambridge University Press.

Blok, P. (2002). Recht op Privacy, Boom.

Cuijpers, C. (2007). "A private law approach to privacy; mandatory law obliged? ." SCRIPT-ed 4(4): 304-318.

David Harris, M. O. B., Edward Bates and Carla Buckley (1995). Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights, Butterworths Tolley.

De Hert, P., Gutwirth, Serge (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalization in Action. Reinventing Data Protection? S. Gutwirth, et al. Berlin, Springer: 3-45.

De Hert, P., Gutwirth, Serge (2003). "Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies." Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview.

De Schutter, O. (2000). "Waiver of Rights and State Paternalism under the European Convention on Human Rights." N. Ir. Legal Q. 51: 487.

Donna Gomien, D. H., Leo Zwaak (1996). Law and practice of the European Convention on Human Rights and the European Social Charter. Strasbourg, Council of Europe Publishing.

Gomien, D., Harris, David, Zwaak, Leo (1996). Law and Practice of the European convention on human rights. Strasbourg, Council of Europe Publishing.

Neil Robinson, H. G., Maarten Botterman, Lorenzo Valeri (2009). Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office. Santa Monica, RAND.

Prins, J. E. J. (2006). "When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?" SCRIPT-ed 3(4): 270.

Răman, J. (2008). "European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008." Computer Law & Security Report 24: 5 6 2 – 5 6 4.

Rouvroy, A., Pouillet, Yves (2009). The Right to Information Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for

Democracy. Reinventing Data Protection? S. Gutwirth, et al. Berlin, Springer: 45-77.

Solove, D. J. (2002). "Conceptualizing Privacy." Cal. L. Rev. **90**: 1087.

Wegener, B. (2007). Economic Fundamental Rights. European Fundamental Rights and Freedoms. D. Ehlers. Berlin, De Gruyter Recht: 130-151.