Conference Essays

Radim Polcák

Some Notes on Current Paradoxes in the Law on Personal Data Protection*

1. Introductory note

Teleology is the core of any legal regulatory instrument. As legal language has limits, we often need to use a purposive interpretation to focus the mind of the lawmaker in respect of the meanings of particular black-letter law terms. Unlike as in Czech law and in some other legal systems, EU law uses recitals to clarify the intention of the lawmaker and so the recital to Directive No. 95/46/EC plays the key role in the interpretation of EU and national data protective regulations.

It is not the writer's intention to analyse the particular provisions of the Directive and confront them with its aims. Rather, the intention is to offer a brief summary of recent experience with the development and application of data protection laws with reference to their most basic and most general teleology. The reason is to emphasise the emerging need for questions, even very basic ones, to be asked frequently – in fact, whenever we speak about this area of legal regulation, its methods and instruments.

In many cases, we are simply used to analyse and process the existing legal norms without feeling a need to question their legitimacy or, in other words, the reason for their existence. As noted by one of Europe's leading legal philosophers, Gustav Radbruch, the law is destined to serve three main purposes, i.e. certainty (safety), fairness (whatever that might mean!) and welfare[1]. Another highly influential legal theoretician, Lawrence Lessig, keeps the task even more simple (and more metaphorical), when he speaks about the need for the legal regulation to "do good."

In the last part of his book "Free Culture", Lessig argues that[2]: 'The law should regulate in certain areas of culture - but it should regulate culture only where that regulation does good. Yet lawyers rarely test their power, or the power they promote, against this simple pragmatic question: "Will it do good?" When challenged about the expanding reach of the law, the lawyer answers, "Why not?"

We should, rather, ask, "Why?" Show me why your regulation of culture is needed; show me how it does good – and, until you can show me both, keep your lawyers away.'

In both cases, Radbruch and Lessig argued that we need to ask whether the particular law makes sense or not, and so the writer decided to attempt to confront the recent regulatory personal data protection framework with the very basic question: does it serve the purpose of certainty/fairness/welfare, or, in Lessig's words, does it do good?

Firstly, we shall define what we mean by 'doing good' in terms of personal data. The answer to is to be found in articles 1 and 2 of the recital to the Directive. They read as follows:

'(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

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

We can, in fact, extract from the recital the main aims of the Directive, which are:

1) to create a safer environment for individuals,
2) to protect individual rights and freedoms,
3) to remove barriers to the further integration of Europe, and
4) to enable economic progress.

The main part of the essay attempts to address some of the recent tensions between these aims and the praxis of the data protection concept, and the author thought it rational to show these as regulatory paradoxes.

Paradox 1: safety and fear

National government Acts adopting totally new patterns of protection, as required by the Directive, came into force in many European countries almost literarily overnight. In this way the introduction of personal data protection (PDP) legislation was widely promoted by various public and private institutions in order to ensure that the majority of people would be sufficiently informed of their new rights relating to their personal data.

There is no doubt that, from the legal standpoint, the new protective legislation gave individuals more means of protecting their privacy and discretion (their freedom to

The author is the head of the Workgroup for Law and ICT at the Faculty of Law, Masaryk University, Brno, Czech Republic. His main areas of interest are the theory of cyberlaw, law of e-commerce, public sector information, domain names and e-justice.

act). What should, however, be evaluated is whether, in fact, the beneficiaries of the new regulations both are and feel safer - rather than the changes in their legal position.
Despite the fact that no up-to-date, official public surveys are available, it is not difficult to guess that what resulted from adopting this legislation and from its promotion was less a sense of safety and rather one of anxiety. The chain of logic used by the man in the street to interpret these new measures is likely to be:
1) there is new legislation protecting my personal data;
2) the value and relevance of my personal data must have grown;
3) the reason for protection is obviously a higher risk of the abuse of my data;
4) I need to look after and protect my personal data more carefully.
In this way, adopting the new protective legislation had an effect very different from the creation of a safer environment for European citizens. As many authors observe, the protective legislation developed the concept of individual rights to personal data similar to the concept of property[3]. It is, therefore, obvious that the new form of (value) ownership implies new psychological needs for self-protection, observance and, consequently, a fear of what will happen 'if I am not vigilant enough'.
In the case of many services of the information society, the providers had to start asking their users for permission to collect and use their personal data. This obligation, once again, did not create public trust, but rather raised suspicion and doubt over what negative effects might affect the individual in question if permission were given.
As a result, we can draw the partial conclusion that there was, in fact, no basic change to the value of personal data with the introduction of the new protective legislation, the solitary change appearing in the form of legal (administrative) protection. Notwithstanding this, the reaction of the public was, logically, one of fear and even hysteria.

Paradox 2: subjective values and objective regulation

The limits of privacy and discretion are objectively identifiable, but "ad hoc" always depends on individual circumstances. More than a hundred years ago, in one of the most influential publications on the protection of privacy, Samuel Warren and Louis Brandeis named privacy simply as the 'right to be left alone[4]'. This, more or less metaphorical, expression was later amended by numerous concepts always emphasising both the legal and ethical dimensions of privacy[5].
In any case, determining the particular boundaries of privacy and, consequently, the limits to causes of actions depend always on the extent to which it is reasonable or desirable to 'leave' the particular individual 'alone', and so it differs greatly whether we speak about the privacy of a university professor, a politician or a porn-star.
The privacy protection measures which are incorporated mostly to the central codes of civil laws fully reflect the above features of the construction of privacy and essentially rely on the social position of the individual in question. It is then necessary to prove that the particular infringement is real, i.e. that the conduct violates the private sphere of the particular person.
If we focus on personal data, there is no doubt that they form one of the key elements of the concept of privacy.[6] However, unlike the privacy concept in itself and its other elements such as secrecy, intimacy, etc., the recent administrative protection of personal data is strictly objective. In other words, protection in no way depends on whose personal data are being used or abused. Paradoxically, there is even no need for the existence of real harm to someone's privacy in order to establish a reason for administrative action against a subject dealing with personal data.
Moreover, when there is real harm or an infringement of someone's privacy caused by an abuse of personal data, defence is possible using the existing concepts of tort or civil delict. Whenever such an abuse emerges, it is also possible to receive active state protection under the penal law. Consequently, we can conclude that the objective administrative protection of personal data can be regarded either as redundant or 'overprotective', i.e. going beyond the protection of privacy.
In the first case, we might ask whether it is really necessary to invest public money into new administrative measures which can already be altered by existing legal instruments. In the latter case, we can question the reasons for protecting personal data when privacy is neither infringed nor threatened.

Paradox 3: integration and diversity

The regulatory model used for protecting personal data is based on directives and their adoption into national law. This model should ensure the development of generally applicable standards whilst allowing individual states sufficient opportunity to fine-tune the particular regulatory provisions in accordance with local social norms, custom and usage etc.
In the case of objective administrative regulations, their key element is the axiom, the basic principle, and their actual meaning. The law is, of course, not to be understood as a simple axiomatic deductive system.[7] However, certainty based on the clear and accepted meaning of the words of the law is crucial in the area of administrative regulations.
In respect of the law on data protection, the key principles are obviously 'personal data' and the 'processing of personal data.' In order to prevent differing interpretations, the EU decided to define the meaning of the basic term 'personal data' in Article 2(a) of the Directive. Despite the fact that the definition is contained in the directive and in national law, there arise numerous practical questions over what is, in fact, considered as "personal data". We understand that, currently, over the whole of Europe, there are diverse interpretations as to whether it is possible, for example, to describe as personal data:
- internal personal identification numbers used in organisations such as companies,
- IP addresses single-user computers,
- personal opinions concerning individuals ('I think she must weigh at least 80 kg!')
- personal cell-phone numbers,
- unverifiable identification data entered anonymously (such as those required for various free internet services)
- data of deceased persons[8]

Besides differing interpretations of the key term 'personal data,' there are substantial differences among national laws in their further attempts to distinguish amongst various categories of personal data with their specific forms of treatment. Whilst some laws do not distinguish among categories of personal data[9] and some make a simple distinction between "personal" and "sensitive personal" data[10], on occasion we can find distinctions among multiple categories such as 'personal data', 'sensitive personal data,' 'private personal data[11]' or even 'judicial data[12],' 'special data' or 'criminal personal data[13]'.
To summarise this paradox, we can state that the differences in interpretation and even in basic legislative measures give data protection in Europe important country-specific features. It then varies from one country to another whether certain data are considered as personal data and what is the legal framework for their protection. Moreover, the administrative procedures concerning registration, fees, information rights, etc. also differ, and the overall effect is to force businesses to develop country-specific policies and citizens to be aware of different standards.

Paradox 4: competitiveness and constraints

Various businesses have no other option but to handle numerous types of personal data in

their everyday business. Regardless of whether we speak of the data of employees, partners or consumers, the data have to be regularly collected, processed and communicated in huge quantities in order to keep the business running. Whenever new administrative constraints or additional legal requirements appear, this means additional costs for the business (at best) or disruption (at worst). We should also make brief mention of certain situations which meant, and still do mean, significant problems for any commercial activity:

- Uncertainty,
- Unreasonable strictness,
- Unclear outsourcing requirements and
- Unclear processing requirements.

As the legislation itself, and, consequently, the government departments administering personal data protection are all newly established, the first constraint for companies was visible initial total uncertainty. In most of the practical examples of gathering and processing personal data in business, the answers to the simplest of questions were not to be found in the legislation, and so the company had to predict the way in which the regulations would be applied and wait either for official advice or for themselves or others to be penalised. This effect was multiplied where companies operated in more than one European country.

The definition of "personal data" is relatively broad, the protection measures enacted are strict and administrative procedures are complicated. Consequently, data protection becomes a dangerous weapon which can cause harm even intentionally to a company. Using the example of the Czech Republic, most of the investigations carried out by the Office for the Protection of Personal Data are undertaken on the office's own initiative, but on the basis of information frequently made by:

- Habitual complainers,
- Business competitors or
- Disaffected ex-employees

Almost immediately following the adoption of national data protection legislation, problems emerged relating to outsourcing services and the collection or processing of personal data (with companies, the data mostly relating to employees and customers). In many cases, the legal requirements imposed on the quality of transfer destinations and service contracts necessitated large-scale investment and even brought about the closure of certain business activities.

Some of these problems mainly relating to local requirements for protection standards have already been solved, at least partially, but the EU had to soften their initial requirements and, as we say in Czech, "blink" by, as one example, allowing transfers to semi-privately or even privately created 'safe havens[14].' However, there still remain questions over the requirements concerning the quality, reviewability and enforcement of data transfer contracts. In particular, and by way of example, we are still not sure whether:

- a company is obliged to sue the contracted data processor in the event of an infringement of the contract,
- the data subject is entitled to sue the contracted data processor directly,
- the data subject is entitled to sue the company for a breach of the contract committed by the contracted data processor or
- the state administration in the company's country of domicile is entitled to impose sanctions in the event of a breach of contract by the contracted data processor

As in the case of contract processing of personal data, the requirements for the internal transfer of data to non-EU countries represent a major constraint for many multinational companies. A ban on the transfer of data to other countries might mean serious problems for attempts to concentrate activities and to enjoy the benefits of distributed task management. In addition, the requirements relating to protection standards in the destination country apply not only to cases of simple data transfer, but also to any access to the data (including technical maintenance of the information infrastructure).

Summarising this paradox, we can conclude that data protection meant, and in certain respects still means, a competitive disadvantage for European multinationals. Residual uncertainty, complicated and country-specific administrative procedures and unclear rules for the movement of data between jurisdictions causes serious concerns and the need for high investment, especially in the multinational company sector. This may lead to a weakening of their competitive ability in the global market.

Paradox 5: strictness and benevolence

The legal definitions of "personal data" are objective and relatively broad. The administrative procedures are strict and formal. Consequently, we soon understood that, in practice, in many cases it simply makes no sense to require the controllers or processors of personal data to register at data protection offices and to require the consent (even, in some countries the written consent) of the data subjects for collecting and processing their personal data.

Whenever the black letter law is too harsh or does not make sense, it is, especially in the case of the administrative law, possible to assume the broadest of interpretations and to argue even for an interpretation *contra verbis legis*[15].However, objecting to the wording of the lawmaker puts state institutions in a delicate situation and always requires a sufficient level of legitimacy and perfection in argumentation[16]. Consequently, such an interpretation has to be adopted by high-level state bodies engaging in the authoritative application of the law, i.e. mostly by High Courts.

In the case of personal data protection, we note that various data protection authorities are now in fact deploying very reasonable and enlightened policies in respect of the interpretation of the very broad and strict data protection legislation. This benevolence on the part of data protection offices, in fact, allows many laudable activities to exist and develop, something which would never be possible if the data protection laws were fully applied.

There is, for example, a non-commercial, anonymous chat server operated by one of the writer's former students. The users, mostly university students, can (although need not) register using their names and personal university numbers. These data, without doubt, fall into the category of 'personal data' and the subject collecting them is administratively liable for all the subsequent duties. However, the founder, rather than registering at the data protection office, took up the 'phone and rang the Office to ask whether there was really any need for him to register there. He was questioned about the size of the server, the most common discussion topics, the type of user and a number of other features and was finally advised that registration was not really necessary.

Obviously, it does not matter how many users the server has, what the topics are or who the users are – at least from the legal point of view when considering obligations arising from the data protection legislation. Equally obviously, it would make no sense to require my former student to register at the Office. The problem is that, in this case it was neither the lawmaker who allowed the uncontrolled processing of personal data, nor a judge, but a clerk.

The paradox here is not to be seen in the difference between a strict and a benevolent application of the law (such tension occurs in many other legal areas and the law has already developed sophisticated methods of dealing with it). The paradox is rather to be seen in the difference between the factual weakness of the lawmaker and the powerfulness of a clerk[17].

Concluding remarks

It might seem from the above text that I do not like the recently applicable data protection provisions of the European and national laws. Frankly speaking, I do not.

However, this article was not aiming to demonstrate that the administrative protec-

tion of personal data makes no sense; its aim was, rather, to point out that substantial questions remain unanswered over the basic conceptual features of the recent regulation and its European background.

Instead of discussing the real basics of the data protection regulations, their purpose and effects, we often tend to analyse only internal questions and problems. However, the concept is not so well-grounded in the legal system and in legal practice that we need to ask "Why should we not have this regulation." Instead, we should ask (analogically to Lessig's question about intellectual property rights): "Why should we have it?"

Personally, I think that there are, in fact, very solid grounds for argument in favour of the administrative protection of personal data. However, in order to reach the desired legitimacy at European and national level, the regulatory model needs to be confronted with these paradoxes and, consequently, reshaped. Otherwise, there is a danger of a conflict of validity[18] in which the law can never succeed.

Notes

* This article was created under the research project no. MSM0021622405.

1 As the core of the Radbruch's works was still not translated into English, we have to study his teachings from the secondary works – see for example Taekema, Sanne: The Concept of Ideals in Legal Theory, Kluwer Law International, The Hague, 2003. p. 69

2 Lessig, Lawrence: Free culture, Penguin Press, New York, 2004. p. 305

3 See for example Schwartz, Paul M.: Property, Privacy and Personal Data, In: Harvard Law Review, 2004. vol. 117(7), p. 2094

4 Brandeis, Louis D. – Warren, Samuel D.: The Right to Privacy, In: Harvard Law Review, 1890. Vol 4, p. 193

5 See for example Solove, Daniel J.: Conceptualizing Privacy, In: California Law Review, 2002. Vol 90, p. 1099

6 Ibid. p. 1109

7 Such an approach to the law was present in Europe namely at the end of the 19th and the beginning of the 20th century led by the German school of the so-called "Jurisprudence of Terms" (in German die Begriffsjurisprudenz).

8 While some of the national laws strictly define the personal data as only such that identify a living person, some of the laws including the harmonization directive do not solve the problem and leave the question open.

9 No further categories of personal data are used for example in the Cypriot Law "The Processing of Personal Data (Protection of Individuals) Law 138(I)2001.

10 As an example, we can use the Czech Act No. 101/2000 Sb., on "The Protection of Personal Data" and on "Amendments to Some Acts".

11 This example was taken from the Estonian Data Protection Act (RT I 2003, 26, 158).

12 This category is used by the Italian Personal Data Protection Code adopted by the Legislative Decree no. 196 of 30 June 2003.

13 Both defined in the Hungarian Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest.

14 The most important safe haven policy for EU companies was developed by the U.S. government on the grounds of the semi-private contractual basis – see the Safe Harbor page at the U.S. DoC Export Portal at http://www.export.gov/safeharbor/index.html [15.05.2007.]

15 The mere concept of principles of good governance was historically developed not legislatively, but by the courts arguing their interpretations of administrative laws making sense but being contrary to their black-letter wording. For a simple understanding of what the "reasonable application of the administrative law" means, we can unreservedly recommend the simple guide developed by the Australian government in an attempt to help developing countries – see Good Governance – Guiding Principles for Implementation, published by the Australian Government's Overseas Aid Programme, available on-line at http://www.ausaid.gov.au/publications/pdf/good_governance.pdf [15.08.2007.]

16 Very relevant formalist counterargument against, however wise and reasonable, interpretation contra legem is that, by allowing it, the state dissents from the rule of law in favour of the rule of men. Thus, there is a strong need for the respective 'men' to be equipped for the highest possible level of social and legal legitimacy. For the analysis of formalist arguments, see for example Posner, Richard Allen: Legal Formalism, Legal Realism and the Interpretation of Statutes and the Constitution, In: Case Western Law Review, 1986-1987. Vol. 37(2), p. 179

17 When the clerks are benevolent in such cases, it is in practice impossible to review or revise their interpretations – no one goes to the administrative court and asks for an additional obligation or punishment.

18 The conflict between legal (formal) validity and other types of validity was explained by Robert Alexy in Alexy, Robert: The Argument from Injustice – A Reply to Legal Positivism, Oxford University Press, New York, 2002. p. 83 Besides the conflict of legal and social or ethical validity, we also see now the emerging conflict between the legal and economic validity of laws which is dealt with by the popular stream in contemporary legal theory named "The Law and Economics".

Eleni Kosta – Jos Dumortier

Implementation Issues of the Data Retention Directive*

In March 2006 the European Union adopted a directive on the retention of traffic and location data which aimed to put an end to a vigorous debate on this issue among European Union institutions, industry players and privacy advocates. In this paper we shall offer a critical analysis of the detailed provisions of the directive in the light of the implementation procedures in the various Member States.

Eleni Kosta is a legal researcher at the Interdisciplinary Centre for Law & ICT (ICRI) of the K.U.Leuven, Belgium, and a doctoral candidate at the Faculty of Law of the same University, under the supervision of Prof. Jos Dumortier, on "Consent as a legitimate ground for data processing in electronic communications".
Jos Dumortier is Professor of Law at the K.U.Leuven, Belgium, and Director of the Interdisciplinary Centre for Law & ICT (ICRI). He is also a member of the Brussels Bar (time.lex)

1. Introduction

The retention of traffic and location data has been at the centre of discussion for several years within the European Union. Notwithstanding the existence of major differences in the approaches to the issue among the bodies of the European Union, privacy advocates and industry players [1], the European Union adopted in March 2006 a directive[1] to regulate it. However the debate regarding telecommunications data retention did not appear to stop. Ireland has challenged the directive before the European Court of Justice[2], arguing that the legal basis chosen for its adoption was not correct and that the relevant legal instrument should have been taken under the Third Pillar. The directive should be transposed into national law by the 15th of September 2007,