LEGAL PRIVACY

LEGAL PRIVACY

Ahti Saarenpää (ed.)

Prensas Universitarias de Zaragoza

LEFIS
LEGAL FRAMEWORK FOR THE INFORMATION SOCIETY

FICHA CATALOGRÁFICA

LEGAL privacy / Ahti Saarenpää (ed.). — Zaragoza : Prensas Universitarias de Zaragoza, 2008
305 p. ; 22 cm. — (LEFIS Series ; 5)

ISBN 978-84-9252-117-3
1. Internet–Derecho–Europa. 2. Protección de datos–Derecho–Europa. 3. Derecho a la intimidad–Europa. I. Saarenpää, Ahti. II. Prensas Universitarias de Zaragoza. III. Serie: LEFIS Series (Prensas Universitarias de Zaragoza) ; 5
34(4):004.738.5
342.738(4)
343.45(4)

Ilustración de la cubierta: David Guirao

La AECID ha subvencionado parcialmente la edición de este libro

Director de la colección: Fernando Galindo Ayuda
Coordinadora de la colección: Pilar Lasala Calleja

Prensas Universitarias de Zaragoza. Edificio de Ciencias Geológicas, c/ Pedro Cerbuna, 12. 50009 Zaragoza, España. Tel.: 976 761 330. Fax: 976 761 063
puz@unizar.es http://puz.unizar.es

Prensas Universitarias de Zaragoza es la editorial de la Universidad de Zaragoza, que edita e imprime libros desde su fundación en 1542.

Impreso en España
Imprime: Servicio de Publicaciones. Universidad de Zaragoza
D.L.: Z-3142-2008

TABLE OF CONTENTS

PREFACE

As a word, legal concept and institution, privacy is exceptionally challenging. It is easy enough to understand but difficult to define and identify. It is not particularly easy to legislate either. For the legislator, privacy very much resembles Tantalus' fruit: just when it seems to be in reach, it withdraws yet remains temptingly visible. The end result has been an extensive body of legislation in various forms both nationally and internationally. There is more to come, and no end in sight.

Privacy is every bit as daunting when considered as a subject to be taught to prospective lawyers and others interested in the law. We are forced to ask where, to whom and how privacy in the legal sense should be taught. As yet privacy does not seem to have a real disciplinary home to call its own in legal research or teaching in any country. Academically, law has thus largely overlooked one of our main fundamental rights – the right to privacy. We have every reason to ask how this is possible and what we can do about it.

One thing is absolutely clear here, however. Privacy is the fundamental basis for organising the relationship between the individual and society and between the individual and the state in a democracy governed by our constitutional rights and the rule of law. It goes the core of our right to self-determination, and it is through this right that we interact with and become part of society, the state and organisations. If our right to self-determination is seriously impinged, we can no longer say that we live in a democracy. The form of government in such a state would be something very different, even if it still called itself as a democracy.

It is crucial to note that privacy is also part of security at the level of the individual. We can speak of different forms of security. The need

for security is one of the human being's basic needs and privacy in fact was one of the oldest ways to fulfil this need. Religious and other cultural variations in the notion of privacy have always played a critical role and continue to do so. However, the European Union is undeniably doing much to harmonise our conceptions of privacy and of the need to protect it. With sophisticated data protection legislation a threshold criterion for membership in the EU, a consistent view of privacy in the legal sense now extends over an ever-broader landscape to different cultures. One implication of this development is that we will not be able to avoid societal tensions; efforts will emerge to establish different forms of privacy.

We have become accustomed to saying that our right to privacy is one of the hallmarks of the democratic constitutional state. But even as we adhere to the tenets of democracy, we easily find ourselves slipping in the direction of the administrative state – a state that supervises and controls us effectively but at the expense of some of our privacy. Recent decades have shown that Europeans want no part of such a form of government. Yet the effective use of the rapidly developing information technology we see today would provide such a state with just what it needs to thrive. Like democracy itself, the constitutional state is sensitive to changes that have negative impacts – direct or indirect – on people's rights. Changes for the worse are a ready consequence of the technological imperative – a blind faith in the effective use of information technology. The imperative has been one of the long-term research interests in legal informatics – and with good reason. Information technology enables developments that easily jeopardise the rights of the individual.

In the democratic constitutional state, defending the individual's right of privacy is the responsibility of not only the legislator, but also, and above all, teaching and research in the field of law. Science should – as is traditionally thought – create order, simplify matters, make the invisible visible and criticise development where it goes askew. All of these tasks come to the fore saliently in the study and teaching of privacy and how it is regulated and restricted.

In this connection, we should not forget the important role that different expert organisations can play in the protection of privacy.

Dialogues such as that seen in the EU on the realisation of privacy in the market and in government require a significant level of expertise. This is partly provided by international watchdog organisations, whose activities are based on the work of experts. Creating the legal protection privacy requires must consist of more than a dialogue between the legislator and the market or an attempt to make public administration as efficient as possible. Negotiated lawmaking alone can be a dangerous approach to drafting legislation when it neglects the protection of people's fundamental rights.

The contributions in the present volume are based primarily on the presentations and interesting discussions at the January 2007 LEFIS seminar in Finland, held in Rovaniemi and at Pyhätunturi Fell. This is far from a random collection of articles, however. The articles are accounts of what the position on privacy has been in the work of LEFIS for some time now. They exemplify how legal informatics as a discipline studying the relationship between law and information technology examines the issues involved.

The authors did not set out to put together a comprehensive work. Many very important issues have had to be dealt with in passing. This is the case, for example, with the use of national basic registers for research purposes. It is an important subject in its own right, one where the concept of research in itself gives us a great deal to think about. Such a special theme could not be accommodated in this basic presentation.

Considerations of scope have also made it necessary to exclude the topic of transfer of personal data from one country to another – one of the biggest stumbling blocks in data protection legislation in the network society. The relevant European legislation safeguards the transfer of personal data within the EU; transferring such data to other countries is a rather different matter. This is such a broad and complex issue that it would require a treatment of its own, preferably to be read after one has a thorough grounding in privacy and personal data protection.

In my own article, which begins the work, I describe and assess privacy briefly from a conceptual perspective. I then proceed to the level of the

general categories of law, taking up privacy as part of the law of personality in some detail. This approach opens up an important but often forgotten area in the teaching of privacy. The modern law of personality is one of the key academic fields in law dealing with respect for the individual, but it has often found itself overshadowed by teaching and research dealing with the market. I also take up the principles of modern information law – principles desperately needed in the new network society.

My article primarily deals with examples of some Finnish legislative solutions. On the one hand, these reflect European regulation that is guided by directives, on the other the Nordic tradition in legislative drafting. My aim here is to provide an instructive presentation of the issues and to offer insights into the legislative culture. This is one of the central goals of the work being done in LEFIS. We are constantly engaged in practical, small-scale comparative law.

The introductory article is followed by a chapter presenting various approaches to privacy – both positive and critical. At the beginning of the chapter, Pieter Kleve and Richard De Mulder draw attention to the dangers that lie in a one-sided emphasis on privacy: it may well compromise our right to information. I also deal with this theme briefly in the introductory article. Mr. Kleve and Mr. De Mulder offer a much more thorough and critical treatment of the issue in their contribution.

Philip Leith, the Grand Old Man of legal informatics, takes an even more critical tack in his contribution. He fears that privacy has become a split legal institution. On the one hand, in its present form it offers ordinary citizens rather poor protection; on the other, it is used to further the economic ambitions of some celebrities. Privacy has thus become a slogan of sorts. It is becoming detached from its conceptual and ideological foundations. Leith brings out an issue that genuinely merits our attention.

The general part of the book concludes with a contribution by Fernando Galindo, the primus motor and tireless engine of the LEFIS project. Among other things, he adds the conceptions of the average citizens to the discussion. He presents the results of the interesting

Kingston survey and reflects on their significance where fundamental rights are concerned. When we look at these results and those of the earlier Eurobarometer on people's conceptions of data protection, we see additional support for the idea that privacy has become an increasingly well-defined value, one that a lack of awareness of the importance of legislation can no longer undermine.

In the second part of the book, we go on to discuss privacy on open networks. Tatiana Stefanova starts out with a review of the focal questions. She emphasises the importance of having a privacy policy, which is often neglected, and of providing illustrative examples of it. One can find any number of web pages that have no information on the data protection or privacy policy of the person or organisation that maintains them. Then again, we see more and more sites where these policies are set out in documents running into dozens of pages. This cannot be the best way to communicate the information either.

Tatiana Stefanova presents Bulgarian data protection legislation too. Her opinion is very critical. Anyone reading her comments can understand, how difficult it is to open the doors to modern data protection legislation.

In the second contribution, Jari Råman takes us into the world of mysterious supervision and surveillance. We know that various forms of clandestine listening and technical surveillance are on the rise. An open network provides fertile ground for such activity. Legal listening and surveillance must be set out in the law, but most of the relevant statutes in different countries date from the era of fixed telephone and data networks. Mr. Råman asks with good reason what types of provisions we should use to regulate these activities as we enter the era of the network society.

When dealing with information and communication privacy in the legal sense, it is inevitable to underline the dangers for privacy and data protection especially during the criminal investigations. This topic becomes more important after the approval of the EU Draft Treaty in October 2007 in Lisbon that intensivates the judicial cooperation in criminal matters within Europe. This fact in connection with the setting

of different standards of data protection when such activities take place, provide this issue with dramatic aspects.

Irini Vassilaki illustrates the legal framework that regulates the European judicial cooperation in criminal matters. Furthermore she presents procedures that can guarantee a high level of data protection without preventing the collaboration between the European law enforcement authorities.

Chapter four of the volume is dedicated to a more detailed examination of the relation between privacy and data protection. In the first contribution, Mindaugas Civilka and Rita Barasneviciute provide a very interesting account indeed of the price we pay for our privacy. This is not a perspective to be overlooked by any means. On the path from human rights to an information product that has been produced in a legally sound way with consideration for our privacy, we may find ourselves dealing with a very complex value chain, one involving a very dear price at the end of the line. This is the case particularly where we are not able to navigate the legal superhighway I describe in the introductory article.

The information systems used in health care and social services are currently being put on networks throughout Europe. In both of the sectors, information is sensitive information and data protection legislation imposes various restrictions on even the conventional processing of such data. Likewise, combining such data is only allowed under certain conditions. Placing this information on a network to improve access to it creates significant new challenges in the area of information security. The planning of the systems, as the authors – Cesare Maioli and Chiara Rabbito – demonstrate, is an extraordinarily demanding task that requires not only insights into the legal issues, but also an ability to combine professional skills in law and information technology.

A second important environment in the new regulation is working life. Privacy and data protection are very much part of the workplace, too. This is a significant topic internationally. Given that Finland was a pioneer in enacting legislation on privacy in working life, I briefly describe the purposes and content of the relevant Finnish law in my

contribution here. These aspects of the Finnish legislation might well puzzle, at least in some measure, readers who are still working under the old approach whereby all aspects of control and supervision in the workplace were the employer's prerogative. This is not the case any longer in today's constitutional state. Privacy in the workplace is very much an everyday fundamental right. Europe – all of Europe – is gradually going to have to come to terms with the seriousness of this issue.

Data protection legislation is institutional legislation. It involves – and must involve – the work of authorities. The Personal Data Directive requires that every EU Member State have data protection authorities that guide and supervise the implementation of data protection.

The data protection ombudsmen and their cooperative organisation, WP29, play a crucial role in applying data protection legislation and in providing guidance in its application. Accordingly, it was considered essential to include the perspective of those authorities in this volume. This is provided by Finland's Data Protection Ombudsman, Reijo Aarnio, who describes his day-to-day work during 2006 and reflects on the latest projected developments in the field.

Concluding the volume is a brief description of the relationship between privacy and crisis management. This issue has taken on bewildering forms internationally in the debate on how to combat the ubiquitous threat of terrorism. We must counterbalance this debate by reminding ourselves that crisis management always entails information management too. The state should be prepared to use and to protect its data stores in exceptional ways when faced with exceptional circumstances. Rimantas Petrauskas and Kristina Spalveters provide us with an insightful example of how this issue has been addressed in one particular country.

I have edited the volume such that each article can be read on its own. This is often the practice – perhaps too often. Lawyers in particular, often referred to as 'text crunchers', are used to homing in on specific problems when they read. Reading legal works holistically has become a dying art. Accordingly, the reader will find that many aspects of the

concept of privacy recur throughout the volume. This is should be taken as sign of how important they are as well as of consideration for the reader.

It is my hope that this volume will help the reader better understands the importance of the legal framework of privacy in the rapidly changing network society. In spring of 2007, the European Commission stated that there is no immediate need to amend the Data Protection Directive. Despite many sceptical voices that would have it otherwise, the Directive is here to stay. But society is changing at a dizzying pace. In the thick of that change, we need more and more people who are increasingly better at identifying and solving the legal problems associated with privacy. It is my sincerest hope that the present volume will play its part towards achieving this end.

Ahti Saarenpää
University of Lapland
Finland

CHAPTER ONE
INTRODUCTION

PERSPECTIVES ON PRIVACY

Ahti Saarenpää[1]

1 The Concept

Much of our view of the world depends on language, with concepts and terms playing a key role in both life in general and in law. Legal theorist Aulis Aarnio has observed, most aptly, that especially a lawyer is a prisoner of language. The importance of concepts should never be overlooked. We would do so at our peril, given that law is largely communication. We are always looking for meanings for concepts – legal and otherwise.[2] In this light, a brief examination of privacy as a concept is no doubt in order.

As a general concept, privacy is a very old one. In antiquity we see a fundamental distinction drawn between private and public. Given that classical thinkers were involved, the concept took on philosophical and political meanings, meanings that have played a crucial role in the social debate on the issue. Similarly, we find mention of privacy in the history of religion. This background is often overlooked as we tend to focus narrowly on the comparatively short legal history of the concept. In a multicultural Europe the influence of religion on the understanding of privacy – also in the legal sense – cannot be emphasised enough.

---

1 Professor, Dr., Institute for Law and Informatics, Faculty of Law, University of Lapland, Finland, e-mail: <asaarenp@ulapland.fi>.

2 In one of its decisions in 2003 (KKO:2003:83), the Finnish Supreme Court had to vote on whether the concept of a fire included flames or not.

The legal history of privacy is generally viewed as dating back to an interesting article published by Samuel D. Warren and Louis D. Brandeis in 1890.[3] This was unquestionably a milestone in the history of the legal concept. An old, in fact very old, issue was provided with a new, conceptual description. What in fact happened was that Warren and Brandeis identified the principle of privacy in the legal system of the United States, and the terminology changed quite rapidly with that observation. The right to be left alone became intertwined with the notion of privacy. This is one good reason for citing Warren and Brandeis whenever writing about privacy.

But this was not where privacy and the protection of privacy really began. In fact, even Warren and Brandeis referred to the French legislation at the time and Tom Gerety has pointed out to us the work of Sir James Fitzjames Stephen, which dates back to 1873.[4] Upon closer examination, the history of privacy proves to be almost as long as the history of humankind. The literature sometimes even describes the origin of privacy as the moment when Adam and Eve realised they should cover themselves so as not to be seen by one another. This point is well worth remembering today too if and when privacy is criticised as being a fad. This has happened.[5]

In the English-speaking world, the concept of privacy initially developed for the most part in the United States. Its legal history and later development are intensely connected with American legislation and the American courts. This rich history is reflected in the still frequent references in the literature to Alan Westin's well-known classification of privacy in *Privacy and Freedom*, yet, at the same time, this focus entails two risks to our understanding of the concept.[6]

---

3 'The Right to Privacy', *Harvard Law Review*, no. 5/1890. The direct impetus for the article was yellow journalism, which featured news items dealing with people's private lives.

4 Tom Gerety, 'Redifining Privacy, Harvard Civil Rights', *Civil Liberties Law Review*, 12 (1977), p. 238.

5 At the end of the 1980s, a leading Finnish sociologist described data protection as a fad. His statement was uttered as part of a dispute as to whether people's voting behaviour could be freely studied.

6 Westin, *Privacy and Freedom*, New York, 1967.

First, Westin's classification is closely linked to the society of the time, which was largely an industrial society or, at most, a service society.[7] In the world that individuals lived in at the time, Westin's definition provided an insightful foundation for discussion. Just a few years later, however, the Swedish scholar Stig Strömholm produced a far more comprehensive list of the legal 'sore spots' where privacy was concerned.[8] Westin has since published a number of studies on privacy, but they seem to be less frequently cited in the international literature than his book. This is an interesting example of how classics in a field take on a life of their own regardless of when they were written. That can later be misleading and harmful too.

The second problem is that privacy as a concept has long been linked to the American thinking on fundamental rights and to American jurisprudence and case law.[9] When brought to Europe, the concept was – in terms of comparative law – a transplant of sorts that in being adopted as a general concept became, or is becoming, a more comprehensive notion than its American precursor.

Thus, when privacy is mentioned, we have to determine in each case whether we are talking about privacy as it relates to information and the processing of data or privacy more broadly in the sense of an individual's right to be left alone. Later in this volume, Fernando Galindo avoids this problem by explicitly equating privacy and the protection of personal data. In the United States, Canada, Australia and New Zealand, for example, legislation enacted under the heading 'privacy' deals primarily with the processing of personal data.

---

7 The four forms of privacy which Westin distinguished are anonymity, reserve, solitude and intimacy.

8 Strömholm, 'Integritetsskyddet', *SVJT*, 1971, p. 695. Strömholm's list had no fewer than 14 special items. Westin's classification and Strömholm's list, based as it was on the Nordic legal systems, do not, however, proceed from the same level of abstraction.

9 Here it should be noted that we have often linguistic difficulties when comparing European and American fundamental rights. See West, 'The Council of Europe's French–English legal Dictionary: an American Lawyers Analysis' (p. 431), in J. Gémar and N. Kasirer, *Jurilinguistics: between law and language*, Bruylant, Brussels (2005). See also Mattila, *Comparative Legal Linguistics* (p. 261), Ashgate (2006).

Privacy as a legal concept was making its entrance in Europe in the 1950s with adoption of the European Convention on Human Rights. The earlier United Nations' Universal Declaration of Human Rights – in its Article 12 – recognised privacy.[10] However, the Convention adopted the expression 'private life', a term often considered synonymous with 'privacy'. One could further say that the scope of Article 8 of the Convention, with the developments that have taken place since 1950, has expanded from private life to privacy more generally. Here I view 'private life' in a restricted sense as referring to an individual's private activities in everyday life. Today, when interpreting Articles 6 and 8 of the Convention, for example, the European Court of Human Rights consistently uses the expression 'reasonable expectation of privacy'.[11]

Articles 7 and 8 of The Charter of Fundamental Rights of the European Union distinguish between private life and the processing of personal data. This reflects the view embodied in the 1995 Personal Data Directive whereby protection of personal data is an aspect of the protection of privacy. Article 1 of the Directive expresses the situation clearly: 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.

In Finnish legislation the confounding of privacy concepts can be seen in the Finnish Constitution's references to the protection of private life. The Constitution was drafted using the original terminology of the Human Rights Convention. The protection of one's private life is a fundamental right. In contrast, privacy appears as a basic concept in the

---

10 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

11 See, for example, Copland v. The United Kingdom 03/07/2007, where the Court states:
The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see Halford, § 45). The same expectation should apply in relation to the applicant's e-mail and Internet usage.

Personal Data Act and the Finnish Penal Code, with private life being one aspect of privacy when applying this legislation. What is more, the English translation of the Finnish Constitution uses the term 'privacy' rather than 'private life'. The terminological framework is really unstable.

But we are not alone. Privacy as a concept is understood in many different ways also in the international literature. For example, the Norwegian scholar Lee Bygrave has distinguished four general ways to understand privacy.[12] The first of these I have mentioned already – the notion put forward by Warren and Brandeis of the right to be left alone. The point of departure there is non-interference by in others' affairs. The second group consists of ideas of limited access to things. Ruth Gavinson's widely known conceptions of privacy can be put in this category. The third group is more squarely concerned with information, with the work of Alan Westin occupying a central role. The fourth group is the narrowest in scope, comprising notions closely linking privacy and the intimate sphere. Only sensitive matters fall within this last definition of privacy.[13]

For present purposes it is not necessary to go about looking for a single, optimally precise legal or philosophical characterisation of privacy. Such an undertaking would warrant an extensive study in its own right. Accordingly, I will be content to examine privacy as a relative concept connected with the formation of our right to self-determination, which is also referred to as personal autonomy.

Human beings basically have, and should have, a right to be alone in society in relation to something. This is the core of the right to self-determination. Private and public are profoundly different spheres. However, the right to privacy is clearly not absolute or inviolate, for

---

12 Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, The Hague/London/New York: Kluwer Law International, 2002, pp. 128–9.

13 The idea that only the intimate sphere falls within the definition of protected privacy is philosophically misleading inasmuch as the intimate sphere cannot, by definition, be known. Indeed, like Westin's view, the well-known definition of privacy put forward by Tom Gerety in 1977 is very problematic in this light. Gerety said: 'Privacy will be defined here as an autonomy or control over the intimacies of personal identity' (Gerety, p. 236).

society and democracy would be rendered impossible. Moreover, the right is constantly changing, a trend profoundly influenced today by the development of the European democratic constitutional state as well as of our society and its technological advances.

Democracy is a very multifaceted form of state. Administration can be implemented in many different ways within the basic mould. For example, the latter half of the twentieth century in Europe can be characterised as the era of the democratic administrative state. A citizen was, to use the term common at the time, an administrative subject – or object only. The transition from the administrative state to the democratic constitutional state did not begin in most countries until the late 1980s and early 1990s. For example, the fundamental rights of Finnish citizens were reformed in 1995 to accord with those set out in the European Convention on Human Rights. This was a crucial step on the path to the new constitutional state. In much the same way, the European Personal Data Directive, adopted in the same year, imparted clear direction to development in Europe in general. The importance of the Personal Data Directive as an exemplar of the European conception of the human being cannot be overstated.

In the democratic constitutional state, our right to privacy is – as it should be – broader in scope and more effective than before. As the individual's right to self-determination becomes stronger, the importance of privacy in society becomes all the greater. I must point out here that what I refer to here is not the privatisation we hear so much about today but, rather, the strengthening of the position of the individual both in relation to public authority, other people and the market. We have the right to be alone if we want to be. In many situations privatisation may jeopardise it.

Then again, with advances in technology and the increased use of information technology, the risks that privacy will be violated or compromised are on the rise. The technological imperative, that is, the belief in the inevitability of ever increasing and more extensive use of information technology, creates new, often surprising risks. As our society changes into a network society, risks increase even further given the very modest standard of information security on open networks. In

the network society, privacy requires sophisticated information security.

These developments have led in recent years to a significant increase in the legal regulation dealing with privacy, as well as a greater diversity in the forms of regulation. People and their rights are being earnestly protected. However, at the same time, we must remind ourselves yet again that we are not alone in a democracy. This fact restricts our privacy and makes it difficult to legislate it. Privacy necessarily involves tensions, and is without question one of the most difficult areas to regulate.

With privacy being a relative concept and society and the state changing at an intense pace, a transitory comprehensive definition of privacy is unnecessary and would even be misguided. We must recognise that we are dealing with not only a legal concept and principle but also, and above all, with a broader description of the right to self-determination that is associated with the rights of the individual. We explain things as aspects of the right to self-determination using the notion of privacy. If privacy was defined as a legal concept with utmost precision, that definition and any regulation that relied on it would have to be amended constantly to keep up with the development of society and technology. This would contribute to the ill-being – to quote Georg Henrik Wright – that we experience otherwise in democracy when our rights are restricted.

The fact that privacy cannot in principle be defined in detail has even been put forward as a strength and a weakness.[14] It is a weakness in the sense that the frequent demand that legislation be precise and clear cannot be met when dealing with a relative concept such as privacy. It is a strength in that the relevant legislation dynamically adjusts to changes in society. If given a precise definition, the different dimensions of the protection of privacy could suffer due to the occasional delays in drafting introduced by what is known as 'legislator risk'.[15] The

14 One scholar to make this assertion is Lee Bygrave. See Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, p. 125.

15 By 'legislator risk' I mean that those in charge of drafting legislation either do not notice changes in society in time or overreact to the changes that they notice.

impossibility of an exact definition of privacy was one of the significant insights in the drafting process of the world's first national data protection law, Sweden's datalag.[16] Doubts had been expressed in the legal literature about the viability of the law.

More recently in Sweden a committee appointed to examine legislation on the protection of privacy generally came to the same conclusion about defining 'privacy'. The committee, which began its work in 2004 and completed it in 2007, took as its point of departure the concept 'integrity' and characterised it as being narrower in scope than the American 'privacy'.[17]

2 The dimensions of privacy

To recap, we have in the democratic constitutional state, within the scope of our right to self-determination, essentially a right to be alone. This old expression is most apt. It creates an important linguistic association.

There are many ways in which we can be alone. With complete privacy being an impossibility in light of society's needs, our privacy is opened up legally in relation to certain things, people and organisations. There must always be acceptable grounds for doing so. Yet a significant proportion of the legislation in different countries still dates from a time when this was not the prevailing approach: we were administrative objects of the government and our personal data could be freely sold. Public authority regarded our information as its own when it had collected it for its own purposes. This is why we do not get an accurate picture of the importance of privacy merely by examining the legislation only; its significance does not come out in older legislation as well as it might.

---

16 Mindaugas Civilka and Rita Barasneviciute have later in this work a short historical overview about data protection legislation.

17 SOU:2007:22, *Skyddet för den personliga identiteten*. Unfortunately this interesting committee report is available only in Swedish.

To offset the essentially indeterminate nature of privacy as a concept, legal research – in particular the law of personality and legal informatics – approaches the issue in terms of themes. This means that attention is drawn to phenomena and legal relationships where our privacy may be jeopardised, where it is already specifically regulated or where its protection requires special legislative measures. Privacy is thus a systematic 'narrative umbrella' that embraces matters which – when we have drawn the line between the public and private spheres – we can justifiably count among the liberties and freedoms that we are entitled to and that must thus be protected.

Against this assessment of privacy in our modern network society, we can identify at least the following eleven main core areas that closely affect our right to self-determination:

2.1 Physical privacy

The traditional and perhaps oldest form of the protection of individual privacy is the right to our physical integrity. This liberty, recognised as a human right and generally protected by a variety of criminal penalties, is easily overlooked when talking about privacy precisely because of the nature of traditional regulation. We approach the matter – in typical lawyerly fashion – in terms of assault. But there is room for quite a few other things between a human right and assault.

The crux of the issue is the right to freedom that follows from our right to self-determination. Physical integrity is at once one of our liberties and an aspect of privacy. Provisions on assault only describe our tradition of enacting laws on consequences, not on things themselves and the rationale for them. This is in fact a central problem in criminal law otherwise. Regulation easily becomes distorted and is less informative when it seeks to resolve issues exclusively through sanctions. The reasons for regulation must be sought elsewhere. The old notion of criminal legislation as a natural, easily understood collection of everything that is prohibited has long been a dysfunctional ideal in what is an increasingly complex society.

From the standpoint of privacy, physical integrity is much more than protection against ordinary violence. It includes by definition all exercise of power involving interference in our integrity. Accordingly, the law must provide various coercive means. And for the same reason we have legal provisions today pertaining to violations of our integrity in the supervision of prisoners and the mentally ill, for example. Such cases are no longer automatically covered by the traditional idea of so-called institutional power.

Similarly, the prohibition against corporal punishment of the child, which did not come into force in Finland until the early 1980s, is part of the child's right to personal integrity, part of his or her privacy. The limits of privacy and private life are thus not the same as the limits of the family. It has taken time for us to realise this.

2.2 Spatial privacy

Spatial privacy refers to the right to be alone in one's home and out of the reach of various forms of supervision and disturbance. This area of privacy, like many others, has traditionally been addressed by individual sanctions in criminal law. With the penalisation of clandestine viewing and listening, the regulation has – albeit slowly – followed technological developments in modern society.[18]

A more modern, ideologically inspired model of regulation where spatial privacy is concerned is the restraining order. For example, restraining orders were not adopted in Finland until the end of 1990s.[19] Given that freedom of movement is one of our basic freedoms, a restraining order can be considered a very strong means of protecting another person's privacy. Moreover, as a restraining order may involve

---

18 For example, one of the elements of clandestine viewing or listening in Finland is the use of a technical device. Thus even our being monitored in our yards using technical devices constitutes clandestine viewing even though we have not fenced the yard in.

19 One must also bear in mind that the restraining order has a long history internationally. For example, it was used in the United States as far back as the late 1800s. In the Nordic countries it was not used as part of the regulations to combat domestic violence until the 1990s.

other restrictions on fundamental rights – for example, in Finland a prohibition against approaching another person by a means of electronic communication – what we see is a very effective restriction of the fundamental rights of one individual in order to protect the privacy of another. The restrictions are designed to ensure the physical and social security of the individual.

2.3 Social privacy

Social privacy, as the term implies, pertains to our social position. We have – and should have – the right to keep our human relationships, way of life, hobbies and convictions to ourselves and beyond the reach of supervision and the exchange of information. Here the focus is the range of interfaces that we have with other individuals, communities, markets and society. We may have a lot different identities. As a matter of principle it is we who decide on such matters.

Today social privacy is protected – or at least should be – primarily through the protection of personal data and the development of data and information security. In practice, the problem areas where social privacy is concerned are the surveillance and supervision of individuals in public places and the transparency of the activities of various private associations and public bodies. A more recent concern is the ease with which unofficial online communities – cyber communities – can be monitored due to the poor information security of open networks.[20] We might even describe the Internet as a permanent record of our social relations if and when our relationships with others are made accessible on an information network.

2.4 Media privacy

Every person has the right to remain unknown in society in relation to the media, that is, a right to refuse media publicity. This principle is unequivocally recognised in today's constitutional state. It is part of the

20 This is a problem affecting organised diasporas in all countries, not just countries in which a diasporic community is monitored effectively by authorities.

right to self-determination – one of its pillars. We are more than just raw material when it comes to public communication.

Warren and Brandeis's article originated for the most part in a single case in which the media revealed details of a person's private life. Even in those days our privacy sold well. Today, the yellow press has established itself as part of the media, a development that can be attributed not only to people's curiosity sustaining the market but, and above all, to the difficulty of regulating the media in democracy.[21] It is difficult to address the freedom of the media systematically by legislative means without interfering in freedom of speech as a fundamental societal value. Neither should we forget that many public figures crave publicity. In certain fields, establishing media visibility is a necessary condition for financial success.

The principal sore spot if we look at the relation between the media and our privacy is the question of when the media have the right to divulge aspects of our privacy as part of their watchdog role in society and not just to make a profit. The underlying notion here is that of freedom of speech as a safeguard of democracy that is on a par with other human rights. In a democracy, freedom of speech may only be restricted to the extent that is absolutely necessary. In this way, freedom of speech changes in step with democracy. For example, when the Personal Data Directive was adopted it drew a very a prominent distinction between the protection of privacy and freedom of speech. Personal data may be dealt with in the media only when it is essential in a democracy.[22]

---

21 One regrettable fringe phenomenon is professional clandestine photographers, known as paparazzi, who attempt to photograph public figures in different situations. One illustrative example of the low ethical level at which the media operate is that they spread secretly taken nude photographs worldwide. Previously, such a practice was considered dealing in stolen goods; today it is practical 'freedom of speech'.

22 Article 9 of the Personal Data Directive addresses the tension between privacy and journalism. As the provision shows, the principal value to be protected is privacy: 'Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression'.

The Finnish approach to legislation in this field since the early 1970s has been to enact criminal prohibitions against publishing details of a so-called ordinary individual's private life without his or her consent.[23] The provision distinguishes between a natural person and a public one. Details of the private lives of public figures – politicians and senior officials – can be divulged if the issue being covered involves their public duties or role. What is at issue here is primarily the exercise of freedom of speech by the media in its overseeing the credibility of public actions and actors. In practice, the media are attempting to broaden their rights by making politicians' and officials' private lives a facet of their public credibility.

2.5 Anonymity

The right to anonymity, meaning our right to act in and have an impact on society with respect to the government without revealing our identity, is rarely mentioned – particularly in the Nordic countries – but is an absolutely crucial form of privacy in an advanced democracy. The traditional legislative manifestation of what internationally is an essential principle for the transparency of society has been our right to receive information on public matters and public documents without divulging to officials our name or details of how the information is to be used.

The right to anonymity also has a connection with freedom of speech. We have the right to make our views public with anonymity. In practice, however, this is severely limited, as the media often insist that even letters to the editor have the contributor's name and not a pseudonym. On the other hand, as communication on computer networks has grown, different kind of anonymous communication has increased as well.[24]

---

23 As a rule, the Finnish Personal Data Act leaves the media outside its scope of application. The supervision of the information security of editorial archives is entrusted to the Data Protection Ombudsman. The general purposes of the Act also apply to the media but with no sanctions for infringement. In light of the Personal Data Directive and its objectives, the Finnish legislation is open to criticism.

24 In Finland, the law governing the exercise of freedom of speech in the media provides for *protection of sources*, that is, the right to withhold the name of the source of a message. This has been extended to apply to a private individual when maintaining a home page.

The border between anonymity and responsibility has proven to be unclear in a number of cases. For example, the question of the acceptability of various anonymous hotlines is a thorny one, one that will require a legislative – a European legislative – solution at the end of the day. After all, anonymity is supposed to be primarily a right of the individual *vis-à-vis* society, not another individual.

The issue of anonymity takes on a fresh prominence when we move into the realm of e-Government. Citizens are entitled to anonymity even when using electronic services. This necessarily means the strong identification of an individual may only be used when it is a question of a right, benefit or obligation that is closely linked to the person or his or her attributes. In contrast, anonymity should be ensured when a citizen uses electronic services to request information on his or her rights, obligations and their application. This distinction has not always been noticed when emphasising the importance of strong identification.[25]

2.6 Privacy in the processing of personal data

Protection of personal data through data protection legislation has been commonplace for years in the Information Society, where it can be largely regarded as an area of privacy related to the opportunities to exploit technology. However, the history of personal data protection goes back much farther than that of the Information Society. In fact, the first attempts to enact legislation for the purpose were a response to experiences during World War Two – well before the development of the information society as we know it today.

---

25 In developing the information systems that electronic services require, respect for anonymity means that systems should be designed so as not to require strong identification and that users' footprints cannot be used to identify them after an information retrieval session. In this light, the conventional front office/back office distinction used in information systems is not sufficient, not at all.
For more on these issues see Saarenpää, 'e-Government and Good Government: An impossible Equation in the new Network Society?', p. 256, in Wahlgren (ed.), *IT LAW, Scandinavian Studies in Law*, volume 47 (2004). Cf. what Maioli and Rabbito write in this volume.

As in Finland, data protection legislation in most countries covers more than the automatic processing of personal data. Nevertheless, it was unquestionably especially the opportunities made available by information technology that accelerated the development internationally of legislation to protect our privacy in the processing of personal data.

In the final analysis, the European Personal Data Directive of 1995 brought together in a meaningful way the data protection legislation of different countries as part of the effort to restrict, control and guide the processing of personal data.[26]

All in all, the protection of personal data has become established as a significant, essential area of legal regulation in today's society. Occasionally, when its importance is being stressed, one encounters the image of the individual's informational domestic peace. The German expression 'informational self-determination' is a more descriptive term. It shows that it is primarily we ourselves who decide what happens to our personal data.

The development of data protection legislation into significant legislation has not been easy. In addition to the fact that drawing a distinction between the public and private spheres always results in tensions, there are at least four reasons for the unenthusiastic attitude we see towards data protection legislation.

First, information – including that related to people – has generally been considered only simple raw material. When information technology made more effective use of that information possible, government and the market both found it difficult at first to get used to the idea that personal data enjoyed special protection other than in times of crisis. The notion that the development of information technology means no more than advances in office automation was – and still is – a strong one.

---

26 Reference is often made to the Council of Europe Convention and the OECD Guidelines of the 1980s. Both instruments have had a significant impact on the regulation of data protection; one must bear in mind that it was the Directive that first clearly combined privacy as a fundamental right on a par with human rights and the processing of personal data.

A second, closely related reason lies in the bureaucracy. The protection of personal information, which by definition covered all the processing of personal data on the everyday level, unquestionably hampered certain, in fact many activities at the beginning.[27] Given that the design of information systems failed to anticipate the protection of personal data and that the legislation did not take into account the path of information as a whole, data protection legislation often led to surprising results.

The third reason has to do with the economics of information. The design, renewal and use of information systems that take the protection of personal data into account are costly. When people's rights and economics are juxtaposed, it is usually economics that is considered more important. In addition, given that the data protection legislation allows one to take advantage of the principle of proportionality when creating the information security essential to data protection, the negative attitude towards protection of personal data has at least to some extent been reflected in a weak information security culture. And the transition to the network society has noteworthy increased information security risks.

The fourth simple reason can be seen in the terms we use. In most countries we talk about data protection but this is in fact a misleading term. What we are talking about is protection of the individual, not of data. Attention was drawn to this linguistic problem already by Germany's first data protection commissioner, Hans-Peter Bull.[28] Things might have been easier if we had used a different term and spoken sometimes of information violence and combating such violence. I have tried to promote the use of this term in the Finnish literature when considering the protection of personal data. The central aims of the protection of personal data are respect for the individual

---

27 Here it should be noted that the Finnish data protection legislation has from the very outset been comprehensive, including, for example, even the processing of personal data by the police. When understood properly, this provides better opportunities for the comprehensive regulation of privacy that strict adherence to the scope of application of the Personal Data Directive.

28 See Bull, *Datenschutz oder die Angst vor dem Computer* (1984).

and his or her privacy, as well as the prevention of informational violence.[29]

It is also important to observe that data protection is a very comprehensive legal institution. With personal data being defined as information pertaining to a person that is recorded on any medium, video surveillance, for example, falls within the scope of data protection unless the law provides otherwise.

2.7 Ownership of information

The notion of ownership of information is closely connected with the idea of informational self-determination. The issue involves not only protection of our privacy but also the fact that we ourselves can profit financially from the information on us. In other words, we all have the right to our names, photographs and character as well as to their commercial exploitation. In addition to our privacy being protected by restricting and guiding others' rights in the processing of our personal data, we have the right to publish our personal data and to exploit them commercially too.

For public figures in the entertainment field, ownership of information is a significant form of protection of privacy. They do not become 'national property' through publicity, although the media have a different view on the matter, however. Once again we encounter the tension between privacy and extensive freedom of speech. From our perspective, public figures mostly lack reasonable protection of privacy. Later in this work, Philip Leith presents a critical review of issues related to the privacy of contemporary entertainers and other public figures.

The expression 'ownership' has been an alien one in this context especially in the Nordic countries. It is essentially American in origin. As information and the commercial value of personal data increase, it is more than fitting to speak of ownership. We own our information. The

---

29 For a detailed treatment of this issue, see Saarenpää, 'Informaatioväkivalta', p. 551, in Lohiniva-Kerkelä, *Väkivalta. Seuraamukset ja haavoittuvuus, Terttu Utriaisen juhlakirja*, Talentum, Helsinki (2006) (in Finnish).

fact that the government collects this information by law does not vitiate our title to it. Indeed, we can, for example, refuse to make our personal data available for commercial purposes. This right to object is one of the crucial and essential rights provided by the Personal Data Directive.[30]

2.8 Right to be assessed in the proper light

This expression, largely originating in the earlier debate in the United States, is rather more difficult to adapt to European legal culture, for it involves elements of respect, protection of personal data and the activities of the media. The bottom line here is respect for individuals when processing information related to them and in sending out messages about them. Here one must compare a person's private and public image. What is important is 'how the person appears'. For example, combining databases compiled for different purposes can yield very special, misleading 'false light' images of an individual. Accordingly, combining files created for different purposes is contrary to the purposes of the Personal Data Directive.

In terms of private law, the issue is essentially one of where portraying a person in the wrong, false light entitles him or her to damages for any resultant suffering. This is also the outcome where data protection legislation is concerned when, for example, the improper combination of data creates a false image.

---

30 Article 14: The data subject's right to object. Member States shall grant the data subject the right:
(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;
(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.
Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

2.9 Patient privacy

In the regulation of the protection of privacy, social welfare and health care represent an area that has become juridified in a new way in recent years. In these sectors, confidentiality has been a traditional practice and the protection of sensitive information in the processing of personal data has involved a rather more recent form of regulation.

The issue here is not merely confidentiality but a view of the right to self-determination in terms of freedoms and privacy. Thus, for example, according to the Finnish Patient Act, patients have the express right to keep the state of their health confidential if they so wish – with the exception of certain communicable diseases – and, if necessary, to enjoy physical integrity during their care. For these reasons, it can be said that today patient privacy has also become established as a central area of modern privacy. The primary power of the care-giving institution has had to yield to respect for the individual.[31]

In the health care sector, privacy issues centre on the living conditions of chronic patients. When a hospital or other facility becomes permanent home, one must ask what is to be required of that living environment where privacy is concerned. In Finland, the Supreme Administrative Court took a clear position some years ago on the issue in one of its rulings. According to the Court, having two or more dementia patients living in the same room on a long-term basis is a violation of their right to privacy.[32]

In the 1990s, telemedicine brought to light problems that can arise when transferring patient data in electronic form from one health care facility to another or from a patient's home to a health care facility. A more recent development with the advent of the network society is the work begun on national prescription and patient data systems. These projects must address the question, among others, of a patient's right

---

31 The Act on the Status and Rights of Patients came into force in 1993. It is one of the world's first laws on patients' rights.

32 This decision (KHO:2002:75) pertained to a situation in which plans for an addition to a care facility called for two dementia patients to live in each room. We can see in this decision a clear contrast between old and modern society.

to view his or her records on a network.[33] Later in this volume, Cesare Maioli and Chiara Rabbito provide an example illustrating the development of a patient data system in Italy.

2.10 Privacy in working life

Privacy has come – or is coming – to working life throughout Europe. We enjoy at least a limited protection of privacy in the workplace as well. Much as the traditional institutional power in various institutions has yielded, the exclusive control of the employer over matters involving employees' privacy has diminished. Fuelling this trend have been the general changes that have taken place in working life, data protection legislation, the decisions of the European Court of Human Rights and special legislation.[34] The adoption of the Personal Data Directive meant that data protection legislation as such applied to working life. In many companies that at first was not understood at all.

The real understanding of privacy in working life and the need for legislation to govern it range from considerations of recruitment to what employees are allowed to tell after they have left the company and how the information on them and the equipment they have used are to be dealt with. The content of the Finnish Act on Privacy in the Workplace illustrates well the wide range of issues involved. The law covers the following:

— the processing of a job applicant's personal data
— how an applicant may be tested
— the processing of an employee's personal data
— how an employee may be tested
— protection of an employee's email messages

---

33 A new law entered into force in Finland in July 2007 on the electronic processing of client data in social welfare and health care, but the transition to using national registers will not be complete until 2011. There is a huge project to build this new national system.

34 Finland has been a pioneer in this development. Our first special law on the protection of privacy in working life came into effect in October 2001. It has since been replaced by more detailed legislation under the same title, enacted three years later.

— technical surveillance in the workplace; and
— procedures for implementing protection of privacy.

This list alone tells us how heavily charged an issue privacy in the workplace to day is. The employer's traditional right to manage and supervise employees is now restricted in many ways. These may sometimes even be surprising. For instance, the principle that an employer must, as a rule, ask the employees for their personal details entails a prohibition against searching for such details on an open network.[35] Later in this volume, I will take up in more detail the principal solutions that have been adopted in this regard in Finnish legislation.

2.11 Communicative privacy

According to European notions of human and fundamental rights, the confidentiality of a letter, telephone conversation and other confidential message is in principle strongly inviolable. Earlier, the confidentiality of communication was addressed primarily through secrecy provisions. Today, electronic communication is so complex and information networks so vulnerable that communicative privacy has become a regulatory concern in its own right. The shape of the regulation in this area is determined by fundamental rights and, in a crucial way, by the European Directive on privacy in electronic communications.[36]

When we talk about communicative privacy, it is important to notice that the issue involves more than just the content of messages. We must examine all of the stages in what might be termed the path of the information. Thus, for example, the forwarding of a message via a proxy

35 This prohibition is of course difficult to supervise. It prompts us to think – if we consider our careers – what kind of information and images we produce and project on information networks. In Finland, the Data Protection Ombudsman has had to deal with a case where an applicant did not get the job because his name appeared on the web pages of a mental health organisation. The potential employer drew its own conclusions from this on whether the applicant had mental health problems.

36 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.

server and the footprint of the message left on different devices are important considerations where our privacy is concerned. These range from the attaching of an individual message to a platform to its archiving or deletion. It is a long, long way.

In the network society there are many numbers of stages in the processing of a message in which our privacy can be compromised in various ways. The potential difficulties range from problems in understanding and identifying issues of privacy to the modest and variable standard of information security in government. Electronic communication is one of the most difficult areas to legislate too.

2.12 Conclusion

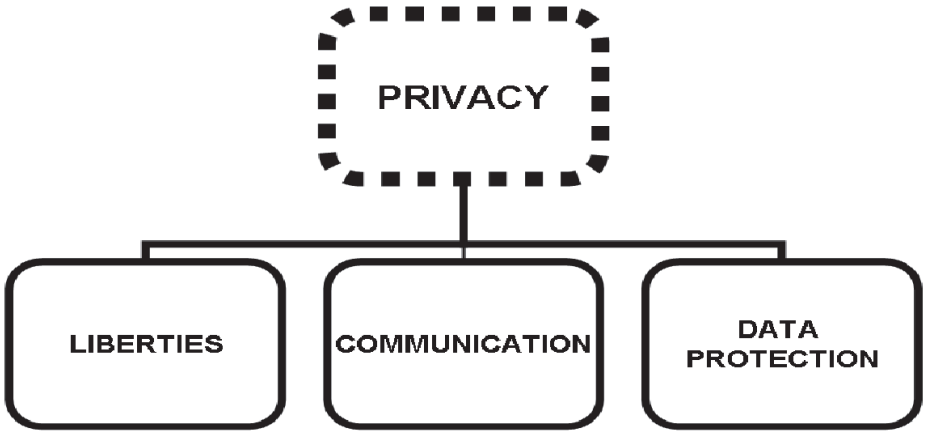
The above list of eleven privacy areas does not purport to be an exhaustive description of the areas of privacy, not at all. Being a relative concept, privacy is constantly changing. As society changes, new situations constantly emerge in which privacy has to be taken into account as a factor in interpretation or as a factor prompting changes in legislation. Likewise, every new provision that uses the expression 'privacy' or 'protection of private life' necessarily prompts a closer examination of what privacy is. Yet it goes without saying that legislation on privacy is enacted that describes it in other terms. The standard of legislation also varies considerably in this area.[37]

If we look at the manifestations of privacy listed above, it is easy to see that in terms of the network society and the digital environment in which we operate they can be grouped into three main categories. We may speak of privacy as (1) liberties, as (2) communicative rights and as (3) the protection of personal data.[38] These are all of course profoundly interconnected.

It is also important to bear in mind the distinction between privacy in the everyday sense and privacy in exceptional situations. It is necessary

37 The Swedish Committee on privacy legislation, whose report (SOU:2007:22) was mentioned above, drew particular attention to this problem.

38 Tatiana Stefanova does later in this work use a classification of four main areas.



that we be able to restrict privacy when emergencies, disasters, criminal investigations or state security so warrant. In a democratic constitutional state, this should be set out in legislation. As part of the development of the network society, networks and communication have become a significant object of regulation where management of exceptional situations is concerned. Among the activities that are typically regulated are the use of electronic positioning data in emergencies and various forms of monitoring telecommunications. Rimantas Petrauskas and Kristina Spalveters draw attention to this problematic area later in this work.

The list I have presented is deficient in another respect as well. What is lacking is the demarcation between privacy and publicity as these relate to the transparency and principle of openness that are essential to any democracy. I mentioned the issue briefly in connection with anonymity but it merits a longer presentation in its own right.

3 The privacy of the citizen and the openness of society

We often speak of the principle of public access. In the Nordic countries we also hasten to emphasise that Sweden was the first country in the world to adopt the principle in government. I should add here that Finland was part of Sweden at the time, and the idea of public access actually originated in my country.

When first introduced, the principle of public access was short lived, but today it is once again of crucially significance in the Nordic countries. Indeed, this is why the recitals in the Personal Data Directive expressly mention that the principle of public access to official documents is to be implemented in the protection of personal data.[39]

This recital to this effect was added to the Directive at the special insistence of Finland and Sweden. It has since proved problematic, however, because it has sometimes been seen as suggesting that public access should prevail over privacy, which would be a clear throwback to the traditional administrative state. Things should of course be the other way around in the constitutional state, which is based on the rights of the individual in a democracy. Public access to official documents serves these rights while respecting our privacy. Particularly salient in this regard is our right to know – an aspect of our right to self-determination – for it is realised to a considerable extent through public access, especially public access to official documents.

The relationship between public access and privacy is a thorny issue indeed in both principle and practice. With the principle of public access to official documents well on its way to becoming a general principle of administration in Europe, its practical significance in the network society will grow by leaps and bounds. When we highlight the importance of privacy, we easily overlook the requirements of public access and vice versa. Let's take here the example of the situation that arises when placing public documents on information networks. The problem is a common one but once again I will take a real example from Finland.

In today's Finland, authorities have an obligation to communicate. Their decisions must, as a rule, be made available to the public and they should be notified where necessary. Now that sophisticated office automation allows public bodies to publish their decisions cheaply and easily on networks, most municipalities even have begun to publish

39 Recital 72: Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive.

decisions regarding individuals on open networks, with the documents appearing in their original form and thus including the personal data in its entirety.

This is a graphic example of what is known as the technological imperative – how our faith in technology blinds us. Communication has been understood as the ready transfer of documents to networks, made easy by computer technology.[40] Yet, in terms of personal data protection, this has meant transferring personal data to an undefined range of users for processing – a violation of personal data protection in light of human rights, fundamental rights, the Personal Data Directive and data protection legislation. It took a number of years to wake up to this simple realisation of priorities and to change the procedure.[41] The Finnish Parliamentary Ombudsman took the matter under consideration in the spring of 2007 and proposed that the relevant legislation be made more specific.

The principal means for implementing public access are the rule governing access to official documents and to various procedures, for example, trials. Interestingly, the related terms vary. The Anglo–American and, more recently, also the German preference is to speak of freedom of information. For example, in the United Kingdom, the Freedom of Information Act regulates the availability of documents held by public authorities.[42] In the Nordic countries, we speak of legislation on public access to official documents. For example, in Norway the title of the relevant act is the Act on Public Access in Administration, which is shortened to Public Access Act

---

40 This idea of using the advances in computer technology in document logistics draws considerably on the American thinking on the information superhighway.

41 Finnish municipalities have surprisingly few lawyers on the payroll. In contrast, their central organisation, the Association of Finnish Local and Regional Authorities, has a legal affairs unit that guides the municipalities' work closely. The Association's most recent guidelines note that the requirements of privacy outweigh the principle of public access. The guidelines issued previously tended to accord a primacy to public access.

42 The Act begins with the words: '(1) Any person making a request for information to a public authority is entitled – (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and (b) if that is the case, to have that information communicated to him...'.

(offentighetsloven).[43] In Finland, the title of the act refers to the openness of the activities of public authorities, as indicated by its unofficial English translation, the 'Openness Act'.[44]

A special facet of the relation between privacy and public access is the traditional notion that trials are public. We have become accustomed to thinking that this is an essential aspect of overseeing the judiciary. Closed trials arouse suspicions that the principles of a fair trial are being compromised. The media in particular are quick to play up this angle.

In the network society, it is a short step in technical terms from public access to trials to real-time transmission of the proceedings on information networks or electronic media. This has been done in fact.[45] The rationale put forward is openness but it is here that we seem to readily forget that openness and a public event are two fundamentally different things. In the constitutional state, seeing that justice is done cannot require the organisation of public events. It is a different matter entirely to determine what issues in our society are important enough to warrant more extensive publicity by being transmitted over a computer network.

In this connection, it is also worth pointing out that a crime, too, is an aspect of our privacy. The fact that the legislator classifies an act as a crime should not automatically mean that it is given extensive publicity. Our privacy becomes public during the investigation and trial, but when we have served our sentence, the sanction involved should, as a rule, be a strictly private – not public – affair. This is a sensitive matter in light of the Personal Data Directive as well, and one that the media do not always realise or acknowledge.[46]

---

43 The unofficial translation of the act reads: 'Act relating to public access to documents in the public administration' but it is also referred to as the Freedom of Information Act.

44 The translation can also be explained by the fact that the act entered into force during the Finnish EU Presidency in 1999. Given that openness was one of Finland's principal policy goals at the time, the term was chose as the name of the Act. The legislation is nevertheless a typical access-to-documents act.

45 For example, in some places in the United States, court proceedings have been broadcast in real time on the Internet. On the other hand, there are places where it is prohibited to even take photographs when court is in session.

46 A new Act on the Publicity of Court Proceedings came into force in Finland in autumn of 2007. The legislation will mainly make things easier for the media. The

Tax records form a problematic area of their own. They are personal data but in some states public data as well that are handed over to the media in electronic form. For example, in Norway this service to the media began in the autumn of 2007.

People's curiosity has made publishing tax information in the media very popular but this has precious little to do with ethical journalism. The practice is largely a matter of satisfying people's curiosity and pandering to their envy of others. Tax information sells well; indeed, a lot more media than just the yellow press publish it.

The tension between privacy and public access can be defused to a significant extent if we adopt the concept of a dynamic document, by which I mean a document that can be printed in a document system for different purposes and with differing content. It is a system that takes advantage of the opportunities afforded by information technology; it is an information system solution designed to protect our privacy. However, new legislation in Europe would have to be enacted before we could implement such a system.

4 Privacy, teaching and our view of law

The complexities of regulating privacy that I have pointed out above show that privacy is difficult, really difficult topic in teaching the law as well. It does not fit neatly into any of the traditional categories we use, for example, property law, family law, criminal law or, for that matter, intellectual property law. Unlike most of the traditional branches of law, privacy does not form the same kind of coherent whole that is linked to a particular activity, phenomenon and market.

The systematic classification of law serves to show a division of responsibilities and to highlight the differences between and importance

---

grounds for the act state that it is the media that will implement the publicity of court proceedings. This is a very strange view indeed – utterly artificial in fact – and is ill-suited to a society that emphasises privacy. Courts should communicate their judgments with all due consideration for our privacy.

of fields of law in what is an increasingly complex society. Along with the division of teaching content into subjects, the process of classifications opens and closes eyes as the society around us changes. Often it takes a good deal of time before law and teaching in the discipline realise its importance.[47]

And what often happens is that we have to abandon our static classifications in favour of a dynamic approach that looks at the same phenomenon from a variety of perspectives. In Europe, for example, this development now presents us with some 60 established fields within the discipline of law. This is a very large number and is something we should reflect on seriously when planning academic legal studies.

Privacy can also be considered a topic that has a number of established 'homes' in the discipline. It is perhaps most comfortable, however, in the fields of legal informatics and the law of personality.

Privacy became associated with legal informatics early on, primarily through data protection legislation. With rapid developments in IT enabling the extensive use of personal data, it was natural to make privacy a substantial component of the teaching and research agenda in legal informatics. The term 'Computer Law' was adopted in the United Kingdom in largely the same meaning. Later developments in the network society have only fore grounded the importance of this connection.

At the same time, a greater need has arisen to carry out more extensive analyses of privacy dealing with the relationship between the individual and the network society.[48] The role of legal informatics as a pioneer in

---

47 A telling example of this is that when the first data protection act in Finland – the Personal Data File Act – entered into force, 'Suomen Laki', the systematic compilation of Finnish law, placed it in the same section as legislation dealing with general administration and similar matters, which included provisions on, among other things, the state lottery and the use of knives. The editor simply did not understand what the Act was all about.

48 In Sweden, which enacted the world's first Data Protection Act, the legislation at first classified privacy as an aspect of public law in that privacy related to the line demarcation between private and public. Research and teaching on the topic very quickly came to be the province of Legal Informatics, however.

assessing the legal impact of developments in computer technology has thus taken on a more profound content. It is not enough that the computer lawyer understands the technical end of things. He or she must understand society and human rights as well.

The second natural home base for legal privacy is the law of personality – Persönlichkeitsrecht, Droits de la personnalité, Diritti della personalità, Derecho de la personalidad. There we are not dealing with technology only but with the protection of the individual's personality more generally. Where legal education is concerned, I find this association an increasingly fruitful one today. It provides a clearer path to the core of the constitutional state: the notion of the rights of the individual. Let us look briefly at how the law of personality is understood today.

5 The law of personality

5.1 The law of personality and the right to self-determination

The law of personality has a very long history. At the very least, we can trace it back to the law of the person in the Roman tradition. However, as people were far from equal in that era and equality and protection of that equality are central concerns in today's constitutional state, the term 'law of the person' is best replaced with the expression 'law of personality'.[49]

Underpinning the general doctrines of the law of personality is the notion of the individual's right to self-determination or personal autonomy in society. While self-determination has a venerable history as a concept in philosophy, today the foundation of the right is seen as lying primarily in the thinking of John Locke and Immanuel Kant, as well as in that of John Stuart Mill.

---

49 One topic I am responsible for as professor of private law is protection of the personality of the individual. This designation aptly highlights the distinction between the new law of personality and the old law of the person.

The concept of the right to self-determination is very much alive outside of the history books, however. Our conception in the twenty-first century of the interface between the human being and society can be and must be seen in terms of the right to self-determination. On the abstract level of social contracts we view the human being as a free individual who uses his or her right to self-determination within the essential constraints imposed by democracy. In scientific perspective, what we are dealing with here is a theory. We have deeply accepted a theory of the right to self-determination.

The right to self-determination as a right of the individual to decide on maters that affect him or her, to oversee their implementation and to enjoy legal safety in society can be broken down into a variety of components. The following division into five categories is only one possible breakdown but seems to fit today's legal order rather well. I divide the right to self-determination into the following five core components: (1) the right to internal liberty, (2) the right to external freedom, (3) the right to competence, (4) the right to power and (5) the right to know.[50]

Our right to internal liberty can also be characterised as a right to mental inviolability. It is a right protected in any number of provisions guaranteeing equality, freedom of speech, freedom of religion and protection against defamation. A person has, should he or she so desire, the right to be alone with his or her own thoughts and ideas or the right to develop these with other people; outsiders do not have the right by interfering with these rights to compromise a person's honour or equality in respect to others.

In this sphere of regulation, equality legislation and anti-discrimination legislation represent in a very prominent way the new justice of the modern constitutional state.[51] In a similar vein, the protection of a person's honour is assessed not only in traditional criminal sanctions

---

50 For a more detailed treatment in the Finnish literature, see Saarenpää, 'Henkilö- ja persoonallisuusoikeus', p. 272, in Haavisto (ed.), *Oikeusjärjestys*, osa I, Rovaniemi, 2007 (in Finnish).

51 A good example is the role of lesbians and gays in society. See Samar, *The Right to Privacy. Gays, lesbians and the Constitution*, Temple University Press (1991).

against defamation but also in new regulation on harassment and bullying in the workplace.

The right to external freedom primarily refers to the right to be physically alone (integrity) and to move about freely. It has traditionally been protected by provisions on physical inviolability and domestic peace.

One new legislative guarantee of external freedom is the restraining order that has been adopted in many countries. The order, imposed by a court, limits the freedom of movement of one individual in order to protect the physical inviolability, domestic peace and freedom of movement of another. The restraining order applies not only to approaching the individual but also to following, observing and various ways of contacting him or her.[52]

In the new digital network society, external freedom increasingly means the right to remain beyond the reach of various forms of technical surveillance. We now find ourselves in a society where the possibilities for technical surveillance have increased many times over. This development has been one of the focuses of the international debate on the protection of privacy for a number of years. Accordingly, the provisions in criminal and procedural codes on clandestine viewing and listening will have to be updated so that they are consistent with technological developments and the prevailing conception of the protection of privacy.[53]

The right to competence, that is, capacity, is part of the right to self-determination that pertains to our activities in society. The point of departure is the notion of individuals managing their own affairs. Efforts to protect this right primarily involve legal capacity and various

---

52 In Finland, the Act on the Restraining Order came into force at the beginning of 1999. The default situation addressed by the Act at first was repelling attempts by a former spouse to approach the person protected by the order. Since the beginning of 2005, the Act has been extended to allow for restraining orders inside the family.

53 At the beginning of 2007, the Institute for Law and Informatics at the University of Lapland began an extensive survey and analysis of the actions needed to reform the legislation and practices for the electronic surveillance taking place in the IP environment.

other capacities based on assessments of a person and his or her abilities.

On the most general level at which interests are protected, institutional legislation is used to achieve a better balance in the relationship between the weak and the strong. In this context a material right is augmented by an official machinery that protects an individual's rights pursuant to certain legislation. The relevant authority guides, oversees, advises and, in some cases, represents an individual. An illustrative example of such authorities established pursuant to modern institutional legislation are the data protection authorities set up in accordance with the Personal Data Directive.[54] They assist us if necessary in exercising our competence.

The right to power – the fourth component in our right to self-determination – entails the right to decide on what happens to our bodies, our health and information pertaining to us. If we think in commercial terms, we could say, using an expression long in use in philosophy, that in legal terms a person owns his or her body. This perspective has become more important than before now that people's organs and information are being traded as raw material in various markets. However, individuals principally find themselves exercising their right to self-determination in deciding on the use of images of them for commercial purposes. They thus have an informational right to self-determination as regards the information pertaining to them.

In relation to the societal machinery, the right to power means not only an informational right to self-determination but also the right to enforce legal claims in an equitable fashion. Society is correspondingly obligated to provide appropriate and effective machinery to this end.[55] This is an important part of the idea of the modern constitutional state.

---

54 Personal Data Directive, Article 28.1: Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them.

55 Article 14 in Personal Data Directive is a good example of our rights.

The right to know and to obtain information has taken on heightened importance in recent years as part of the right to self-determination and as a means for realising the other components of the right. The time-honoured saying that knowledge is power aptly describes this component of the right to self-determination.

In order to make reasoned decisions on matters pertaining to ourselves and to society, we need increasing amounts of appropriate information on ourselves, society, different organisations and, occasionally, on other citizens. Where society and organisations are concerned, we speak today more in terms of the requirement of transparency. This is a crucial concept in the law of personality, also because when poorly implemented or misunderstood, transparency may well significantly circumscribe individual freedoms. Later in this work, Pieter Kleve and Richard De Mulder take an interesting look at the average person's right to information and in that connection the issue of dissemination of information.

On balance, the right to self-determination may be characterised as an essential social theory that describes our conception of the human being and the rights following from that conception. It is a theory on the level of general legal doctrines that is essential for enacting rights and fundamental rights and for understanding those rights.

Human rights and our basic constitutional rights are the principal guarantees of our right to self-determination. For example, in this perspective the right to information is a meta right of sorts that is furthered through human and fundamental rights. In other words, human and fundamental rights implemented in legislation are not the highest-level rights in the legal system. Above them lie meta rights, which tell us something about them. This level of rights is often forgotten when a person's rights are assessed solely in light of the rights expressly inscribed in the Constitution. The legal superhighway should lead from meta rights to the interpretation of single provisions in favour of the individual unless the law prescribes otherwise.

It is important to point out that the five components of the right to self-determination do not exhaust all aspects of the right. The division can and should be revised to fit the world we live in, i.e., the basic situations

we face. This would bring up the question of the right to life, the right to health and, in the final analysis, the right to death as well; these, too, are all legally significant facets of the right to self-determination. These rights are protected through various provisions and statutes in the law, primarily the law of personality. Among the central aspects of the law of personality today are – this is my personal opinion – identification law, guardianship law, patient law and privacy.[56]

5.2 Central principles and concepts of the law of personality

In proceeding from the general right to self-determination to the level of the related legal principles and legal institutions, that is, closer to the current legal system – we again find five key principles and concepts: (1) respect for the individual, (2) the right to individuality, (3) the right to privacy, (4) identity and (5) control. All of these are crucial when it comes to the individual's relation to society but they have all proved to be highly problematical principles and concepts, in fact ones that have often been overlooked or violated outright.

It should be pointed out that the above principles and concepts are by no means dichotomous, i.e., mutually exclusive. They are interrelated in the sense that the same issue or phenomenon can generally be examined using one or more of the principles and concepts mentioned. On the other hand, each of them is necessary if we are to be able to understand sufficiently the complexity of the position of the individual in the constitutional state. Accordingly, I will take up each of the principles and concepts here briefly.

Respect for the individual is perhaps the most straightforward right in the law of personality but one that is surprisingly often overlooked. Communication, expertise and various forms of the exercise of power may easily take on subjugating and denigrating elements. A case in

56 The right to an identifier clearly reflects the change that has occurred in society. Previously we spoke of the right to a name. Now that people have acquired a number of different identifiers from personal identity numbers to electronic identifiers, it is more appropriate to speak of the right to identifiers.

point is that citizens exercising their rights in society were previously referred to as administrative subjects and patients were regarded as subject to the authority of the care-giving staff. Similarly, various ethnic and religious minorities were judged in a different fashion than the mainstream. What is more, a single criminal sanction readily resulted in a person being labelled a criminal in various connections, for example, in the media.

Proper respect for the individual is an essential element of the law of personality, one enshrined in international human rights agreements. Any legal order exists for the human being; it has been and is to be created with respect for him or her. The importance of this respect can be clearly seen in Article 8 of the European Convention on Human Rights:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

What is worth noting here is that honour and respect are at once the same and different. Respect for the individual is a broader concept than his or her honour. Respect in a legal sense means broad recognition of the right to self-determination in matters related to the individual. This has many manifestations, extending from consideration of equality in drafting legislation to the presumption of innocence in criminal investigations. A person is legally innocent until proven otherwise. He or she is respected. At the end of the day, it is a question of our attitudes.

When we speak of respect for the human being and of privacy, we should draw attention to the question of how provisions are applied when processing personal data: they are primarily applied in order to protect the fundamental rights of the individual. This demonstrates the singular importance of respect for the individual in processing personal data.

Individuality as a basic concept in the law of personality is also an important yardstick for measuring our concept of the human being and, by extension, democracy. Individuality urges us to respect human beings primarily for the unique individuals that they are and want to be. This is connected with the holistic concept of the human being that refutes rationality. It is acknowledged that people are different but without these differences entailing inequality.

The protection of individuality is ultimately a question of the degree of similarity that the constitutional state requires of individuals, their skills, their customs and their culture. When operating at the boundary of allowable individuality, one must address the question of how we relate to the various exceptions from the norms. In all forms of society, social control is directed at persons who behave and act differently.

Among the new and very involved questions affecting everyone where the protection of individuality is concerned are the questions of how people can be protected from the use of psychological tests and genetic tests in the workplace. These challenges have been addressed in the current Finnish legislation, the Act on the Protection of Privacy in Working Life, enacted in 2004. Psychological tests are permitted but require expertise and openness. Genetic tests and even requiring the information needed to conduct them are prohibited. An employment relation does not entitle the employer to information on an employee's genome. I will take up this issue in my article on privacy in working life later in this volume.

The third key concept in the law of personality is then privacy. As we have seen, it can be considered a significant legal institution in its own right. In the context of the right to self-determination, as emphasised above, people are seen as having a right to privacy in society. Democracy – our controlled statutory coalition – circumscribes privacy but by no means eliminates it. If that were the case, we would no longer be living in a democracy.[57]

---

57 Later in this work Mindaugas Civilka and Rita Barasneviciute mention: 'The very concept of privacy is absolutely necessary for all modern democratic societies and hopefully, will remain'.

With the transition to the network society, one hears more and more about the identity of the individual as a fundamental question and concept in the law of personality. The issue as such of course goes back a bit further. It has to do with societal development. One of the prominent pioneers in the field internationally was sociologist Amitai Etzioni, who is nowadays well known in the field of privacy too.[58] We have different identities in different contexts.[59] They depend to a significant extent on the type of information we make use of, what kind of information is available on us and what kind information is used with reference to us.

One crucial distinction when talking about identities is that between profit-oriented organisations and socially oriented organisations. They have significantly different information needs. Where stores want to build profiles on their customers in order to make their operations more effective and to maximise profits, an organisation cantered around a particular hobby or pastime needs to know about its members' skills and readiness to take part in its activities. This has a crucial impact on the identity that we adopt when we interact with – or want to interact with – an organisation.

A look at the different forms of identity in the network society suggests that one would be well advised to use a more precise categorisation of different organisations: profit-oriented organisations, power organisations, service organisations, socially oriented organisations and nowadays virtual organisations (cyber communities).[60]

Profit-oriented organisations operate primarily in the marketplace; power organisations are found in public administration and other organisations that exercise public authority; service organisations offer services without advance commitment that involve information and skills related to an individual's position, characteristics or problems; socially oriented organisations are professional and other organisations

---

58 See Etzioni, *The Limits of Privacy*, New York, Basic Books (1999).

59 In the Finnish literature, professor of sociology Erik Allardt had put things aptly: 'A person's identity consists mainly in the fact that he or she belongs with certain individuals or groups: he or she needs communities and groups that define with who he or she belongs'. This is indeed the case.

60 For example Facebook is some kind of virtual organisation.

that rely on joint characteristics, interests or expertise; and virtual organisations – cyber communities – are organisations that operate on information networks and as yet have no particular legal structure.

It is essential to notice that one's identity may vary considerable depending on the type of organisation one is dealing with. The needs of the organisation are different and for the most part we have the right to choose the kind of identity we adopt in any particular case – unless the law prescribes otherwise. We may have – and in the network society do have – a lot different identities. This is usually not illegal.

It is also crucial to note that identification of an individual and his or her identity are significantly different matters.[61] Typically, less information is required for identification than for the formation of an identity. This distinction is not always realised. For instance, recording a personal identity number on a credit or debit card in connection with a purchase is primarily designed to expedite operations between the seller and the company issuing the card; there is no good reason for doing so if one thinks about the relationship between the buyer and the seller. Identifying the buyer does not require the recording of his or her details for the card-issuing company. However, the market operates on the seller's terms for the time being.

A new type of crime has emerged in the network society where identity is concerned: identity theft. Poor information security on information networks and in the different situations in which networks are used have made identity theft using networks an increasingly common phenomenon, particularly in the United States. Identity theft is easy to carry out and often has extensive repercussions. Accordingly, identity theft has been made a category of crime in its own right there. In this light – this light too – the network society is an interesting phase in social development where legislation and criminal law are concerned. We speak of cyber crimes and try to control those.[62] Irini Vassilaki will be taking up these issues later in the volume.

---

61 We should keep in mind, that identification, authentication and authorisation are different things and even tools for those different purposes should be diverse.

62 In Europe this regulation has been guided in recent years by the Council of Europe Convention on Cybercrime of 2001 (ETS 185). A broader concept connected to technological evolution is digital crime.

Control is perhaps the most interesting and difficult of all the key concepts in the law of the personality and the person. When our focus is on the rights of the individual, we easily overlook societal supervision. We prefer to speak of rights and freedoms rather than their opposites. Yet society is an organisation, one for which supervision of individuals is both an essential tool and an attractive chance to make the organisation more effective. The more comprehensive the supervision, the easier the work of the organisation and its exercise of power become. What is more, supervision is routine in many situations in the work of other organisations as well, those that do not exercise public power.

In the era of the digital network society, it has become very easy indeed to set up technical surveillance. Video surveillance, wiretapping, electronic positioning (decoding), applications of ubiquitous computing and joint use of information systems have opened up opportunities for nearly real-time monitoring of individuals and their activities. When this is seen in connection with the openness of society in the form of public access to events and documents and the freedom the media enjoy in the name of freedom of speech, it becomes all too clear how easy it would be to build a society with efficient – and secret – surveillance. This would, however, run contrary to the liberties of the individual that are central to the modern constitutional state. Accordingly, the surveillance of individuals must be based on a careful weighing of private and public interests and – most importantly – given that statutory and public power are involved, its legality must be carefully supervised.

When one speaks of supervision, it is necessary to remember that the maintenance of public security and order is one of society's central tasks, designed to guarantee the rights of individuals. Limitations on the rights of the individual are usually motivated by considerations of the collective interest. By restricting a single party's rights, one guarantees that the rights of many others are realised. If and when one strives for the utilitarian aim of the greatest happiness for the greatest number, a variety of interests must ultimately be weighed. This is not easy, nor should it be. Genuine democracy is a very difficult way indeed to organise affairs in a state. But it is essential that we approach democracy from the standpoint of the rights of the individual and the law of personality.

6 A brief word on information law

It is still not enough to locate privacy within the law of personality, however. It is an important and essential step but an inadequate one. We must go on to ask what our attitude towards information should be in the network society and what principles of information law we can find.[63]

Information is – as I have already noted above – no longer merely raw material that helps us to achieve an end. It is an important element in society in a new way – on the information superhighway and in other contexts as well. The legislative development that has brought us here began with data protection legislation. When we look at this in combination with the development of the constitutional state and its strengthening of the individual's right to self-determination, it has become necessary to speak more forcefully on behalf of information law and its central principles and not – contrary to the earlier practice common in the EU– merely of information markets and how to regulate them.

In Europe the concept of information law was first introduced by the Norwegian scholar Jon Bing in the early 1980s.[64] Later, in the context of legal informatics, information law has been characterised as a field of law that studies the legal regulation related to, as well as the need and opportunities for regulating, the production, processing, transfer, marketing, protection and storage of information. This basis is fairly straightforward. At work are the rights of the human being in the constitutional state. In a developed form, information law would safeguard our exercise of the right to self-determination and ensure the functionality of the information market.

Previously, the notion that information law was a field in its own right was considered dubious. The argument was that since information is everywhere, it would be difficult or even impossible to find the common

63 Information law is one part of legal informatics. In my teaching the other parts are legal data processing, legal information and IT law.

64 See Bing, *Information law. Journal of media Law and Practice*, 1981, p. 219.

principles needed to give the field an internal consistency. Clearly, rules of form and, say, the protection of personal data were worlds apart – or so the logic went. Rules of form can be described as information-bound rules. They are designed to verify things. The legislation that guides the processing of personal data, by contrast, protects fundamental rights. The question is one of information processing.

Today, however, we can justifiably speak of the principles of information law, the most important of which in my view are the right to know and to information, the right to communication, freedom of information, the free flow of information, the informational right to self-determination and the right to information security. Each of these is a fundamental meta right in the constitutional state; that is, they are goal-oriented, moral rights on the level of social contracts. As a rule, these meta rights have no express, direct reflections as legal provisions on the level of fundamental rights but they are clear backdrops for regulating and understanding human and fundamental rights.[65]

The right to know, which was mentioned above in connection with the law of personality, is a crucial liberty based on the prevailing conception of the human being. A human being has a genuine need to know and to use public and sometimes also private information. In order to exercise his or her right to self-determination in the constitutional state, an individual must have the right to information pertaining to him- or herself and pertaining to society. What we are dealing with here is again the informational dimension of our right to self-determination.[66]

For its part, the right to communication is a new meta right, or at least one appearing in a novel way in the network society. We simply can no longer speak of freedom of speech as a technology-neutral freedom and,

---

65 See also Pöysti, 'ICT and Legal Principles: Sources and Paradigm of Information Law', p. 559, in Wahlgren (ed.), *IT Law, Scandinavian Studies in Law*, Vol. 47 (2004).

66 The right to know is expressed eloquently in section 2(1) of the Finnish Library Act: The objective of the library and information services provided by public libraries is to promote equal opportunities among citizens for personal cultivation, for literary and cultural pursuits, for continuous development of knowledge, personal skills and civic skills, for internationalisation, and for lifelong learning.

for example, speak separately of the protection of confidential messages in communication. What is also essential is the opportunity to use the information infrastructure as the exercise and protection of our fundamental rights has shifted at least in part onto information networks.

The informational right to self-determination is one of the basic elements of the right to self-determination. As individuals we have the right to be alone in society. Supplementing physical privacy and other forms of privacy in the network society we see the rise of informational privacy. Our digital identity also falls within the scope of our right to self-determination. We have an essential right to retain control over information pertaining to us, to keep that information secret if we so desire or to make it public. This has been discussed earlier in conjunction with the right to self-determination.

The principle of freedom of information is a crucial societal principle that has bearing on the functioning of democracy, culture and private economic life. Unlike most important 'raw materials', information must be – or so it has been thought – freely available in private, societal communicative and commercial contexts. In the international debate and in legislation, freedom of information typically is used in a narrower sense to refer to public access to official documents. On a broader level, however, freedom of information is to be counted among the general principles of privacy too. At the same time we must bear in mind that it is not merely the raw material for various activities.

The free flow of information has to do chiefly with education and culture. The development of the knowledge and skills of society and individuals cannot be compromised through secrets or monopolies. Accordingly, the legal system has to provide special rights – above all fundamental rights – that safeguard the free flow of information. Copyright law is a particularly problematic area of legislation in the network society. If greed takes over there, the free flow of information will be hindered. And if peer-to-peer networks or similar arrangements are used for serious violations of copyright, remuneration for such work will be limited and the market will become distorted. When, as we often do, hear people in the Web 2.0 debate advocating the opportunity to

freely pass on and copy any material on a network or that can be made accessible there, this is interference in the status and value of intellectual property in society.

The right to information security is a central requirement for the functioning of the entire information infrastructure in the network society. A democratic society and constitutional state can be built with a reliance on information networks only if proper information security is in place that will safeguard the functioning and use of the infrastructure.[67] We should have a right to information security much as we have a right to other forms of security. This has not been realised as yet at either the national or international level. The information superhighway has never has been – nor is it today – a particularly safe place.

The early European information society policy, which chose codes of good practice in developing information security, was an odd choice if we think of human rights. The importance of the new infrastructure was not realised right away.[68] The establishment of ENISA, the European Network and Information Security Agency, was still not much of a step forward on the road to regulation. And the resolution of 2006 continues on what is an essentially sound but legally inadequate path when it comes to developing an information security culture.[69]

These general principles of information law give a clear indication of just how important a field information law is. Without it, we face the prospect of these concerns becoming scattered among different fields of law, to be regulated without a proper, comprehensive vision of the issues involved. We are witnessing the negative impacts of just such a situation in the network society today: it is a society of fragmented and deficient information legislation without information infrastructure legislation.

---

67 See also the opinions of Jari Råman later in this work.

68 Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security still represented a loose approach that avoids more detailed regulation.

69 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – A strategy for a Secure Information Society – 'Dialogue, partnership and empowerment' {SEC(2006) 656} /* COM/2006/0251 final.

Clearly, we confront issues of privacy – our right to privacy – in the field of information law as much as anywhere else. In terms of legal education it is essential that we be able to bring together different principles in assessing the legal dimensions of privacy. In particular, reconciling the private and public spheres is a significant challenge for both teaching and professional skills in law.

7 General Conclusion

When we speak of privacy, we must always remain mindful of its direct link to human rights.[70] We have the right to be alone; we really do have.

In an advanced constitutional state, this right is a strong liberty that we enjoy. Regardless of what legislation one links to privacy when teaching law, privacy's connection to human rights must not be severed or even obscured.

Yet this is often what happens when one first becomes acquainted with privacy, or the provisions enacted on privacy are only a minor component of a broader field of law or the relevant legislation. Fragmentation weakens privacy as a fundamental right and it easily becomes overwhelmed by critical claims that it is detrimental and inefficient. For this reason, privacy as a visible part of the law of personality, of information law and in general of legal informatics has a prominent role to play in maintaining and illustrating our conception of the human being.

It is in this way that we keep open the legal highway of liberties from human rights to legislation and its implementations. In this perspective, the law of personality and legal informatics belong among the general legal sciences. They are essential law dealing with our conception of the human being.

We often speak of the information superhighway, so it might be once again worthwhile exploring my concept of the legal information

70 That's why you find in this a lot of notes to the European Convention on Human Rights.

superhighway. This would lead us – or should – from human rights to respect for privacy in enacting and applying legislation. Let us use the expression in earnest when talking about privacy and implementing privacy in the legal context. At the same time, we must consider how we can equip that highway with the right and right number of traffic signs.

When dealing with privacy in the legal sense, we must inevitably always come to terms with the consequences of violations of privacy. As a matter of principle, we are entitled to compensation when our privacy is violated. Some of the invasions of privacy – a significant number in fact – carry criminal penalties. The topic is crucial. All too often we encounter in practice a mentality – in police investigations, for example – suggesting that invasion of privacy is not a terribly weighty concern. Oh, but it is.[71]

I mentioned above the difficulty of finding a tidy compartment for privacy amid the categories we are used to working with in law and in the teaching of law and the description I have given here no doubt reinforces the notion that no such place exists. I spoke in favour of discussing privacy in the contexts of legal informatics, the law of personality and information law. Shouldn't this if anything results in the fragmentation of the subject? Indeed, it will unless we are vigilant enough to keep the general doctrines visible. This is where the law of personality and legal informatics can play a crucial role. Both are counted among the general legal sciences, and it is precisely the task of general sciences in the discipline to bind together what the legal doctrines of the various special fields, with their wealth of detail, would tend to scatter. General doctrines of law today can be increasing likened to elevators between human rights and interpretation of the law on the everyday level.

---

71 Later in this work Tatiana Stefanova points out: 'The most significant problem in Bulgaria is that even the existing act is not being observed. No one has ever heard of any penalties for a personal data administrator'.

CHAPTER 2
GENERAL DISCUSSION

PRIVACY CONCERNS IN THE INFORMATION SOCIETY: WHEN WILL WE HAVE A DATA PROMOTION ACT?

Pieter Kleve and Richard De Mulder[1]

1 The world has changed (1)

Information technology is fundamentally changing society as we know it. A new era has arrived: the information age. This is the most obviously apparent in communications. Events from all over the world can be relayed by the mass media within the shortest time. It has deeply affected economics: markets have become global. Indeed it would not be an exaggeration to describe the world as one market place.

These changes appear to have brought economic progress to the western world. Even former communist countries have converted to market economies. Exchanging goods and services via the market mechanisms instead of by controlling polices has been shown to be more advantageous. Some commentators are so convinced of the triumph of the liberal democratic state that the 'end of history' has been announced.[2]

The exchange of information is a characteristic of the market. If this information exchange becomes easier and cheaper, then the markets will function even better and become 'global'. Information directs the

---

1 Prof. Dr. R.V. De Mulder and Dr. P. Kleve work at the Centre for Computers and Law, Faculty of Law, Erasmus University Rotterdam.

2 Francis Fukuyama, *The end of history and the last man*, New York, 1993.

processes. However, information is more than this: it has also become a primary product. In societies saturated with material goods, the information industry has begun to have a huge influence on our behaviour. The same tendency, however, can be seen in less materially affluent lands.

At the same time, 'marketing thinking' has made huge headway. Business administration has gone through a process of becoming more scientific and technologically advanced. The successful businessman is therefore a rational and well-informed decision-maker. When a manager consults a lawyer, he can hardly be expected to be happy if the lawyer answers 'it might not pose any problems' or 'we might win the lawsuit'. Lawyers can expect their clients to become more critical. If a client has to decide whether to start an action, he needs certain information. For example, a client expects to be a € 100 000 richer if he wins the action. Before he decides to sue he will want to know what the legal or other procedural costs are (lets say € 70 000) as well as the chances of winning the suit. There is no point in proceeding unless the probability of success is at least 70%. The manager will require a sufficiently reliable estimation of this probability before deciding to take the case to court.

In the modern economy, marketing, production management and finance are influenced by rational decision-making. Modern managers talk in terms of expenditure and profit, and of the probability of occurrences taking place. Decisions are made on the basis of knowledge of these variables in the past and the expectations about them in the future.

2 Globalisation

Technology has increased mobility and thereby accelerated the process of globalisation. Not only can people travel more quickly from place to place, but communication has become much easier and faster with the advent of Internet and the mobile phone. The world order as we have known it is changing and that makes directing, controlling, enforcing traditional norms or obtaining an overview of society in general more difficult. Change brings uncertainties with it.

In studying how people behave, an initial analysis reveals that rationality plays a role here too. In this respect, a revolution has taken place over the last ten to twenty years. We are referring here to the paradigm (according to Kuhn)[3] that can be used to study human behaviour, and to try to explain, predict and direct it. Many social scientists base their research on a sociological model of man. This model states that people will behave in a way consistent with the norms of the group to which they belong. However, modern economists usually use a different model of man, the *homo economicus* or the REMP (the resourceful, evaluating, maximising person).[4] Processes are studied from the perspective of methodological individualism, in other words described, explained and predicted on the basis of the behaviour of individuals. The REMP is an individual who tries to maximise his own utility in all his decision-making. Ideologically, that may sound undesirable. However, in practice it is often the case that individuals see their own interests are served by taking others into account and by interacting with the outside world in a creative and anticipatory way. Negotiation is natural for the REMP.

3 Changing norms and concepts

The REMP is a relatively new concept. The rational model of man appears to have become the dominant way of thinking. Emotions, norms and values, even irrational elements, seem to be subject to radical changes. For example, the ideas about privacy appear to have changed. In the recent past, it would be unacceptable for many people to show their naked bodies, or naked emotions for that matter, to other people. At the same time it would be immoral or at least 'not done' to observe these things other than under specific circumstances, such as in a doctor-patient situation, or as a form of art. These days, people show their emotions and bodies to mass audiences and seem to feel

3 T. S. Kuhn, *The structure of scientific revolutions*, Chicago, 1977 (1962).

4 M. C. Jensen and W. H. Meckling, 'The Nature of Man', *Journal of Applied Corporate Finance*, 1994-2, pp. 4–19.

perfectly happy with it. A related concept, anonymity, is also subject to different norms and values. Some people claim that they have a right to anonymity as well as a right to take on a different identity, for example while surfing the Internet and chatting with others.

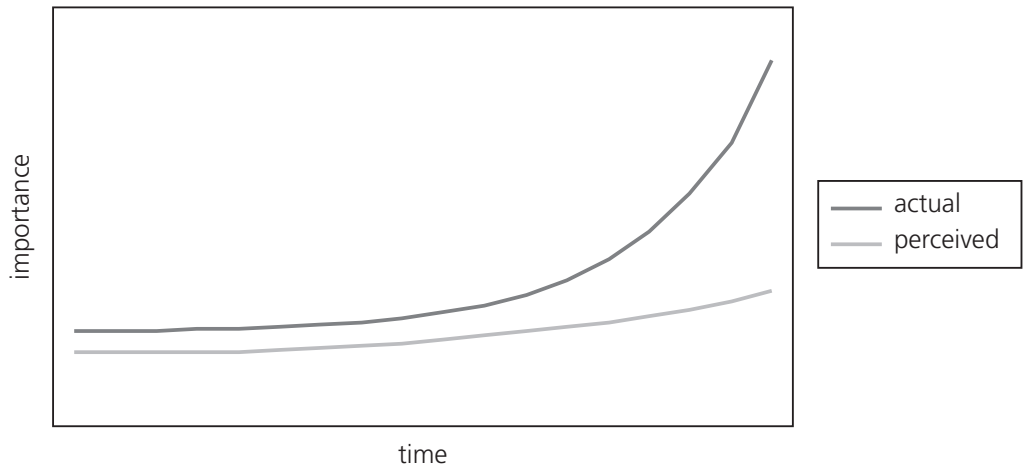
This shift in norms is evident in various situations. Freedom of information and intellectual property are clearly seen in a different way from in the past. The Internet has made it very easy to infringe the intellectual rights of others and at the same time many of those who would have been seen as criminals in the past, are now claiming their 'freedom of information'. The availability of information allows the reliability of accountants and firms, for example, to be challenged, as well as the enormous salaries and option plans for some managers in businesses and even in 'privatized' state bodies. On a perhaps somewhat cynical note, although war is nothing new, it now seems to be acceptable, to some at least, that thousands of civilians are killed during military operations to 'bring democracy' to other nations.

4 New legal questions in the 'information society'

Information technology has, without doubt, made an impact on society. Technological advances, in general, have been considerable over the last 150 years. It is a period that has seen the Industrial Revolution superseded by the Information Revolution. Technological applications are numerous and various, and have become integral to the society we know today. That technology used for the processing of personal data is, in this context, not extraordinary. Indeed, its application is rather obvious given that the techniques are easily applied and that society as a whole has acquired a more technically orientated character.

In the graph below the idea expressed is that the actual impact of technology on society is far greater than perceived by most people. Furthermore, the discrepancy between actual and perceived impact is growing.

Technology has also affected people at an individual level. That there are more and more options open to people, and more and more



information, makes it necessary for people to approach decision-making rationally. Increasing wealth and economic independence have prompted a process of individualisation. Traditional social structures have become less a matter of course, indeed they are sometimes experienced as obstacles in the way of reaching individual goals. The rational model of man is arguably now the best predictor of human behaviour.[5]

The question that arises is whether the information society is simply a modern term meaning nothing more than an increase in information together with an increase in global distribution and access possibilities, or whether a more fundamental change is taking place. This question is important because fundamental changes demand creative and, in particular, unorthodox approaches to new social issues.

Four stages can be pinpointed in the development of technology:[6]

— The first stage is characterised by the ability to influence spatial structures, for example building a hut or a house.

— The second stage consists of the possibilities for changing spatial structures, for example the wheel or hinged doors.

---

5 See note 2.

6 J. Verhoeff, 'Is de chip in de hand te houden?', in *Spectrum Jaarboek*, 1980, p. 247; also R. V. De Mulder, *Een model voor juridische informatica* (A Model for Legal Computer Science, with summary in English) (diss.), Lelystad: Vermande, 1984, p. 95; P. Kleve, *Juridische iconen in het informatietijdperk* (Legal Icons in the Information Age, with summary in English) (diss.), Rotterdam/Deventer: Sanders/Kluwer, 2004, pp. 55 and 361.

— The third stage gives the possibility to control the powers that are necessary to bring things into motion. The invention of the steam engine announced the age of the 'Industrial Revolution'.
— The fourth stage offers the possibility of using the energy stored in an artefact to allow the artefact to start or stop itself, etc.

The information age can be associated with the fourth stage in the development of technology. It is characterised by the ability of machines to process information – something that formerly only people (and animals) could do – just as the third stage was characterised by the ability of machines to perform labour. The computer is to information processing what the steam engine was to the use of energy in artefacts. For this reason, this age is referred to as the 'Information Revolution'. It should be clear, that the answer to our question is that the information society is essentially new because nowadays also machines can interpret data.

The information society has brought with it many new questions, which arise in various areas. These questions range from those on intellectual property, such as the legal protection of software, chips and data, to so-called 'e-Business', with its implications for commercial and contract law, into criminal law, with concerns for enforcement and cross border issues, to questions concerning privacy, which is the subject of this article.

Although, given the nature of the technology, these questions may be new, not all of them raise new legal issues. It is, therefore, not the case that all the new questions which arise from the information society need to be dealt with by new laws. It should not be an automatic reflex for lawyers to resort to legislation when confronted with new questions. A balanced approach would first dictate an examination of which legal domain would be the most appropriate to look for a solution. Then existing legal rules could be consulted. The next step would be to examine the applicability of these legal rules by making use of existing doctrinal interpretation. Only then, if the conclusion is reached that an interpretational method would fail to secure a responsible and desirable application of the rule, should the issue of new legislation be raised. If, as a last resort, a decision is made to amend the law, another issue should be examined.

Does the desirability of a new law stem from the incompatibility of principles or terminology in the existing law with the new factual situation, or does it arise from social developments themselves and a shifting, or even a transformation, of the norms and values behind those principles and terminology? With respect to the latter option, this is not so often the case although the chance of such a shift is greater where the paradigm has altered and where there have been radical technological developments. That is, however, the position at present.

If this approach to legislative initiative is taken into account, then it is rather surprising that in the last few decennia so many new laws have come into force as a consequence of information technology. Examples of law that would have not survived the first stage would be the software, chips and database laws. These new laws have not achieved anything that the application of existing laws to the new questions could not have achieved. Take the law on electronic signatures, for example, where the presumption was made that the terminology of the old law was incompatible with the new factual situation. However, had existing doctrinal interpretation been applied (an 'electronic signature' is still a signature), these new laws would simply have been superfluous.

Examples of the shifting of norms can be found in software and database laws and in file sharing and spam. With respect to software and database laws, when intellectual property laws were declared applicable to software and database, in the slipstream an implicit shifting of norms was implemented. In the case of software, this has taken the form of a clause forbidding decompilation, and for databases a de facto extension of the exploitation rights with a use right.[7] These are actually examples of a shifting of norms where it is not clear if this had been sufficiently realized. As to file sharing, this is an example of a social development which inevitably have to lead to a shift in norms in the

---

7 P. Kleve, R. V. De Mulder and C. van Noortwijk, 'The Amazing Diversity Framework of the Intellectual Property Rights Harmonisation', *Globalisation and Harmonisation in Technology Law, proceedings 21th Bileta conference 06-04-2006*, Brockdorff et al. (eds.), Bileta: Malta, ISBN: 90-5677-286-4.

form of an exception to copyright rules in order to allow copying (in the broad sense of reproduction and transformation) for private use.[8]

The answer to spam is, of course, 'white listing' not legislation. By white listing is meant that people may use the technology to decide for themselves who has access to their communications. The increase in spam will make white listing, allowing access to 'known senders', more attractive than the nowadays frequently used option of black listing, the method of blocking 'undesired senders'.[9]

Why is white listing the obvious answer to spam? That has to do with the fundamental characteristic of the information society, namely that in the fourth stage of the development of technology machines can also interpret data. Until the advent of this fourth phase, white listing was simply not an option because this could not be achieved effectively. The information society has made a fundamentally new problem solving system possible, one that we are discovering the possibilities of step by step.

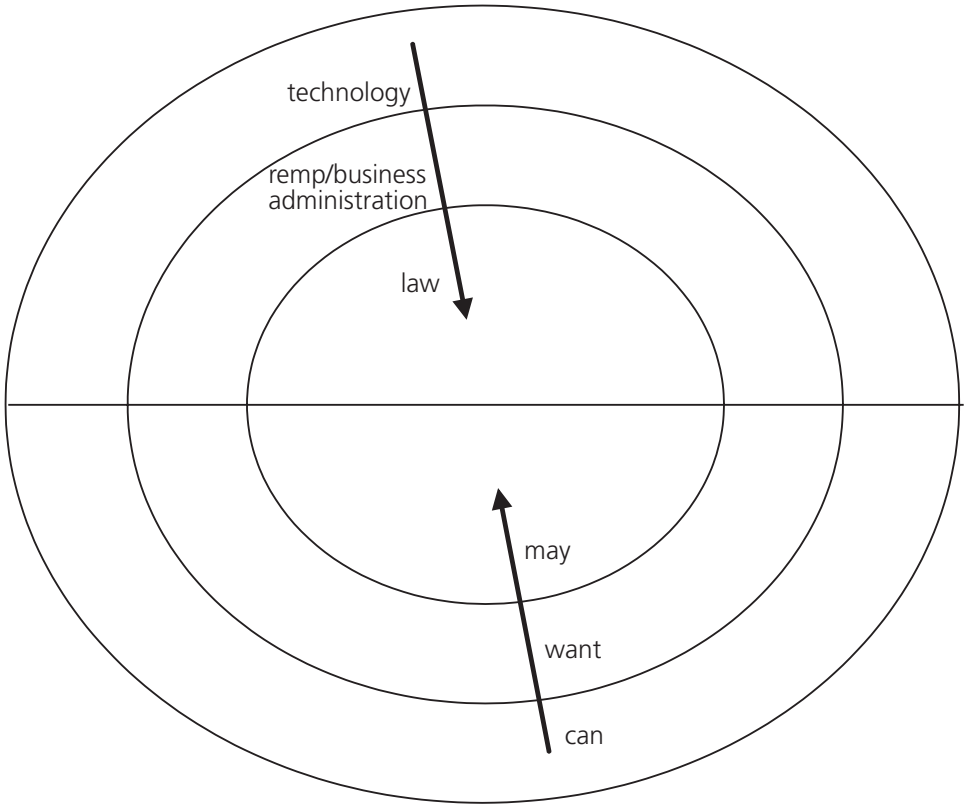
The consecutive dependence relationships between technology, social developments and law are represented in the following model.

The model consists of three concentric circles. The basis for this model is positivism, in other words that one reality exists and that that reality can be known. The outer circle encircles 'can', the technology. The middle circle covers that which people 'want', within the limits of what is possible, using the REMP as the model for describing, predicting, explaining and steering human behaviour. As a multidisciplinary science, business administration offers a structure to obtain insight into (individual) utility considerations. Finally, the inner circle is the domain of law, of 'may' (and 'must') of demands and authorisations, of norms and facilitation. Law is an artefact for the facilitating of human

---

8 P. Kleve and F. Kolff, 'MP3: The End Of Copyright As We Know It?', Proceedings of the IASTED International Conference Law and Technology (LawTech'99), IASTED: Honolulu, Hawaii.

9 It would seem that the *principle* of white listing is better known by law makers (for example in the European Union) than the technique, given the law has chosen for a so-called 'opt in' regime (rather than an 'opt out' regime) for sending unsolicited commercial communication.



Conceptual model for integrated legal science

interactions, for example in the form of 'property', 'majority', 'marriage', 'purchase'. Through fixing norms and sanctions it delineates the external boundaries of human 'want'. Law can steer 'want', but is not decisive, and is itself limited by 'can'.

5 Changing norms and concepts – The privacy concept

In an article by Warren and Brandeis, written at the end of the nineteenth century, a definition of privacy was laid down based on a definition by Judge Cooley.[10] That definition, the 'right to be left alone', is still the current one. Warren and Brandeis describe the development of the concept of privacy from, at the outset, the protection of life and

10 S. D. Warren and L. D. Brandeis, 'The Right to Privacy', *Harvard Law Review*, vol. IV, December 15, 1890, no. 5.

property towards the recognition of men's spiritual nature, of his feelings and his intellect: 'the right to life has become the right to enjoy life [...] and the term "property" has grown to comprise every form of possession, intangible as well as tangible'. Thoughts, emotions and sensations should be covered by a more general right to privacy.

With respect to a general right of privacy, one school of thought is of the opinion that everything that a general law on privacy would protect, is actually already sufficiently protected by property laws, laws dealing with offences against the person and human rights, such as the right not to have private communication tapped.[11]

For some, this offers a too limited vision of the concept of privacy.[12] Yet another school of thought considers that the influence of technology demands a more coherent legal concept of privacy, in which a broad scale of privacy problems can be designated.[13] However, what is interesting about the article by Warren and Brandeis is that it was written as a reaction to 'recent inventions and business methods'. This referred to the growth of the 'yellow press', which was a consequence of the developments in photography and printing, through which 'Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops"'. When positioned within the above mentioned four stages in the development of technology, what attracts attention is that the elegy of Warren and Brandeis takes root in the transition into the 'Industrial Revolution', whereas we are now facing the transition into the 'Information Revolution'. Major transitions apparently lead to strong reactions. The question that is posed in this article is whether such reactions belong to a time long since passed. In other words, isn't privacy – the right to

11 J. Thomson, 'The Right to Privacy', *Philosophy and Public Affairs*, 1975-4, pp. 295–314.

12 F.e. T. Scanlon, 'Thomson on Privacy', *Philosophy and Public Affairs*, 1975-4, pp. 315–22.

13 D. Solove, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*, 2006-154, pp. 477–564.

be left alone – rather a barometer of the level of technological development then a universal and non-negotiable basic right?[14]

An examination of social developments leads to the inevitable conclusion that since the time of Warren and Brandeis the 'right to be left alone' has been diminished. In a society that has become so complex, with so many relations of interdependence, that conclusion is hardly surprising. Limitations on privacy are often associated with totalitarian regimes. However, an unlimited right to privacy could have made the present democratic state, with its rule of law and high living standards, equally impossible. A considerable number of laws are based on infringements of privacy in favour of the operation of the public administration, in order to enforce public order, safety and security. In addition to this infringement of privacy with respect to the classic constitutional relationship between public authorities and citizens, there would also appear to be a similar tendency in the private sector.[15]

The 'yellow press' has become an important element of the amusement industry. Instead of the limitations proposed by Warren and Brandeis, this form of operation has now spread to the television and the Internet. Apart from the philosophical and principled question of whether there is such a thing as a universal and inalienable right to privacy, in practice it would seem such a proposition is unrealistic. To take part in modern society, the citizen is expected to have a job, a bank account, a social security number and health insurance, details of all of which may have to be provided to various other parties. Enforcement of the right to be left alone seems to be confined to situations where freedom of movement is at issue. In the classic constitutional relationship, this comes to the fore in matters such as freedom of the press, freedom of association and meeting, the freedom to gather information. With

---

14 See for the cultural, economic and technological relativity of privacy e.g. A. Allen, *Uneasy Access: Privacy for Women in a Free Society*, Totowa, N. J.: Rowman and Littlefield, 1988; A. Moore, 'Privacy: Its Meaning and Value', *American Philosophical Quarterly,* 2003-40, pp. 215–27; F. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press, 1984.

15 B. J. Koops and A. Vedder, *Opsporing versus privacy: de beleving van burgers*, Den Haag: Sdu Uitgevers, 2001.

respect to the horizontal operation of constitutional rights – the relation between citizens – it affects such matters as aggravated assaults, or threats of violence, harassment and stalking, libel and slander.

Westin gives a very broad definition of the concept of privacy: 'privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[16] Westin even goes as far as to ascribe to institutions a personal life. That is remarkable given legal persons normally have a more onerous duty to make certain matters public than private person (for example compulsory registration, in some countries a minimum level of share capital, and financial obligations).

This definition is, however, of particular interest in this article because Westin lays the emphasis on communication. His definition seems to have taken shape with the rise of telecommunication and the possibilities for tapping these communications. It is also interesting because it can be considered representative of the way in which the concept of privacy was approached in a time in which many countries implemented specific privacy laws (for example, to regulate tapping) as well as more general laws in the form of data protection acts. Whether such laws are practical and/or desirable is a matter that will be dealt with below.

The increased attention for privacy issues seems to have been influenced by technological developments, with privacy moving from a feeling to a more technocratic concept, which in turn is reflected in the legal approach. The more difficult to determine concept of normative privacy now partly overlaps the less controversial concept of data protection.[17] The data protection concept is based on formal rules regulating how data is dealt with, without these being placed in a substantive or normative framework. That the concept of privacy is being diminished is reflected in the popular 'analytical approach', in

16 A. F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967.

17 F.e. the 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.

which privacy is divided up into a spatial dimension, a physical dimension, a relational dimension and an informational dimension. Both developments reveal a shift in the way in which the concept of privacy is experienced; privacy appears to be a difficult concept. Below a number of illustrations will be given.

If freedom of movement, the right to go and to stay where one pleases, is considered to be an important element of the spatial dimension of personal privacy, then the question arises whether the present extensive checks on baggage and persons at airports, the information demanded by the American authorities (where travel to the USA is concerned) is an infringement of personal privacy or a condition for it. If, consequently, some of the physical aspects of privacy are examined, then it becomes clear that the measures taken to protect the safety of persons and goods are, in principle, measures that promote privacy.

With respect to relational privacy, what is immediately apparent is the considerable number of dating programmes on television, dating agencies, the phenomenon of 'speed dating' via Internet and SMS and the multitude of 'news groups' and chat sites. Put against a backdrop of informational privacy, the picture emerges of a shameless exhibitionism hand in hand with an equally shameless voyeurism. Without any apparent embarrassment, the most intimate details exchanged on a mobile phone are shared with others, often random fellow travellers or those who just happen to be in the lift at the time of the call. Similar intimacies, only now with images, can be encountered on countless personal home pages and webcams.

Once 'Big Brother' was a nightmare scenario, set in a future, technological world. Now various countries know it as a television programme. Television has become beset by reality shows and live soaps. Web logs in gossip are both information as well as entertainment.

Given this context, the decision of the European Court in the Bodil Lindqvist case seems to have come from a different universe.[18] In the

18 European Court, 6 November 2003, case C-101/01. This case is originally from Sweden.

first place, the use of her personal page to describe the activities of several of her colleagues – in the phrasing of the Court, 'in a mildly humorous manner' – is just contemporary use of modern communication means, similar in manner to the way in which nowadays millions of people set up there personal pages. Secondly, when actions carried out with the help of computers are characterised as 'processing of personal data' in the sense of the data protection directive,[19] because they are carried out with the help of computers, this leads to the erosion of the whole concept behind the term 'processing'. Processing becomes a completely unworkable concept, which furthermore ignores the fact that processing is only one of the functions of a computer.[20] In informatics, processing means that input data is processed, whether or not together with other data, into new data; the input data is interpreted by the computer (the fourth stage characteristic in the development of technology). However, what is concerned here is the judging whether this sort of behaviour is or is not desirable and this consideration should affect the concept of privacy.

6 The world has changed (2)

Generally speaking, the most important factor in determining the development of society is technology. Knowledge of technology is, therefore, vital in order to describe, explain, predict and influence social developments. The advent of information technology has led to new aspects of society.

6.1 Network society

We live in a 'network society', a term that covers various types of relationships. For example, the economies of different countries become so intrinsically linked that there is a high level of mutual dependence. Individuals may find it important to build up a substantial personal

19 See note 15.

20 In addition to processing, the functions of computers include input and output, storage and telecommunication.

network. Businesses have to participate in networks, not just at a commercial/economic level, but also with respect to technology. Participation is survival. Businesses form so-called 'virtual organisations'.[21]

The relevant technology in this respect is, of course, the Internet and the increasing convergence of the Internet with other forms of communication, such as telephone and television. Children are brought up with personal computers and a mobile phone. Apparently, information technology fulfils a need to be in contact with the outside world, a need that does not appear to be inhibited by considerations of privacy. A 'right to participate' seems to become the new constitutional right in the information society.

6.2 Service society

Modern societies are transforming from production societies to service societies. In order to offer a service, it is necessary to know what potential clients want. This becomes increasingly difficult in an urbanised society. Furthermore, the mobility of both client and personnel makes such knowledge of a fleeting nature. In the information society, personal contact is often replaced by an exchange of electronic data. Information technology has made it possible to improve the level of services, but this can mean that citizens are faced with a choice between an improved service or protection of their private lives. The 'right to enjoy life', once a consideration for privacy protection,[22] may now be a reason to surrender that protection.

6.3 Knowledge society

Society is not only in transition from a production society to a service society, but also to a knowledge economy. Knowledge allows increasing complex issues to be solved or better solutions to be find for less

---

21 This term is used to indicate a cooperation between independent legal entities that work together as if they form one organisation, as well as the cooperation between departments, branch offices and sub-offices as if these offices were located in one physical building.

22 See the quote by Warren and Brandeis cited above.

complex issues. The knowledge economy is reflected in the way products are developed and the way in which services are now provided. It plays a role in the way in which education is approached.

Here again, it is the Internet which acts as the facilitating technology. Internet makes it possible to participate in chains of production and makes a whole variety of services available. The Internet also plays an important role in education, as well as influencing the way an individual gathers information. If 'the development of the individual' is considered to be one of the objectives of privacy protection, then a choice has to be made as to whether that development will not be better achieved by using the Internet.

6.4 Safety and security

One opinion that is often voiced is that people find it unpleasant to be spied on and to know that their movements can be checked out later. However, when members of the public are asked if they would like to see more uniformed policemen on the street, the vast majority answer in the affirmative; most people apparently find a police presence on the streets reassuring. Is it, then, a question of finding the right balance: yes to surveillance in itself but no to surveillance in an extreme form?

With respect to the relationship between privacy and safety, the question seems to be how much privacy are we prepared to surrender in order to increase our safety?[23] When law students ask us what we think of the fact that the US National Security Agency secretly monitors Internet traffic using the Echelon program, our answer is what they would think if the US National Security Agency would not do this. These two basic rights, the right to privacy and the right to protection, seem to be uneasy partners. However, the question itself is not as straightforward as it may seem. Why is it that most of us are perfectly

23 F.e. Moore (A. Moore, 'Employee Monitoring & Computer Technology: Evaluative Surveillance v. Privacy', *Business Ethics Quarterly*, 2000-10, pp. 697–709) argues that trading privacy for security strikes the wrong balance and in many cases undermines both. See also the quote attributed to Benjamin Franklin (published in *An Historical Review of the Constitution*).

prepared to have our baggage examined in airports but resent our past being looked into? And if our past was looked into, would the examination of our baggage no longer be necessary? Privacy and safety do not have to be opposites, but the one can affect the other. It would be hard to think of something that was a greater infringement of a person's privacy than having to undergo a body search, or having personal belongings searched, or even the threat of it.

Constitutional rights have a special place in the relationship between the authorities and members of the public. Rights and freedoms are formulated that are intended to protect citizens against the arbitrary use of power by the authorities. In the course of time, the concept of the horizontal working of constitutional rights has developed. The right to respect for personal privacy is not just between the authorities and the public, but also between members of the public themselves. In former times, it was necessary to protect citizens from the arbitrary behaviour of the authorities (or the monarch). Today, in the developed democratic states of the West, it would seem that the 'danger' emanates not so much from the authorities, which are open to public review, but from those who reject authority. Fear restricts the movements of citizens, either because they are not sure if it is safe to take an airplane or the local metro, or to voice a possibly controversial opinion. It would now appear that it is often the authorities that champion constitutional rights, rather than being the body which could be guilty of flouting them. The question now before us is which aspects of privacy must weigh heavier in a given situation? The means used will depend upon how that question is answered.

Another question that comes to the fore in determining whether someone's privacy has been infringed, is what criteria should be used. Where there is a choice or where there is an advantage to the person concerned, it is less likely that an infringement of privacy will be considered as unacceptable. In order to respect one's private life it would seem more important to formulate these criteria rather than paying attention to actual forms of behaviour, as this does not sufficiently take into account the personal character of privacy.

However, the choice for applying surveillance technology, or being placed under such surveillance, is often not one made at an individual

level. This runs counter to the present day tendency whereby the individual plays a central role. That is because the protection of privacy is not just an issue for individuals; it must also take collective needs into account. Paradoxically, it would seem that the 'protection' of constitutional rights justifies a certain selective infringement of those rights. This can be explained in terms of the relative utility of the application. To the extent that it affects individuals, legislators must be careful not to make unwarranted generalizations, as this could result in the public rejecting the use of technology. This would be a pity as research into such matters as the registration of DNA and the use of extensive databanks holding sensitive information, has shown that many people attach more importance to safety than to privacy.

The influence of technology on safety is twofold. On the one hand, social safety is increasingly threatened by technology, in particular the use of weapon technology (chemical, biological and nuclear), and the use of computers and communication systems[24] is often said to be dangerously monopolized by state authorities and large corporations.

On the other hand, technology can be deployed precisely to promote social safety. A whole range of technological applications to enhance safety is already available: security systems (such as camera supervision), the identification of both goods and persons (the tagging of products and people as well as tracking and tracing methods based on GMS or GPS or DNA), information processing (image processing, biometrics, sensor fusion and data mining), communication and process support (group decision systems, virtual reality, coordination systems) and, finally, in law enforcement and criminal investigation (shared reporting systems, camera supervision systems and the 'information pistol').

6.5 Information technology and social control

The use of information technology does not always entail an extension of an existing competence. It is more often a means by which

24 E. R. Muller, R. F. Spaaij and A. G.W. Ruitenberg, *Trends in terrorisme*, Alphen van den Rijn: Kluwer, 2003, p. 87 e.v.

that existing competence becomes more effective and efficient. The simple fact that something is useful, or more useful than it used to be, leads in itself to a certain shift in norms. It is, however, important that it is borne in mind that technology is itself primarily a 'means'; it is a means to make possible those things people find useful. Information technology is, in this sense, a tool to enforce norms, in the same way as the law itself is a tool to enforce norms.

When people go on holiday, they may ask their neighbours to keep an eye on the house. If someone hangs around the deserted house, the neighbours might ask whether they can 'be of help'. That a police car would drive past the house more often while they were gone would also be welcome. In former times, it was far more common for people to keep an eye on the behaviour of others. There are various reasons why that is less the case today. One reason is the tendency noted above for increased mobility and individualization. People are also aware that an intervention may not be without risk.

The social control and cohesion typical of society several decades ago no longer exist, at least not in that form. It is generally recognized that social control and social cohesion have a useful function. The gap left by the lack of social control can be filled by the use of technology; it can give social control and social cohesion form once again.[25] In any evaluation of information technology, factors to be taken into account are not only the costs and disadvantages, but also what it contributes and its social advantages.

6.6 Information technology and solidarity

Whether a decision is made to use information technology seems to be largely a matter of efficiency. Efficiency is a norm more often associated with the private sector, yet this consideration is relevant with respect to the public sector as well. Although it would seem that efficiency as a norm has achieved greater acceptance in the private sector than the

25 A contrary concept is that, for example voiced by Schoeman, that privacy actually provides protection from a too extensive social control (F. Schoeman, *Privacy and Social Freedom*, Cambridge: Cambridge University Press, 1992).

public sector, it is not the case that the aim of efficiency is without criticism in the private sector, for example with respect to commercial profit at the cost of service.

When this criticism is analysed, it would appear that the services sacrificed are those that were not sufficiently profitable or provided at a loss. What the private and public sectors share is that those individuals who are affected want a result that suits them, even if it is disadvantageous for others, although they are not personally willing to contribute more. This leads to a conservative approach. Efficiency as a criterion is nevertheless an important guarantee of solidarity. The use of technology can promote efficiency.

An important question is to what extent people will be prepared to contribute financially to an expensive system of means redistribution, in which not all those who are intended to benefit from the redistribution do so, and some of those who do benefit were not intended to do so. Many of the organizations charged with the task of redistribution are founded on the principle of solidarity. This solidarity could be in the form of unemployment benefits, insurance, housing or social security benefits, contribution to church funds, or charitable organizations.

An important factor here is the tendency pointed out above; the increasing complexity of society, increased mobility and individualization. As a consequence, it has become more difficult to reach those who have the right to such assistance, and more difficult to prevent fraud by those who do not have the right to this assistance. This puts solidarity under pressure and makes it crumble away. Information technology contributes to efficiency, for example to prevent the fraudulent use of social security systems, and indeed its use could be demanded.

In practice, it is no longer possible to implement complex legal projects without the use of technology. Technology has, in turn, influenced the content of these legal rules, as the automation process itself may impose certain requirements and restrictions. Creating and keeping consensus depends on correct implementation, certainly in the long term.

Using technology as a means of control or as a means to support the enforcement of control, could give those involved a greater feeling of certainty. It is because we have computers that we can refine general rules, so that relevant individual circumstances can be taken into account. It is this very ability to distinguish between cases that makes it possible to uphold the principle of equality. In this way, technology could contribute to a feeling of solidarity.

6.7 Subsidiarity and proportionality

The use of information technology cannot, in general, be seen as irreconcilable with the right to the protection of personal privacy. Safety is not in opposition to privacy, but an aspect of it. Furthermore, it could be argued that the right to personal privacy is not an absolute right; other factors can, and sometimes must, be taken into account. Thirdly, it has already been pointed out that the scope of the concept of privacy, and its interpretation, must be seen against a background of technical and social developments. There are positive effects, such as the use of technology to increase the usefulness of services to the public and to respect the enforcement of basic rights.

It is often not necessary to change the law in order to implement information technology. Technology can already be implemented within the existing legal context. However, the use of technology can lead to shifts in norms. With respect to information technology, just as with other means, attention should be paid to the legal issues that may arise from one situation to another. The boundaries for legal application are usually determined by the principles of subsidiarity and proportionality. In setting down legal conditions for use, it should be realized that a too conservative approach could unfairly favour the abusers.

Information technology should not only be seen as a means of repression: it is also a means of providing protection. It gives a high quality service and is cost effective (for consumer and tax payer). It is possible to organise surveillance in such a way that not all the information need be made known. It is sometimes sufficient that it can be made known. Much work is taking place in the field of so-called privacy enhancing technology (PET) and techniques to ensure anonymity. It is, of course, necessary to

consider safety precautions, any loss of data and possible claims by those affected by a loss of data, misuse of data or use that causes damage. In general, it would seem wise to make the legal framework known on the introduction of the technology.

6.8 Transparency

In part, the objections to information technology arise when people become the objects of surveillance. Nonetheless, the public appears to benefit from surveillance by the authorities, as well as by private companies. Most of the criticism emanates from lawyers and institutions, such as the national Data Protection Authorities. Given the rational model of man, it is quite easy to explain why the objections come from this direction: it is in the self-interest of these groups to protest (which is not the same as saying that their interest is a selfish one).

Furthermore, it would seem that resistance is a characteristic of the assimilation process of new technology. It is resistance to technology and resistance to change. Not knowing whether there is surveillance, what the scope of that surveillance is, who is carrying out the surveillance and what will be done with the data can make people feel uncomfortable. It is rather like the situation of 'I can't see you, but you can see me'. Without transparency with respect to these issues, it is quite possible that people feel more vulnerable rather than less. That would inhibit the assimilation process, which would be a pity given how important it is that the usefulness of information technology is acknowledged; one conclusion that is rarely seen in legal literature is that technology, also surveillance technology, actually makes it easier to respect and protect basic rights.

6.9 Final remarks

The conclusion has to be that the information society leads to a new consideration of values and interests. The right to privacy – and other rights that have arisen from technological and social developments like copyright – are ripe for review. The automatic reaction of support for these rights is no longer adequate.

In the information society the right to privacy is not the universally desirable value for which all other values have to give way. The right to privacy is transformed by the advance of technology. Warren and Brandeis' remark that 'what is whispered in the closet shall be proclaimed from the house-tops' just appears to be a reflection of modern times. It is self evident that the gossip that took place in the village square now moves to national television. The right to privacy is not only a 'barometer' for the advance of technology, but also appears to be subject to the law of communicating vessels, for example with safety and security but also with 'wanting to participate'. In the more complex information society, there is an increasing number of alternatives available, which makes it more likely that the interests of privacy will be weighed against other interests.

The right to privacy is not only increasingly in conflict with the desire to use information technology, but also with some of the basic rights of others. In the first place it seems that many people these days prefer the right to be free in public to the right to privacy. Furthermore, the right to privacy of one person may conflict with the 'right to know' of others. In our changing world, with increasing threats to safety and security, it is in the interest of most people to have the right to know. Modern information technology has made it relatively easy and inexpensive to make that information available.

In the information society the unconditional protection of privacy is becoming less important than weighing off interests. Many individuals prefer to be able to maximize utility to have their privacy rights protected. Nevertheless, it should be realized that information technology can be abused as well. It does not seem rational, however, to abandon the gathering and processing of personal data altogether because of the fear of its abuse. Ignorance of the facts is seldom preferable to decision-making based on knowledge. Knowing facts about people, on the other hand, does not mean that these may be used for all purposes. Knowing that a person is suffering from a serious illness, for example, gives insurance companies the opportunity to determine risks and costs accurately. This does not necessarily mean that people with such an illness will not have the same rights as other people to enter into an insurance contract.

A pre-requisite to prevent abuse of information technology is that its use has to be transparent. Those involved then have the opportunity to know how the information about them is used, and may take appropriate action. As information technology is used by government agencies as well as private parties, it is increasingly important that the monitoring of this use is organized in an independent way. Openness and transparency – as well as proper monitoring – are more important to the protection of the private life of citizens than secrecy and the hiding of information.

7 Conclusion. The 'monitoring power'

With the advent of the information society, the rules governing privacy have been affected by those regulating the protection of personal data. Given the perspective outlined above, it can only be concluded that these rules reflect the old way of thinking, rather than give form to new relationships. Within the European Union, there were legislative developments before the adoption of the privacy directive,[26] usually arising from the Convention of Strasbourg[27] and after the EU directive. What can be seen is that neither of these developments has been successful as a way of connecting to the new paradigm.

In the Netherlands, the Data Registrations Act came into force in 1987. This law is the result of the discussions which took place at the end of the 1960s and reflects the thinking at that time.[28] The 1960s and 70s were characterised by the use of the sociological model and a belief in a society which could be moulded. The law is based on control, licences, permits and regulations. The subject matter of the law is static personal registration, with the Registration Authority acting as the supervisor charged with the granting of licences and approving

---

26 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, OJEC L281, 31.

27 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981.

28 See, inter alia, the definition of privacy by Westin above.

regulations. At the time the law was introduced, it was already out of date because it had in the meantime become possible to couple registrations and have automatic exchange of data.

After the implementation of the privacy direction on 6 July 2000, it was announced that the Data Protection Act would replace the Data Registrations Act. This new act was necessary to implement the privacy directive, but also to accommodate the coupling of registrations and computer networks. The 1980s and 90s were characterised by the increasing prominence of the rational model of man and the embracing of the market economy. The law is based on open norms and transparency, making private enforcement possible. The subject matter of the law is the processing of personal data, the supervisor is the 'Authority for the protection of personal data'. The Internet meant that the law was already out of date at the time it was introduced.

The Internet has made a third transformation of the legislation on personal data necessary, although that transformation resembles more the phoenix arising from the ashes than the snake shedding its skin. Instead of a Data Protection Act, we should think in terms of a Data Promotion Act. The 'Authority for the protection of personal data' would become the 'Authority for the promotion of personal data'.[29] Any attempt to control the stream of information on the Internet is straightforwardly impossible. Even the idea that the exercise of control would have some effect now seems to be out of date.

Furthermore, not only is it in practice impossible to influence the data stream, in many cases it would not even be desirable to protect personal data. On the one hand, an individual wants to prevent the misuse of personal information by third parties. On the other hand, third parties wish to prevent possible abuse by individuals. The tasks of the 'Authority for the promotion of personal data' would be to ensure that individuals are not excluded, that personal data is freely available, but that the supervisors are monitored and that action is taken against abuse.

The most important factor in the implementation of new technology is the expected level of efficiency and effectiveness. The use of

---

29 Even though the data protection authorities will have to get used to this.

technology depends on what it can achieve and how much it costs. Less obvious perhaps is that it is also responsible for a shift in norms. Technology has made things possible that were once not possible; this ranges from copying films from the Internet at home to interactive television to in vitro fertilisation. New technology has made existing norms less self-evident; indeed some norms seem to change with the times. A person who would not dream of going to a cinema without paying for a ticket, could easily be prepared to download a new film at home.

Technology is not only responsible for a shift in norms, in a more complex way it leads to a new organization of state power. This is possibly the most important point of discussion with respect to legal and social change as a response to technological progress. It has been argued[30] that a new fourth power is inevitable; just as the appearance of an executive power was inevitable once the law could not only be written but also printed. That development led to the large-scale bureaucracies we see today. The technical possibilities offered by computers and the Internet will not be less far-reaching. The appearance of a new power, a monitoring power, would seem likely. We have already witnessed this development in the form of such institutions as the Ombudsman, the National Audit Office and the National Competition Authority.

This new power, the result of social change, will have far-reaching consequences for the law, and for the functioning of the rule of law and the legal profession. The growth of the executive power led to large-scale bureaucracies. Bureaucracies may be of use, but can easily lead to excesses. The systematic monitoring of those in charge of the use of surveillance technology in a democratic state is a necessity. In a globalizing and increasingly technological world democracies will need monitoring powers to supervise the use of surveillance techniques and to strike the right balance between personal privacy and other interests.

---

30 R. V. De Mulder, 'The Digital Revolution: From Trias to Tetras Politica', in I. Th. M. Snellen and W. B. H. J. van de Donk (eds.), *Public Administration in an Information Age. A Handbook*, pp. 47–56, Amsterdam: IOS Press, 1998, ISBN: 90-5199-395-1.

PRIVACY AS SLOGAN[1]

Philip Leith

> Using slogans involves risk. One danger is that you won't be able to live up to the benchmark you've set in your slogan.[2]

1 Introduction

The rhetoric underlying developments in data protection and privacy law has been that of individualism and 'choice': that is, the choice by that individual to allow or disallow others to store, manipulate and sell information about the individual. This is a rhetoric which matches the call to 'choice' in the new 'third way' political agenda.[3] However, in the real world, individualism is constantly being mediated by the needs of others just as 'choice' is only available in a context of competition for scarce resources. Thus, for example, when we examine 'choice' in practice, we find that the difficulties of reducing inequality become even more pronounced:

---

1 Queen's University, Belfast.

2 A fuller paper outlining the author's objections to current privacy developments is P. Leith, 'The Socio-legal Context of Privacy', *International Journal of Law in Context* (2006), 2: 105–36. All cited judgments are available via <www.bailii.org>.

3 'The term "choice" was one of the Prime Minister's four principles of public service reform. "Modernising government", published in March 1999, set out the Government's plans for reforming its machinery. One of its five commitments was to have responsive public services that would meet needs of citizens rather than the convenience of service providers'. See the discussion in IDeA (a support system for local government) at <http://www.idea.gov.uk/idk/core/page.do?pageId=753236>.

> The extension of choice needs to include practical steps to prevent inequalities increasing. Promoting 'choice' does not necessarily mean there will be losers. In many cases it will depend on the service being provided. There is no reason why, for example, a meals-on-wheels service cannot ensure that every customer receives their choice. However, for many services – if there are not to be winners and losers – it will depend on there being sufficient capacity existing, to meet the choices of each individual or community.[4]

There is, of course, never sufficient capacity and even 'meals on wheels' are the choice of those who accept their low gastronomic aesthetic.

We appear – I suggest – to be beginning to live in a world where government (and now law) is being sold to the citizen much in the way that products are sold by commerce: that is, through relatively meaningless catch phrases and with little in-depth consideration – slogans. A slogan is a short phrase, easily repeatable, which links merchandise with an idea, or provides a motto. Good ones are certainly difficult to produce, but they are hardly the basis upon which we should be developing law in the field of new technology or social relationships. For example, one guide suggests:

> There are seven ways to make a slogan memorable:
> (1) Make it exciting
> (2) Be boastful or exaggerated
> (3) Self-referencing
> (4) Metaphorical, playful or humorous
> (5) Inspirational or uplifting
> (6) To trigger painful memories or possibilities
> (7) Use of vivid or freshfull language.[5]

Such a use of slogans is understandable in some ways: we live in a world where politics happens quickly and via the new electronic media, so politicians have had to use the language of the media, which is unfortunately the slogan. Politicians using slogans are one thing – they usually have to persuade a sceptical audience – but more insidious, perhaps is that the judiciary appear to be becoming affected by this new

---

4 <http://www.idea.gov.uk/idk/core/page.do?pageId=836370>.

5 C. Franz, 'Slogans: Creating and Using Them In Life, Career and Business', <http://ezinearticles.com>.

approach. In no area is it more obvious than in the developing field of privacy law – and none of the above list of techniques to make slogans memorable have, to my knowledge, appeared in any 'good judges guide'.

The situation – as I argue below, where the law cannot deliver what it promises in terms of protection for an individual's information – leads to 'privacy', like 'choice', becoming more clearly a slogan than a reasoned concept. This is not to say that there are no side effects to the legislative and judicial creations in the fields of data protection and privacy, but that they are not providing what they promise – they cannot, 'live up to the benchmark'.

This has considerable potential for a loss of trust in the judiciary, which may mirror the loss of trust in politicians who have undertaken the path of basing policy upon sloganising. Such a loss of trust has been well recognised in UK politics, with the Phillis Report being produced to analyse the breakdown in trust between citizen, government and press,[6] where it was argued that the techniques used to present information have been a partial cause of the public's disengagement from the political process.

There are, of course, any number of ways in which trust can be lost, and an institution which values that trust must tread a careful path. However, there are indications – from the developing field of privacy – that the UK judiciary are not treading in such a manner.

2 Privacy is a slogan

What is being offered by the rhetoric of privacy? Basically we can say that it is the choice to control the release and the use of personal information. Such an offering has become a political promise not just in Europe but also, as evidenced by the US presidential election of 2001, where privacy has not to date been viewed as a priority goal:

---

6 *An Independent Review of (UK) Government Communications – The Phillis Report*, 2004. At <http://archive.cabinetoffice.gov.uk/gcreview/News/index.htm>.

— Bush stated, 'I believe privacy is a fundamental right, and that every American should have absolute control over his or her personal information'.

— Gore similarly suggested: '[...] I have called for an Electronic Bill of Rights for this electronic age. It includes the right to choose whether personal information is disclosed; the right to know how, when, and how much of that information is being used; the right to see it yourself; and the right to know if it's accurate'.

— And, unsurprisingly, Nader was most aggressive in the promotion of rights to control over data: 'We should support the human right to privacy over corporations' desire to trade information'.[7]

This promise certainly feeds into an existing desire in the citizen.[8] For example, whilst the Younger Committee[9] found no need for a privacy law in 1972, they did find that perceptions were important since 46% thought the following was an invasion of privacy and 37% thought it should be made illegal:

> Suppose you had wanted to buy a new washing machine recently and you had asked for hire purchase terms, and the dealer told you that before giving you credit he would have to check with a credit rating agency. Would you regard [this] as an invasion of privacy?

What are we to make of this? Such a choice to control information is impossible. The world of commerce relies upon the collection of data and credit would be impossibly expensive if there was no means by which credit agencies could supply firms with risk assessments of customers. It is *naiveté* from the respondents to Younger's scenario. This

---

7 Edited from '3 statements by Presidential Candidates', at <http://www.cptech.org>.

8 But a desire which is not – as some suggest – an innate part of the human psyche. See H. W. Arndt, 'The Cult of Privacy', *The Australian Quarterly*, Sept., 1949, pp. 68–71: 'What is difficult to understand is that people who really have nothing to hide should so firmly believe in a principle which enables those *[e.g. income tax dodger, black marketer]* to escape retribution' (p. 69).

9 HMSO (1972), *Report of the Committee on Privacy*, Cmnd. 5012, London.

is not to say that the actions of commercial firms are always within the bounds of normal expectation – this is certainly not the case. A good example is Tesco (particularly because of its importance in the UK marketplace)[10] and its dunnhumby subsidiary which has set up a database collecting data on every household in the UK which is then sold on to other large commercial firms:

> 'It contains details of every consumer in the UK at their home address across a range of demographic, socio-economic and lifestyle characteristics', says the marketing blurb. [...] It has 'added intelligent profiling and targeting' to its data through a software system called Zodiac. This profiling can rank your enthusiasm for promotions, your brand loyalty, whether you are a 'creature of habit' and when you prefer to shop. As the blurb puts it: 'The list is endless if you know what you are looking for'.[11]

This collection is certainly not illegal since Directive 95/46/EC (the basis for the Data Protection Act 1998) does not prohibit a very wide range of activities which involve collection of personal data, so long as it is done either with the consent of Tesco's customers (via their 'loyalty card' agreement) or the consent given to others to sell information to Tesco. So long as 'consent' is gained (or there are other legitimate interests) the information can legally be made use of. Tesco's loyalty card application form has a Data Protection Statement which meets the requirement of unambiguous consent (i.e. 'choice' to participate). Despite the happiness of customers to sign up to this system and to allow the collection of their data for what some see as intrusive processing, when they are questioned on their perceptions as to privacy some immediately take a more concerned position.

---

10 Over £ 1 in every £ 7 of UK retail sales is spent at Tesco.

11 *The Guardian*, Tuesday, September 20, 2005. The Data Protection Register entry for dunnhumby describes the purpose of its information handling to be 'Trading/Sharing in Personal Information' and 'The sale, hire or exchange of personal information'. See the ICO's Register entry for sources and disclosures: 'Data subjects themselves; Relatives, guardians or other persons associated with the data subject; Business associates and other professional advisers; Employees and agents of the data controller; Other companies in the same group as the data controller; Suppliers, providers of goods or services; Persons making an enquiry or complaint; Survey and research organisations; Traders in personal data; Data processors'.

The reality of the data protection field is that much data is collected and processed in ways at which those giving 'consent' would probably be extremely surprised. The literature of data mining;[12] the growth of commercial entities utilizing and selling personal information products and services, and the rise of large interrelated enterprises which can maximize information use all point to a significant growth in a new information industry. We have moved a substantial way from the 1980s when simple list trading was the norm to much more extensive and complex processing of personal data.[13] Yet neither the perception that this new industry exists or even that it is possible (due to the new communications technologies) seems to have fully entered public consciousness. The public further does not yet appear to understand the near impossibility to communicate without a digital audit trail being left.[14]

The sloganising lies in 'the choice' of controlling your personal information: yet any even minimal substantive examination of what is being collected and how it is being processed clearly indicates that the individual has very little choice in the matter at all. 'Consent' is assumed through acceptance of cookies, or signing up for customer loyalty cards or having one's car license recognized automatically when filling up at a fuel pump, or using a credit card and there is, in reality, little choice for the consumer to choose or not to choose in the participation of collection of their personal data. One may refuse to fly (to save data being transferred to other countries), one may pay in cash (to avoid credit history), etc., but the task to remain out with the data collection system of the modern world is an immense one.

---

12 Data mining is the use of collected data to extract meaningful information from the interrelationships between the data elements. For an introduction see Hand, 2001.

13 L. Bergkamp, 'The Privacy Fallacy: adverse affects of Europe's data protection policy in an information–driven economy', in *Computer Law and Security Report*, 18, 2002, pp. 31–47, suggests this is a positive step for the consumer.

14 C. Nicoll et al., *Digital Anonymity and the Law*, The Hague: TMC Asser Press, is interesting in that the contributors are almost all pro-privacy enhancing technologies (PETs), but the message underlying all their attempts is that privacy enhancing technology is very difficult to implement indeed. These security issues are part of the reason why the US is keen to control Internet governance and the technical implementation of TCP and IP protocols.

If you have a normal citizen's life in the early 21st century, then you have very limited control over the collection of your personal information. This is why 'privacy is a slogan' – it offers a benchmark (control of personal information through personal choice) which cannot be achieved in a world based upon the transfer, storage and processing of large quantities of data. There may not yet be a realization amongst the public that this is not achievable, but this must grow. The risk, for those who have jumped on the bandwagon of utilizing this slogan, is that their judgment will be seen to have been faulty and confidence in them will have been lost.

Yet, if the information pertaining to the man in the street is scarcely protected, that of the celebrity is – we find – being given more and more protection by national and European courts, amounting to the judicial creation of rights of publicity[15] under the guise of privacy.

3 What is Privacy anyway?

We talk about privacy as though there was a common understanding of what we mean. This is not true – each culture has its own view of what privacy is. For example, Lloyd notes that in Sweden a publication can be purchased which contains: a 'name, address and a string of numbers [...] the digits represent the subject's declared income for the tax year in question'.[16] And, further, though not something which will be dealt with here, is the confusing relationship between private information and ownership of that information[17] where privacy rights, freedom of expression rights and property rights conflate and confuse in each individual jurisdiction.

---

15 A commercial right to profit from one's image and to control that image in a commercial setting.

16 I. Lloyd, *Information Technology Law*, 4th Edition, Oxford: Oxford University Press, 2004, p. 45. This has recently caused controversy in Sweden when it was put on-line – some felt that the information was too accessible.
See <http://technology.guardian.co.uk/news/story/0,,2106189,00.html>.

17 For a popular outline, see A. W. Branscomb, *Who Owns Information? From privacy to public access*, New York: Basic Books, 1994.

Privacy as a legal concept is based upon Art 8 ECHR. This was, of course, drawn up in the post-war world and was directed towards how the state should interact with the citizen – the state should not behave as the Nazi regime did to the subjugated European population. Recent developments have substantially altered this public law conception,[18] so that Art 8 is now viewed as an individual's right against other individuals which should be protected by the state. This is the notion of 'horizontal effect'. How did we get to this position? Certainly not through any legislative programme – the UK parliament has consistently refused to enact a privacy law. Instead, the law has been a legal development by the European courts (ECHR and ECJ) and also, in the UK, as a development of 'judge made' law.

Yet there is no definition of 'privacy' which produces a clear grounding upon which rights can be based. The situation is the same as that with notions of 'technology' which are currently causing so many problems in patent law:

> We sense that we know 'technology' when we see it. And no doubt that is correct, most of the time. But it is not correct all of the time. Therein lies the delusion. You can prove that for yourself by trying to find a definition of 'technology' that everybody can agree on. The more you try, the more you will discover what a horribly imprecise concept it is.[19]

Replace 'technology' with 'privacy' and the revised quotation also makes perfect sense. The similarly woolly concept of 'balance' is usually brought in to add a modicum of reasonableness to the definition, but the notion of balancing is itself (between Art 8 and Art 10 ECHR) just as problematical.[20]

---

18 In large part because the state – for anti-terrorist reasons – has been using more and more surveillance upon the public at large.

19 Peter Prescott QC sitting as Deputy Judge in *CFPH LLC, Patent Applications by [2005] EWHC 1589 (Pat)* (21 July 2005).

20 The notion of balance as a metaphor is, for example, being more closely examined in areas such as intellectual property where traditionally theoretical underpinnings have been based on this idea. See, for example, R. Burrell and A. Coleman, *Copyright Exceptions*, Cambridge University Press, 2005, where they argue confusions exist between balance being a method or process for achieving resolution of competing interests and being 'harmony of proportion of design'.

In the UK, the judiciary – in their attempt to enact some form of protection for privacy – have utilised an approach which bases privacy on a development of trade secret law – 'Breach of Confidence':

> A duty of confidence will arise whenever the party subject to the duty is in a situation where he either knows or ought to know that the other person can reasonably expect his privacy to be protected.[21]

This is a psychological definition, since I have to know what you *think* rather than what you *do* ('that the other person can reasonably expect'). There is a feeling amongst some of the judiciary – as well as others – that this definition is not in accord with the jurisprudence of the ECHR. Certainly Lord Woolf who produced the definition did not explain why he felt that the law of confidence was equivalent to a privacy right and although the House of Lords has utilized this definition, neither have they looked at it in any depth. This should, one would imagine, be an essential requirement so that we clearly know the difference between the commercial right of confidence and the new tort of privacy. However, the UK courts have shied away from any analysis or discussion of Woolf's transformation of privacy into breach of confidence and we are left with a concept being applied without any theoretical basis, discussion, explanation or any of the other aspects by which such a radical change in law might be underpinned.[22]

The Law Commission in 1981[23] had pointed that the primary difference between a privacy right and breach of confidence was that if A gives information to C about B, then B has no rights against C – only A has rights against C. Privacy rights mean B would have rights against C – just what Lord Woolf outlined in A v B.

---

21 *A v B & C* [2002] EWCA Civ 337 (11th March, 2002).

22 G. Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act', *Modern Law Review*, 66, 2003, pp. 726–58, has seemingly been persuasive to the UK judiciary. A critical reading of this article would still find a lack of conceptual clarity about the relationship between confidence and privacy.

23 Law Commission (1981) No. 110, *Breach of Confidence*, Cmnd. 8388, London.

There are two main reasons for the UK having difficulty in producing a reasonable definition of privacy: first, it is difficult for anyone to define with every attempt being – like 'technology' – something we think we know until we try to so define it. Second, the UK courts have had much difficulty in attempting to elucidate the reasoning of the European courts.

They too, have provided little real exegesis in their judgments upon which these extent and limitations of this new right is based – for example in von Hannover v Germany[24] the court gave protection to Princess Caroline from photographers when she was shopping and doing other mundane activities. The basis of the decision appears to be that Princess Caroline was not a public person '[...] as a member of the Prince of Monaco's family, represents the ruling family at certain cultural or charitable events. However, she does not exercise any function within or on behalf of the State of Monaco or one of its institutions' [62] and that:

> 65. As in other similar cases it has examined, the Court considers that the publication of the photos and articles in question, of which the sole purpose was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public...

It is difficult to understand this reasoning. This is a Princess who represents a ruling family and whose behaviour in a public place is 'private' because she does not have a formal role in her state system? A sceptic might suggest that simply being a Princess should mean that she has to accept a different relationship to the press from commoners.

A third problem in producing a useful legal definition in privacy is that Art 8 right to a private life has to be measured against Art 10 rights to receive and impart information. Most of the cases involve what are seen to be press intrusions on celebrity lifestyles, where the press claim public interest and the celebrity claims an interested public but no 'public interest' in formal terms. We see that in the von Hannover

---

24 *Von Hannover V. Germany* – 59320/00 [2004] ECHR 294 (24 June 2004).

decision: the readership is dismissed as the 'particular readership' by the ECHR – in fact a huge swathe of the European population purchase one or more of the many magazines which appear to be entirely composed of photographs of public figures. *Bunte*, one the magazines involved in von Hannover is reported as selling 700 000 copies per week and each copy is no doubt read by more than one person.

In a situation such as this where there is a lack of clarity over just what the tort of invasion of privacy actually is, one might imagine that the UK judiciary would take careful steps in developing law and giving judgment. This has not been the case: no such care has been taken and the judges appear to be more than happy to produce decisions ever extending the rights of celebrities in this new field of law which they are creating. We look at two in the next section.

But this is not all – what appears to be happening is that there is a lowering of the privacy hurdle so that any engagement with Art 8 is likely to be seen as problematic. As Wilson and Elliott have in literature argued:

> It is of course easier to establish that a substantive Convention right is 'engaged' than that it has been breached. However, the two are now in danger of being conflated in misuse of private information claims. The effect of a claimant passing the threshold stage appears to be that he has shown a breach of article 8 (unless subsequently justified under the balancing exercise), yet the question being asked is not 'Was there a breach?' but 'Was article 8 engaged?'. No wonder interim injunctions have become easier to obtain.[25]

This essentially undermines the Art 10 right, which becomes a much less important right – rather than something which produces a balancing effect. In some readings, though, this appears to be a deliberate tactic by the judiciary as they attack the press in a manner which the legislature has not felt either necessary or willing to do.

---

25 K. Wilson and R. Elliott, *New Law Journal*, 16th March 2007. Available online at <http://www.onebrickcourt.com>.

4 Celebrity Decisions Emanating from the UK Courts

A number of cases have overcome the previously asserted situation that 'the UK has no privacy law'. Some have produced a whole host of decisions – as for example Douglas v *Hello!*[26] Some have been seeking an interim injunction before publication of information, and others cases (as with Douglas v *Hello!*) have been brought after information has been published.

For example, mirroring the von Hannover decision in terms of state role, a member of the British royal family wrote a diary of which he sent copies out to almost 50 selected individuals:

> On his return to this country the completed handwritten journal is photocopied by a member of staff in the claimant's Private Office and circulated to members of his family, close friends and advisers. The claimant does this because he finds it valuable and interesting to have the views of family and friends in response to what he has written. For this purpose he draws up a list of those to whom a particular journal is to be circulated. Accompanying the copy is a handwritten letter from the claimant, or more recently a typed letter from his Personal Assistant or Secretary, to the recipient in question. The copy journal and accompanying letter are sent in an envelope marked 'Private and Confidential'.

Sometimes statements in these journals are counter to UK government policy (for example, Chinese government officials are referred to as 'the group of appalling old waxworks'). Unlike von Hannover these acts are not mundane: they are related to a political role from which the head of state is, in formal terms, barred.[27] Prince Charles will undertake that

---

26 The following are all available:
Douglas & Ors v Hello! Ltd. & Ors [2003] EWHC 55 (Ch) (27 January 2003).
Douglas & Ors v Hello! Ltd. & Ors [2003] EWCA Civ 139 (12 February 2003).
Douglas & Ors v Hello! Ltd. & Ors [2003] EWCA Civ 332 (3 March 2003).
Douglas & Ors v Hello! Ltd. & Ors [2003] EWHC 786 (Ch) (11 April 2003).
Douglas & Ors v Hello! Ltd. & Ors [2003] EWHC 2629 (Ch) (7 November 2003).
Douglas & Ors v Hello! Ltd. & Ors [2004] EWHC 63 (Ch) (23 January 2004).
Douglas & Ors v Hello! Ltd. & Ors [2005] EWCA Civ 595 (18 May 2005).
Douglas & Ors v Hello! Ltd. & Ors [2007] UKHL 21 (2 May 2007).

27 'I do not believe that any full record was kept of the numerous people who received the journals, but I would estimate that at least fifty to seventy-five people would

head of state's role at some point in the future and – one might think – that his views were of interest to a public who supports him financially and who might expect him to respect the limitations required by the chance of birth. The publication, anyhow, related to a political occasion – the handover of Hong Kong. As the defendants suggested:

> The defendant denies any wrongdoing. It contends that the information in the Hong Kong journal was not confidential and denies that the claimant had any reasonable expectation that it would be kept from the public. It contends that the information in the journal was not intimate personal information but information relating to the claimant's public life and to a 'zone of his life' which he had previously put in the public domain. It claims that, as a result, much of the information was already in the public domain and that other elements of it were of the same or substantially similar character as information that the claimant had made public. It alleges that in any event the information concerned the claimant's political opinions which the electorate had a right to know as being within the ambit of the Freedom of Information Act 2000, alternatively because it relates to the claimant's political behaviour whereby, departing from established constitutional conventions affecting the Heir to the Throne, the claimant has intervened in and lobbied on political issues. Alternatively and for the same reasons, there was a powerful public interest in the disclosure to the public of the information which outweighed any right of confidence the claimant might otherwise have.

Extracts were published in a newspaper, publication of which the author disapproved and sought resolution through the courts.[28] Is this an invasion of privacy? In the new UK scenario, such a question is not really relevant. Rather, the question under the new legal regime becomes: 'Are the recipients of the information under an obligation of confidence?'. We see here one of the problems of conflating privacy and

---

have received each of the journals. I know that the recipients of some of the journals included, for example, some politicians, media people, journalists and actors as well as friends of the Prince.' [Para. 22]

28 *HRH the Prince of Wales v Associated Newspapers Ltd.* [2006] EWHC 522 (Ch) (17 March 2006). The torts were breach of confidence and copyright. The copyright issue is interesting but not discussed here.

breach of confidence – the two become intermingled and we are not really sure whether we are protecting the privacy of a member of the royal family, or some sort of business confidence. As the judge concluded (in Prince Charles' favour) it was really a privacy case:

> On what I have seen in the evidence there is every reason for concluding that the claimant establishes, as much in relation to the other seven journals as he does in relation to the Hong Kong journal, a reasonable expectation of privacy in respect of their contents.

This conclusion reflects the criticisms of Wilson and Elliott that the engagement of Art 8 rights appears to deflect rights under Art 10. Where does this leave us? Prince Charles' father is well known for making unwelcome comments (often with a racial basis). Are Prince Philip's comments to be self-censored by the press given that he, too, might reasonably expect such comments not to be reported in the press? Would a politician involved in the Hong Kong handover – having sent out his diary to over 50 people – have fared as well in gaining protection as a member of the royal family? Perhaps, but it does not seem so likely given the current torrent of publications from ex-civil servants, ex-government advisors and cabinet members after they leave their posts.[29]

A number of UK privacy cases have involved sexual matters, and one such recent case was well publicised in the press. A married celebrity had been sleeping with the wife of a non-celebrity for two years, taking her abroad on holidays, etc. His public image was that of being 'clean cut'. The cuckolded husband wanted revenge – through publicity of the celebrity's behaviour – and approached a newspaper with details. The celebrity sought restraint of publication, and suggested that publishing the story is an invasion of privacy.[30]

---

29 Tony Blair's press advisor (Alistair Campbell), for example, published a book on the occasion of Blair's resignation (*The Blair Years*). The potential contents had caused heated debate, but a number of other books have similarly appeared over the past few years. Those in power, or around power, appear to have little publishing modesty after they leave that circle.

30 *CC v AB* [2006] EWHC 3083 (QB) (4 December 2006).

The question became, does the husband owe the celebrity a duty of confidence?:

> In this case the [celebrity] (CC) conducted an adulterous relationship for some months with the [husband's] wife, and now seeks the court's assistance in preventing him from telling anybody about it. There is no direct precedent for this, so far as I am aware, and it does not at first glance appear to be a very compelling case.

It is a very strange outcome that someone owes a duty of confidence to the seducer of one's wife, but an injunction was given:

> [...] unless restrained by a court order, the [husband] will publish as many details as he knows about the [celebrity's] relationship, whatever the consequences likely to flow for the [celebrity] and his family.

Once again, we see the eccentric world which is being produced by this judicial creation of privacy as breach of confidence. Art 10 gives an individual a right to receive and impart information, yet – following on the Wilson and Elliott point – appears not to be relevant in a case where claims to privacy are involved.

The peculiar world being produced under this privacy rhetoric is, of course, not simply located in the UK. In Lindqvist,[31] Mrs. Lindqvist was prosecuted by the Swedish data protection authority for publishing 'sensitive' personal information about a church member on her church-based web site. The ECJ ruled that charitable web site usage was not exempt from the DP regime and that reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46'.[32] The full implications of this reasoning – that publication of traditional local journalistic detail is unlawful when in computer based format – has not yet fully percolated. If it does, it may have striking effect.

---

31 *Lindqvist v Kammeraklagaren,* Case C-101/01, ECJ, November 6, 2003.
32 Para. 50.

5 What is wrong with current Privacy/Data Protection developments?

There are two major problems, apart from the fact that we are not really dealing with 'privacy' as such (the implementations are artificial since privacy is so hard to define). These are:

1. The general population is being given rights which are relatively ineffective and which are more slogan than actual.
2. Celebrities are being given commercial rights which essentially allow them to control the presentation of information about themselves.

The first point is clear from the evidence which can be gathered on the workings of data protection. The DP regime, since it allows 'consent' to be the primary method of control, gives those who can gain 'consent' a wide range of methods to store and process personal data. It may have differed in effect if a concept such as 'informed consent' was required, in that for each of the processing tasks the information user had to explain and request the specific agreement of the data subject. Of course, this would cause the probable collapse of an information industry which is based upon collecting, comparing and extracting marketing information from that data. The overhead costs to the information industries from applying an 'informed consent' requirement would mean that costs would be astronomical. Governments are users of the information provided by these commercial firms so they would also feel the effect of over-regulation.

Data protection law has anyway biased information processing in favour of capital since tools such as data mining, matching and processing of data require large data sets. The companies thus most able to perform these tasks effectively are those with large data sets – that is, well capitalised and with a large commercial presence. Data protection law will always – in terms of information utilisation – favour Tesco over the local corner shop.

On the second point, the current developments in breach of confidence give enormous power to someone to control information

which is (effectively) already public. We see this in the existing privacy law of France:[33] Ségolène Royal's public termination of her marriage after her unsuccessful bid for the Presidential post is a case in point. Journalists from *Le Monde* had been sued for reporting (in a book) her husband's adultery just three weeks before her announcement, yet she was enabled to control this information until a politically opportune time arose at which she publicly stated: 'I have asked Françoise to leave home, and to pursue his other affair'. No doubt, the celebrity in *CC v AB*, too, can choose the time when it is most convenient for him to discuss his personal life: when, for example, he wishes to promote his autobiography.

Overall, then, the promise of choice that these new privacy developments were to bring are not working: they are more slogan than achievable benchmark. But they are having significant effect in changing the manner in which the public can know about and discuss the behaviour of a small – and privileged – section of the community. That is, the public's right to privacy is limited, and their right to receive and impart information is being limited, too. Hardly a great move forward in democratic thinking, we may suggest.

6 Conclusion: Trust

The reader of judgments relating to privacy cannot but help to pick up the undercurrent of judicial dislike for the press, and the feeling that the driving force behind much of these decisions is a distaste for the contemporary interests of the public. We are never, in the judgments, given a true reflection of celebrity and the effort which is involved in ensuring that the celebrity becomes one and stays one. The world has changed and yet judicial perceptions do not seem to have followed: the press is now dealing with celebrity culture which relies for its existence and income upon a market of information between the celebrity and public mediated by that same press and celebrity. When we read the case law, this whole business world almost appears non-existent. Why

33 A useful introduction is at <http://www.ambafrance-us.org/atoz/privacy.asp>.

should the perceptions of courts be so blind to social reality and economic fact?

Giving celebrities rights to privacy without any discussion of the context of celebrity is of concern, since it to a very large extent ignores the rights of others. In McKennitt,[34] a successful musician complained about an ex-friend's publication of the relationship between the two in a book.[35] Most commentators viewed it as a relatively anodyne perspective on an argument between two ex-friends and the nature of celebrity. The court found in favour of McKennitt and her privacy rights, a conclusion which seriously worried publishers who viewed this as a potential problem for any writer of a biography – since the subject of an unauthorized one will most likely be able to claim intrusion into their private life unless the biography meets their view of themselves.[36]

Overall, what is problematical at present in these judgments is a tendency towards control of the press and publishing – indeed, it appears sometimes to be an attack upon the press by the judiciary and that the press is mostly seen to be all of the 'yellow press' type. This, of course, is all being undertaken under the slogan of 'choice to keep information private' but it is a choice which is only being made available to those who benefit from public visibility rather than the public at large whose interest in, and rights to receive, information (or at least more than celebrity approved information) are being lost.

What about the danger to the judiciary which was mentioned earlier? For one thing, these decisions are being made in the public gaze and frequently receive critical response. For example, in a class of first year law students I raised the *CC v AB* judgment as a minor point in a discussion about the nature of law and the role of judges in the system.

---

34 *McKennitt v Ash* [2006] EWCA Civ 1714. See the ex-friend's view of the litigation at: <http://www.dailymail.co.uk/pages/live/femail/article.html?in_article_id=456146&in_page_id=1879>.

35 N. Ash, *Travels with Loreena McKennitt: My Life as a Friend*. Amazaon.com has a series of reader's reviews both pro and anti.

36 'The Court of Appeal judgement, if allowed to stand, has potentially serious ramifications for freedom of speech as it puts greater importance on McKennitt's right to privacy, than Ash's right to freedom of speech', Periodical Publishers Association at <http://www.ppa.co.uk>.

The class were appalled by the outcome and it was near impossible to get them back onto the topic – they saw this judgment as everything which was wrong with the legal system. It is as well that Mr. Justice Eady was not in the class to hear what the students thought of him and his judgment.

In the Campbell case relating to the super-model, too, there have been highly intemperate attacks upon the senior judiciary in the UK. For example, *The Guardian* columnist Simon Jenkins wrote:

> As it is the courts have made fools of themselves. The Douglas case had nothing to do with the right to privacy, notoriously indefinable as it is. Nobody can stage a wedding, sell the publicity rights for £ 1 m and then claim that they were trying to remain private. Managed publicity is not privacy. As for the 'obligation of confidence' on newspapers not to scoop rivals who have paid for so-called exclusives, this is censorship born of madness. Newspapers must guard their exclusives as best they can, not call on law lords to act as their bouncers and heavies. Either way, this is a blatant case of one law for the rich and one for the poor.
>
> The law lords are still hoping to find a new home across Parliament Square from Westminster commensurate with their newly glamorous status. They should go the whole hog and move up the road to the Ritz, where they clearly belong.[37]

Other criticisms of the judges, too, are becoming commonplace amongst those who would be considered the respectable face of journalism who wish to distinguish themselves as against the less seemly parts of the press. For example Roy Greenslade – journalist and academic – wrote:

> Yet, despite our foolishness, despite examples of misused power, despite the problems caused by a hydra-headed competitive media [...] we must not allow the courts to encroach on rights that prevent us from acting in the public interest.

---

37 'Angry celebrities, come to Britain: our judges are suckers for a glamour trial', *The Guardian*, Friday, May 4, 2007. <http://www.guardian.co.uk/commentisfree/story/0,,2072115,00.html>.

> Of course the people don't necessarily agree with that argument right now. And they never will until, or unless, we in the media clean up our act and thereby regain their trust. Without public support our claims to act in the public interest will sound hollow – and the judges will eat further still into our freedom to publish.[38]

The drive towards privacy at the expense of freedom of speech is a danger arising from the behaviour of the judiciary. The rhetoric of balance is missing, and only the privacy of those able to litigate becomes important. That, perhaps in essence, is why privacy is a slogan and why there is a danger if the judiciary are seen to be so responsible for its introduction. A judiciary which is well ahead of, or out of kilter with the public perspective – whichever way one wants to express this – is in danger of losing trust. Without the trust of the public that they have no particular political agenda or bias towards one group of society, the judges will be in an highly undesirable position.

38 <http://blogs.guardian.co.uk/greenslade/cat-304/>.

SURVEILLANCE, PRIVACY AND PARTICIPATION

Fernando Galindo[1]

1 Introduction

The investigation on privacy/personal data protection has been till today in the hand of the experts' opinions on the matter. They (the 'experts') understood that the citizens, the jurists, the judges or the politicians didn't have knowledge or even interest on the matter.

It was an opinion with juridical basis also. The fact is that special administrative procedures on privacy/data protection were articulated since the start of the discussion on the phenomenon privacy/personal data protection in the seventy years of last century. Coherently, these procedures were in charge of new institutions like the agencies of protection of personal data, dedicated to claim responsibility for the infractions in the area of privacy or, best, in the protection of personal data.[2]

The moment has arrived to complement to the specialized or 'expert' opinions. And it is this way, because it is no longer only the case that the jurists of the very diverse existent knowledge area are in charge of the researches on privacy/data protection and putting practice of the respective regulation, but rather empiric investigations exist on the opinion of the citizens on the matter. It happens, especially, in

1 Universidad de Zaragoza, Facultad de Derecho, Zaragoza, e-mail: <cfa@unizar.es>.

2 It is not the objective of this paper to discuss a complex task as it is the concepts on privacy or data protection. For this reason the two concepts are used here indistinctly.

connection to the problems of surveillance outlined in the last years starting from the terrorist attacks of September 11 2001. These results must be kept in mind by the investigations in course without doubt.

This paper has the objective to present, shortly, taken as reference several European experiences specially the Spanish, 1) some information about the change of the times in relation with the expansion of the knowledge society and the need of opinion of citizens, jurists, judges... and not only 'experts' on the privacy/data protection matter and another related to the implantation of the knowledge society (2); 2) the results of an empiric investigation in which citizens have been consulted with regard to their opinion on surveillance and privacy (3); 3) how these results can be kept in mind by two investigations related with personal data protection that the author of this paper puts in practice (4); and 4) some conclusion (5).

2 The change of the times

The step forward towards the information and knowledge-based society has already been taken both in Spain and in other countries: it is a fact.[3] In spite of this, the theoretic studies[4] and government measures that analyse it and foster it, still place greater emphasis on its development, or in other words, on adopting measures to support its expansion,[5] than on verifying how the implementation is taking place and the results already attained by it.

---

3 The evolution of the number of users of Internet of 'yesterday' has grown in Spain between April-May 2006 and April-May 2007 a lot. The annual growth was about 3% and more, years before. See Asociación para la Investigación de los Medios de Comunicación 2006, 'Audiencia de Internet', Madrid, Retrieved 25 September, 2007 (<http://www.aimc.es/aimc.php?izq=egm.swf&pag_html=si&op=cuatr&dch=2egm/24.html>).

4 See as example of this kind of literature: Enrique Pérez Luño, 2005, 'Internet y la garantía de los derechos fundamentales' in A. Murillo and S. Bello (eds.), *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías*, Burgos: Servicio de Publicaciones Universidad de Burgos, pp. 13–39.

5 This is the case of the Spanish Government with the 'Plan avanza': Ministerio de Industria, Turismo y Comercio 2007, 'Plan avanza', Madrid, Retrieved 25 September, 2007 (<http://www.planavanza.es/>).

Studies, therefore, hardly ever make considerations that are focused, for example, on verifying the quality (the way and extent to which this society has been implemented), the consequences and changes that this implementation is starting to have on different social organisations, its acceptance by the citizens, or, for example, the consequences of the measures adopted by the Governments in connection with energising the use of Information and Communication Technologies (ICT).

And this occurs in all fields: both related to the design of 'parts', tools or machines such as computer or mobile phones, and related to the construction of applications or programs, be they used to buy and sell (e-Commerce) or to carry out transactions between the Administrations and the citizens (Electronic Government or Administration).

As we have expressed above in relation with privacy/personal data protection research and we shall see in this paper, this approach seems wrong. This is because there was a reason behind the exclusively energising attitude until not so long ago, when the number of users was limited, and indeed, both Governments and the companies that wanted to sell their products with the help of instruments such as the Internet or mobile telephones had to spread the use of ICTs. Theories were not necessary in this regard, either: these had to emphasise the importance and interest of the technological change and the relevance of its inclusion in people's daily lives. The current situation is quite different as we set forth below.

Circumstances have changed: the degree of expansion attained by the introduction of ICTs into daily life over the last few years, because, basically, a considerable number of users exist in the majority of the countries.

This is the case of Spain. In this country we can see that although the relative Internet penetration number is not high compared with that has happened in other countries, the absolute number, on the contrary, is high: look at what happens when we use the data that, according to internetworldstats news, 43.9% of Spanish people currently access Internet, we have a user population of 19 765 033 million people, which represents a similar, more or less, number of users than the Belgians (5

millions), Dutch (12 millions) and Danes (3 millions)[6] together. This demands, at least in the experts' opinions, a different role to be satisfied than the one played thus far.

Indeed, even though Governments may be demanded to persist in their policies to spread the use of ICTs among the population in order to overcome events such as digital division, which occurs in practically all the countries of the world, demanding the execution of good research on the matter is a different matter. Good research must be demanded because in practice it can be seen that one thing is what results from the, often catastrophist, proposals made in literature: aimed at presenting the characteristics of the innovations and pushing forward the use of ICTs and at making forecasts or future hypotheses on the consequences of technological development, and another thing is what we see around us: citizens are using ICTs, without prevention and without sufficient knowledge. The question to be asked is: would it not be a good thing for the theories to be based, as they are in other fields, on real data rather than just on lucubrations, that is, studying the opinions and uses expressed by the citizens when they assume the use of ICTs in their daily lives?[7]

The need for this approach becomes obvious, even if the field of study is limited, for example, to the use by the citizens of the resources that the Administrations place at their disposal to contact them or solve their claims. As we point out below, the figures here also express the existence of a real application of technologies.

Some data in this regard are given below, continuing with the Spanish example.

— Study about the Internet in Spain. BBVA Foundation (October, 2005):[8]

---

6 See: Internet World Stats 2006, 'Internet Usage in the European Union', Retrieved 25 September, 2007 (<http://www.internetworldstats.com/stats9.htm#eu>).

7 A good example on methods to make these studies in relation with privacy is: J. Bennett Colin and Charles Raab, 2003, *The governance of privacy. Policy instruments in global perspective*, Aldershot: Ashgate, pp. 187–210.

8 See: Fundación BBVA 2005, 'Estudio sobre Internet en España', Madrid, Retrieved 25 September, 2007 (<http://w3.grupobbva.com/TLFB/dat/presentacioni_internet. pdf>)

- Surfers: 37% of the Spanish people over the age of 14 have accessed the Internet over the last 3 months.
- Search for information from the public Administration or government: 28.2% of the surfers.

According to these figures, four and a half million Spaniards access the Public Administration on a regular basis, using the Internet.

— EGM. AIMC (May, 2007):[9]
  - Surfer: 41.4% of the Spanish people over the age of 14 have accessed the Internet over the last month.

— Net surfers. AIMC (February, 2007):[10]
  - Transactions with the administration through the Internet over the last 30 days: 27.8% of the surfers.

The figure is similar to the results of the previous data.

— Eurostat July, 2007:[11]
  - Surfers: 39% of the Spanish people have accessed the Internet at least once a week.
  - Transactions with the Administration through the Internet:
    – Obtain information: 23.7%.
    – Download forms: 13.6%.
    – Send completed forms: 7%.

These figures are similar to the previous ones.

In general, the same occurs as in all other countries, namely, once there is a certain degree of Internet 'penetration', the users or 'surfers' use the

---

9 Asociación para la Investigación de los Medios de Comunicación 2006, 'Audiencia de Internet', Madrid, Retrieved 25 September, 2007 (<http://www.aimc.es/aimc.php>).

10 Asociación para la Investigación de los Medios de Comunicación 2006, 'Navegantes en la Red', Madrid, Retrieved 25 September, 2007 (<http://www.aimc.es/aimc.php>).

11 Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens, 'e-Government Factsheets- Spain', Brussels, Retrieved 25 September, 2007 (<http://www.epractice.eu/files/media/media711.pdf>). The data are from 2006.

same means to contact the Administrations. This is what in literature is called Electronic Government and, more accurately, at least in Spanish, Electronic Administration.

The government authorities have detected that, indeed, something is happening and thus on 1 December 2006, Spanish Council of Ministers approved bringing a bill before the Parliament aimed at regulating Electronic Administration. More specifically, the foreseen regulation was on the access of citizens to Public Administration using ICTs. The norm has been approved by the Parliament as Law 11/2007, 22nd June, with the name of Law to the electronic access of the citizens to the Public Services.[12]

3 The Kingston' Survey

As we have seen we have needs today of opinions as the 'expert' opinions made from a new perspective, and also another opinions. This is proposed by the Kingston' Survey.

The data provided by the empirical study conducted by Queen's University of Kingston, Canada, Department of Sociology, entitled The Surveillance Project, Global Privacy of data, International Survey,[13] are especially interesting in connection with everything we have just mentioned. The study is interesting because it deals directly with what has been pointed out up to here as a need for scientific works: to be knowledgeable about the scope, reactions, acceptance or rejection that life in the ICT or knowledge-based society is having among the citizens. The study was conducted by way of a survey on phenomena of universal extension such as considerations on the 'surveillance' and 'privacy' of people that have considerably increased all over the world due to public requests and private companies since the events of 11 September 2001 in the United States.

---

12 BOE n. 150, 23/6/2007, <http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/12352>, Retrieved 25 September, 2007.

13 David Lyon, Elia Zureik and Yolande Chan, 2006, 'The Surveillance Project and the Globalization of Personal Data', Queen's University, Kingston, Retrieved 4 January, 2007 (<http://www.queensu.ca/sociology/Surveillance/?q=media>).

This is what the study deals with, pointing out, after performing a survey in several countries, some of the reactions that are occurring among citizens in connection with the social co-existence that is generated, in short, in the ICT or knowledge-based society. Namely, as we have said, it focuses on the citizens' opinions about 'global surveillance' and respect for 'privacy' of different human activities which, carried out by public institutions and companies, has been occurring over the last few years in practically all countries, and which has several reasons, one of them being the possibilities offered by the ICTs to put it into practice.

The study was conducted by way of a survey among people who live in the following countries: Canada, United States, Mexico and Brazil in America, and France, Hungary and Spain in Europe. The surveys were conducted between June and August 2006.

In Spain the surveys were conducted among 1000 people between 30 June and 11 July 2006. A similar number of people in the other countries were polled.

The questions and answers or the information compiled in the survey refer basically to:

— How knowledgeable the people polled are about technologies and the law that regulates their use.

— The opinion of the people polled on the use that corresponds to them with respect to their personal information.

— The opinion of the people polled on the degree of trust they have in the actions of companies and Governments in connection with the use that they make of the personal information that reaches them in their daily work, and the importance that the Governments place on the individual rights and on national security in connection with the use of personal information.

— The steps which, in the opinion of the people polled, individuals have to take to protect their personal information in connection with certain risk situations with respect to the use of their personal data.

— Valued personal experiences that have taken place in connection with measures aimed at collective surveillance in order to prevent crimes or offences from being committed.

— The degree of acceptance of the implementation of national identity cards as a compulsory identification means for citizens.

— The implications of personal data processing carried out by companies and Governments for identifying people, which is facilitated by the use of the Internet.

— The consideration, in the opinion of those polled, made by the media with respect to topics such as personal information processing.

— Terrorism and security: the opinion of those polled on the way both problems are solved by the laws and Governments, and the balance struck by the latter between respect for individual rights and safeguarding national security.

— The opinion of those polled on the transfer of personal information compiled by companies to national Governments or other Governments, and vice versa, the transfer of personal information compiled by Governments to Governments of other countries or to companies of the same country or of other countries.

— The effectiveness of video cameras to prevent and avoid offences or crimes.

— The situation of workers, travellers and users related to possible uses of personal information compiled about them at work, the use of airports and the acquisition of goods and products.

— The stance taken by those polled with respect to contexts, vignettes, specific events or cases related to the use of personal information by companies and governments, and to the use of personal data by companies and governments when arranging to travel by plane.

The questions were mainly asked by telephone interviews using computers. This was the case in Spain.

4 Research in progress

On the other hand, the content of the researches that is going to be taken here as context in order to complete its development with some of the answers given to the survey, and which is being conducted by the author jointly with several interdisciplinary research groups, has the following objectives and denominations:

— Industrial standards. The execution of proposals aimed at designing tools, systems and programs that are respectful with rules and standards referring to the safeguarding of privacy and management of identification, PRIME project, and

— Governability policies. Suggesting policies to governments that can be used as a content for the rules that they create and for the governability policies ('governance') they put into practice, insofar as these government are agents of public funds, in agreement with the rules aimed at exercising the principle of separation of powers and the rules of the market per se, GERSOCO project.

As we can already see, there is a certain relationship between the contents of the surveys and the objectives of the research. To a certain extent, it can be said, and this is what this paper wishes to show in a practical way, that the contents of the surveys are basic proposals that must be taken into consideration when carrying out research such as that indicated herein or other similar research.

Here we are just going to present the opinions compiled in the survey that can be taken as a complement or future guidance for research in progress, comparing, above all, the answers given in the Spanish context, which does not mean that answers given to the questions in other countries are not going to be taken as reference, too, at specific times, as the studies targeted by the research that is presented herein have a global reach, in the majority of the cases.

As we can see, the point of reference in each section is going to be the contrast between the contents achieved and foreseen in the projects presented, and the content of some of the answers given to the survey

that are of interest for its development. On other occasions, the reference will be the verification of the adaptation or not of the results of the projects attained to date related to what the answers of the citizens compiled by the Kingston study suggest.

In agreement with the contents of the research expressed, the sections that comprise this work are going to deal with industrial standards (4.1) and governability policies (4.2). A brief conclusion or corollary of the paper is made in every section.

4.1 Industrial standards

The possible changes that the use of ICTs can bring about in the lives of people through access to the Internet are so obvious, for example, that the existence of industrial type initiatives and projects whose objective is to design new network access mechanisms is not surprising, understanding by these both the machines and the programs, that are concerned with safeguarding 'privacy'. This is the case of the PRIME project.

PRIME stands for Privacy and Identity Management for Europe (ref. IST-2002-507591), and it is an Integrated Project of the Sixth Framework Programme FP6, Information Society Technologies IST Programme of the European Union (<https://www.prime-project.eu/>). The project is headed by IBM.

The aim of PRIME is to safeguard the management of digital identification and data protection in the Information Society, so that users of the information system can safely act in the Information Society and be able to preserve their private sphere. This is the reason why the companies and research centres participating in the project have developed the PRIME standard, whose aim is to become a work prototype for an identification management system that guarantees privacy.

New solutions are being developed and tested for its extension on the marked, aimed at managing the identity of people in different real scenarios. Thus, for example, in connection with the communications on the Internet, passenger admission processes by airline companies

and airports, the use of situation-based telephone services (use of mobile phones to purchase goods, for example) and distance teaching.

Within this project, the author of this work compares the achievements of the prototypes with the opinions on their use of possible citizens that live in the South of Europe.

After setting out the general objectives of the project it is worth asking, how interesting are the Kingston survey answers for PRIME?

4.1.1 The Kingston survey and PRIME

The interest, from the perspective of the author of this paper, is focused on the fact that the answers include the citizens' stance with respect to, for example, the following questions, of interest for the development of PRIME:

— Are the users knowledgeable about the standards on personal data protection?

— Do citizens accept the use of identity cards?

— Do citizens trust in the protection of personal information systems referring to data contained in identity cards?

— And, as occurs with respect to other questions, answers to a general question, are the reactions to the questions the same in all the countries of the European Union?

We are going to present some of the replies given in the Kingston survey to similar questions, below.

Before indicating the questions and answers we must point out that we are going to compare the answers given by citizens from European countries (France and Spain), as PRIME as a project bears in mind citizens from all over Europe.

Are users aware of the standards on personal data protection?

The question most related to the matter was: How knowledgeable are you about the laws that deal with personal data protection in government department?

The possible answers were: a) Very knowledgeable, b) Somewhat knowledgeable, c) Not very knowledgeable, d) Not at all knowledgeable and e) Don't know/unsure.

Another question, coherent with the above, referred to companies. The question was: How knowledgeable are you about the laws that deal with the protection of personal information in private companies?

The possible answers were: a) Very knowledgeable, b) Somewhat knowledgeable, c) Not very knowledgeable, d) Not at all knowledgeable and e) Don't know/unsure.

The answers are given below. We have reflected the answers given by all those polled to both questions, asked in their respective languages, in the charts (charts 1 and 2) below, in agreement with the applicable legislation in their country, mentioning the countries where they live.

The first general conclusion to highlight, and thinking more in the line of an industrial type project such as PRIME, is the different knowledge and appreciations that arise in the different countries with respect to the legislation on data protection. Which is nothing new with respect to the rest of the answers of the survey, where practically the same occurs.

If we fine-tune a bit more, and look at the European answers, there is a certain similarity between the Spanish and French data.

Indeed, if we consider the knowledge of the legislation on data protection related to government institutions the data tell us the following:

	Very knowledgeable	*Somewhat knowledgeable*	*Not very knowledgeable*	*Not at all knowledgeable*
France	9.5%	37.8%	35.5%	17.2%
Spain	4%	37.1%	20.9%	22%

In connection with the knowledge on the legislation on data protection related to private companies the data for France and Spain are the following:

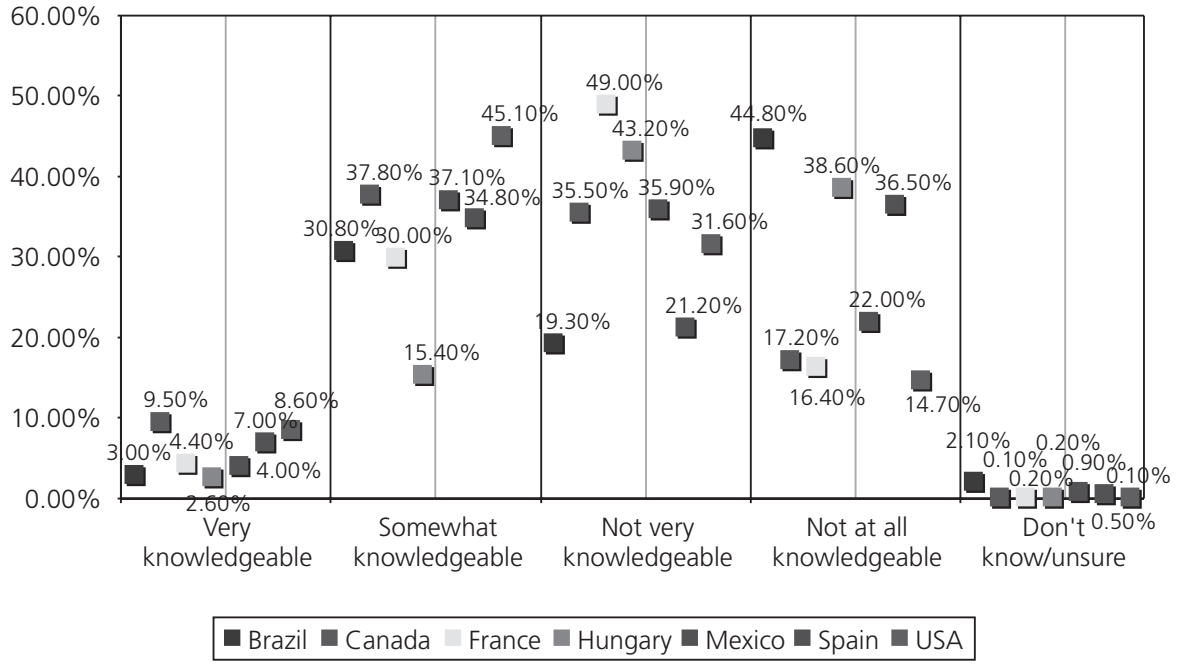


Chart 1. How knowledgeable are you about the laws in government departments?

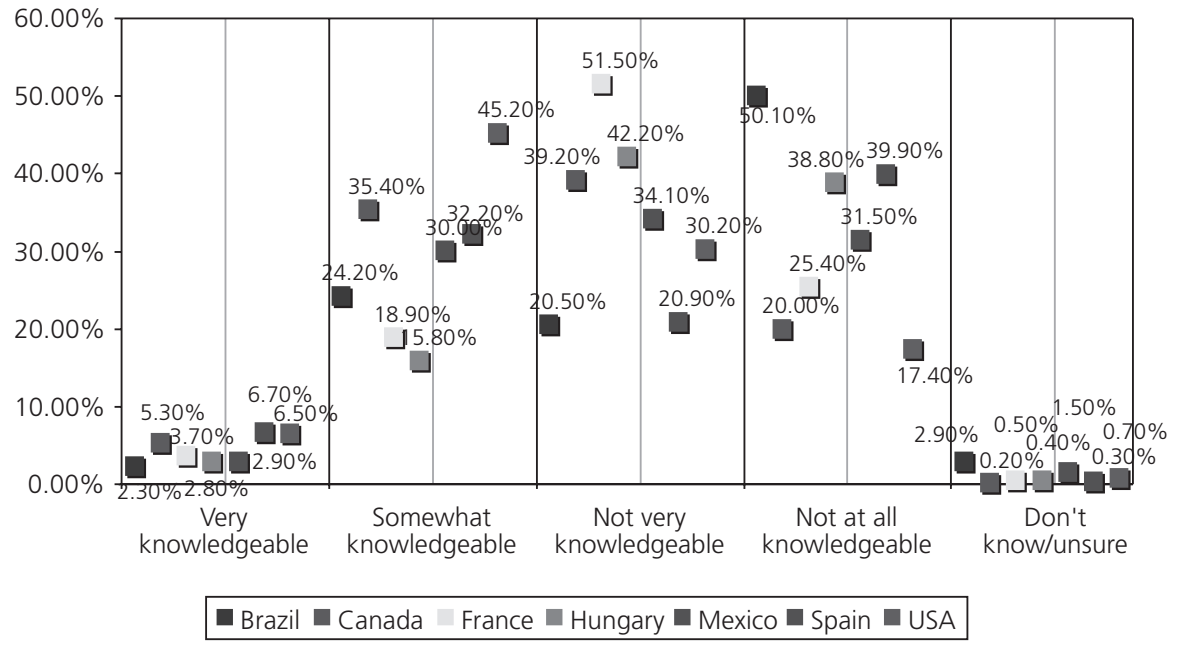


Chart 2. How knowledgeable are you about the laws that deal with the protection of personal information in private companies?

	Very knowledgeable	*Somewhat knowledgeable*	*Not very knowledgeable*	*Not at all knowledgeable*
France	3.7%	15.8%	39.2%	20%
Spain	6.7%	32.2%	20.9%	39%

It can be observed that not much is known about the legislation on data protection in France or in Spain: the higher percentages refer in all cases to the sum of those who are not very knowledgeable and those who are not at all knowledgeable (52.7% in France and 42.9% in Spain, Governments; 59.2% in France and 59.9% in Spain, Companies).

More is known about the legislation referring to government organisations in France (4.73% of those polled compared with 41.1% in Spain). In Spain, on the contrary, more is known referring to private companies (38.9% of those polled compared with 19.5% in France).

In any case it must be pointed out that not only in Spain and France: in all the countries, there are almost always answers to these questions. The number of answers: don't know/unsure, is very small, which may indicate that there is a certain general sensitivity about personal data protection even when, as a general rule, they are not familiar with the application legislation.

Another outstanding difference appears in the tables: the fact that in Europe more is known about these laws than in America. This is coherent with the European tradition in the regulation on the subject, the contrary is a fact in America.

4.1.2 Do citizens accept the use of ID cards?

The survey also asked other questions directly related to PRIME: identification management. Two questions were asked: one referring to the acceptance of the idea of identity cards and another referring to the construction of databases on identity cards.

The first question was as follows: Do you: a) strongly agree, b) somewhat agree, c) somewhat disagree, d) strongly disagree, or e) not sure? The answers can be seen in chart 3.

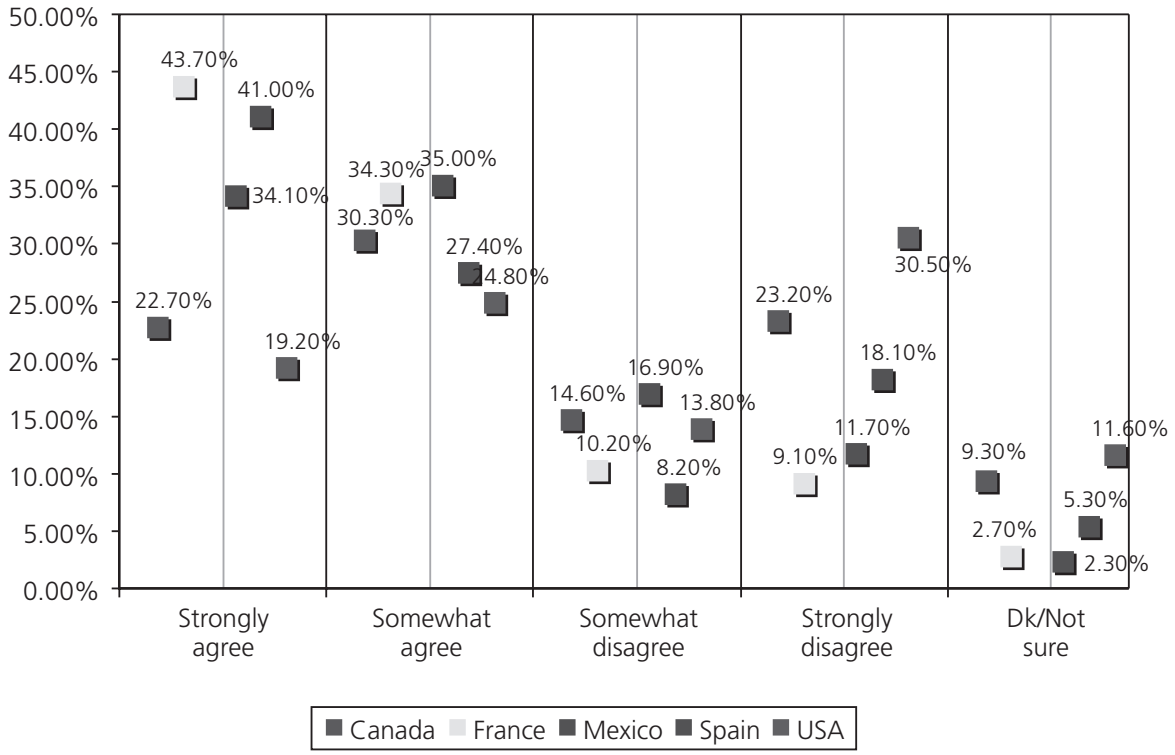


Chart 3. Some have suggested that everyone should have a government-issued ID card that they must carry on them at all times and to all places, presenting it to the police or any other security corps when necessary. To what extent do you agree or disagree with this idea?

We are also going to see here the European opinions referring to France and Spain.

	Strongly agree	*Somewhat agree*	*Somewhat disagree*	*Strongly disagree*	*DK/ Not sure*
France	43.7%	34.3%	10.2%	9.1%	2.7%
Spain	41%	27.4%	8.2%	18.1%	5.3%

In this case there is majority agreement with the identity card in France and Spain: in France 78% agree and in Spain 68%. The percentage of those who strongly disagree is greater in Spain (18.1% compared with 9.1% in France) even though the difference decreases if we add the percentage of somewhat disagrees to the percentage that strongly disagrees (France: 20.3% and Spain 26.3%).

It is worthwhile commenting that the acceptance of ID cards in Europe contrasts with the reticence that is observed with respect to its introduction in Canada and the United States as seen above in chart 3.

Do citizens trust in the protection of the personal information systems referring to the data contained in the identity cards?

Another question of the survey that differs from the previous one but which has certain connections referred to the following:

Would you say that they would be a) very effective, b) somewhat effective, c) not very effective, d) not effective at all, or e) not sure? See the systematised answers in chart 4.

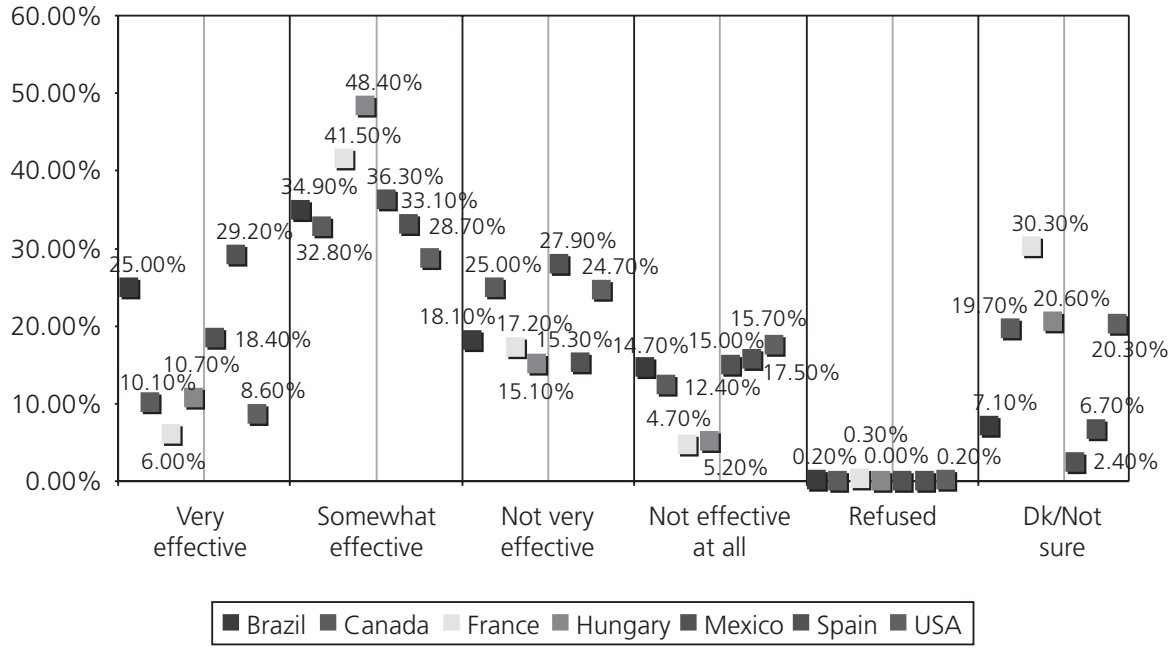


Chart 4. In order to put national ID cards into use, the government would need to have a national database containing personal information on all citizens. This information could include address, gender, race and tax information. How effective do you feel the protection of this type of information would be in order for it not to be disclosed?

Again we are looking at the answers given in Spain and France.

	Very effective	*Somewhat effective*	*Not very effective*	*Not effective at all*	*Not sure*
France	6%	41.5%	17.2%	4.7%	30.3%
Spain	29.2%	33.1%	15.3%	15.7%	6.7%

As we can see the opinion of the majority is that they trust in the virtues of the use of ID cards and that their use is not going to bring about risks for them because the personal data protection is going to be effective and it is not going to be possible to disclose these data (62.3% in Spain and 47.5% believe this in France). It must be pointed out that, notwithstanding the above, 30% of the people polled in France have their doubts: not sure, and 21.8% in France and 31% in Spain have their fears: they do not believe that this protection is effective.

4.1.3 The survey and industrial standards: conclusion

As we can see from the information expressed by the citizens, the industries are correct in pondering, with projects such as PRIME, on new designs for computer products: citizens are aware of the limitations of the existing ones to preserve data protection. On the other hand, and this is something governments must consider, the data protection laws must be reformed because they are important but their content is mainly unknown by the citizens.

Governments and companies must also bear in mind that citizens express that certain control mechanisms, such as ID cards, are necessary, even though they have some doubts about the measures devoted to preserving their personal information, in the case of the use of ID cards, using information systems. This requires the need for transparent computer systems that will reduce citizens' doubts.

4.2 Governability policies

As we have already mentioned when listing the topics that the Kingston study dealt with, the answers obtained from it are not just relevant for policies to be taken into account in industrial development, but they are also of interest for preparing policies in connection with the implementation and development of what is called Electronic Administration: that is the construction of applications and programs aimed at making it easier for citizens to contact the Administration, using electronic resources. This is the topic we are going to refer to in this section, taking the initiatives that are carried out in the GERSOCO project as reference.

About GERSOCO

GERSOCO is equal to Governability and regulation strategies in the knowledge-based society. It is a project to be developed between 2004 and 2007.

It is financed by the Spanish Ministry of Education and Science within the framework of the National Research Plan (ref. SEJ2004-00747). The project aims at preparing a theoretic governability model ('Governance') for the knowledge-based society.

4.2.1 Legal-philosophical objective

The objective of GERSOCO is to analyse what conditions the regulation systems must satisfy in a society that is marked by the omnipresence of new technologies and by the exchange of messages with legal relevance that take place through telecommunication networks. The hypothesis of omnipresence was taken for granted as a fact when the project was initially proposed.

The central hypothesis of GERSOCO is that a democratic conception of governability must be characterised by being citizen-oriented.

In agreement with this hypothesis, the governability model, whose development proposes carrying out research, pivots around two basic elements. On the one hand, on the new ways in which citizens participate in the government, legislation and administration tasks, provided by the ICTs. On the other hand, on the development of social self-regulation as an appropriate mechanism to involve citizens and social agents in the regulation of the knowledge-based society.

As a result, both elements will comprise a theoretic e-Governance model, which must be used to design legislation and regulation strategies that combine the operative needs of public institutions (economic efficiency and effectiveness) with the growing demand for democratisation in collective decision-making.

The project has already established several conclusions compiled in a book,[14] several articles and different sub-projects. In any case it has not

14 Fernando Galindo (ed.), 2006, *Gobierno, Derecho y Tecnología: las actividades de los poderes públicos*, Pamplona: Thomson Civitas.

been possible thus far to use contrasts like those that are included in the answers given to the Kingston survey.

4.2.2 Legal-political objective

From a legal viewpoint, the central aim of the GERSOCO research, taking for granted the scope of use of ICTs in Spain, is focused on establishing government formulas that will permit taking stock, in the knowledge-based society, of the extent to which, in practice, the Public Administrations use the organisation rules per se of the Rule of Law, and of the rules of 'governability' or 'governance', the management adapted to the functioning principles of the market, which, since the eighties of the last century, are typical of the action of Governments all over the world. These rules are fostered by the progressive rationalisation of government methods and the demands which, in this sense, are made on the policies and objectives of the governing bodies. Also by something that is the consequence of these government practices: the use of ICTs in the activity of the Public Administrations in their relations with the citizens.

From hereon, the research aims at establishing formulas that will permit, in any case, making the principle of democratic participation in the decisions, which is present in democratic Constitutions, a reality.

4.2.3 GERSOCO and the Kingston study

The GERSOCO research did not deal with several preliminary questions, as it took them for granted. These are the following:

— Is it worthwhile dealing with these topics now?
— Is the ICT and knowledge-based society so widespread?
— Are citizens familiar with the technologies?
— Are citizens aware of the expansion of the actual governance practices of the business world in the exercise of the power received from the citizens?
— Do the citizens accept that the information compiled about them be used for different purposes than those which they were compiled for?

— On the other hand, who is responsible for processing the citizens' personal information?

— And now, the main question, what data does the Kingston survey afford to these and other questions raised by the GERSOCO project?

As we have already mentioned, the survey pursues a different aim to the aim of the GERSOCO project, notwithstanding which, the answers given in the survey in Spain to the following questions are of interest for the project, as they are, to a certain extent, answers to the questions that the GERSOCO project asks.

— Are citizens familiar with the technologies?

— The first question of the Kingston survey referred to the knowledge about technology. More specifically it said: In general, could you tell us how knowledgeable you are about the following systems?

— Would you say that you are very, somewhat, not very or not at all knowledgeable?

Here we are initially going to look (chart 5) at the answer given in Spain with respect to the knowledge about the Internet.

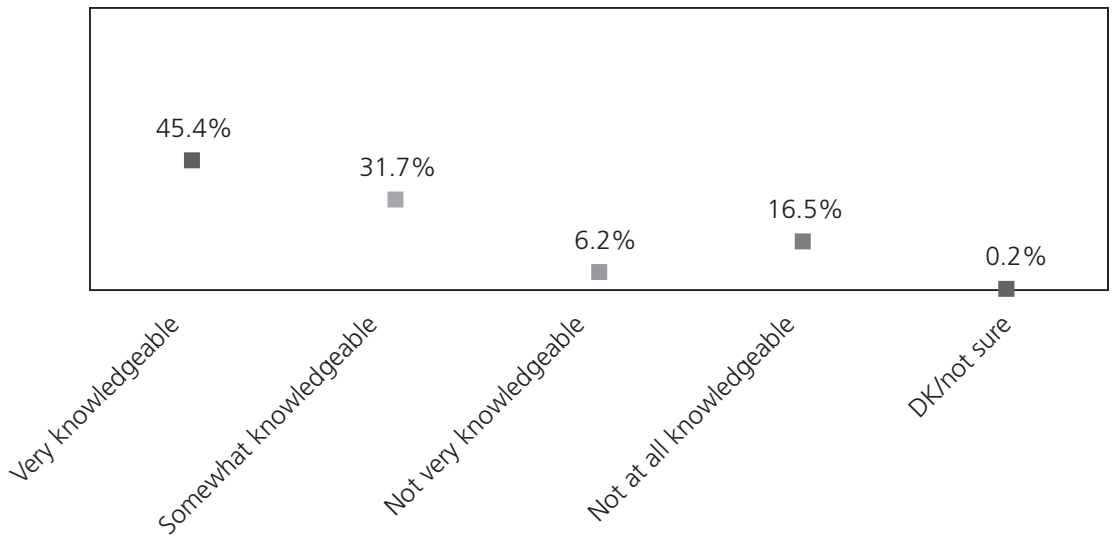


Chart 5. In general, how knowledgeable are you about Internet?

We observe that the answer confirms how significant it is to carry out research such as GERSOCO: the step forward has been taken towards the knowledge-based society. As we can see, it is verified that the majority of the citizens (77.1%) interviewed[15] responded that they are very knowledgeable or somewhat knowledgeable about Internet. This answer is coherent with the appreciations situated in section I of this work that indicate that a considerable percentage of use of the Internet has been attained in Spain.

Another matter is the answer that was given to the question related to the knowledge of 'data mining of personal information' systems. The question referred to the practice, fostered by the use of the Internet, which focuses on the possibility of analysing the profiles of network users through techniques such as 'data mining'.

The answer given by the Spanish people polled was as follows (chart 6):

It can be seen that 68.3% of the people polled were not very knowledgeable or were not at all knowledgeable about the technique of 'data mining of personal information'.

The figure is not so special if we compare it with the figure that indicates what occurs with people polled in other countries, which is reflected in the following chart (chart 7):

It can be seen in the chart that in the majority of the countries polled the largest number of answers to the question about 'data mining' is the one that referred to them being not very knowledgeable or not at all knowledgeable.

These data bring about a concern: that government agencies or companies, mainly concerned with the expansion of ICTs as mentioned above, are not so concerned with disseminating or preventing some of its disadvantages, such as the one reflected here: in

15 1000 from the whole of Spain, who were selected from a representative sample of the population, work, studies and age, of the national means that are taken as reference by other surveys. Of course, when they were selected the fact that they were Internet users or 'surfers' or not was not taken into account.

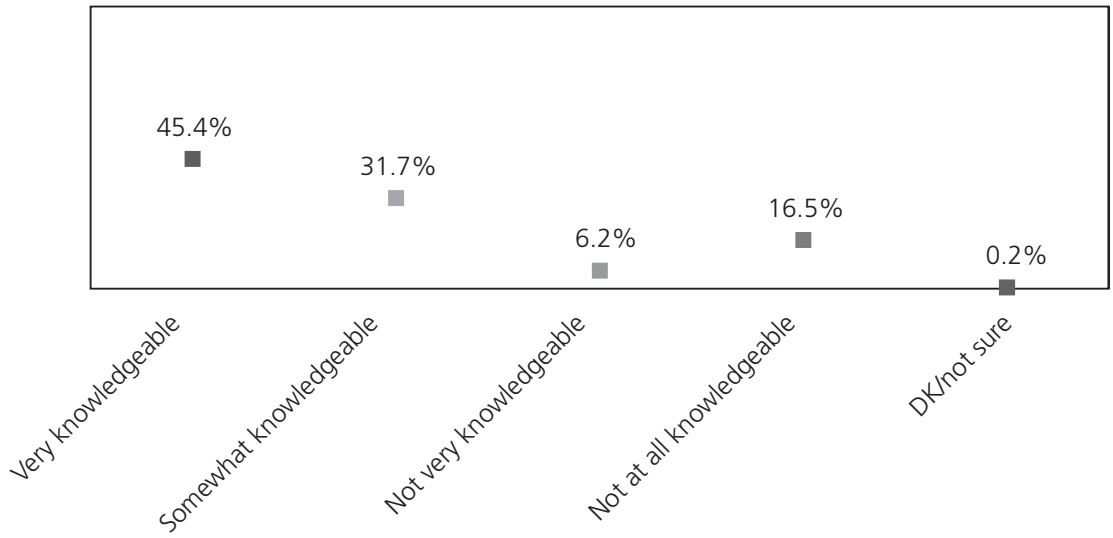


Chart 6. In general, how knowledgeable are you about data mining of personal information?

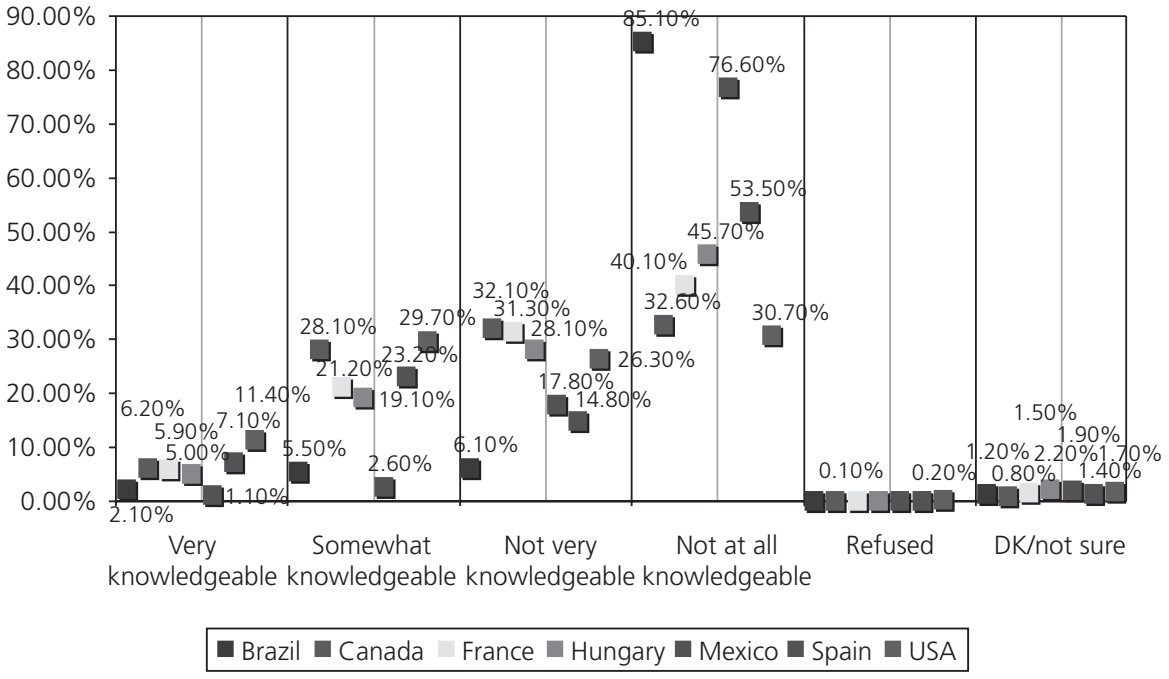


Chart 7. In general, how knowledgeable are you about data mining of personal information?

general, citizens are not aware that the normal functioning of the Internet and the ICTs permit carrying out actions such as 'data mining': the study and automatic storage of personal information and the tracing of purchasing practices or carrying out consultations on web

pages, which permits recording and predicting future behaviours and therefore have an influence on them.

These appraisals are of interest for GERSOCO: it is necessary to insist on the fact that Governments, in their policies, should make sure they provide citizens with training and information on the characteristics of the use of ICTs. This will foster their awareness-raising about its virtues and defects, qualifying them to make informed decisions in this regard. As we have seen in the previous section with respect to industrial standards, citizens are aware that information systems must be used but they have their doubts about the measures adopted for their parliamentary and industrial regulation. In the answers to the Kingston questions expressed herein it is obvious that there is a lack of clear information.

As we mentioned above, another question of interest for GERSOCO is the following: are citizens aware of the expansion of 'governance' practices carried out by the governing bodies in the exercise of the power received from the citizens?

There is not a similar question in the Kingston survey, generically oriented towards privacy and surveillance matters in terms that can be understood by the citizens polled, but the data provided by the answers given to the following two questions by those polled can be used by GERSOCO. These questions referred to their trust in the use of legal measures on personal data protection made by government departments and private companies.

The first question said: To what extent do you believe laws are effective at protecting your personal information that is held by government departments?

Do you believe that the laws are very effective, somewhat effective, not very effective, not at all effective, DK/not sure? The answers given in Spain are shown in a chart below (chart 8).

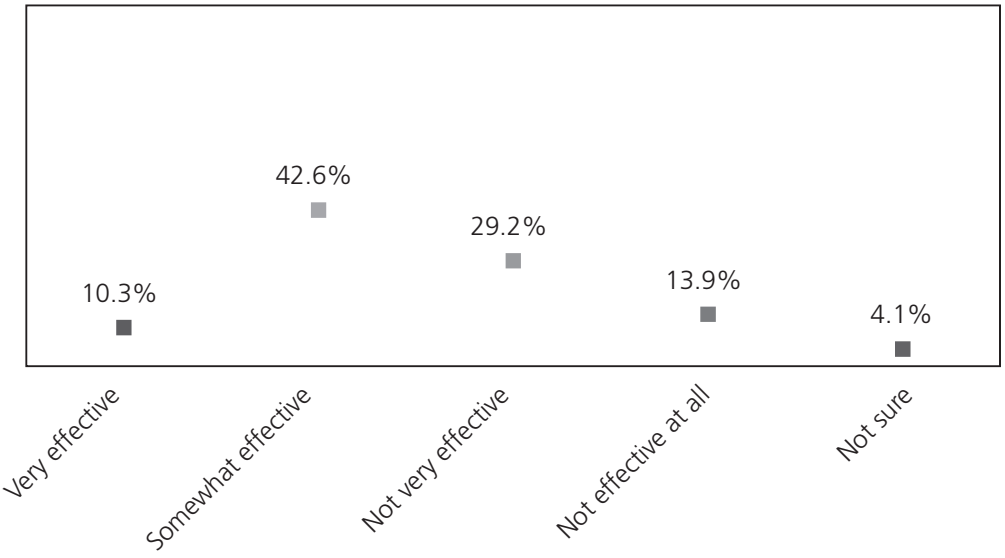


Chart 8. To what extend do you believe laws are effective at protecting your personal information that is held by government deparments?

The second question referred to: To what extent do you believe laws are effective at protecting your personal information that is held by private companies?

Do you believe that the laws are: very effective, somewhat effective, not very effective, not effective at all, DK/not sure? (see chart 9).

The difference in trust which, in spite of the degree of privatisation of the Public Administrations, the citizens have in the Administration compared with the degree of trust they have in private companies can be seen in the answers.

More specifically, the two answers indicate that Spanish citizens trust more in government agencies in connection with the compliance with the laws on data protection (52.9% believe they are effective), than in private companies (42.5%), undoubtedly, as we say, trusting in that the former represent the citizens or general well-being to a greater extent than the companies do.

The consequence for GERSOCO: it is, therefore, important to recommend when preparing governability policies that in the application of the governance policies those responsible for the Public Administrations should not lose sight of the government or public character of their actions.

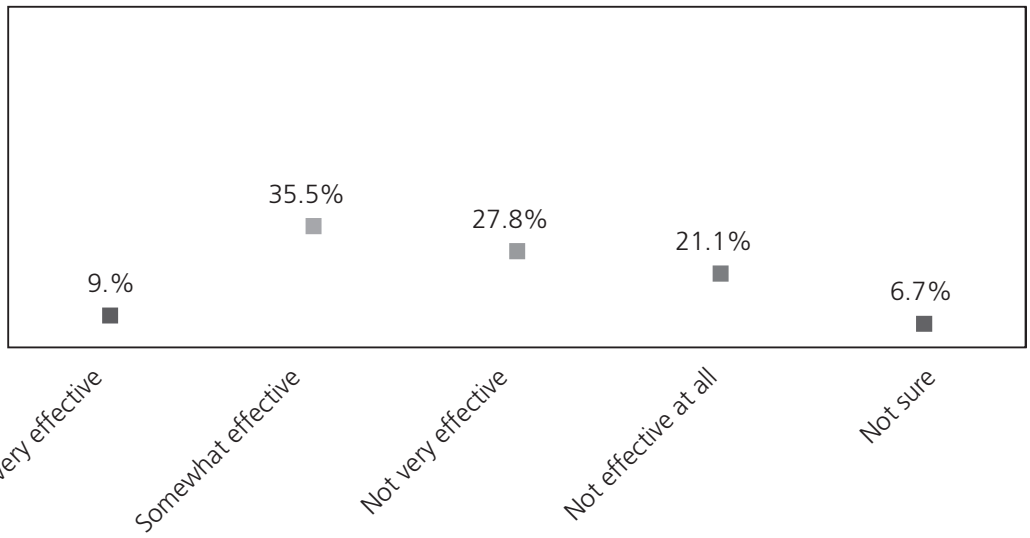


Chart 9. To what extend do you believe laws are effective at protecting your personal information that is held by private companies?

Notwithstanding the above, the answers to another question qualify the trust in the government.

These are the answers to the question:

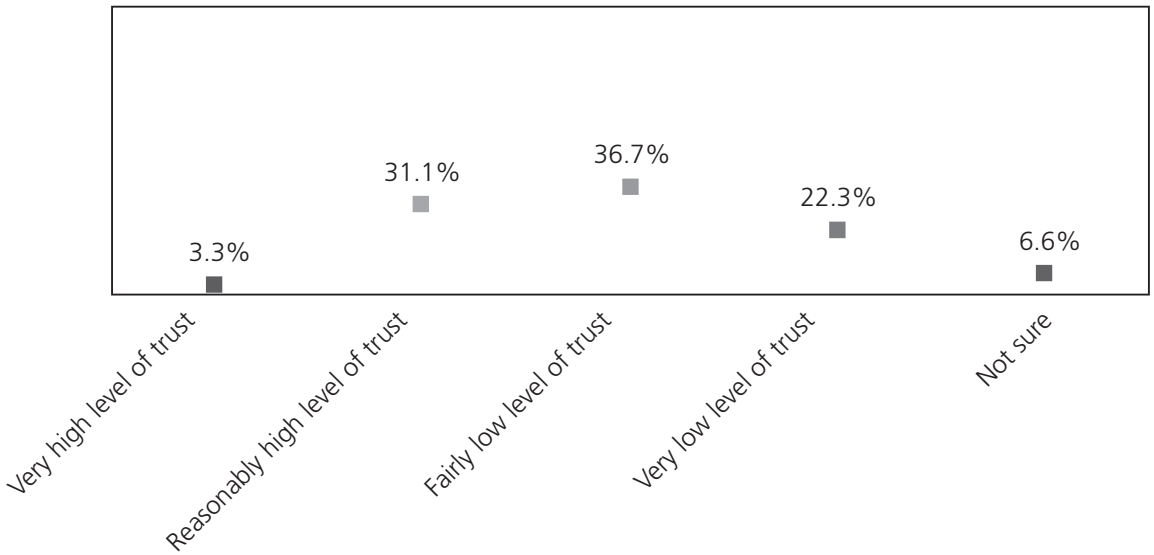


Chart 10. When it comes to the privacy of personal information, what level of trust do you have in that the Spanish government is striking the right balance between national security and individual rights?

Do you have a very high level of trust, a reasonably high level of trust, a relatively low level of trust, a very low level of trust, are you not sure?

These are the answers (chart 10):

As we can see, there is not a lot of trust in the Government, referring to national security topics, in connection with 'fair' consideration of the subject with respect to the safeguarding of individual rights. Only 34.4% of the people polled trust in the Government striking the right balance, on the contrary 59% do not trust in this. And this is regardless, as we have seen in other answers, of the fact that they trust the Government more than companies in matters such as data protection, or they trust in the expansion of the use of the ID card as a general identification means.

The next question, to complete the above, said (see chart 11):

As we can see, they do not trust very much in the preservation of personal information by private companies, either, but, of course, their trust is greater than with respect to the balance that the Government strikes between security and individual rights. Thus: 44.8% of the people polled trust in the protection of personal information by companies, and only 51.8% has a low level of trust. In the case of the Government, only 34.4% of those polled trust in the Government striking the correct balance, on the contrary 59% do not trust in this.

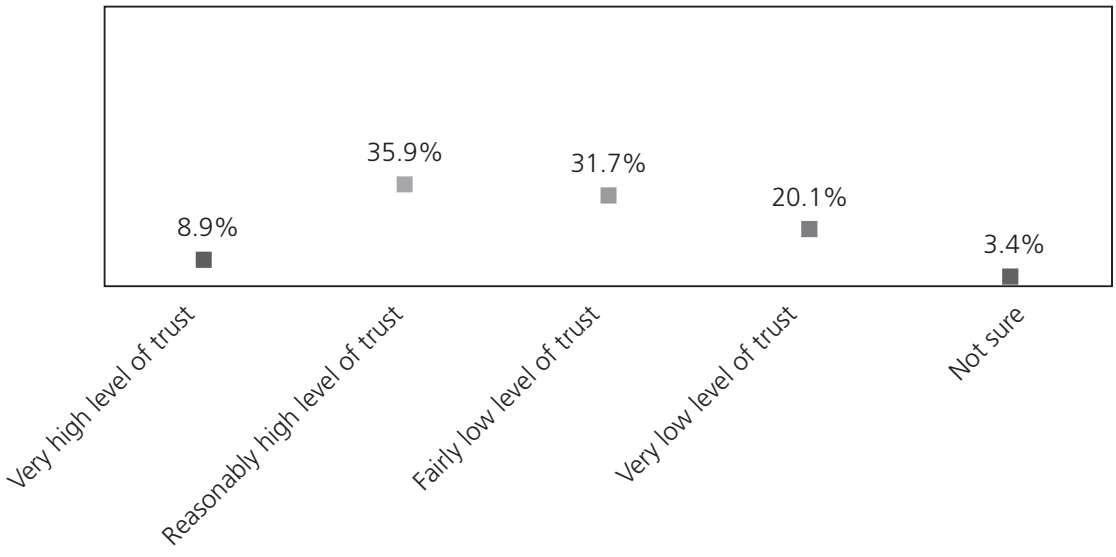


Chart 11. What level of trust do you have that private companies, such as banks, credit card companies and places where you shop, will protect your personal information?

Have you got a very high level of trust, a reasonably high level of trust, a relatively low level of trust, a very low level of trust, are not sure?

In both cases, Governments and private companies, the citizens have little trust in personal data protection.

These appreciations are relevant when proposing policies for a project such as GERSOCO. That is why enlightenment, clarity, transparency, are values that can be demanded from these measures if we want to actively involve the citizens in them.

Or otherwise, and as we will see below, the numerical data will increase, referring to the following dangerous answer given by those polled to the question: To what extent do you have a say in what happens to your personal information?

Would you say that you can a) have a complete say, b) have a lot of say, c) have some say, d) have no say/DK/not sure? The answers are given in chart 12.

31.5% estimate that they can have a say on what occurs to their personal information, whilst 65% estimate that they can have some say or do not know or are not sure.

The answer is not satisfactory due to the fact that it is a sign of the unclear policies carried out in this regard, in this case and according to those polled, by the Spanish government... and by other Governments because, sadly, what happens in Spain can also be said about other

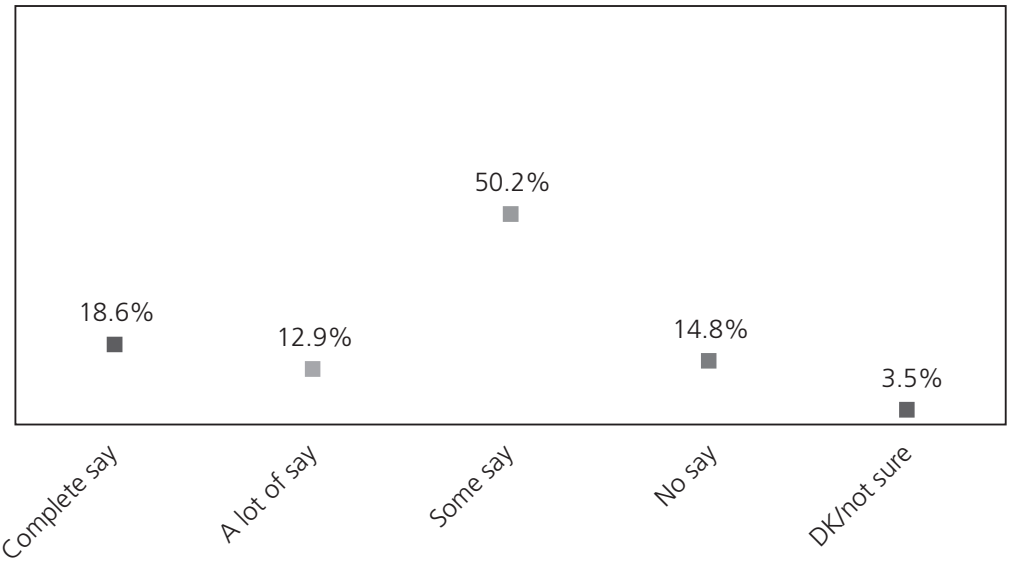


Chart 12. To what extend do you have a say in what happens to your personal information?

countries as observed in the answers given to the same question in them, unlike what happens in France, as we can see in the following chart (chart 13).

As we can see the Spanish figures are repeated in other countries but not in France: here 60% of the people polled estimate that they can have a say on what occurs to their personal information, whilst 39.6% of the French polled estimate that they can have some say or they do not know or are not sure.

The complete comparison tables between European countries and Canada and the United States are the following:

	Have a complete say	*Have a lot of say*	*Have some say*	*Cannot have a say*	*DK/not sure*
Spain	18.6%	12.9%	50.2%	14.8%	3.5%
France	35.5%	24.5%	30.1%	9.5%	0.4%
Hungary	13.6%	12.9%	39.9%	29.8%	3.8%
Canada	9.6%	21.3%	49.4%	16.5%	3.1%
United States	11.9%	17.3%	53%	16.5%	1.2%

Summing up the above in order to clarify the answers:

	They can have a say	*They can have some say or no say*
Spain	31.5%	65%
France	60%	39.6%
Hungary	26.5%	68.7%
Canada	30.9%	65.9%
United States	29.2%	69.5%

As we can see, France is the country where the largest number of citizens express that they must have a say and a lot about what occurs to their personal information, in other countries, on the contrary, the figures are similar to those of Spain: almost two thirds of those polled estimate that they can have some say or no say.

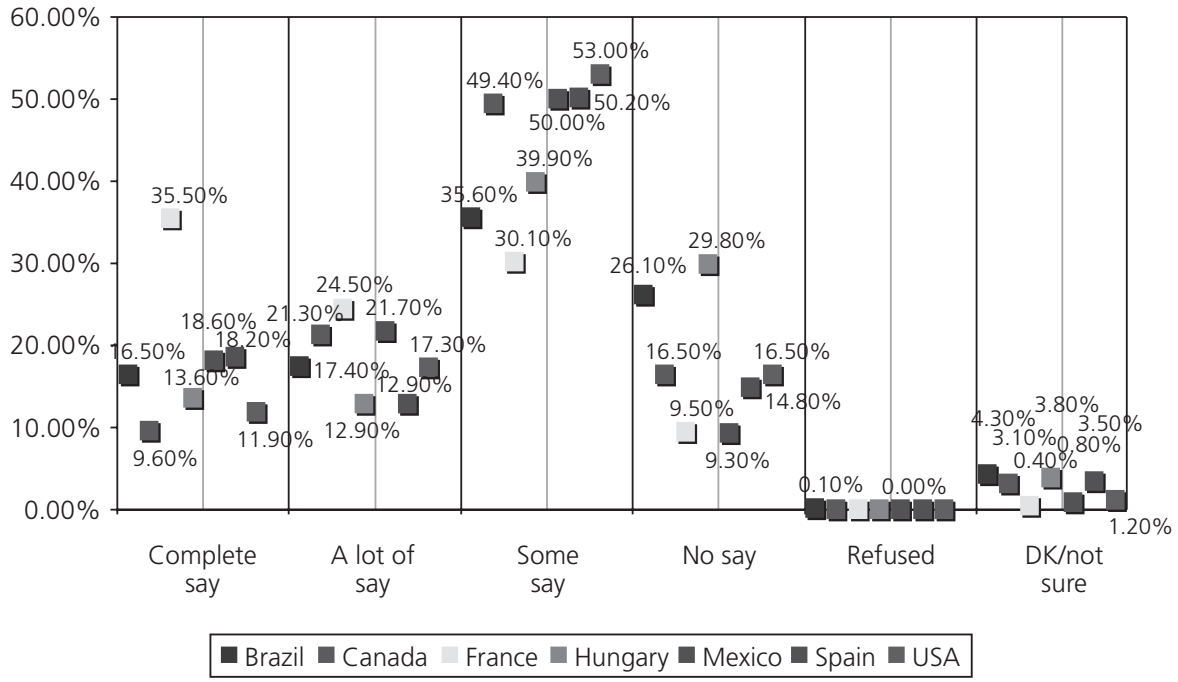


Chart 13. To what extend do you have a say in what happens to your personal information?

There is no doubt that these data need to be completed with surveys aimed at throwing further light onto these statements, but there must be no doubt, either, about the fact that the answers also indicate the need to continue carrying out research such as the Kingston research and in the matter that concerns us now, the research related to the GERSOCO project: the governability policies. In short, we must ask about the quality of the initiatives that are being adopted by the Governments in order to energise the use of the Internet by the Public Administrations in their relations with the citizens.

5 Conclusion

As we have seen from the presented examples, the Kingston study is an excellent approach to what it has shown must be carried out more and more, from hereon in, by research, R&D actions and the development of industrial or government applications: ask the citizens what their opinion is with respect to the problems that affect them on a daily basis

in connection with the fact that they live in the ICT or knowledge-based society.

Surely, the answers will give some more reliable indicators about the characteristics of the ICT or knowledge-based societies than those given by some of the scientific literature expressed in this regard, which is based mainly on intuitions or opinions compiled from opinions given in books and theoretic or merely analytical studies, but hardly ever compared with real data.

The aim of this paper has been to demonstrate that, by linking together two different types of research, empirical studies on the citizens' opinions help compare information and reflections obtained by other means both in the field of surveillance and privacy and in the field of ICT or knowledge-based society. Furthermore, the proposals of the Kingston survey, as an auxiliary method to the legal type research presented herein, have proved to be essential to make the demands for citizens' participation in the creation of laws, codes of conduct or industrial standards, which are implicitly or explicitly included in the constitutions of the democratic systems, a reality. Which is no mean task?

CHAPTER 3
PRIVACY AND NETWORKS

PRIVACY ON THE WEB

Tatiana Stefanova[1]

1 Introduction

The 'Net' affects almost every part of our lives from how we apply for jobs and where we get our news to how we find friends.

Today, the Internet is the world's largest international computer network. There are 'slip roads' to this 'information superhighway' in about 200 countries. At the beginning of 2007 Internet consists of more than 108 million web sites; more than 1 billion users from all over the world can use at least one of the different Internet services and have the facilities to communicate with each other. Users have access to a boundless pool of information, at different locations all over the world. The Internet can be considered the first level of the emerging Global Information Infrastructure. The World Wide Web the most modern Internet user interface is a basis for new interactive multimedia services.

The Internet absorption into our society is extraordinary – it enables us to improve communication, erase physical borders, and expand our education.

The participants in the Internet have different aims, interests and opportunities:

— The software companies design the networks and the services available.

---

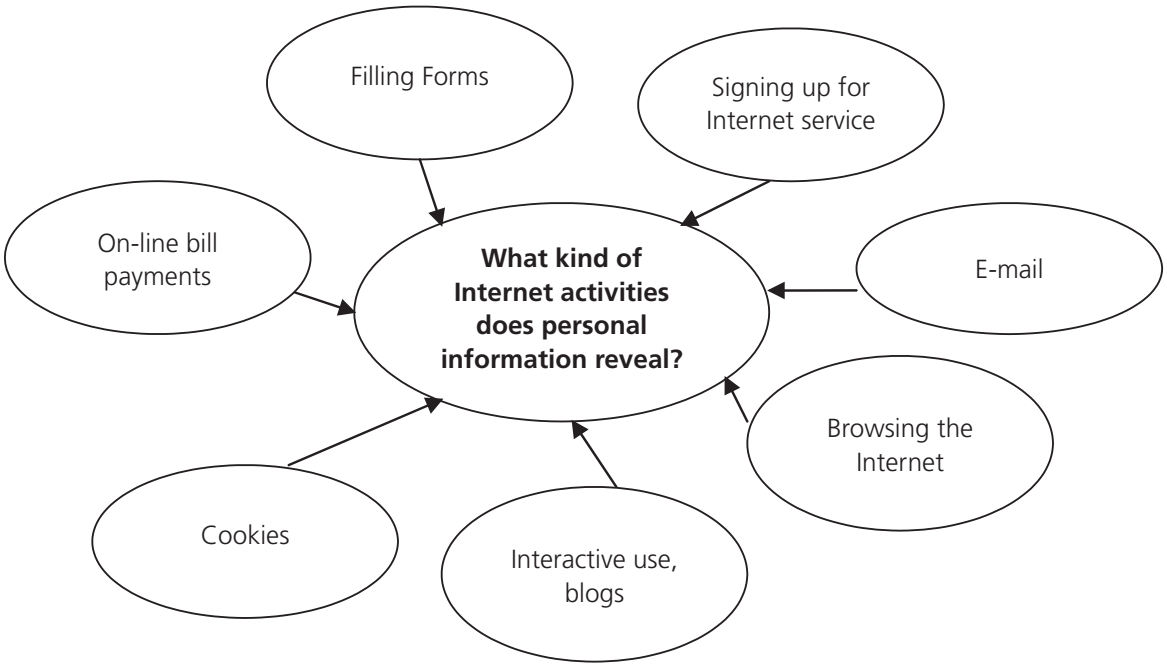
1 LEX.BG (Bulgaria).

— Telecommunications organisations provide basic networks for data transfer (point-to-point or point-to-multi-point connections).
— Access providers supply basic services for storage, transmission and presentation of traffic data.
— Information providers supply information stored in files and databases to users.
— Users access different kinds of Internet services.

Technological development and computerisation in all sectors further facilitate the access to and processing of personal data. In our daily activities, many of us are required to use personal data of other people and therefore to obey the rules for the protection of those data.

2 What kind of Internet activities does personal information reveal?

The most common ways we give information to others when using the Internet are summarized below:



— Filling in forms – registration forms, on-line application forms, on-line surveys, interest lists and e-mail subscription forms.

— Subscribing to Internet service – if you pay for the Internet ourselves, we sign up with an Internet Service Provider. Our IP address by itself doesn't provide personally identifiable information. But, because our Internet Service Provider knows our address, it is a possibly a poor link when it comes to protecting our privacy.

— The problem is that for personal data resemble as a 'black box' – once caught by the web site, the regular citizen does not know what happens to this data. Usually one only knows that he/she is obliged to present his/her personal data without knowing either for what exact reason or the data's final destination. The only thing that the regular citizen knows is that he/she is obliged to present his/her personal data when requested. Furthermore – often he/she is forced to present it in exchange for a service that he/she needs – access to information, library, payments, etc. Companies set the following principle: 'You are obliged to provide your personal data, but you are not obliged to know why you have to do so'.

— E-mail: undoubtedly people who correspond through e-mail are aware that they are giving information to the recipient. Very often the e-mail addresses of the members of these lists are easily available, sometimes on the e-mails sent and often through the group's web site. Although a subscription and sometimes a password is required to use such lists, there are no ways to avoid another member of the list gathering and spreading our e-mail address and any other information we post.

— Browsing the Internet; use search engines – our browsers likely provide our IP address and information about which sites we have visited to web site operators. Search engines have and use the ability to track each one of our searches. They can record our IP address, the search terms we used, the time of our search, and other information.

— Interactive use (Instant Messengers; Internet social networking sites): instant messaging conversations have a sense of casualness about them, which can lead some to let down their guard. Although seemingly informal, our instant messaging conversations can be easily stored, and recorded on our computers, social networking sites pose the same problem as blogs, message boards, and personal web sites – no one ever knows who will read his/her profile or look at his/her pictures. Employers, friends, dates, and parents can all access our information only with few difficulties.

— Cookies/Web beacons are a mechanism that allows a web site to record our comings and goings, commonly without our knowledge or agreement: In many cases, information obtained by means of cookie technology may constitute personal data (for example, in those cases where they are used to gather passwords and logins for access to information resources and services), while in many other cases it does not (as in cases where the only information stored in cookie files is the addresses of the sites the user visited).

— Personal websites and blogs: Anyone can look up the owner of a domain name online by using 'Who is' service.

— Managing financial accounts and on-line bill payments: online banking also requires us to transmit a lot of sensitive information over the Internet.

3 How do others get information about us online?

The Internet was arranged as an inherently insecure communications vehicle. Hackers easily penetrate the most secure facilities of financial and military institutions. Web companies have designed multitudinous ways to track web users as they travel and shop throughout cyberspace. Identity thieves are able to shop online anonymously using the credit identities of others. Frequently web-based information brokers spread sensitive personal data in order to increase the sales based on prior consumer choices.

We may presume that the same laws or social rules that protect our privacy in the physical world are in force in the digital world as well. But the Internet remains largely unregulated and the policies governing it underdeveloped. As we continue to adopt the technology it is important to be aware that in many ways it is still unexplored territory.

4 Personal data protection as part of the right to privacy

Due to the lack of specific provisions that would explain the types of information to be treated as personal data, one finds various approaches to the question of what part of the data collected and processed on the Internet is protected by law, and what part is not. It is possible to interpret this issue as proceeding from the concept of personal data as defined in the Personal Data Protection Act. This does add crucial criteria such as personal identification in determining whether or not a certain type of information constitutes personal data.

The expansion of the right to privacy cover four sub-categories:

— Physical inviolability – protection of the person in his or her physical aspect against procedures of interference such as tests for medications, experiments and so on;
— Confidentiality of correspondence – security and confidentiality of the post services, telephone lines, including electronic mail and other means of communication;
— Privacy of private property – posing restrictions against trespassing into the home and other kinds of environment;
— Inviolability of personal information – definition of rules managing the gathering and transferring of personal data such as credit information, medical expertise and so on.

The last category is also known as protection of personal data. It is a subject to special attention and regulations in Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and it forms the foundation of the Directive of the European Union concerning the personal data protection – 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.

To sum up, one may deduce that the argument for classifying all collected information as personal data goes too far. Nonetheless, this information constitutes a class of information that may become personal at a certain point. In other words, the information may be unimportant in itself, but should be protected by law from the moment that a basis exists for connecting it to a given individual. This possible connection introduces the necessity to ban its collection, maintenance, use and distribution without the agreement of the persons concerned.

5 Personal data protection in Bulgaria

At the moment, domestic legislation refering to privacy protection exhibits of a significant number of deficiencies and a needs for systematisation. Therefore, it is impossible to conclusively classify given

types of information about individuals and system configurations as personal data. Moreover, it is difficult to reliably and definitively specify whether certain actions in the use of a resource or system constitute constructive consent to the collection of personal data. It would seem, thus far, that the Personal Data Protection Act contains the standards, which are best suited to the predominant, level of social relations.

5.1 Legal Environment of Privacy Protection

The Bulgarian Personal Data Protection Act has been in force since January 1st 2002 and this Act represents the basis regulating the relationships in the field of processing and protection of citizens' personal data. The Personal Data Protection Act aims at guaranteeing the basic human rights of privacy and personal life by protecting the individuals from illegal processing of their personal data.

Bulgaria has ratified Convention No. 108 and it has been in force in the country since 2003. The adoption of a Personal Data Protection Act also took place and it is addressed towards the adoption of the rules of Directive 95/46/EC. The Act is based on the principles agreed in the European legislation facilitating the free movement of personal information within the European Union and guaranteeing equal level of protection. Bulgaria, however, is facing a greater challenge than the mere adoption of the necessary regulations and it is the effective enforcement of these regulations.

5.2 Principles

The principles of personal data processing are designated in Art. 2 of the Personal Data Protection Act and they are conform to the corresponding principles in Convention 108 of the European Council and the Directive 95/46/EU. According to those provisions conditions that guarantee high quality data processing should be provided.

When processing personal data, the data controllers must comply with the 8 key principles set out in the Data Protection Act. They can be summarised as follows:

- Fairness – 'personal data must be processed lawfully and in good faith'. A key point is that the individual must have given his or her consent to the data being processed. In the absence of consent, data processing will only be permitted if it falls within the other restricted circumstances as provided under the Data Protection Act.
- Purpose – personal data must be processed only for concrete, precisely defined and lawful purposes, and should not be processed additionally in a manner incompatible with these purposes.
- Relevance – personal data must be proportional, relevant and not excessive in relation to the purpose for which they are processed.
- Accuracy – personal data must be accurate and up to date.
- Preservation – personal data must be maintained in a status which allows identification of the respective natural persons for a period not longer than that required for the purposes for which the data are processed.
- Rights of individuals – personal data shall be processed only in accordance with the rights of the individual.
- Security – appropriate measures must be taken to keep the personal data secure to prevent unauthorised or unlawful processing or access of personal data and to prevent damage or accidental loss.
- Transfer of personal data – personal data shall not be transferred to a country or territory outside the European Union unless that country ensures an adequate level of protection for the processing of personal data.

These principles are a significant part of the regulation, because they serve as guidance for a proper reading and executing of the law, as well as guidance for personal data administrators.

Also of practical significance is that when no regulation of certain relations regarding personal data is available, the principles may be used in order to decide if there is an infraction of the requirement of

processing data lawfully, in good faith and proportional: that is as well as if the corresponding rights of the citizens have been violated.

5.3 Rights guaranteed by the Act

Personal data protection is accomplished through the rights guaranteed by the Act:

- The right to access to personal data related to natural person;
- The right at any time to require from the administrator of personal data confirmation if the data referring to him/her are processed, information about the purpose of this processing, about the category of the data and the recipients or the categories of recipients to whom the data will be disclosed;
- The right at any time to require from the administrator to delete, correct or block his/her personal data, the processing of which does not meet the requirements of this law;
- The right to object before the administrator against the processing of his/her personal data if legal ground for this exists; where the objection is grounded, the personal data of the respective natural person may not be processed any longer.

6 Problems

Undoubtedly at present the legal and technical protection of Internet users' legal privacy in Bulgaria is insufficient.

In spite of the fact that Personal Data Protection Act generally transposes the *acquis communautaire*, several requirements which are not in correspondence with the principles and the purposes of the Directive are laid down. These problems include the compulsory registration of the controllers, the restricted opt-in regime for processing personal data for marketing purposes and the gaps within the legislative regulation of the transfer of personal data to third parties could be mentioned.

Personal data protection is a new legislative sphere that penetrated the national legislation under the EU requirements. The low level of

protection in Bulgaria is mostly explained by the lack of knowledge, resources and some opacities in the acts. In the context of forming a new understanding of the citizens' protection a new legislation framework is being created. The lack of legislative traditions in this sphere influences how the 'personal data protection' theme is formulated and forces reconsideration of the current legal doctrine with a view to some other rights that compete with the right for private immunity. Thus, except for the problem with the enactment in various spheres other contradictions between the fundamental human rights and their legal understanding arise.

The intensively growing relations between juridical subjects and private individuals leads to the necessity of personal data security in national and international aspect. National legislation should ensure the main instruments for protection, while Community legislation aims to assign some general standards for personal data exchange.

As the Bulgarian Act was accepted in the course of the integration to the EU it mostly quotes the European directives and is deficient as to local specifications. The main critiques are towards the text itself (it is obscure) as well as towards the organisational framework of its enactment (need of interpreting, rights of the controlling structures, administrative capacity for realisation of these rights).

The most significant problem in Bulgaria is that even the existing act is not being observed. No one has ever heard of any penalties for a personal data administrator.

6.1 Problems of the Act itself

— Badly formulated aims that should correspond to the main requirements of the European legislature. Traditionally the European acts should guarantee free exchange of data and information and at the same time ensure observance of the main civil rights. In Bulgaria it is perceived that this Act should prevent gathering any kind of personal information.

— Incorrect formulation of the notion of personal data. The current law enacts that personal data protection is valid even for

persons that are participants in the ruling structures of the state's institutions. So this means that representatives in the public power are may stay hidden behind this act.

— Inadequate control over personal data protection that is currently expressed only in useless registration regimes.

From practice, and above all from intensive relations between legal and natural entities, the need arises for safeguarding personal data in both national and international terms. Local legislative authorities have to provide the main instruments of protection, while EC directives and the Council of Europe convention aim to harmonise the rules (within the EU at least) and establish common standards that allow for the exchange of personal data.

6.2 Personal data protection and e-Commerce

Effective legal mechanisms for personal data protection are needed in order to secure private life when personal data is required, processed and used for e-Commerce. However the regulations in the personal data protection sphere should not hinder the free flow of information and stop the development of the services in the information societies. A significant defect in the Bulgarian legislation is the lack of any regulation in the sphere of using non-requested messages for the aims of marketing (spam). More steps should be taken so that in the Bulgarian legislation to be implemented the best practices in this sphere.

7 Good practices

Regardless of the problems there are also a number of good practices followed by organisations processing data in order to ensure an adequate level of protection of the personal information of their users. The controllers of personal data that are web service providers adopt and implement general terms for the provision of their services in correspondence with the Personal Data Protection Act adopt internal technical and organisational rules for processing personal data, ensure

permanent possibilities for access to and correction of the user's data through the web and inform the users about their rights under the Personal Data Protection Act:

— The right to access and to correct their data;
— The right to object against processing of their data for the purposes of the direct marketing;
— The right of information about the processing of their data and the categories recipients to whom the data may be revealed.

Having a good privacy policy is the basis for gaining natural persons' trust, expanding the growth of companies, and indicating a high level of professionalism. Recent surveys show that the mainconcern of people who use the Internet is privacy – a fear of losing personal privacy is keeping consumers 'off' the Net. A plain and easy to access privacy policy indicates that a web company has taken a proactive approach by establishing guidelines for protecting privacy and sticking to them.

7.1 Privacy policy

A good privacy policy should form part of the terms and conditions for use of the website. To be effective it must be brought to the attention of the user. It is generally thought that the safest route is to include a scroll down window containing the privacy policy or at the very least a hyperlink to the privacy policy before the visitor submits his/her personal data. By clicking the 'submit' button, the user confirms expressly that the privacy policy has been read and that the terms of the privacy policy are accepted.

Most web sites make use of a user name and a password mechanism and require the visitor to log-in in his/her profile before placing or viewing an order or using a service. Having a restricted part of a web site only for members helps web sites to protect the privacy of their users. Even with restricted access, one should still gain consent from members as to whether they wish to be listed where all other members can view their information.

7.2 Opt in/opt out options

Opt in is the standard whereby the entity that gathers information from individuals assumes that it cannot disclose it or use it for secondary purposes without first getting permission from those individuals.

Opt out is the situation where the information-gathering entity can further use and disclose the information by default until such time as the individual says 'no'.

7.3 'Netiquette'

Netiquette requires member states to promote the elaboration of rules of ethics to aid the application of national EC Directive 95/46/EC legislation and account for the specific characteristics of the various sectors.

The rules created by means of self-regulation mostly aim to be part of legislative and national initiatives in the field of the web and Internet and to give assistance and encourage the acceptance and observation of ethical standards and practices in web business. The codes to a great extent guide for the corcect enactment of the edicts, regarding personal data processing.

The active participation of various groups from a certain branch – providers and users of some services – in building a system of rules guarantees the voluntary observance of these rules as well as covers the interests of all the sides that dispose of and proceed personal data.

The self-regulation of a certain branch appears to be a fundamental condition for 3 main purposes:

— An adequate level of security for the branch in using a certain service is created and ensured.
— The level of users' trust is increased.
— The legislation vacuum is filled and as a result the expenses for enacting the legislation are decreased.

In order to ensure the compliance of self regulation acts with national regulations Directive 95/46/EC introduces the obligation for institutions to consult the representatives of different sectors through all the stages

in developing the Personal Data Protection Act and that would ensure improvement of the conditions for citizens protection.

Despite the fact that the Bulgarian Personal Data Protection Act does not provide for this kind of self-regulation, there is no reason why the practice of consulting the Commission on Personal Data Protection on draft codes should not be established.

A code of the kind should contain the following:

- General principles of personal data protection in the respective branch of industry;
- Particular rules on protection in view of the specifics of the activities in the respective branch of industry;
- Procedures for adoption of the standards;
- Procedures for updating of the standards;
- Procedures in case of violation of the Code.

8 Social sensibilities towards the personal data protection problem

Nevertheless, the effective application of personal data protection, being a new element of the Bulgarian legal system, depends equally on the one hand on a good knowledge of the regulations on the part of the institutions and citizens, and on the other, on the effectiveness of the protection mechanisms, the activity and cooperation between the supervisory bodies and the good interaction between the institutions and the civil society. A wide public awareness is needed – the citizens in their capacity of subjects of personal data processing should know more about their rights, and the data controllers should know more about their obligations. Raising awareness among them of the commitments and the philosophy of personal data protection is extremely important for the practical effectiveness of the new legislation.

It is hard to speak of a serious social sensibility regarding this problem. There is no evidence that would amount to a certain statement of the public opinion concerning this issue.

9 Role of the controlling body

9.1 Surveillance

A key aspect of a good working regime for the protection of private life is the surveillance. Most of the countries that have passed an act for personal data protection also have created an independent structure that observes its execution. In different countries this structure and its representatives may posse variable power.

According to Art. 28 Directive 95/46/EC all the countries in the European Union should have created an independent structure that observes the enactment of the corresponding national regulations. According to the directive such structures should have broad and serious rights.

The commission – or commissioner – is obliged to take control over personal data protection and analyse the results according to the following parameters:

— Reason for taking the register;
— Aim of the register;
— Data groups in the register;
— Person's agreement;
— Means of data keeping;
— Means of data organizing;
— Means of organizing the access to data;
— Means of organizing the electronic protection.

9.2 Analysis of the activities

The final checks of Internet providers and Internet services sphere by the Bulgarian Commission show that:

— Reliable protection is ensured for the internal net of the personal data administrators. The public information (DNS, NTP, Anti-Virus Update) is secured by:
— Username and password needed for starting the OS on every single computer.

— The systems are safe in separated rooms and are under constant video surveillance.

— The information systems are secured at different levels.

— A client is installed to each system in order to be built a IPSec/VPN secured communication.

— All the data from the informational infrastructure is being reserved and the critical data is being archived.

— Usually the system administration is being handled locally by authorised officials but it is possible to administer the system from a distance.

— The register archive is being kept in locked metal cases.

— The access to the rooms with the servers is secured by metal doors and bars, magnetic cards and video surveillance. Only authorised officials are allowed to access the rooms. These are also secured by sensors for vibrations and microwaves. All the authorised access is also being archived.

— Internet service providers provide web hosting and guarantee a robust physical and program security to the web servers. They register users of different Internet services (e-mail for example). The registration includes agreement with the rules and terms of usage. The main problems here refer to the full identification of the users and publishing their data in the Internet.

9.3 Main difficulties with the control

The Internet service providers usually deny access to the personal data registers. Another problem is the absence of an administrator – mainly when the servers are not owned by the company being checked of the verification and the administrator is not an employee of this company. The ISPs also may deny access to their documentation.

In addition to ISPs other important sectors are the banks, international data transfer and electronic communications. Here we face problems with insufficient knowledge of the law and refusals to cooperate during verifications.

Improvements needed:

— More adequate amendments and supplements to the Act as well as creating the necessary acts;
— The work of the commission must become visible to the members of the society – free access to the register of the personal data administrators;
— Creating working offices of the commission.

This short analysis may be summarised in this way. The confidentiality of user information and the public nature of users' actions that arises from the nature of Internet services, standards and protocols are essentially two sides of the phenomenon of Internet access and use. At present it seems impossible to fully provide for one or the other by technological, or administrative and legal means.

10 Technological aspects

It is necessary to develop technical means to improve the users' privacy on the Net. It is mandatory to develop design principles for information and communications technology and multimedia hardware and software which will give individual users control and feedback with regard to their personal data. In general users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.

Furthermore, secure information networks, secure access to them and personal data protection are significant elements for safeguarding providing users confidentiality. The European Commission and the European countries are conducting a number of initiatives for fully implementing the Directive for electronic sign, that to a great extent will guarantee secure data exchange and the users' confidentiality. The legislative initiatives aim to encourage innovations in all the security issues and thus to prevent non-regulated interventions in the communication networks, which are a real threat to the users' confidentiality.

Measures against unauthorised access to information adequate to the contemporary technological achievements and relevant to the risks are

also undertaken by the web service providers. In the automated processing of personal data a trend can be seen towards overcoming the existing practice of relying on the protection offered by certain OS, software products, telecommunication devices and creating new measures for protection against unauthorised access to information using technological advances that provide a level of protection relevant to the risks connected with the processing and to the nature of the data to be protected. For access to the products and the services of certain web sites, login through username and password is introduced. Thus the access to the personal account (mail/service account) is secured.

Basic Internet security measures including online ISP, online filters, firewall, and virus, Trojan, worm, spyware and spam protection are only the beginning.

For corporate security Domain Controller, DNS, Proxy Server (URL Filters, Content protection, Anti Virus, Anti Spam, Data Security), encryption technologies (SSL encryption certificate) are used. For example the proper installation and the use of SSL mean that information sent by the individuals to a merchant's web site will be encrypted en route.

The development of the Internet to some extent places personal data protection in the hands of the individual users. The technologies that provide this opportunity are known as 'Privacy Enhancing Technologies' – PET. Internet users may apply a number of programs and systems that provide different levels of communication and personal data security. Among those are encodings, proxy servers, message forwarding, e-Payment, Ad-Blockings, browsers clean-Up, cookie managers, password managers, form fillers, and others. However there are some concerns about the safety and reliability of these systems.

11 Conclusions

Finally it will be decisive to find out how self-regulation by way of an expanded 'Netiquette' and privacy-friendly technology might improve

the implementation of national and international regulations on privacy protection. It will not suffice to rely on any one of these courses of action: they will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.

Web sites should make available a privacy policy that is easy to find. Ideally the policy should be accessible from the home page by looking for the word 'Privacy'. Privacy policies should state clearly how and when personal information is collected. Web sites should make it possible for individuals to get access to their own data. Cookie transactions should be more transparent. Web sites should continue to support anonymous access for Internet users.

All of the above requires guarantees for privacy of our personal data and personal lives while at the same time it demands the development of clear rules guaranteeing this protection.

Protecting privacy will be one of the greatest challenges for the Internet.

References and further reading

Center for Policy Modernisation, *Survey: Business and Personal Data Protection – Competition, Self-Regulation and Data Protection* (2005).

Swartz, *Internet Privacy and the State* (Connecticut Law Review, 2000).

Poster, *CyberDemocracy: Internet and the Public Sphere* (University of California, Irvine, 1995).

Birdsall, *The Internet and the Ideology of Information Technology* (Dalhousie University, Canada).

Landauer, *The Trouble with Computers: Usefulness, Usability, and Productivity* (Cambridge, Massachusetts: MIT Press, 1995).

Castells, *The Rise of the Network Society* (1996).

Kollock, *The Sociology of Cyberspace: Online Communities and Markets.*

Sandvig, *The Structural Problems of the Internet for Cultural Policy.*

Walton, *Internet Privacy Law* (2000).

Givens, 'Computer and High Technology' (*Law Journal*, February 11–12, 2000).

<http://www.sscnet.ucla.edu/soc/faculty/kollock/papers/vcommons.htm> (visited 27-May-07).
<http://www.sscnet.ucla.edu/soc/faculty/kollock/classes/cyberspace/resources/Jensen> (visited 27-May-07).
<www.datenschutz-berlin.de/doc/int/iwgdpt/bbmem_en.htm> (visited 04-June-07).
www2.warwick.ac.uk/fac/soc/law/elj/jilt/1996_3/data/?textOnly=true> (visited 04-June-07).
<http://www.firewallguide.com/privacy.htm> (visited 27-May-07).
<http://www.cpdp.bg/> (visited 23-May-07).
<http://www.privacy.org/> (visited 27-May-07).
<http://www.privacyinternational.org/> (visited 27-May-07).
<http://epic.org/> (visited 27-May-07).
<http://www.privacyalliance.org/> (visited 01-December-06).
<http://www.privacyresources.org/> (visited 28-May-07).
<http://www.privacyrights.org/netprivacy.htm> (visited 01-June-07).
<http://privacy.gateway.bg> (visited 23-May-07).
<http://www.cpdp.bg/> (visited 01-December-06).
<http://www.aip-bg.org/index_bg.htm> (visited 10-June-07).
<http://www.afcea.org> (visited 12-June-07).
<http://www.russianlaw.net/english/ae04.htm> (visited 12-June-07).
<http://www.netlitigation.com/netlitigation/privacy.htm (visited 15-June-07).
<http://www.eff.org/Privacy/> (visited 15-June-07).

PRIVACY, SECURITY AND LAWFUL INTERCEPTION: THE QUEST FOR A NEW BALANCE

Jari Råman[1]

1 Introduction

Surveillance in its many forms has always been at the core of discussions concerning privacy. The issues reach far beyond the narrow legal and governmental boundaries.[2] Surveillance is omnipresent and undertaken both by public and private actors for various reasons. Even governmental actors employ it, in addition to traditional counter-terrorist, law-enforcement and public-order purposes, also for reasons of government efficiency, productivity, and the provision of public services.[3] Surveillance technologies, practices and policies change rapidly.

---

1 LL.D., Post-doc researcher, Institute for Law and Informatics, Faculty of Law, University of Lapland, Finland.

2 This is what the multi-disciplinary research under surveillance studies has made visible. Of the long line of research see, e.g., David Lyon, *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press, 2001.

3 This is what the researchers of the Surveillance Studies Network point out in the follow up report for the 28th International Conference of Data Protection and Privacy Commissioners in London, 2–3 November 2006. See Kirstie Ball, David Murakami Wood and Charles Raab, *Part E: Postscript following the Conference of Privacy Commissioners* (2007), point 2.3.3., <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/surveillance_society_follow_up_report.pdf> (visited 24-Aug-2007).
The roles of the public and the private sectors in conducting surveillance was one of the major themes of the full report presented as the main theme of the London conference. See closer David Murakami Wood (ed., 2006), *A Report on the Surveillance Society*, <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf> (visited 24-Aug-2007).

When looking at the traditional reasons for surveillance by the government, the recurrent tendency, at least in the western democracies, to confer more investigatory powers upon law enforcement and security authorities is evident. The war against terrorism, together with the consequent need for and possibilities of increased cooperation between these agencies in Europe and worldwide, has long furnished the main justifications.

Technological change has also been one of the driving forces of the widening investigatory powers. The threats for and possibilities of surveillance provided by new information and communications technologies have significantly contributed to the everlasting conflict between governmental needs for surveillance and the rights and freedoms of the citizens. There are a host of issues that reflect the tension, such as data retention, camera surveillance, biometrics, the use of encryption, the use of location data in electronic communications, and governments' demands for the private sector to hand over databases.

While acknowledging the variety of means of surveillance and the wide range of private and public sector actors employing it, this paper focuses on one of the investigatory means of the law enforcement and security authorities: lawful interception and its regulation in the wake of another technological change. The study of surveillance as a social issue from a wider multi-disciplinary perspective does not take priority in this study. A much more modest approach is adopted for the sake of highlighting the problem area in a specific field.

Lawful interception refers here to the interception or recording of electronic communications in secret by law enforcement and security authorities in accordance with local law, and after receiving proper authorization from competent authorities. It is one of the central means for acquisition of information that these authorities use in the protection of national security, in the prevention of crime and in criminal investigations. It is an integral part of the state's obligation and ability to guarantee public order and security.

Lawful interception has often been at stake as technology and markets have developed. Earlier the fax, call forwarding and waiting possibilities,

together with the mobile communications, challenged the methods and extensiveness of lawful interception. More recently, the digitalisation of communications and the convergence of the different means of communications have meant changes for lawful interception capabilities. Furthermore developments in the market, such as the privatisation of former national monopolies (i.e., liberalisation) have changed the operational environment for lawful interception radically.[4]

The most recent challenges come from a paradigm shift in communications: circuit switching, where a dedicated point-to-point connection is required during the communication, is giving way to packet switching where data is moved in separate small blocks (packets) based on the destination address in each packet. Even though the current regulatory framework seems capable of addressing new technologies and associated services in many respects,[5] the changing operational environment for electronic communications has challenged lawful interception on many fronts.

2 The challenging operational environment

Lawful interception has traditionally been directed towards voice communications in public telecommunications networks. For a long time, it was performed by applying a 'tap' on the telephone line of the target (a.k.a. wiretapping). In the second phase of technological

---

4 Whitfield Diffie and Susan Landau depict the development of interception measures and consequent regulation in the US in an updated and expanded second edition of their book *Privacy on the Line: The Politics of Wiretapping and Encryption* (The MIT Press: Cambridge, 2007). For a short introduction from a wider perspective, see Gleave, 'The Mechanisms of Lawful Interception', *Network Security,* 2007(5), 8–11.

5 The need to change the current regulatory framework has been addressed in Europe especially in the Commission Communication on the Review of the EU Regulatory Framework for electronic communications networks and services COM (2006) 334 final (Brussels, 29.6.2006) and in the associated responses available at the EU Thematic Portal <http://ec.europa.eu./information_society/policy/ecomm/tomorrow/index_en.htm> (visited 28-Aug-2007). For developments at international and national developments in different countries, see the NGN Policy and Regulatory Resources page of the International Telecommunications Union's (ITU) Strategy and Policy Unit (SPU) at <http://www.itu.int/osg/spu/ngn/index.phtml> (visited 28-Aug-2007).

development the communications telephone switches could produce call records, and analogue voice records could store the content. Digitalisation, together with mobile voice and data communications, did not change the situation; lawful interception in the core networks was still possible. Even though the increasing sophistication of networks, e.g., in the case of later generation mobile networks (UMTS, 3G), has required new means of lawful interception, it has still been relatively easy. The networks and access to them have been at the control of few large telecommunications companies.[6]

The operational environment is, however, in a state of flux. The paradigm shift in communications from circuit switching to packet switching is changing the way we communicate. Email, instant messaging, chat, voice over Internet Protocol (VoIP) are just a few examples, and they keep on converging into new means of communicating in both mobile and fixed networks. Mobile telephony no longer delivers just voice but also text, image and video messaging, as well as location-based services utilising global satellite information and position systems. Video messaging combined with chat and document transfer is already in everyday use.

There are a host of challenging technical issues. Already the basic feature of packet switching, i.e., that data is moved in separate small blocks (packets) based on the destination address in each packet via different routes without point-to-point connection, causes many problems for the identification and collection of only those packets that are under the specific interception warrant. It also makes it more difficult to make the necessary separation of the content of the message from the traffic information that tells from where and when the message was sent and to whom it is going to. These have by no means been

---

6 For a short overview of the development of lawful interception, see for example Gleave, 'The Mechanisms of Lawful Interception', *Network Security*, 2007(5), pp. 8–11 and the report of the Information Technology Association of America (ITAA), Bellovin et al., *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP*, ITAA, June 13, 2006, pp. 5–6. <http://www.itaa.org/news/docs/CALEAVOIPreport.pdf> (visited 18-Sep-2007). For lawful interception technology in more depth, see the handbook of Paul Hoffman and Kornel Terplan, *Intelligence Support Systems: Technologies for Lawful Intercepts* (Auerbach Publications: Boca Raton, 2006).

unsolvable issues, but at least they have required much more computing power and storage capacity than in the case of interception of traditional point-to-point communication.[7]

While both mobile and fixed networks have largely converged into IP-based networks where traffic can also be transmitted also over open networks such as the Internet, the need to protect communication from the inherent security threats such as eavesdropping has gained increasing significance. For example, while the way we telephone in changing when VoIP technology, e.g., Internet Protocol based phone services (such as Skype), is becoming more common, there is a consequent change in way, the communication is protected. It is done in the terminal equipment by the user instead of the network operator encrypting the communication. This complicates lawful interception, because the access to the decrypted communication becomes more difficult.

At the same time the role of the traditional telecommunications operators in the supply of communication services diminishes and the number of service operators and types of networks to be covered increase significantly. The diversification of communications operators that, in theory, would have to equip their networks and services with capacities for lawful interception makes the enforcement of the lawful interception obligation more difficult. The increasing use of peer-to-peer protocols creates real problems even for the identification of the correct parties which are obligated to equip their systems with capabilities for lawful interception. There is a pressing need to find cost-effective solutions that are simple enough to be used in a secure manner by communications operators with varying capabilities.

---

7 For technical solutions, see the products and services gathered in to the web pages of the Global LI Industry Forum at <http://www.gliif.org/> (click 'LI Products' and 'LI Services' on the left) (visited 30-Aug-2007).

3 The constitutional context

Lawful interception has a strong legal basis. It has to have, due to the inherent infringements on the central constitutional and human rights of the communicating parties as well as on the freedoms of the communications operators that it entails. In western constitutional democracies the balance between the state and corporate interest and the rights and freedoms of the citizens has been set down in constitutions. Constitutional and human rights have been developed to limit the power of the government to use surveillance as a central means of control.

Article 8 of the European Convention on Human Rights (ECHR), entitled 'Right to respect for private and family life' is illuminating:[8]

> Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The first subsection expressly recognises privacy and confidential communications as fundamental human rights similar to other regional and international human rights instruments.[9] The loss of privacy and that of confidential communications has naturally been the primary concern in relation to surveillance in general and lawful interception especially. The challenges of integrating data protection principles into Community legislation and of making effective data protection a basic condition for the success of EU policies has been emphasised by the

---

8 Council of Europe (CoE) Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 005, is available on the official treaty web site of the Council of Europe at <http://conventions.coe.int/> (visited 30-Aug-2007).

9 See, e.g., Bygrave, 'Privacy Protection in a Global Context – A Comparative Overview', p. 332, in Wahlgren (ed.), *IT Law*, Scandinavian Studies in Law, 47 (Stockholm Institute for Scandinavian Law: Stockholm, 2004), pp. 319–48.

European Data Protection Supervisor, Peter Hustinx, who, in the Foreword of the Annual Report for the year 2006, notes that '[I]t is clear that this also involves an effective integration of privacy perspectives in some areas – such as public security and law enforcement policies – that sometimes seem to be at a different course'.[10]

Privacy remains as the main concern also with the changing operational environment. As communications networks, services and technologies converge, which is followed by the convergence of the related markets and regulation, the potential for surveillance in general grows exponentially. The possibility to gather more data from communication devices which are constantly becoming more complicated naturally provides benefits for the law enforcement and security authorities, but also, at the same time, increases the risk of infringements on the communicating parties' right to privacy.

Privacy is not, however, the only concern in relation to lawful interception. The security of communications and of information systems is an equally significant concern. The means of interception developed within communications protocols, networks and devices open a hole in the security of a network. With the centralised circuit switched telephone systems the control of authorised access has been relatively effective; the lawful interception capability has been accessible only at the relatively well protected premises of the communications operator.[11] When the networks are increasingly

---

10 See European Data Protection Supervisor, *Annual Report 2006* (Luxembourg, 2007), p. 11, <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2006/AR_2006_EN.pdf> (visited 17-Aug-2007).

11 There have been incidents of lawful interception capabilities being misused by outsiders. For example, the lawful interception system in place of a major Greek mobile communications operator was misused by crackers in an illegal interception scheme of several mobile phones of members of Greek government and high level civil servants. For a wider depiction of the case that was exposed in 2006, see Prevelakis and Spinellis, 'The Athens Affair' (2007), *IEEE Spectrum*, July, <http://www.spectrum.ieee.org/jul07/5280> (visited 4-Sep-2007). But these cases are rare, and as Bellovin et al. point out in *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP*, p. 12, the protection of the premises keeps the lawful interception in the hands of authorised personnel to a sufficient degree.

interconnected and interoperable, the risk of misuse of the interception tools is higher. The increasing number and the differing capabilities of the new types of communications operators obliged to equip their systems for interception by no means mitigate the risk. The threat of a hacker gaining control of the means of interception is real.

Information security is a serious constitutional concern. The role of information security in the context of human rights is not, however, as clear as with the case of privacy.[12] Information security is a multi-faceted concept that permeates the whole legal system.

The traditional view of security is that of national security or public safety. In this sense also information security is part of the assumption of efficiency of the state machinery to which the constitution sets limits. It is part of the security interests of the government against whose expansion and abuse the human and constitutional rights provisions give legal protection.[13] This is clearly visible in the second subsection of Article 8 of the ECHR, which stipulates that privacy is not an inviolable right and then spells out the bases and requirements for the infringements on the right to privacy. These requirements also apply to the use of lawful interception.[14]

Information security is not, however, only a justification for the limitation of rights. It is among the factors that define the de facto efficiency of some fundamental rights and freedoms. This has recently been acknowledged also at the policy level of the EU, when the

---

12 The concept of information security is used here as a generic upper level concept. It covers all the different areas of specialisation, including communications security, computer security, network security, etc.

13 In the background of the constitutions of democratic states there is an assumption of efficiency of the exercise of public powers that also concerns the use of coercive and investigatory means, to which the constitution sets limits. Central limitations to the power of this machinery is set by the basic rights provisions; basic rights and liberties, stated not just in national constitutions but also in international conventions on human rights, are prerequisites for democracy that have to be protected also from abuses of power by the state.

14 From this perspective information security is a collective good for the purposes of which the rights and freedoms of individuals can be limited, provided that the requirements set out in the system of human rights and constitutional law are obeyed.

Commission in its communication on a strategy for a secure information society stipulated in 2006 that security is one of the prerequisites for guaranteeing fundamental rights on-line.[15] Information security guarantees the functioning of the society and the use of rights therein.

In the face of the law, information security is also an object of legal protection in criminal law. The main features or characteristics of information security, i.e., confidentiality, integrity and availability, are protected in themselves. At the international level, this is most clearly visible in the Council of Europe Convention on Cybercrime (ETS No. 185) which requires (Chapter II, Section 1, Title 1) that certain core computer-related offences, i.e., offences against the above mentioned three basic elements, or qualities, of data, data processing and information and communication systems, need to be established as criminal offences by the signatory states.

In addition to being instrumental for the effectiveness of many informational rights in the network society, information security is also a right in itself. Information security no longer just guarantees the functioning of the information infrastructures where we use our rights, and thus promotes the efficient realisation of those rights; it also protects us as individuals, as participants in the network society, against arbitrary interference with the security requirements of our information.

This is visible in the basic regulatory approaches of European data protection regulation. The explicit objective of the Personal Data Directive is to protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data.[16] For the achievement of this objective the

---

15 Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions – A strategy for a Secure Information Society – 'Dialogue, partnership and empowerment' (SEC (2006) 656), COM (2006) 251 final, heading 2, paragraph 6.

16 Article 1 titled 'Object of the Directive' of the 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, OJ L 281, 23.11.1995, pp. 31–50.

Directive sets, among other things, specific information security obligations for the controllers of personal data. Information security is thus a substantive right of an individual, who can demand a certain level of security from those controlling their personal data. Preamble 46 of the Personal Data Directive spells is out clearly:

> [...] the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing.

Information security could be conceptualised even as a basic right in itself. The Article 5 of the ECHR entitled 'Right to liberty and security', could be constructed to include a right to informational security of an individual. If it is constructed as including a right of access to the information, ideas, and communication media that allow people to take part in society, it can, at the same time, also be seen as including a right to do it in a secure manner. The normative argument is that, whereas the right to physical privacy (i.e., domestic peace) has been amended in the information society with the right to informational privacy (especially personal data protection), the right to physical security has to be amended with the right to informational security.[17]

There currently is, however, little authoritative support for such an interpretation. The right to security of person enacted in the article continues to be tightly connected to physical security. In addition, there is very little room for the independent meaning of the right to information security. The rights to liberty, integrity, privacy and to

17 From this perspective information security is an individual right, instead of a collective good of the society. The separation of these two aspects of the legal principle of information security is not absolute but important. One of the central differences between collective goods and individual rights is the indivisibility of the former: collective goods cannot be divided up into individual rights. When understanding information security as an individual right, the probability of the realisation of a threat has to revert to the individual level and, the concreteness of the threat has to be higher at the individual level than in the case of information security as a collective good. The security of the individual is advanced even when information security is enhanced as a collective good, but it does not have to revert to the individual level.

confidential communications which guarantee our right to informational self-determination, together with the informational property rights, already cover almost all aspects of the right to information security. In a preliminary national analysis information security as a constitutional right could derive independent significance especially from the horizontal relations between private actors in society and the public authorities' obligation to secure the realisation of basic rights also on this horizontal axis.

Despite these problems, the understanding of the dual nature of information security in relation to basic rights and liberties is essential for the legal definition of information security. Without a comprehension of this duality of information security as a necessity for the effectiveness of other rights and as a right in itself, the importance of information security and its role in the network society becomes blurred, especially in cases where either the public authorities or the private actors interfere with the basic rights and freedoms of others.

4 The changing regulatory framework

The balance between the competing interest of law enforcement and security authorities, communications operators and intercepted parties, respectively, has been set in the law. It has to be, due to the inherent infringements on the central constitutional rights of the communicating parties visible already in the Article 8 of the ECHR. It is not just about the right to privacy, to confidential communication and information security, but also about the communications service operators' freedom of action and freedom to engage in commercial activity.

Regulation has largely concentrated on the requirements under which lawful interception can be conducted (e.g., the nature of the offence that may give rise to an interception order) and how the gathered information can be used (by whom and for what purposes; e.g., as evidence in court). The majority of the national legal provisions and international cooperation concerning lawful interception, as with any other investigatory and coercive means employed by the law

enforcement and security authorities, concentrates on the use of lawful interception in the acquisition of information.[18] It poses the biggest risk of infringement on basic rights and liberties.[19] These are the issues that, at minimum, have to be stipulated in the national statutes concerning lawful interception and other covert measures of surveillance developed in the case law of the European Court of Human Rights.[20]

There is also an important underlying issue that has been seriously affected by changes in technology and markets. The changing communications environment has challenged the execution of lawful interception in the new networks and services and, at the same time, the extensiveness of lawful interception as a means to acquire information. At the regulatory level this concerns rules obligating communications operators to equip their systems with the capabilities for lawful interception, and the requirements for the development of needed systems for interception.[21]

---

18 For example, the mutual assistance between member states in relation to the interception of communications has been a central focus in the development of the area of freedom, security and justice in the European Union. It has resulted in, for example, the provision on the interception of telecommunication in the Council act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, p. 1, Title III, Articles 17 to 22). For more information, see the web pages of the European Commission responsible for the policy on freedom, security and justice at <http://ec.europa.eu/justice_home/index_en.htm> (visited 6-Sep-2007).

19 For recent privacy related developments in the area of freedom, security and justice see the annual report of the European Data Protection Supervisor for the year 2006, pp. 50–6, <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2006/AR_2006_EN.pdf> (visited 17-Aug-2007).

20 See *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, No. 62540/00, § 76, ECHR, 28 June 2007 and *Weber and Saravia v. Germany* (dec.), No. 54934/00, ECHR 2006.

21 For example, the relevant Finnish provisions can be found in the Communications Market Act (393/2003) sections 95 to 98. An unofficial translation of the Act can be found from the Finlex service at <http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf> (visited 6-Sep-2007). In the US the basic provisions are in the Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C. §§ 229, 1001–10, 1021).

Countries, depending on their level of technological neutrality in regulation, have also amended these provisions to the changes in technology and markets and the consequent changes in criminal communications. An important contributor to the development of regulation concerning the design and development of lawful interception systems in the EU has been the European Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications.[22] It presented, on a pan-European basis, requirements of law enforcement agencies relating to the lawful interception of telecommunications similar to CALEA in the US Member States have passed legislation to comply with the requirements under their specific jurisdiction.

At the same time, different standardisation groups have been defining interfaces for lawful interception systems. The way the communications network is to be intercepted and the intercepted information is to be delivered to the law enforcement and security agencies has been highly standardised.[23] This also applies to modern mobile networks.

The new IP-based operational environment has also called for a re-evaluation of the extensiveness of the scope of the provisions obligating communications operators to equip their networks and systems with lawful interception capabilities. The convergence of networks and services together with peer-to-peer protocols and the increasing number of new types of communications operators with varying capabilities are, among other things, issues that have questioned the extensiveness of these obligations.

Lawful interception is a regulatory reality in most European countries and outside Europe; VoIP providers and other operators of new communications services have not been immune. Several countries have already amended, or are in the process of amending, their laws to

---

22 Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, Official Journal C 329, 4.11.1996, pp. 1–6.

23 For standards worldwide, see the web pages of the Global LI Industry Forum at <http://www.gliif.org/> (click 'LI Standards' on the left) (accessed 30–Aug–2007), which is an independent non-profit trade association concentrating on lawful interception (LI) products and services.

adapt to the new IP-based operational environment where necessary.[24] Legislators and national communications regulators have acted as a central location for discussion in relation to the possibilities and limits of lawful interception in relation to new communications media.

For example, in the US the Federal Communications Commission has obligated providers of certain broadband and interconnected Voice over Internet Protocol (VoIP) services to be prepared to accommodate law enforcement wiretaps.[25] In Finland, the national communications regulator FICORA (Finnish Communications Regulatory Authority) has made explicit its interpretation of the legislation concerning communications markets, according to which a the telecommunications operator providing publicly available voice services that are implemented by means of IP technology (i.e., VoIP services) also has the obligation to equip its systems with the capabilities for lawful interception.[26]

There has, however, been a long delay in the introduction of standards for IP-based communication. The standardisation of the interception

---

24 For international policy considerations in relation to IP-based communications environment and the VoIP services especially see, e.g., OECD Working Party on Telecommunications and Information Services Policies, 'VoIP: Developments in the Market', <http://www.oecd.org/dataoecd/56/24/35955832.pdf> (visited 5-Sep-2007) and OECD Working Party on Telecommunication and Information Services Policies, 'Policy considerations of VOIP', DSTI/ICCP/TISP(2005)13/FINAL <http://www.oecd.org/dataoecd/59/55/36316212.pdf> (visited 5-Sep-2007).

25 See, *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, Second Report and Order and Memorandum Opinion and Order, FCC 06-56 (released May 12, 2006) (*Second Report and Order*), available, e.g., at <http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf> (visited 7-Sep-2007).

26 This implies that lawful interception no longer is as an extensive means to acquire information of the contents of voice communication as it has been. This could be the situation if we simply accept the conclusion FICORA makes about the non-applicability of the Finnish communications market legislation to communications services based on peer-to-peer network applications such as the Skype Classic, where users of the provided software programme may make VoIP phone calls to other users of the same software. See the White Paper in the matter of the regulation of Skype services in Finland, 587/532/2005, <http://www.ficora.fi/attachments/englanti/1156489126854/Files/CurrentFile/Skype_final_English.pdf> (visited 7-Sep-2007). Note that the consequent wider FICORA guideline totally ignores such services; see FICORA, *Application of the Communications Market Act to VoIP Services in Finland* <http://www.ficora.fi/attachments/suomi_R_Y/1158858995280/Files/CurrentFile/VoIP-ohje_eng.pdf> (visited 7-Sep-2007).

of IP-based communications turned out to be a complicated issue without a clear responsible actor. The Internet Engineering Task Force (IETF), one of the most central bodies in Internet standardisation, hurried a decision not to support standards track work on lawful interception already on 1999.[27] Some have considered this lack of involvement of the Internet community in the development of lawful interception systems as having a negative influence on the information security of lawful interception systems and on the privacy of users of IP-based communications systems and networks.[28]

In this millennium ongoing work has continued on many fronts, including the IETF. Specific IP related standards have been and are currently being developed in such standardisation bodies as the Third Generation Partnership Project (3GPP) for mobile communications and the European Telecommunications Standards Institute (ETSI) in Technical Committee Lawful Interception (ETSI/TC LI).[29] Even though lawful interception is considered under EU law to be a national matter regulated only by non-binding secondary legislation,[30] such as

---

27 For a depiction of the reasoning behind the IETF's decision see IETF Network Working Group, *IETF Policy on Wiretapping*, Request for Comment (RFC) 2804, May 2000, available at <http://www.ietf.org/rfc/rfc2804.txt> (visited 30-Aug-2007).

28 For a depiction of the negative consequences of this decision from the point of view of developing interception systems, see the critical arguments of Philip Branch in 'Lawful Interception of the Internet' (2003), *The Australian Journal of Emerging Technologies and Society*, 1(1): pp. 38–51, <http://www.swinburne.edu.au/sbs/ajets/journal/V1N1/pdf/V1N1-4-Branch.pdf> (visited 30-Aug-2007).

29 For the ongoing work in the European Telecommunications Standards Institute (ETSI), see the status report of the TC LI at <http://portal.etsi.org/li/status.asp> (visited 30-Aug-2007). TC LI is the leading body for lawful interception standardization within ETSI, even though interception standards have also been developed by other ETSI technical bodies. For more details, links and official sources see the web pages of ETSI/TC LI at <http://portal.etsi.org/li/Summary.asp> (visited 5-Sep-2007). For ongoing standardisation work for lawful interception worldwide, see the web pages of the Global LI Industry Forum at <http://www.gliif.org/> (click 'LI Standards Activities' on the left) (visited 30-Aug-2007).

30 This approach has been restated in Framework Directive 2002/21/EC recital (7) and in the 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), OJ L 201, 31.7.2002, p. 37, Article 15(1) and Preamble 11, as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, OJ L 105, 13.4.2006, p. 54.

the above mentioned resolution that suggests certain lines of action without imposing any legal obligations, the European Commission, in its 2004 Green Paper on the treatment of VoIP under the EU Regulatory Framework, urged Member States to agree on common standards for lawful interception in VoIP in order to make it easier for equipment manufacturers to develop necessary products and mechanisms.[31]

5 Need for new type of regulation?

The regulation of the design and development of lawful interception systems is essentially standards based. In many countries there are only general provisions on the obligations of telecommunications operators to equip their systems for interception. For example, in Finland only two provisions in the Communications Market Act (393/2003) concern the issue of requirements for the design and development of LI systems: the obligations of telecommunications operators to equip their systems for interception (section 95) and the process by which technical requirements for LI are decided and when the required instruments and features ought to be installed in the communications networks and services (section 96).[32]

Currently it is the Finnish Communications Regulatory Authority (FICORA) that decides in individual cases on the technical requirements imposed on an instrument or feature used in lawful interception. This happens, however, after consulting both the telecommunications operator and the public authority performing the interception of communications. There are no general legal rules on the technical requirements or even on the substantive considerations under which they have to be decided.

---

31 European Commission, 'The Treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework: An Information and Consultation Document', Commission staff working document, Brussels, 14.6.2004, heading 5.5.2., <http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/commiss_serv_doc/406_14_voip_consult_paper_v2_1.pdf> (visited 5-Sep-2007).

32 An unofficial translation of the Act can be found from the Finlex service at <http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf> (visited 6-Sep-2007).

The justification for these provisions in the Government Proposal 112/2002 on the amendment of legislation concerning the communications market concentrates mainly on the benefits and costs of required devices and systems together with their interoperability, reliability and security. These are all important concerns in the design and development of lawful interception systems, but by no means sufficient. The basic rights and liberties such as the right to privacy and the individual right to information security ought to have been given much more emphasis.

The sparseness of the regulation and the lack of consideration are surprising considering the constitutional background of the regulations and the influence they have on the privacy of users and the security of their information and the systems used in communications. Already the Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications acknowledged the need to observe the right to privacy as enshrined in the territorially applicable national law when implementing interception measures.[33]

In addition, such regulation is commonplace in other areas. Especially in the case of surveillance by private companies the requirements of the systems have been fairly strictly stipulated.[34] Furthermore the general and sectorial data protection regulation obligates the controllers of personal data to consider the best available technology and provides relatively specific requirements for the development data processing systems.[35] The Article 17(1) paragraph 2 of the Personal Data

---

33 Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, Official Journal C 329, 4.11.1996, pp. 1–6. The preamble of the resolution even makes explicit the Council's awareness of the fact that the observing of the right to privacy comes up against specific legal and technical difficulties as technology develops.

34 This is the case, for example, in relation to camera surveillance in workplaces. The preconditions of the surveillance and the transparency of its implementation are regulated in the Finnish Act on the Protection of Privacy in Working Life (759/2004) chapter 5, sections 16 and 17.

35 Actually many of the articles in 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 (OJ L 281, 23.11.1995, p. 31) can be read as giving direct guidance on the development of

Protection Directive (95/46/EC) on the security of processing is especially illuminating in the way it sets down the bases for making decision on information security measures to be implemented: 'Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected'. These regulations do not concern only the use of the systems and the information gathered, but also the requirements of the (surveillance) systems themselves.

The importance of the legal requirements for lawful interception systems is on the rise together with the need for clear rules for their design, development and implementation. This is due to the expansion of the legal obligation to equip communications services and networks with the technical instruments and features that allow interception of electronic communications, to include a variety of new telecommunications operators beside the operators of fixed and mobile communications networks and services. The requirements the law more generally sets for the design of lawful interception systems need to be made explicit as the number of parties needing to comply with the legal obligations rises and the differences in their expertise become deeper.

Of course the requirements can be deducted from general data protection regulation and the principles visible in the basic and human rights provisions. This does not, however, fulfil the requirement of specificity set for the limitations of basic rights and liberties made in accordance with the law. As the European Court of Human Rights in Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria emphasised, '[I]n view of the risk of abuse intrinsic to any system of secret surveillance, such measures [of

---

processing systems. Similarly in 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) (OJ L 201, 31.7.2002, p. 37). Strictly speaking, it is data controllers who bear legal responsibility for complying with data protection rules. However, those who design technical specifications and those who actually build or implement applications or operating systems also bear some responsibility for the data protection aspects from a societal and ethical point of view.

surveillance] must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated'.[36]

The changes in the communication paradigm and the increasing number of communications operators makes one also question the appropriateness of the decisional frames concerning the technical requirements imposed on an instrument or feature used in lawful interception. Is it appropriate to leave such an important decision that centrally concerns the rights of individuals and the security of their communications solely in the hands of regulatory agencies without substantive guidance established in the law?

When comparing the situation to the decision-making in court in relation to the warrants for lawful interception, the answer seems to be no. The basis of the decision-making in court is regulated at the level of parliamentary acts in a relatively detailed manner. The balancing of the interest of the law enforcement and security authorities together with the rights of the intercepted parties done by the court is not that different from the balancing of the interest of the authorities, the freedoms of communications operators and the rights of the intercepted parties done by communications regulators in Finland.

The equipping of communication networks and services with technical instruments and features to allow the interception of electronic communications essentially threaten our basic rights and liberties. It is not only about the right to privacy and confidential communications, but also about the individual and collective right to security together with the freedoms of action and to engage in commercial activity of the operator.

---

36 *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 4 April 1990, Series A No. 176-B, p. 55, § 32; *Amann v. Switzerland* [GC], no. 27798/95, § 56 *in fine*, ECHR 2000-II; and *Weber and Saravia v. Germany* (dec.), No. 54934/00, ECHR 2006. Note that the concept of 'law' does not necessarily restrict itself only to Parliamentary acts; any valid legal rule in the jurisdiction in question is sufficient. The choice of the legal instrument depends on the regulatory culture of the country and the restrictions of its constitution.

This could be a crucial lack in a democratic constitutional state where the basics of the use of constitutional rights ought to be at the level of parliamentary acts.[37] It is no longer appropriate to rely on the old administrative type of regulation. The decision on the technical requirements imposed on an instrument or feature used in lawful interception does not concern just technology; it is decision-making on the informational infrastructure where we use our rights.

More specific regulation of the design and development of LI systems is needed from the constitutional right perspective; the requirements at the general level need to be laid down at the level of the law. The decisional frame ought to include consideration of such issues as state of the art and the associated costs, the rights of individuals and freedoms of the operators, the security of communications and the security interests of the state.[38] The bases for the decisions need to be made explicit.

The standards based approach (where national regulators effectively decide on the requirements of lawful interception systems after consulting the enforcement and security authorities) is not sufficiently informative for the changed operational environment. In addition, in its current form it does not involve the necessary procedural and substantive constitutional protections from the misuse of power by the regulator. It is not sufficient that a non-democratic regulator negotiates the requirements with the actors' possible infringing of basic rights and liberties, stipulating them in an administrative lower level regulation without any substantive guidance set down by a democratic regulator.

---

37 This is especially the case in countries like Finland, where the Constitution (731/1999) requires many matters, e.g., issues concerning basic rights and liberties, to be regulated at the level of parliamentary acts rather than secondary legislation or other instruments, as pointed out also by the OECD in its review of regulatory reform in Finland (OECD, 'Government Capacity to Assure High Quality Regulation in Finland' (2003), *OECD Reviews of Regulatory Reform*, Paris, p. 30, <http://www.oecd.org/dataoecd/32/52/2510133.pdf>). There is a heavy reliance on primary legislation that is very specific and detailed command-and-control type in the Finnish regulatory culture due to the strong legalistic tradition.

38 This is, in essence, a manifestation of the principle of proportionality as already visible in an exemplary manner in Article 17(1) paragraph 2 of the Personal Data Protection Directive (95/46/EC).

The technology – harnessing regulation – has to be subject to the same constitutional self-restraints as the use of the 'law'.

6 Conclusions

Even though the regulation of lawful interception per se is essentially based on basic rights issues, the role of basic rights and liberties has not been of much concern when regulating the requirements for the design and development of interception systems or the process by which they are decided. The regulation of the underlying technology has not been under similar constitutional constraints as the use of lawful interception.

This could pose a risk to our right to privacy as well as with information security as an individual right and a collective good: especially because both the technical requirements set for the product manufacturers and the possibilities of communications operators to conduct lawful interception are in a state of flux. This creates real threats of contradictions between the needs of the authorities, the rights of the intercepted parties and the freedoms of the communications operators.

Whitfield Diffie and Susan Landau argued in the US context at yet another time of pressuring for new surveillance methods in Privacy on the Line that if we are to retain the privacy that characterised face-to-face relationships in the past, we must build the means of protecting that privacy into our communications systems.[39] The same argument applies to the security of communications. In the changing environment we also need better regulations to direct and create an obligation for the development of balanced approaches to lawful interception.

---

39 Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (The MIT Press: Cambridge, 2007). Whereas the original 1998 version of the book was written at a time when pressure for new surveillance methods was mainly due to the possibilities technology faces, the updated and extended 2007 edition has been written furring yet another round of increasing demands for surveillance; this time mainly due to the needs of the 'War against Terrorism'.

There is a pressing need to find means for lawful interception that could serve the needs of law enforcement and security authorities in guaranteeing public order and security in this new operational environment in a manner that does not infringe on the basic rights and liberties of citizens or the basic freedoms of action and engagement in commercial activity of the communications operators more than our Constitution allows. This requires that the regulatory framework for the design and development of lawful interception be seen in the same constitutional context as the exercise of interception; the same restrictions and safeguards ought to apply.

ISSUES OF DATA PROTECTION WITHIN AND BESIDES THE EU REFORM TREATY OF LISBON

Irini Vassilaki[1]

1 Introduction

The EU Reform Treaty that was approved on October 2007 in Lisbon and will be formally signed on December 2007, will rename the EU Treaty (TEU) as the 'Treaty on the Functioning of the European Union' (TFEU) and will have a significant influence on the future of Europe. The adoption of the Charter of Fundamental Rights as a document that has the same legal value as the Treaty, the disappearance of the pillar structure, the new legal bases in many fields such as energy, tourism, administrative cooperation, the qualified majority voting and the simplified procedures for amending the Treaties are some of the new features of the Treaty that will affect the development of the EU.[2]

A substantial change concerns the scrapping of the third pillar of the current regime that concerned Police and Judicial Cooperation in Criminal Matters. The Reform Treaty amends the chapter entitled 'Area of freedom, security and justice (AFSJ)' and will as consequence expand police and judicial cooperation in criminal matters among the EU-Members.[3]

---

1 PD Dr. Irini Vassilaki, Athens/Munich.

2 For the text of the Reform treaty see in: <http://consilium.europa.eu/cms3_fo/showPage.asp?id=1317&lang=en>.

3 See also J. Kokott, *Stellungnahme zu Fragen des Europäischen Strafrechts*, pp. 8 et seq.

This paper will examine whether the new European legal status guarantees during judicial cooperation in criminal matters the fundamental rights of the citizen, taking as example the protection of personal data.

2 The Legal Framework for the Judicial Cooperation in Criminal Matters within the EU Reform Treaty

It has already been mentioned that the 'third pillar' of the EU Treaty on European Union, dealing with policing and criminal law, will be moved to the TFEU and be merged with the provisions of Title IV of Part Three of the TFEU, which, in the current regime, deals with immigration, asylum and civil law. Judicial cooperation is regulated in Art. 69e to Art. 69i of the TFEU. Art. 69e TFEU foresees the procedural presuppositions that permit judicial cooperation, whereas Art. 69f TFEU covers the substantive premises of the judicial cooperation.

69e par. 3 and 69f par. 3 TFEU provide the Member States with the possibility of an 'emergency break' if one of them considers that a draft legislative act may affect fundamental aspects of its criminal justice system. In this case the member may request that the draft directive be referred to the European Council and the ordinary legislative procedure shall be suspended.[4] After discussion, and in case of consensus, the European Council shall, within four months of the suspension, refer the draft directive back to the Council, which shall terminate the suspension of the ordinary legislative procedure. In case of disagreement, and if at least nine Member States wish to establish enhanced cooperation on the basis of the draft directive concerned, they shall notify the European Parliament, the Council and the Commission accordingly.

Art. 69f par. 1, sub. 2 specifies the serious crimes that must be combated on a common European basis. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation

4 See Suhr, *Stellungnahme zu Fragen des Europäischen Strafrechts*, pp. 22 et seq.

of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. In this way TFEU expands the competence of the EU in the area of criminal law in comparison with the current legal situation. Furthermore Art. 69f par. 1, sub. 3 TFEU foresees that the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. The council shall act unanimously after obtaining the consent of the European Parliament. The potential of this possibility of the Council is obvious. The Council obtains the option to establish by means of directives minimum rules concerning the definition of criminal offences and sanctions. This procedure would split the differences between 'European criminal offences' and 'national' criminal law and sanctions. The question, however, whether this development is a positive one for Europe, is beyond the scope of this paper.[5]

In addition to the change detailed above, Art. 69f par. 2 TFEU authorizes the Union, in an area which has been subject to harmonisation measures, to prepare directives that may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. This procedure will be followed, if such steps are essential to ensure the effective implementation of a Union policy as far as the approximation of criminal laws and regulations of the Member States are concerned.

Art. 280 par. 4 TFEU foresees a specific competence for the creation of supranational criminal law as far as the protection of the financial interests of the EU is concerned. The new formulation of this article makes possible the creation of concrete criminal provisions, even though for cases of fraud within EU (EU-fraud), all the Member States should be found. This procedure could be the first step towards the development of a European Criminal Law.

Judicial cooperation in criminal matters in the Union shall be based, according to Art. 69e par. 1, on the principle of mutual recognition of

---

5 See C. Calliess, *Stellungnahme zu Fragen des Europäischen Strafrechts*, pp. 35 et seq.

judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 69f. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures – among others – to facilitate cooperation between the judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions.

To facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters, the European Parliament and the Council may, according to Art. 69e par. 2 TFEU, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules. Such rules shall take into account the differences between the legal traditions and systems of the Member States.

They shall concern:

— the mutual admissibility of evidence between Member States;
— the rights of individuals in criminal procedure;
— the rights of victims of crime;
— any other specific aspects of criminal procedure which the Council has identified in advance by a decision; for the adoption of such a decision, the Council shall act unanimously after obtaining the consent of the European Parliament.

Therefore the Draft EU-Treaty seeks prima facie to intensify judicial cooperation in criminal matters. However there are a lot of exceptions within the TFEU that impede this task.[6] The following section will illustrate the issues that concern the connection between criminal procedure and data protection.

6 See Youngs, *Fusing Security and Development: Just another Euro-platitude?* Working Document of CEPS No. 277, October 2007, pp. 8 et seq.

3 Exceptions concerning the Judicial Cooperation in Criminal Matters within the EU Reform Treaty

The corresponding exceptions are related:

— the form of the cooperation between EU-Member States and

— the legal framework of the cooperation between EU-Member States.

Despite the repeated emphasis on cooperation in criminal matters within the EU, Art. 66 TFEU foresees that the legal framework prepared by TFEU shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security. On the contrary according to Art. 66a TFEU the Member States are free to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.

Therefore, issues of internal security are excluded from the competence of the EU. TFEU reaffirms that this area remains a matter of intergovernmental cooperation and coordination between the Member States. Through the amendment of Art. 66a TFEU, it becomes apparent that the favoured European approach concerning the handling of such issues is the preparation of inter-European agreements like the Prüm Convention.[7]

The fact that the interpretation of the terms 'internal' and 'national security' is very broad, provides the Member States with the possibility of European cooperation in criminal matters besides the EU institutions.[8] This formal possibility is supported by the exceptions that in fact allow the development of a legal framework above and beyond

---

7 For the text of the Convention see: <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf>.

8 See Wichmann, *The Intersection Between Justice and Home Affairs and the European Neighbourhood Policy: Taking Stock of the Logic, Objectives and Practices*, CEPS Working Document No. 275, October 2007, pp. 6 et seq.

TFEU, namely the amendment of the possibility of an 'emergency brake' in connection with the establishment of 'enhanced cooperation'.

This statement can be clarified by the following hypothetical case: Some states propose a directive that would establish, according to Art. 69e par. 2 TFEU, minimum rules concerning the rights of individuals in criminal procedures.[9] They count, however, on the fact that this proposal will never obtain the necessary majority in the Council. Some Member States therefore request[10] an emergency brake. If the European Council is unable to find a solution within four months,[11] is also not able to request the initiating party to come up with a new proposal. In the meantime the initiating parties have a chance to convince other Member States of the correctness of their proposal. If nine Member States are persuaded by the text of the proposed directive, the mechanism of 'enhanced cooperation' can be used and the proposed text that will bind the participant Member States will be adopted.

In this way 'emergency brake' and 'enhanced cooperation' can create different legal frameworks within the EU for issues that concern the fundamental rights of the EU citizens. It is obvious that this procedure does not support the idea of legal certainty and minimum legal rules within Europe.[12]

At the same time the issue of data protection becomes differentiation as far as the level of the protection is concerned. The Charter of Fundamental Rights, a political declaration agreed in 2000, will not be incorporated in the new treaty. However, it is referred to in the treaty as having 'the same legal value as the Treaties'.[13] Consequently, the Union has to preserve and develop and strengthen the level of the protection of persona data as a personal right as this is formulated in

---

9 See S. Peers, *EU Reform Treaty: Analysis 1:Version 3 JHA provisions*, Stratewatch analysis, October 2007, pp. 13 et seq.

10 Art. 69e par. 3 TFEU.

11 Art. 69e par. 3 TFEU.

12 See also the critical remarks of Carerra/Geyer, *The Reform Treaty & Justice and Home Affairs*. In: CEPS Policy Brief, August 2007, p. 5.

13 Art. 8 TFEU.

Art. 8 of the Charter of Fundamental Rights of the Union. This obligation requires common standards concerning the level of data protection within the EU. On the other hand the mandate for the Intergovernmental conference that prepared the Reform Treaty reintroduces the possibility of having different standards and procedures concerning data protection. According to 19f of the Intergovernmental mandate, a specific legal basis for data protection will be introduced in the Common Foreign and Security Policy. A declaration on personal data protection in the areas of police and judicial cooperation in criminal matters will be also adopted, as well as, where appropriate, specific entries in the relevant Protocols on the position of individual Member States clarifying their applicability in this respect.[14]

The above mentioned exceptions have two consequences: a broad area of judicial cooperation in criminal matters is maintained outside the legal framework of TFEU. This happens either through the direct application of Art. 66a TFEU or in the course of the use of the mechanism of 'enhanced cooperation'. At the same time there exists within the EU the possibility of setting different standards and procedures as far as data protection issues are concerned.

The connection between these topics has the following implication: The exchange of personal data between law enforcement authorities at the European level that is essential for police and judicial cooperation can be realized without standardized safeguards. In the name of better cooperation of judicial authorities, the level of data protection can be reduced depending on the need for mutual assistance in criminal matters. Therefore the question is how it is possible to facilitate the intra-European judicial cooperation in criminal matters without contradicting the principles of data protection.

---

14 See Council of the European Union, 11218/07, p. 7.

4 The level of data protection beyond TFEU

The expansion of judicial cooperation matters and the actions that tend to implement the Hague Programme[15] on strengthening freedom, security and justice in the European Union,[16] necessitate the creation of common standards for the protection of personal data. The Commission recognized this necessity and forwarded on 5 October 2005 a proposal for a Council Framework Decision on the protection of personal data processed in the framework of police cooperation in criminal matters (DPFD) to the General Secretariat of the Council.[17] After the consultation of the European Parliament and the delivery of the opinion of the European Data Protection Supervisor, a revised text of the DPFD was prepared on 16 October 2007.[18]

Taking into consideration the legal framework that permits the judicial cooperation in criminal matters[19] beyond TFEU, as well as the draft text of the Framework Decision, it is obvious that the only solution that guarantees common standards in this area is the adoption of such a Council Decision.

The current text still needs, however, amendments – that is improvement. The following proposal highlights the most important topics of the Draft that must be taken into consideration to set an accurate legal basis for data protection beyond TFEU.[20]

— DPFD has to define clearly in Art. 3 the legitimate purposes allowing the processing of personal data in the framework of police and judicial cooperation in criminal matters without maintaining any general clause allowing for further processing

---

15 See the Hague Programme in: OJ C 2005/C 53/01.

16 See also the Council and Commission Plan implementing the Hague Programme (OJ C 198, 12.8.2005, p. 1).

17 See the first Draft of the proposal in: SEC (2005) 1270, COM (2005) 490 final.

18 See 11365/4/07 REV 4.

19 See the Critic of Hustinx: 'A Framework in Development: Third Pillar and Data Protection', in: *Personal Data Protection Yesterday, Today, Tomorrow*, Warsaw 2006, pp. 132 et seq.

20 See also the opinion of the European Data Protection Supervisor, OJ C 139/1, 23.6.2007.

'for any other purposes'. The purpose limitation principle is a key principle in the EU data protection directive[21] and Council of Europe Convention No. 108.[22]

— Specific safeguards should provide guarantees concerning the processing of biometric and genetic data. The Draft, in Art. 7, does not refer to personal data related to criminal convictions, which are undoubtedly relevant in the context of mutual assistance in criminal matters.

— The Draft does not contain distinctions between different categories of data subjects processed for police and law enforcement purposes (criminal, victims, witnesses, etc.). These distinctions are not only necessary for the protection of the personal data of the citizen, but also for the ability of the recipients to be able to make full use of the data they receive. Without these distinctions, the receiving police services cannot immediately use the data, but have first to ascertain how the data must be qualified and subsequently how they can be used and shared for different law enforcement purposes.[23]

— The Draft must develop in Art. 12, 15 common criteria and a procedure for the adoption of the measures necessary in order to assess the level of data protection in a third country or international body before transferring the personal data and not leave it entirely to the discretion of Member States. Fixing an EU standard in such a procedure is a requirement for achieving harmonisation in Europe and the concept of adequacy findings corresponds to the provision in the Council of Europe Convention of 28 January 1981 concerning the protection of individuals.

— Art. 16 of the Draft should be reviewed. The data subject should have the right to have information concerning the identity of the data controller, the possible recipients and the

---

21 Directive 95/46/EC.

22 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.

23 So opinion of the European Data Protection Supervisor, OJ C 139/7, 23.6.2007.

legal basis for processing. Any restrictions should be precise and limited.

— Art. 17 of the Draft should be revised too. The provision should also contain the purpose for which data are processed. Furthermore, the exceptions laid down by Art. 17 paragraph – such as cases when access should be denied in order to protect national interests – are too broad and unforeseeable. In general the right of access must be in line with the requirements of the European Human Rights Convention and the case law.

— Article 11 of the Draft, in order to be effective for the purposes of verification of the lawfulness of data processing, should lay down appropriate mechanisms for logging or documenting not only all transmissions of data, but also all accesses to data.[24]

The above remarks do not mean that the Draft has no value. One has also to admit that it is important that the framework decision should be adopted as soon as possible. However, the Draft still does not provide for a sufficiently harmonised and high level of data protection. The fundamental character of the framework decision not only for safeguarding the rights of the citizens of EU but also for law enforcement, justifies a discussion that is not compromised by an acceptable, strict timeframe.

5 Conclusion

The TFEU contains a lot of innovation especially for the area of Freedom, Security and Justice. The new legal framework foresees flexibility and differentiation. It has its task to intensify judicial cooperation in criminal matters, but the exceptions that it includes do not provide safeguards as far as it concerns the protection of fundamental rights e.g. data protection. Undoubtedly to combat serious

24 See European Data Protection Supervisor, Comments of the European Date Protection Supervisor on the recent developments with respect to the Proposal for a Council Framework Decision on the protection of personal data in the framework of police and judicial cooperation in criminal matters, OJ 14043/07, p. 4.

criminality international cooperation is indispensable.[25] The granting of fundamental rights has, however, the same and possibly higher value. Therefore a long-term strategy for the enhancement of European security presupposes the development of European standards and safeguards that guarantee the fundamental rights within or besides TFEU. Another option could – perhaps – provide quick results during the fight against serious criminality. However, it would never promote democracy within the EU.

25 See the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in: OJ L 386/89.

CHAPTER 4
DATA PROTECTION

DATA PROTECTION AND PRIVACY: CHANGING INTERPLAY WITH HUMAN RIGHTS

Mindaugas Civilka[1] and Rita Barasneviciute[2]

1 Law and privacy – where the social background and individual values meet each other

One may think of the individual's right to full protection in person as of principle as old as the law itself. Privacy has roots deep in history and already the Bible has numerous references to privacy.[3] However, social, economic and political changes involve recognition of new rights, and the law naturally grows to meet ever-changing demands of society.

In ancient times, the law gave a remedy only for physical interference to life and property, for trespasses *vi et armis*. Later, there came recognition of man's spiritual nature, of his intellect, dignity and honour. Gradually the scope of person's rights broadened. Therefore, the right to life has come to mean the right to enjoy life – the right to be let alone, the right to have privacy.[4] The right to privacy becomes more about communicating, interrelating and collaborating, than isolating and alienating. It is something, recent 100 years have brought about into our society. Of course, notion of privacy may vary from country to country,

---

1 Vilnius University, Law Faculty.

2 Law Offices Norcous&Partners.

3 See *Privacy and Human Rights Overview 1999* (International Survey of Privacy Laws and Development), Privacy International and the Electronic Privacy Information Center, available at <http://www.privacyinternational.org/survey/Overview.html>.

4 Samuel Warren and Louis D. Brandeis, *The Right to Privacy*, available at <http://louisville.edu/library/law/brandeis/privacy.html>.

from society to society. And thus Article 8 of European Convention on Human Rights (ECHR) may serve as a minimum standard, benchmark for all modern countries. Similarly, Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 (Directive 1995/46/EC)[5] institutes a set of minimum requirements. However, the balance inherent in data protection regime must be settled individually on country-by-country basis.

Unavoidably today traditional and archaic meaning of privacy is no longer playing its initial societal role. According to Brian Foran, the right to have privacy is simply the right of individuals to control the flow of information about themselves, the right to fair, and reasonable and confidential information practices.[6] Nowadays, a person has less control on his personal information. That is why privacy has become the topic in the discussions on the technological world. Advances in technology and war against terrorism diminish the level of privacy or even led to a death of traditional concept of privacy. However, new and new exceptions and limitations evolve which gradually limit and melt the very concept of privacy to something, which is not a clear legal concept anymore.

The concept of privacy is overwhelmingly becoming a sociological rather than a clearly-cut legal concept. This is why of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe.[7]

However, looking historically, it is the concept of human right to privacy, which has given birth to legal regimes of personal data protection. The inviolability of human right to privacy has been set forth in several international regional and national instruments, including constitutional charters (e.g. Article 22 of the Constitution of the Republic of Lithuania notifies that 'personal correspondence, telephone conversations,

---

5 OJ L 281, 23.11.1995, pp. 31–50.

6 Brian Foran, *Privacy on the Information Highway: Myth or Reality*, available at <http://library2.usask.ca/gic/v2n2/foran/foran.html>.

7 See *Privacy and Human Rights Overview 1999* (International Survey of Privacy Laws and Development), Privacy International and the Electronic Privacy Information Center, available at <http://www.privacyinternational.org/survey/Overview.html>.

telegraph messages, and other communications shall be inviolable; information concerning the private life of a person may be collected only upon a justified court decision and only according to the law').

As a regionally defined human right of modern society it stems from the ECHR. According to Article 81 of the ECHR, everyone has the right to respect for their private and family life, their home and their correspondence.

Civil code of the Republic of Lithuania[8] protected right to inviolability of human image (Article 2.22) may be regarded as one of the few legal paragons of privacy.[9] However, changing legal and technological environment requires proportionality between privacy and data reliability. For instance, biometric data processing is now often used in automated authentication and identification procedures. In Lithuania, passports containing digital facial images are already being issued and it is planned to issue passports containing fingerprints in the near future (three years after the European Commission will establish technical specifications). Of course, it is easier to fool a facial recognition engine than one which recognizes fingerprints. Therefore, on the one hand, biometrical data may be a good solution to prevent falsification of passports, but, on the other hand, the incorporation of such data into the passport may be interpreted as an insult to human dignity.[10] Thus, in line with the changing legal and technological situation, privacy is a secondary matter. More and more is usurped by personal data protection regimes.

---

8 No. VIII-1864, 18 July 2000.

9 For instance, in Lithuania the following statutory instruments contain provisions related to human right to privacy and inviolability of human image: Law on the Rights of Patients and Compensation of the Damage to their Health as of 3 October 1996, Law on Public Security Service as of 19 September 2006, Law on Provision of Information to the Public as of 11 July 2006, Law on Electronic Communications as of 1 May 2004, Law on Operational Activities as of 20 June 2002, Law on Advertising as of 18 July 2000, Law on Legal Protection of Personal Data as of 11 June 1996, Law on Documents and Archives as of 5 December 1995, Penal Code of the Republic of Lithuania as of 1 May 2003, Code of Penal Procedure of the Republic of Lithuania as of 9 April 2002.

10 Public Relations Division of the Seimas of the Republic of Lithuania, Lithuanian Parliamentary Mirror, Amendments to the Passport Law Regarding Integration of Biometric Data into the Passport <http://www.lrs.lt/n/kronikos/pdf/mirror_6.pdf>.

Although unavoidably interrelated, these two regimes have the essential difference – in the regime of personal data protection is necessary a compromise between principles of market-based economy (or other public goods, such as public safety and national security, etc.) and traditional view to privacy, whereas human right to privacy is embedded on the *opinio juris* and general principles of international law and human rights. Thus, regimes of data protection are constantly moving apart from the general concept of privacy if not replacing the latter it in terms of law. Moreover, the concept of data protection is more easy-to regulate, as it is *expressis verbi* established legal regime.

Secondly, legal regime of data protection may pay tribute to such non-legal constructs as efficacy, cost-orientation, networking effects and other social and economic perspective based aspects. Thus, now the more predominant question is not whether the importance of traditional values of privacy are diminishing or not, but whether the existing rule of law in democratic society affords protection of privacy of the individual with the aid of legal measures left after constant deterioration of legal concept of privacy. However, one may not treat this as an attempt to downgrade privacy and its importance in society. On the contrary, privacy is and will always remain key value to the democratic society. The concern, which is raised here, is how the law should interact with these changes in the way the society perceives its individuals, and vice-versa, individuals perceive each other and the society at large.

2 Privacy and personal data protection regimes in the changing legal environment

It is worth to overview how human right to privacy and personal data protection regime has changed since the advent of information technology in the seventies. The powerful computer systems opened new era for collection, processing and dissemination of information, which demanded for specific rules governing the collection and handling of personal information. The genesis of modern legislation in this area can be traced to the first data protection law in the world

enacted in the Land of Hessen in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978).[11]

Two international instruments evolved from these laws. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data ETS No. 108 and the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data articulate specific rules on handling the data in electronic format. These rules form the backbone of the data protection laws in many countries. These rules describe personal information as data which are afforded protection at every step from collection through to the storage and dissemination. The right of people to access and amend their data is a primary component of these rules.[12] In other words, data protection regime is about the right of data subject to control what is happening with its data. In its essence, the data protection regimes are no longer based on assumption that the personal data may not be collected otherwise than through consent of the individual – the law also presupposes other cases where such collection of personal data may be legitimate.

However, the most important legal documents dealing with the personal data were introduced only in the end of 90s. Directive 1995/46/EC[13] is unarguably the basic piece of legislation in Europe relating to the protection of personal data. It serves as a regulatory framework for ensuring a balance between a high level of protection for individual privacy and the free movement of personal data within the European Union (EU).

This Directive is inevitably a compromise between establishment and functioning of an internal market in which, in accordance with Article

---

11 *Global Internet Liberty Campaign Privacy and Human Rights*, An International Survey of Privacy Laws and Practice available at <http://www.gilc.org/privacy/survey/intro.html> (last visited 31 January 2007).

12 EPIC - Electronic Privacy Information Center, *Privacy and Human Rights Overview 2003*: An International Survey of Privacy Laws and Developements, available at <http://www.privacyinternational.org/survey/phr2003/overview.htm> (last visited 24 January 2007).

13 OJ L 281, 23.11.1995, pp. 31–50.

7a of the Treaty, the free movement of goods, persons, services and capital and free flow of personal data between the Member State on one hand, and the fundamental rights of individuals on the other.[14]

The right to privacy is highly developed area of law in Europe, but in order to comprehend the Directive, it is necessary to understand how and why EU and US perspectives on data protection and privacy are different from historical and legal points of view. In opposition to the US 'sector-specifi' approach to data protection legislation, relying on a combination of legislation, regulation, and laissez-faire economics based self-regulation, rather than *ex-ante* regulations, European data protection model strongly relies on the strict and rigid systems of legal rules.

The Directive 95/46/EC sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights.

A key concept in the European data protection model is 'enforceability'. Data subjects enjoy the rights established in explicit rules.[15] The basic principles enshrined by the Directive – the right to know the source of the data about him/her; the right to have inaccurate data rectified; a right of recourse in case of unlawful processing; and the right to withhold permission to use data – in essence concentrate upon the person's right to know what happens with their data and control the subsequent use thereof. Secondly, the European data protection model is premised on the active self-determination of the individual. For instance, individuals have the right to opt-out free of charge from being sent direct marketing material, etc.

On 12 July 2002, the European Parliament and the Council of the EU adopted Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58/EC).[16] The purpose of the new directive –

---

14 Preambule, item 3.

15 See *Privacy and Human Rights Overview 1999* (International Survey of Privacy Laws and Development), Privacy International and the Electronic Privacy Information Center, available at <http://www.privacyinternational.org/survey/Overview.html> (last visited 24 January 2007).

16 OJ L 201, 31.7.2002, pp. 37–47.

member of the 2002 EU e-Communications package family – was to update EU law to reflect continuing technological progress in the field of electronics communications and to establish an equal level of privacy protection to personal data regardless of the technologies used. Directive 2002/58/EC repealed and replaced Directive 1997/66/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 (Directive 1997/66/EC).[17]

The latter Directive aimed to translate the general personal data protection principals laid down in Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, into specific rules for the telecommunications sector. However Directive 1997/66/EC was already outdated at the moment of its adoption in 1997, because it applied only to 'telecommunications' sector.[18]

Directive 2002/58/EC is aimed at particularization of general Directive 1995/46/EC by establishing sector-specific legal and technical provisions. However, in the electronic communications sector Directive 1995/46/EC remains principle instrument applicable to all matters concerning protection of fundamental rights and freedoms, to the extent they are not specifically covered by Directive 2002/58/EC.

However, many privacy advocates are still concerned that basic threats as raised by the development of the new technologies, enabling latent and fast collection of personal information, offering unprecedented ease of access to personal data, are still not appropriately met, especially taking into account that the aforementioned instruments address the new challenges, posed by the information society, only in one aspect – namely, aspect related to data protection within the framework of internal market and fundamental freedoms of the EU First Pillar, whereas the Third Pillar of EU is largely left outside the reach of those instruments.

---

17 OJ L 24, 30.1.1998, pp. 1–8.

18 Frederic Debussere, 'The EU e-Privacy Directive: a Monstrous Attempt to Starve the Cookie Monster', *International Journal of Law and Information Technology*, Vol. 13, Oxford University Press, 2005, pp. 72–3.

3 Human right to privacy and person's data protection in the changing social and technological environment

Of course, sometimes technological changes allowing new possibilities of data processing may cause a negative reaction of the society.[19] Obviously, it is a mistake to assume that every technological change or innovation has a one-sided effect, either good or bad. Every technology is probably both a blessing and a curse. For instance, technological changes made it possible to evaluate person's data by automated means, which is unarguably good – the decision-making process now became more time and cost effective.

This, however, causes number of worries and questions – what happens if the machines provide incorrect data, or even worse – what happens to me if a third party gets unauthorised access to my personal data and further uses it without my actual knowledge? Directive 1995/46/EC, of course, provides a general safety – catch against purely – automated approach to human being – no decision may be taken in respect of the data subject's personal where such aspects were evaluated only by automated means, which are not controlled by a human.[20] This system determines that individuals must be evaluated by other individuals, not only by the machines. However, what may be more important about new technologies to the individuals is loss of control over the personal data.

Technological and economic developments have made it more difficult to ensure that certain social values, such as those favouring privacy, innovation and freedom of expression, will continue to be preserved and balanced in their archaic modes. Furthermore, it is becoming more difficult to secure the rights catalogued in the ECHR, taking into account all the possibilities that may occur in the future as a result of new technologies, when any private data become easy to collect by another person.

---

19 Brian Foran, *Privacy on the Information Highway: Myth or Reality*, available at <http://library2.usask.ca/gic/v2n2/foran/foran.html>.

20 Article 15.

Now one may notice the trend in the society to actively contribute to what's happening around instead of passively consuming what is offered for new massive consumption; mass-oriented media, information, broadcasting, etc. In other words, traditional censorship and content editing based media will always feed the sofa and potato users, although more and more populated active public networking oriented consumers are outweighing this balance towards the new non costs and non investment based social production – blogs, YouTube, MySpace, discussion forums, etc.[21] Unsurprisingly, 'The Times' award for the Person of the Year in 2006 was granted to You – Internet content contributors.[22]

Thus, what the technology brings so different in terms of privacy? Everything. The very concept of privacy is absolutely necessary for all modern democratic societies and hopefully, will remain. But technology has changed the way the society perceives the balance between the right to know and the right to privacy. With such powerful tool as Internet, individuals are informed about what is happening in their 'neighbourhood' better than in those times where such neighbourhood was just two meters away. With such powerful tools for self-expression, access to and dissemination of information the individuals may less rely on traditional values of privacy.

Thus, privacy in its initial form becomes somewhat less necessary for preservation of human dignity, pride and other values, which are protected or even outweighed by new phenomena of social collaboration, right to information, etc. Internet and modern technologies have become (accidentally or coincidentally) instigators for new type of social environment and new type of social rules, based on

---

21 See Reed Hundt, 'Communications policy, economic policy. The inextricable link'. *Communications the next decade* - A collection of essays prepared for the UK Office of Communications Edited by Ed Richards, Robin Foster, Tom Kiedrowski. Ofcom 2006, p. 197; Carolyn Fairbairn, 'Serving the public good in the digital age: implications for UK media regulation', *Communications the next decade* - A collection of essays prepared for the UK Office of Communications Edited by Ed Richards, Robin Foster, Tom Kiedrowski. Ofcom 2006, p. 78.

22 See, Lev Grossman, 'Time's Person of the Year: You', Wednesday, Dec. 13, 2006, *TIME Magazine*.

collaboration, interaction, virtual-communication and virtual-identity based social behaviour. Incidentally or not, data protection rules are much better tailored for such kind of environment than traditional concept of human right to privacy.

As already mentioned, data protection regime is necessarily a compromise which is based on and heavily relies on the assumption of active data subject, as opposed to passive individual for the purposes of ECHR Article 8, on collection of data as opposed to non-interference with the private life of individual under ECHR Article 8, on transmission of data rather as opposed to keeping secrecy and staying anonymous.[23] Privacy is based on non-interference and non-surveillance, whereas pursuant to data protection laws collection of personal data is not necessarily unlawful, provided, however, statutory requirements are met. In its essence one may claim that data protection regime presupposes certain active steps to be made by the individual so that he himself decides whether he will provide the data for those particular purposes and whether he will interact with other society members. Thus, data protection is largely about choices and self-determination of individual himself; Internet too.

4 Interplay with social values and balances

a) Balance with the free movement of personal information

Data protection regime is firstly and mostly based on compromise between the human right to privacy and business realities, reflected by common values of functioning of EU internal market.[24] Thus, the first instance where the very content of privacy is melted down is privacy's interplay with the functioning of internal market. However, it reflects one part of social and legal reality only.

---

23 Of course, it may happen even the other way round – Internet offers new possibilities of becoming anonymous and thus contributes to creation of so-called virtual identities. However, this aspect will not be discussed in this paper.

24 Directive 1995/46/EC, preambule, item 3.

b) Data protection within Third Pillar – new era in modern data protection?

The other part – reality or potentiality embedded in Article 8, part 2 of the ECHR – struggles with national and public security and other legitimate public concern, which by the time the Directive 1995/46/EC was adopted, were only evolving. Taking into account the concept of the right to privacy, as determined in the ECHR, it seems that all the exceptions (Art. 8, part 2),[25] which may justify legitimate interference by a public authority with the exercise of this right, are already exhausted by the governments.

Historically, the data protection regime was about the balance between 'usual' societal needs and business necessities. However, social, political changes (e.g. the threat of terrorism) and technological changes (e.g. development of electronic communications, including Internet and its actors) necessitated the need for the different type of balance – balance between higher protection of privacy and security of public interests. Thus, Third Pillar of EU may become even more controversial as far as even 'traditional' data protection regimes are concerned.

Data protection under the Third Pillar was envisaged as long ago as 1998. At the time, the Justice and Home Affairs Council adopted the Vienna action plan,[26] according to which the horizontal problems arising in the field of police and judicial cooperation on criminal matters required that consideration be given to ways and means of harmonising the rules on data protection.

In 2001, there was a draft resolution on the rules governing the protection of personal data failed under the instruments of the Third Pillar, although it was not adopted.[27] In June 2003, the Greek

---

25 Art. 8, part 2: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

26 OJ C 019, 23.01.1999, p. 0001 – 0015.

27 Council working document 6316/2/05 REV 2 JAI 13.

presidency proposed certain general principles on personal data protection under the Third Pillar,[28] which were inspired by Directive 1995/46/EC on data protection and the Charter of Fundamental Rights of the European Union.[29]

Thus, prior to September 11th personal data regime, falling outside Directive 1995/46/EC, was in essence centring on common criminal offences. However, after September 11th, the concept of the aforementioned regime has dramatically changed – combating and preventing terrorism became a priority to the governments. September 11th has changed a lot for privacy and the society will never enjoy the same level of privacy as before. The Conclusions of the Justice and Home Affairs Council of 19 December 2002[30] underline that, because of the significant growth in the possibilities afforded by e-Communications, data relating to the use of communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

Thus, retention of data, which has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning organised crime and terrorism, has opened the new page on the history of online privacy.[31] Although adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR may be regarded as a necessary measure in democratic society, it may further melt the very concept of privacy.

---

28 2514th Council meeting – Justice and Home Affairs – Luxembourg, 2003, <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/en/jha/76100.pdf>.

29 18.12.2000 Official Journal of the European Communities C 364/3, 2000/C 364/01.

30 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, preamble, item 9.

31 In 2005 German, Spain, Great Britain, France and Italy implemented their common policy of traffic data retention and decided to retain for 1 year data of telephone conversations and Internet records, which might be necessary for investigation of terrorist cases. See: *European Countries Fighting with Terrorism, Prolong the Duration of Data Retention*, available at <http://www.delfi.lt/archive/article.php?id=6260086> (last visited on 6 February 2007).

Most controversial EU policy is retention of communications traffic data. Community legislators enacted Directive 2002/58/EC to regulate processing of personal data, including traffic data, on electronic networks. This Directive only permitted retention measures where 'necessary, appropriate and proportionate' within a democratic society. The unrestricted, blanket data retention was expressly rejected.

After September 11th a number of Member States implemented the policy of traffic data retention into national law. After various discussions the European Parliament and the Council of the European Union adopted Directive 2006/24/EC of 15 March 2006 concerning 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 (Directive 2006/24/EC).[32] The Directive allows for the retention of data 'generated by telephony, SMS and Internet, but not the content of the information communicated'. This data includes email addresses and location data from cell phones.

Also of concern is the broad discretion that is left to EU Member States. For example, data may be accessed for the purposes of combating serious crime and terrorism, but no concrete definition of these concepts has been provided, allowing Member States to transpose their own definitions on the provisions of the Directive.[33] Duration that telecoms has to retain the data is left relatively undefined – from a minimum of 6 months to a maximum of 24 months – and member states may extend these time frames. Already several countries have indicated intentions to. The Directive will be implemented after one of the shortest paths from its drafting to the final vote – until 15 September 2007.

---

32 OJ L 105, 13.4.2006, pp. 54–63.

33 See more on the critics of some privacy advocates: *European Parliament Approves Communications Data Retention, Privacy International*, available at <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-496240> (last visited on 5 February 2007).

5 What is the price?

The opponents of the Directive remind to the European Commission that from economic perspective consumers shall be impacted by different factors: operators shall be forced to take expensive measures in order to keep and classify huge amounts of data for quite long period. This will mean higher price for Internet and content related services. This may mean less comfortable access and fewer possibilities for self expression – various requirements for registration, authorization of users, etc. Is it the only price we are paying for the safer life? Unfortunately, in the hands of evil new technologies may become more dangerous to the society as before. That's why the price we are paying is, *inter alia*, our privacy.

Finally, the recent Commission's Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[34] is to be seen in the context of The Hague programme[35] adopted by the European Council on 4 November 2004 and the action plan for its implementation adopted by the Council and the Commission in June 2005.

6 Big Brother watches you

The remaining part of balance – balance of privacy against any other social realities. Nowadays people are increasingly feeling that someone is keeping a close watch on them. In the words of David Brin, darkness no longer offers even a promise of privacy.[36] For the sake of public security and order (which from the legal point of view must be tested under Article 8, part 2 of ECHR), most of the Member States are

---

34 Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters SEC (2005) 1241, COM (2005) 475 final.

35 <http://europa.eu/scadplus/leg/en/lvb/l16002.htm>.

36 David Brin, *The Transparent Society, The Cameras are Coming. They're getting smaller and nothing will stop them. The only question is: who watches whom*, available at <http://www.wired.com/wired/archive/4.12/fftransparent.html> (last visited on 30 January 2007).

installing cameras on each corner of the street, providing instant data to the data centres at investigation and surveillance authorities, who are live monitoring events and activities in the streets and other public places. It is undoubtedly good, but the key point is that data subject is worried about his personal data and naturally many questions arise: what happens with such data next, what happens to me, if such investigators mistreat my personal life details and I am hurt by that?

Thus, in the police state it is better to hide those cameras so that ordinary citizens are not suspecting that they are being watched by big eye. The more in the future the smaller and more invisible those cameras would be. However, surveillance cameras are only the top of the iceberg.

For instance, even a paper envelope may be scanned and a content of inside is disclosed. In our society solution, however, should be different. We should know that we are under surveillance, but we should have a possibility to monitor those who monitor us. Plus, we need to be compensated for mistreatment if personal data are provided to a third party that has no right to obtain and process it. However, right to know becomes much more essential to the society.

Mobile telephones with small cameras might be another example of how modern technologies are, on the one hand, disturbing the society and, on the other hand, providing more possibilities and convenience. Nowadays people take photos with such mobile telephones and tend to forget about traditional photo cameras. In such case, problems related to person's privacy are unavoidable.

For instance, in Lithuania, the State Data Protection Inspectorate has approved a recommendation,[37] according to which sellers of mobile telephones shall inform their consumers not only about the technical possibilities of such telephones, but also about lawful utilization of photos made by mobile telephones. Consumers are of course happy

---

37 Recommendation on security of person's privacy while using mobile telephones with integrated video and photo cameras as of 20 April 2005 <http://www.ada.lt/images/cms/File/rekomendacijos%20del%20foto_video_telefonu.pdf> (last visited on 25 January 2007).

having a mobile telephone and a camera in one, but how about the privacy of the other persons? The sound of such mobile cameras is hardly audible, so people might even not know that someone has made a photo of them. According to the aforementioned recommendation, in all public places there should be a note asking to respect other's privacy and not to take pictures of other people without their consent. However, as there are no warnings or signals (e.g. light flashes) informing that someone is taking a picture, it is hard to fight with those mobile telephone cameramen.

For instance, a year ago there was an accident in Lithuanian public transport, when a group of boys were taking photos of passengers, in particular girls. The boys did not stop taking pictures of girls even after they were asked to stop. Moreover they threatened to put pictures on the Internet. However, Lithuania is not alone to encounter such problems. Not so far ago, there was a scandal in Japan, when a train controller caught a teenager taking pictures under a passenger's skirt. Thus, mobile telephones containing photo cameras are becoming equipment for sneering and violence.[38]

Cameras mounted on the dashboard in Australia is somewhat different example.[39] The so-called FaceLab system is a system that tracks and monitors car drivers by cameras mounted on the dashboard. FaceLab can tell if you are becoming inattentive to the road by working out where you are looking, how many times a second you are blinking and angle of your head. The first application of the system is in spotting early signs of driver fatigue. If drivers start to display the characteristic early signs of falling asleep, the system can alert them. Thus, FaceLab

---

38 *The Owners of Mobile Telephones with Photo Cameras should be Subject to Ethic Code*, available at <http://www.delfi.lt/archive/article.php?id=8622067> (last visited on 6 February 2007).

39 See *Visionary technology*, FaceLab4, <http://www.seeingmachines.com/facelab.htm> (last visited 31 January 2007). Seeing Machines is a Canberra based award winning technology company with a focus on vision based human machine interfaces. According to the information provided by the company's web page, Seeing Machines is engaged in the research, development of advanced computer vision systems for research advanced driver assistance systems, biometric acquisition, robotics, etc. Their technology faceLAB has revolutionized gaze tracking technology and it has enormous market potential that can forever change the way humans and machines interact.

could become an invaluable safety feature in new cars. However, the system could also turn into an automotive Big Brother, capable of deciding whether or not you are fit to drive.[40]

Few years ago the society of US was also shocked by a watch of Big Brother. The so-called program 'Know Your Customer' has forced customer's banker to monitor customer's bank accounts to determine unusual account activity. The system works by simple principle – banks are forwarding personal financial records of citizens to federal agencies. Any big bonus or estate received from a relative could be deemed 'suspicious'.[41]

Three years ago Lithuanians were concerned by the computer program 'Guardian Monitor', which collected all information about Internet sites visited by a person and even the content of his/her emails. Such information was automatically sent to a person who ordered the program 'Guardian Monitor' (e.g. to an employer). According to the State Data Protection Inspectorate the usage of the aforementioned program roughly violated privacy of many persons. Therefore, the program was prohibited. However, it is doubtful whether such or similar programs are no longer in operation.[42]

All these examples are clear manifestation that today higher priority may be accorded to the security of the society as a whole than to the protection of personal data. And the society is accepting such new and not so strict rules of privacy.

However, the right to know what happens to the data that have been collected becomes the most important factor. May we say that if no third party receives such data without the consent of data subject, there is nothing to be worried about?

---

40 Christian Mahne, *Big Brother Watches You Drive*, 9 September 2002, BBC News, availiable at <http://news.bbc.co.uk/1/hi/technology/2246115.stm> (last visited on 27 January 2007).

41 Wes Vernon, *Big Brother Wants to Watch You Even More,* 23 May 2001, available at <http://www.newsmax.com/archives/articles/2001/5/22/155845.shtml> (last visited on 28 January 2007).

42 Experts affirm: *Software used for Following Employees should not be Distributed in Lithuania*, available at <http://www.delfi.lt/archive/article.php?id=5462518> (last visited on 6 February 2007).

7 What's so special about the Internet?

In nowadays Internet content has become vaster than printed era production, or traditional media, audio-visual production. Internet has become the biggest, most powerful and ubiquitous printing, copying, media-creating, disseminating machine. Consumers are contributing to creation of public content to such an extent that traditional media content production is relatively low output in comparison with the former.

Internet becomes so different, that it literally changes our lives. As Lev Grossman puts it, it's about the cosmic compendium of knowledge Wikipedia and the million-channel people network YouTube and the online metropolis MySpace.[43]

Unfortunately and unavoidably illegal Internet content takes great variety of forms, starting from intellectual property rights violations, ending up with the criminal offences of defamation, child pornography, etc.

a) Personal-created content

While discussing about violations of data protection in the Internet it is worth to overview the decisions of European Court of Justice (ECJ) on the scope of the Directive 95/46/EC. For instance, in Case C-101/01, Bodil Lindquist,[44] Ms. Lindqvist, a Swedish national, posted on her website text about her volunteer work in a local parish of the Swedish protestant church, including information about her co-workers, including names and phone numbers, hobbies. She also mentioned a colleague's injured foot. Although she removed the disputed content at their request, the authorities started procedures against her under Swedish law implementing the European Data Protection Directive. Afterwards the case appeared in the ECJ. The question was whether loading certain personal data on a personal

---

43 See, Lev Grossman, 'Time's Person of the Year: You', Wednesday, Dec. 13, 2006, *TIME Magazine*.

44 European Court of Justice Decision C-101/01, *Lindquist v. Sweden,* 6 November 2003.

homepage falls outside the scope of the Directive or, failing that, whether the Directive allows for such processing of data. The ECJ has determined that notwithstanding the fact that the Directive covers personal information published on the Internet, such publication does not violate automatically the EU's restriction on international data transfer. May YouTube anticipate the same qualification? What about rights of other persons who are by chance or otherwise depicted or filmed or shown in the personal media (i.e. birthday party) created and loaded into Internet by one of the party participants?

b) Cookies and Spamming

Cookies were traditionally spelled-out as a typical example of how modern technologies may undermine the privacy and expectations of anonymity on the web. At the same time, cookies are good example of how different business-oriented modes of online services customisation and individualisation may be from the traditional forms of customers monitoring and related practices.

A cookie resides on a user's hard drive and contains information about the individual that can be read back by the website that deposited it or by anyone else with an understanding of that website's data format.[45] A cookie can contain any information the website wants to include in it: pages viewed, advertisements clicked, user identification number, etc. In some cases, cookies may be useful for providing a certain service through the Internet or to facilitate the surfing of the Internet user.[46]

---

45 Cookies can lead to an invasion of the privacy of Internet users. This is how it works: whenever a web browser requests a file from the web server that sent it a cookie, the browser sends a copy of that cookie back to the server along with the request. Therefore, a server sends to a user a cookie and a user sends it back whenever he requests another file from the same server. In this way, the server knows a user has visited before and can coordinate his access to different pages on its web site. For instance, an Internet shopping site uses a cookie to keep track of which shopping basket belongs to a certain user. See 'Phare programme twinning project No. LT02/IB-JH-02/-03, Strengthening administrative and technical capacity of personal data protection', *Data Protection on the Internet*, p. 13.

46 'Phare programme twinning project No. LT02/IB-JH-02/-03, Strengthening administrative and technical capacity of personal data protection', *Data Protection on the Internet*, p. 14.

For instance, according to the Directive 2002/58/EC, cookies 'can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions'. However, the use of cookies is allowed on condition that users are informed about the purposes of cookies so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Of course, users should have the opportunity to refuse to have a cookie stored on their terminal equipment.[47]

However, if cookies are sometimes useful and user-friendly, the other form of unsolicited communications so-called spam is a real evil.[48] There is really little that can be done to prevent electronic junk or bulk mail. However, keeping up-to-date on the techniques to eliminate or reduce spam is very important. The problem of spamming from the user's point of view is threefold: firstly, the collection of one's e-mail addresses without one's consent or knowledge; secondly, the receipt of large amounts of unwanted advertising; and thirdly, the cost of connection time.

The rules of the Directive 2002/58/EC provide a clear answer to the privacy issues raised by spam and give a clear picture of the rights and obligations of those involved: 'Electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent'.[49] This means that a consumer must have expressed

---

47 The research completed in Belgium has shown that over half of the sites using cookies (51 percent in 2001 and 67 percent in 2002) use permanent cookies and only 12% informed their visitors about the reason for doing so. See Prof. dr. Michel Walrave, University of Leuven, *Websites Privacy Statements Fall Short of Privacy Laws*, p. 2.

48 According to the Communications Regulatory Authority of the Republic of Lithuania, 87% of active residential Internet users and 76% of business enterprises received spam into their mailboxes during the year 2006; available at <http://www.rrt.lt/index.php?-481929782> (last visited on 31 January 2007). According to mail monitoring firms, more than 95% of e-mail is 'junk'. Therefore, less than 4% is legitimate traffic. See: Mark Ward, *More Than 95% of E-mail is 'Junk'*, <http://news.bbc.co.uk/2/hi/technology/5219554.stm>.

49 'Phare programme twinning project No. LT02/IB-JH-02/-03, Strengthening administrative and technical capacity of personal data protection', *Data Protection on the Internet*, pp. 22–4.

his/her explicit willingness to receive unsolicited commercial e-mail, faxes or telephone calls from automated calling systems before these communications can be legally sent. However, reality is such that vast majority of daily Internet traffic is unsolicited mail, which shows that just rule of law, is helpless here. According to the statistical data provided by Message Labs, spam constituted 70% of all e-mails during the year 2005 (while in 2001, only 7%).[50] Pursuant to the experts of SophosLabs, most spam is sent from US computers (23.1% of all unsolicited emails). China, including Hong Kong, takes the second place with 21.9%, South Korea is the third with 9.8%. France with 4.3% takes a leading place among European countries.[51]

Only those two examples suggest that the possibility of identifying the Internet user exists in many cases and that large masses of personal data to which the data protection directives apply are therefore processed on the Internet. However, the issue is that people have no real choice – they rarely may choose the Internet without data mining and data surveillance. But users should know what (a) happens with their data, (b) what rights of control they have, and (c) whether this would mean that they can not afford the services because of increased price, or that use of services becomes less acceptable. In reality, users are rarely that much concerned about their privacy when they access Internet or new media services. What is more important here – that users must have the right to know and the right to self-determine.

8 Location data

Article 9 of the Directive 2002/58/EC requires the processing of location data other than traffic data, relating to subscribers of publicly available electronic communications services. Such data is defined as 'any data processed in an electronic communications network,

50 Statistics, spam rate, available at <http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/threat_statistics/DA_112495.chp.html>.

51 Sophos report reveals latest 'dirty dozen' spam relaying countries, 20 April 2006, <http://www.sophos.com/pressoffice/news/articles/2006/04/dirtydozapr06.html>.

indicating the geographic position of the terminal equipment of a user of a publicly available electronics communications service'. Under Article 9 of Directive 2002/58/EC, people who have given their consent for the processing of location data other than traffic data may withdraw consent at any time and must have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data. The service provider should regularly remind the individual concerned that his terminal equipment has been, will be or can be located. This would allow a person to exercise the right to withdraw.

However, the location data may cause breach of personal data requirements. Usually the direct subscriber is an enterprise and the user of a certain mobile telephone is a private individual – an employee. This leads to a situation, when the consent for the processing of location data is received not from a direct user, but from an enterprise. Thus, mobile telephones allow companies to identify the geographic position of their staff at a given moment in time or continuously by locating objects in their possession. Such processing raises two issues: the dividing line between work and private life and the degree of monitoring and permanent surveillance.

Surveillance of cargo, vehicles, etc., may be justified from the business perspective however, pursuant to the opinion of Working Party Article 29,[52] the surveillance of employees may be justified processing location data can be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge.

52 Working Party 29 Opinion on the Use of Location Data with a View to Providing Value Added Services, 2130/05/EN 25 November 2005, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf>.

9 Interplay with other social values

a) Intellectual property

On 29 April 2004, the European Parliament and the Council of the European Union adopted Directive 2004/48/EC (Directive 2004/48/EC) on the enforcement of intellectual property rights.[53] It is the most relevant intellectual property rights' (IPR) directive for data protection purposes and privacy concerns. However, the Directive 2004/48/EC itself does not affect Directive 95/46/EC and the data protection principles. According to Directive 2004/48/EC, the protection of intellectual property should allow the widest possible dissemination of works and not hamper the free movement of information or the protection of personal data, including on the Internet.[54]

The Directive notifies that in the context of proceedings concerning an infringement of an intellectual property right, the competent judicial authorities may order to disclose certain information on the origin and distribution networks of the goods or services (Article 8). However this provision shall apply without prejudice to the protection of confidentiality of information sources or the processing of personal data. Therefore, the Directive upholds the principle that intellectual property rights should be protected by avoiding the breach of rules on the data protection.

Thus, again the right to privacy is about the balance – the right balance is needed between the protection of privacy and the protection of intellectual rights. Therefore, legitimate concerns of IPR holders must be carefully balanced against the right to privacy of society. It is always necessary to recall that investigations performed by private actors such as copyright holders must be performed in a clear legal framework and with absolute respect for individual privacy.[55]

---

53 OJ L 157, 30.4.2004, pp. 45–86.

54 Directive 2004/48/EC, preambule, item 2.

55 The European Consumers' Organisation, Data Protection Issues Related to Intellectual Property Rights Article 29 Data Protection Working Party Consultation, 31 March 2005, <http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/beuc_en.pdf> (last visited on 29 January 2007).

The following examples show a warning that the present situation may be dangerously posing the question as to the privacy and new content. Internet forces us to re-think the balance between intellectual property, i.e. holder's rights, and privacy issues once again.

The first example is with YouTube and the other video website – LiveDigital. The user of the aforementioned websites illegally uploaded entire episodes of the hit TV show *24* and *The Simpsons* before they premiered. It was the Twentieth Century Fox that had intellectual property rights of TV show *24* and *The Simpsons*. Twentieth Century Fox did not resign with the situation and issued a legal summons to YouTube and LiveDigital. According to the claimant – the Twentieth Century Fox – the offending material could cause the company much harm, because the *24* episodes appeared on YouTube 6 days prior to their January 14 premiere on the Fox broadcast network.[56]

The problem is that the Twentieth Century Fox cannot determine the violator's identities without the help of YouTube and LiveDigital. Therefore, it requires from YouTube and LiveDigital to disclose the user's e-mail and IP address.[57]

This case could be a precedent if YouTube and LiveDigital disclosed the identity of a user who uploaded copies of entire recent episodes of prime-time series *24* and *The Simpsons*. The question is – who will be responsible. The entertainment industry is of the opinion that the sites do not reveal such offenders, thus they should be held liable for such incidents. However, YouTube and LiveDigital, like other similar video-sharing sites, normally inform content providers they will delete copy written material when alerted by the relevant parties. Thus, YouTube and LiveDigital wishes to be irresponsible for illegal activities. On the other side of such debate there is alarm that websites are monitoring users' identities and activities, and are ready to disclose all these data.

Another example of how privacy and consumer protection problems might be created by the entertainment industry is Sony BMG and its

---

56 Dan Glaister, *The Guadian*, 27 January 2007, see <http://technology.guardian.co.uk/news/story/0,,1999879,00.html>.

57 Reuters, 'Fox subpoenas YouTube after *24* clips poste', <http://www.nzherald.co.nz/section/story.cfm?c_id=5&objectid=10420951>.

music CDs. Sony BMG has placed on the music CDs software technologies to restrict copying of CDs. It was Windows expert Mark Russinovich who found that Sony BMG was using a so-called rootkit to conceal the program used to stop some of its CDs being copied. The problem was announced – the CD that is played on a computer, identifies the IP number of the computer and is able to monitor and report user behaviour back to the firm, manipulates parts of the computer memory, and, accidentally, offers shelter for viruses, and etc.[58] Sony BMG has taken some steps to respond to the security risks.

Notwithstanding, the cases were settled, the problem is still alive. According to the EFF, a non-profit consumer advocacy group which attempts to address the balance between new technologies and civil liberties, it is extremely difficult to remove the software and this can mean users have to reformat their computer's hard drive.[59]

To conclude, privacy and intellectual property rights always exist near to each other. But reality is such that nowadays both of them have the potential be violated at the expense of each other. The above examples may suggest that the society and its individuals are not protected from illegal Internet content (starting from intellectual property right's violations and ending with criminal offences) and illegal data surveillance. However, the balance between intellectual property rights and data protection regime must be carefully preserved. It is a topical question whether our society justifies a disclosure of personal data in order to protect the rights of intellectual rights holders? Who is the master, who will decide, what is wrong, and what is good on the Internet? Who will compensate the loss of privacy if at the end of the day it appears that intrusion and disclosure of IP address was not worth a candle as the alleged IPR infringement was at the end of the day disapproved or rejected?

---

58 Natali Helberger, *The Sony BMG rootkit scandal,* 9 January 2006, available at <http://www.indicare.org/tiki-read_article.php?articleId=165>.

59 *Sony sued over controversial CDs*, 22 November 2005, BBC News, available at <http://news.bbc.co.uk/2/hi/technology/4459620.stm>.

b) Freedom of expression/the right to self-expression

Freedom of speech is a constitutional guarantee that the government will not oppress your right to self-expression. Of course, human dignity is always to some extent in tension with freedom of expression, thus, it must not be forgotten too (especially when talking about mass media).[60]

In the information society, each citizen should be able to benefit from the new content which becomes available through the advanced communications: 'The information society is not only affecting the way people interact but it is also requiring the traditional organizational structures to be more flexible, more participatory and more decentralised'.[61]

Reuters is already carrying blog postings alongside its regular news feed.[62] The new phenomenon of the web is about social networking, meaning that end-users connecting to each other fashioned their own content, and demand low-price, high-speed connections to make it happen. Individuals intensely create user-managed and user crafted content of both voice and video dimensions.[63]

Again, but not lastly, it is about the balance of values. Where one should draw the line between the (a) Internet commentators' right to comment and express his/her views on the public phenomena, (b) the right of

---

60 However, a tendency of privacy in mass media is not changing. Violations of honour, dignity and privacy still exist. For instance, in Lithuania, in the year 2005 The Journalists' Ethics Inspector's Authority received 107 complaints (16 fewer than in the year 2004). The majority of all complaints (75) were received because of information published in mass media; 27 complaints were about the content of television programs, one complaint about radio content and one about Internet content. During the year 2005 35 warnings were addressed to mass media (2 warnings fewer than in the year 2004). See Rasa Lukaityte, *Journalists' Ethics Inspector does not Dramatize the Situation in Mass Media*, available at <http://www.delfi.lt/archive/article.php?id=9353177>.

61 *G7 Summit*, Conclusion of G7 Summit 'Information Society Conference', Doc/95/2/, Brussels, 26 February 1995.

62 Lev Grossman, 'Time's Person of the Year: You', Wednesday, Dec. 13, 2006, *TIME Magazine*.

63 Reed Hundt, 'Communications policy, economic policy. The inextricable link', *Communications the next decade* – A collection of essays prepared for the UK Office of Communications Edited by Ed Richards, Robin Foster, Tom Kiedrowski. Ofcom 2006, p. 197.

other Internet users to share the views with other internet users; and (c) the right of the commentator to stay anonymous online?

10 Analysis and assessment of data protection in social and economic aspects in Lithuania and other countries

a) Do the surveys of public opinion reflect the social reality?

According to the society research conducted for the exhibition 'Infobalt-2000', convenience and quick search as well as comfortable navigation in the Internet was valued most by Lithuanian consumers by the end of the year 2000 (60%). While the anonymity and security of personal data was deemed as a matter-of-course (54%). In addition, only few respondents determined privacy as a problematic aspect of the Internet (7%) (among several other key aspects such as copyrights, security, etc.).[64]

Two years later, in 2002, the majority of the respondents assumed that their personal data should not be public, however, less than 10% of respondents could determine who has a right to collect their personal data.[65] Thus, lack of information and public knowledge about data protection seemed to be the biggest problem in Lithuania in those days. However, thanks to the efforts of the State Data Protection Inspectorate and other public institutions, the situation is changing to the better.

It is interesting to compare those surveys with the surveys conducted in US, where public opinion polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities. In addition, the Americans demonstrated their strong support for Internet Anonymity.[66]

---

64 The society research conducted by the organisation 'Sociumas' for the exhibition 'Infobalt 2000' <http://www.sociumas.lt/Lit/ataskaita/ataskaita_privatumas.asp> (last visited on 28 January 2007).

65 Vaidotas Bla_iejus Abraitis and Alfredas Otas, *Privacy and Security of Information in Lithuanian Internet*, 17 September 2002, available at <http://www.leidykla.vu.lt/inetleid/inf-mok/23/str2.html> (last visited on 28 January 2007).

66 Public Opinion on Privacy, Electronic Privacy Information Center, availiable at <http://www.epic.org/privacy/survey/> (last visited on 27 January 2007).

Today, from the perspective of data subject, one may already claim that the most important thing is to know what will happen with his data; in other words, the data subject is much more concerned about the control over his data as collected and used by third parties rather than by the very fact than his data are collected and used. Thus, it is a general tendency that people no more expect the absolute privacy on the Internet, which may also suggest that self-regulation is the most viable solution. Since individuals realize that existing laws do not adequately protect their personal data, they often engage in privacy 'self-defence'. When polled on the issue, Americans regularly claim that they have withheld personal information, have given false information, or have requested that they be removed from marketing lists.[67]

According to the Eurobarometer survey,[68] in 2003 on average 60% of all EU citizens were concerned to a greater or lesser degree, about the broad issue of protection of their personal privacy. As so often happens in surveys of this kind, this average figure hides a wide variation in opinion. Only 13% of Danes, Spanish and Portuguese were very concerned about this issue. However, at the other end of the scale, were more than half the Greeks and Swedes who were polled with figures of 58% and 54% respectively.

Talking specifically about the Internet privacy, around 64% of EU-15 citizens polled tended to agree that they were worried about leaving personal information, such as their name, address, date of birth on the Internet. In a technological extension to the telephone monitoring question, the issue of monitoring Internet use was reviewed. Overall, the main response from 40% of those polled was that monitoring should only take place on those suspected of terrorist activities. This figure is identical to that in the previous question on telephone monitoring. High figures were noted in Finland (55%) and Sweden (51%).

---

67 Public Opinion on Privacy, Electronic Privacy Information Center, availiable at <http://www.epic.org/privacy/survey/> (last visited on 27 January 2007).

68 European Union citizens' views about privacy (Special Eurobarometer 196), this survey was requested by Directorate General Internal Market, Unit E4.

However, there was less support for the rights of the individual when related to the Internet than the telephone and, accordingly, only 25% of the EU-15 considered this to be the stance that should be taken.[69]

So, are we right when suggesting that those public poll results may imply that new technologies (basically, Internet) bring more possibilities to a society, thus, the requirements, expectations held by the society are changing? May it be suggested that the right to information, right to self-promotion is becoming more important than privacy? May the results show that people do not refuse to stay anonymous, but they do not expect privacy anymore? This sounds quite controversial, although it may well be true in information society.

b) Direct marketing

Personal data protection regime should match the business realities, because it is largely premised on the balance between privacy and freedom of personal information flow. Direct marketing regulation is a good example of how Lithuanian data protection authorities mistreat the economic rationale behind. According to the Directive 2002/58/EC, Member States shall take appropriate measures to ensure that, unsolicited communications for purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications. Pursuant to the law on data protection, personal data may be processed for the purposes of direct marketing provided that the data subject has given his explicit prior consent (Article 14). However, direct marketing still causes various discussions between business and the State Data Protection Inspectorate.

Business normally perceives the personal data on consumers as the tool for business activities or as economic good, commodity. However, most of the consumers treat their data as something which belongs to them, although in case of economic benefit most of the users may tend to

---

69 European Union citizens' views about privacy (Special Eurobarometer 196), this survey was requested by Directorate General Internal Market, Unit E4.

disclose their data or relinquish of their rights to privacy. Bonuses, promotions, offers, ads, individualized or customized solutions may not be effectively conveyed without the knowledge of the customers and their data. And in most of the cases those activities create value to the consumer itself. Thus, one may pose legitimate question - why it should be anybody else than the consumer, who shall decide which value is more important and valuable for him/her, bonus, discount, information about the new product, or his right to be left alone? Using of personal data may in the end mean that the consumers are better served, provided with more new, more individualized and better quality products, more new opportunities to participate in the consumption.

In practice usually business enterprises have no possibilities to get a prior consent from consumers, because, a consumer is not a client of a certain business enterprise. Thus, the only way for business to get a consent from consumers is to contact them, e.g. by phone, and to ask their consent. However such action would be considered as a breach of the provisions of data protection.

On 18 June 2006 the round table discussion of open problems in direct marketing and processing of personal data was held by one of Lithuanian enterprises.[70] Business representatives and officers from the State Data Protection Inspectorate tried to find a solution on the following: how to communicate with clients, with whom agreements were concluded many years ago, and where such agreements did not determine a possibility of direct marketing or processing of personal data for the purposes of direct marketing, and how to receive consent from those clients to process their personal data? According to business, enterprises are helpless to communicate with their clients, to send an e-mail or SMS about new services, products, because they have no client's consent. Pursuant to opinion of Lithuanian businesses, rules of direct marketing are too strict and unfavourable to business. According to them, communication, including direct marketing, should be only a matter of agreement between an enterprise and its clients. Another

---

70 *The Usage of Personal Data in Direct Marketing*, available at <http://www.itella.lt/ilwww/lithuania/lt/Naujienos_ir_Jvykiai/Jvykiai/ivykiai2006/060518-1.html> (last visited on 31 January 2007).

problem determined by business is the definition of direct marketing, which is far from being clear enough. Where one is supposed to draw the dividing line between mere communication and direct marketing? For instance, can a birthday greeting be considered direct marketing? These questions are still open. The rights of those who do not wish to receive information are protected, but what about those who want to be informed about new events, products, want to receive e-mails or calls informing about new possibilities? Who will protect their rights? Pursuant to the opinion of officers from the State Data Protection Inspectorate, individuals who wish to receive information must be active and show their interest to business.

Thus, from purely business perspective, application and enforcement of data protection rules in the field of direct marketing may run counter the logic of economics. That is why the law should carefully look for a right balance.

c) Economic perspective

Of course, privacy is not about economics; privacy is, *inter alia*, about human rights; but personal data protection regime is also about economics among other things. Thus, one may easily grasp the idea of privacy as a 'commodity that you trade for the benefits of living in a connected world'.[71] You can easily waste and loose understand about human right to privacy by such kind of expressions like '[...] if you don't want people to find you, stay the heck offline'.[72] Of course, we may not place efficacy ahead of justice, economy ahead of human rights. Data protection was always about the carefully sought balance.

However, one thing about such economic perspective is true – let the users and individuals decide themselves. New society is about making choices. The issue that in reality Internet rarely provides with real choices already merits a separate discussion.

---

71 Jeff Kirvin, *The Myth of Privacy*, available at <http://www.writingonyourpalm.net/column010212.htm> (last visited on 31 January 2007)..

72 Jeff Kirvin, *The Myth of Privacy*, available at <http://www.writingonyourpalm.net/column010212.htm> (last visited on 31 January 2007).

11 Conclusions

At this stage, this article cannot do much more than jut hint at the need for a new perspective in data protection and privacy law – the new social and economic reality perspective – for rules that carefully balance the traditional human right to privacy and evolving societal needs of modern society. Further research should be carried out to explore the question of how the interplay and balance between idea of privacy and various aspects of social reality should be struck.

1. New technologies have vested the society with new instruments and made individuals' lives more convenient. The society has happily accepted those new technologies and new opportunities, it can avail and enjoy using such new ways of communication. Evolution of technologies and social life enhanced individuals to access to information and knowledge; thus it inevitably may lead to a situation when members of society recognize the right to know, right to communicate, right to express views and contribute to the society (even with stuff of little or no value or interest at all) as a more vital and valuable than traditional and straightforward 'right to be left alone'. On the other hand, this straightforwardness has proved to be a robustness of the concept of privacy.
2. Thus, the very idea of privacy is ever-green vitality of each democratic society, covering fundamental constitutional and fundamental human right; but legally speaking it is a concept which is more and more difficult to grasp and define. Legally speaking, it is hardly possible to enforce the system which is difficult to define. Furthermore, the idea of privacy, as a very general idea, may act as a paramount check and balance mechanism, ready for action in those cases, where rule of law (data protection regime) is at flaw. It may even differ from jurisdiction to jurisdiction.
3. Personal data protection regime may be regarded as a compromised and balanced version of pure idea of privacy.
4. New technologies are transforming our lives and even the concept of the right to have or expect privacy. Personal data

protection regime implies more active participation of the data subject in the societal relationships; modern life is about preferences, choices and self-determination, therefore if the individual does not want to be disturbed or interfered or otherwise approached, he/she may choose or opt out of such intrusive events (i.e., to object that their phone numbers are publicly listed in the subscribers' directory, etc.). Thus, data protection regime is largely about choices and self-determination of individual himself/herself. Being such, at least conceptually data protection regime is more tailor-made and more suitable for Internet and other technologies, which also reside on the premise of self-determination and choice.

5. However, the individual is already required to MAKE A CHOICE. Thus, individuals, no more expect the absolute privacy on the Internet; what they are concerned most is what will happen with their data collected on the Internet (cookies, financial information, etc.). Knowing the purpose for which data is collected and processed is very important to a data subject.
6. Of course, we may not place efficacy ahead of justice, economy ahead of human rights. Data protection was always about the carefully sought balance.
7. Thus, the law should avoid imitating and mimicking one-sided patterns of societal behaviour – complexity and vitality of this phenomenon should be carefully explored as much as possible.
8. It is incorrect assumption that person's dignity and other personal values are downgrading. Assumingly, the correct assumption is that person's dignity and other personal values may be also properly protected and secured with additional type of societal values, such as interaction, socialisation, and networking.
9. Third Pillar of EU once again reminds us of the price for safer life in society. Unfortunately, in the hands of evil new technologies may become more dangerous to the society as before. That's why the price we are paying is, *inter alia*, our privacy.

PRIVACY AND IDENTITY MANAGEMENT IN A EUROPEAN e-HEALTH SYSTEM: AN EXPERIENCE IN THE MAKING

Cesare Maioli and Chiara Rabbito[1]

1 e-Government and e-Health

The use of ICT is tied to the development of computer science and the Internet in the process by which the public administration is modernized: this use is called e-Government.

e-Government involves both back-office and front-office operations, the former focussing on the internal efficiency of each public administration, and the latter on providing easy access to the information held by the public administration. This also means the citizens with providing services, and hence making public-administration services more interactive.

1.1 e-Governance of Health

The European Union policy aimed at promoting an innovation society in which social and economic benefits are extended across the entire

---

1 Cesare Maioli (<cesare.maioli@unibo.it>), professor of computers and law in the Faculty of Law of the University of Bologna, is a member of CIRSFID at the same university. Chiara Rabbito (<chiara.rabbito@unibo.it>), Ph.D, in computers and law, is a lawyer and a contract researcher of CIRSFID. The two authors worked jointly in the I-Care project. For what it concerns this paper, Cesare Maioli wrote parts 1.1, 2.2, 3.4, 4, and Chiara Rabbito wrote parts 1.2, 2.1, 3.1, 3.2.

population, and in which information technology is recognized as playing a major role, has found in e-Government one of the key tools in the process of modernizing and reorganizing public administrations.

This has progressed in parallel with the emergence of a new form of democratic government, i.e. governance,[2] which entails a building up of experiences of exchange and co-operation between public and private participants.

After a long period of legislative inactivity, the European Union became aware of the importance that information technology has for the modern society, and so began focussing on the need to provide member states with guidelines on which basis to regulate the sector.

A key moments in this effort lies with the Bangemann report of 1994,[3] which indicates three ways to achieve technological development: (a) by interconnecting networks and making services and applications interoperable through a process of standardization responsive to the needs of the markets; (b) by increasing the demand for new online services by public administrations and making these services more visible; and (c) by working out a set of shared rules for solving the most pressing technical and legal problems (such as protecting privacy and ensuring information security).

These general guidelines have given place to three important directives: no. 96/9/CE, regulating the legal protection of databases; no. 1999/93,

---

2 Although we lack an internationally agreed definition of governance, good governance has become a key development concept over the last decade. The Organisation for Economic Co-operation and Development Assistance Committee (OECD) considers governance as 'a process oriented, broad, inclusive and multidimensional concept encompassing democracy, human rights, participation and the rule of law'. One can see it as the way in which societies develop rules, processes and behaviours necessary for their survival and their accomplishment. Governance is the management of relationships between human beings, between societies, between mankind and the biosphere.

3 See M. Bangemann, *Europe and the global information society. Recommendations to the European Council* (EU 1994), whose essentially liberal approach hinges on the activity and investment of the private sector. The earlier *White Paper on Growth, Competitiveness and Employment* (Bruxelles, 1993) has been submitted by the 'Bangemann Group' to the European Council in Corfu.

regulating digital signatures within a European frame work; and no. 99/46/CE, concerning the processing and circulation of personal.

Also relevant in Italy, especially for the impact on e-Government policy, is eEurope 2002, which singles out some main objective to be accomplished in working to make Europe the world's most competitive and dynamic in economy, taking advantage too of the opportunities offered by the Internet.

The 2002 eEurope Action Plan is instrumental to the objective of the ICTs to enable citizens to have easy access to the information hold by the public administrations, and to this end it suggests (a) sharing the most successful experience of online administration on the model of the knowledge exchange that has taken place in Europe and (b) reusing technological solutions. European lawmakers have thus detected a weak point in many processes by which the public administrations are automating their work: an inability to take local experiences and make them available on a wider scale in planning and implementation.

The European Union has laid out its main health-care objectives in the document 'i2010 initiative', and ICTs play a crucial role in this respect too.

The technological evolution of local and natural social and health services is thus considered a decisive strategic tool for the growth of health systems across Europe, which through 2004 e-Health Action plan has launched an initiative for coordinated planning among the member states, with provisions to be adopted by 2009.

As is known, the term e-Health was coined in the United States to designate medical assistance provided to patients at a distance by using ICTs; the practice originated in the 1970s with the space missions, which brought to light the need to develop a technology by which to provide real-time first-aid and assistance to the astronauts.

e-Health does not, however, confine itself to medical services but also includes related activities such as communicating test results remotely (i.e. telemedicine) and sharing clinical information for diagnostic purposes.

In 1990, the member states of European Union settled on an agreed definition of e-Health as consisting in monitoring and managing patients as well as training personnel through the use of systems giving experts fast access to patient information, regardless of where such information is stored.

The following year the World Health Organization gave a narrower definition of e-Health as 'the combined use of electronic communication and information technology in the health sector'.

These definitions give evidence of a shift over the years from a circumscribed idea of e-Health to a very wide range of applications capable of renewing the health system entirely.

e-Health can therefore significantly improve patients' living conditions, since the patient can benefit from real-time services, and this reduces the time needed for certain services, thus making for greater latitude in managing medical emergencies.

By the same token, the patient has greater access, and at lower costs, to specialized medical skills.

From a broader perspective, e-Health applications can bring benefit to the health system by making for faster, more economical services at a higher quality, using fewer personnel, and making it possible to quickly process routine procedures, so as to allow greater room for medical emergencies and prevention. e-Health therefore makes up an essential component of welfare provision, by offering tools such as tele-reservations, tele-diagnosis, tele-consulting and tele-delivery of documents, images, graphs, and records – all of which travels with the patient.

There are three strategic objectives in the European Union e-Health plan mentioned above: (1) developing shared strategies and methods among member states; (2) implementing common actions to accelerate the uptake of e-Health; and (3) using and sharing best practices as well as evaluating the performance of e-Health methods.

So far the technological solutions adopted in Europe have issued out of a need to manage the single health facility or out of the direct needs of health professionals. Each facility would make its own decisions,

independently of other facilities, as to when and how to automate. Future information systems will have to be centred on the needs of the citizen. This will make it necessary to integrate clinical, organizational and financial information not only within the single health facility but also, and especially, among different facilities. The objectives set out by the European Union require that all health providers work together to find coherent and adequate ICT solutions supported by infrastructural projects in the regions and the member states.

It will be particularly important to involve the regions into this effort, so as to have them cooperate in promoting the development of ICT infrastructures, thus achieving lower costs than what so many isolated systems would make possible.

The development of health services based on the use of ICTs calls for special analysis, since the process is so decisive as to suggest a complete remake of the concept of e-Health itself. The current approach – based on a massive use of the Internet, mainly as an information channel or as a way to provide health or pharmaceutical services to a passive patient and user of services – will have to be gradually superseded in favour of a use of ICTs that makes the patient the focus of interest on the part of health-service providers, taking a global and integrated view of the patient as a person and not simply as a 'case'.

1.2 Health Informatics

There are doubtless great advantages that ICT provides in health care, especially at home for the elderly or the disabled (e.g. people with cardiac insufficiencies, asthma, or diabetes). Indeed, we can use telephone lines to communicate biomedical signals and data to a hospital centre or other specialized facility, and can use broadband networks to transmit diagnostic radiograph images at the same resolutions as those used at the source radiology lab.

In this framework, the family doctor takes a new strategic role, becoming the main ICT operator capable of reporting and communicating diagnosis directly to the citizen over the Internet or making therapeutic treatment and diagnosis faster.

The change underway is happening on such a scale as to require a new name for the group of actions that ICTs make possible in promoting citizens' health: no longer e-Health but health informatics, which not only provides the technology for certain health services but also includes back-office and administrative processes, in an effort to create a network of relations among health institutions, pharmacies, public administrations and social participants, in such a way as to better manage the complexity of information flows.

In health informatics the patient is clearly identified and directly involved in the health and technological process revolving around him or her.

From this operational perspective it becomes essential to focus on the way the patient's personal data is handled, especially as concerns health data, which will have to be processed in a legitimate way, ensuring the appropriate level of data security.

Here we cannot stress enough the need to bring under legal scrutiny the legitimacy of a process by which health data is exchanged using complex information systems such as those being experimented worldwide, an exchange made possible by the explosive growth of the Internet and of wireless technology and encouraged by government sensitive to welfare issues.

Indeed, technological innovation is doubtless a sign of progress, for it enables us to improve the quality of human life and to more effectively share knowledge; at the same time, however, as happens with any new technology, we in society have to consider its critical aspects, such as an improper use of technology which may infringe on our rights as individuals.

Therefore, it will not suffice to single out the vulnerabilities the ICTs expose us to with respect to our legal protections – we will also have to find solutions to these problems, by working out rules or legislation for a reliable system of health informatics, a legally legitimate system which is also technologically and economically sound.

Furthermore, ICT has transformed medical information, and two kinds in particular: information used in diagnosis and information used in the

provision of health care itself. This new information, i.e. medical data, is offered in a digital form throughout the procedure, from the time it is collected to its further processing and interpretation, and finally to its filing and access.

Processing this new kind of information can be seriously damaging to the person if the use is discriminatory or is done without obtaining the data subject's consent; at the same time, this information must be processed if we are to protect the data subject's physical integrity as well as the integrity of third parties and of collectively in general.

There are great advantages to be had in science from the development of information technology, especially in the shape of software for processing clinical data, electronic databases for its collection, and networks for carrying the data, since it is now possible to find, process, and compare health data in a matter of seconds.

Yet this development has increased the number of people having access to health data, as well as the amount of data and the speed of its exchange, and in doing so has made its processing dramatically riskier to confidentiality and privacy. In consequence, European and Italian lawmakers have increasingly been concerned about data protection.

In fact, even though humans have always processed data in various ways, information technology has caused this practice to expend impressively by making it possible to access and manage much more data for each individual and to collect data on many more individuals than before.

2 The role of Legal Informatics

The basic innovation introduced with the use of information technology consists in its making it possible to compare and merge personal data from different sources. But while this merging and comparing of data enables us to more accurately profile patients and keep track of their medical histories, it also by the same measure exposes the patient to a greater risk of breached privacy and confidentiality, because information that proves trivial if considered in

isolation can form a piece of a very informative puzzle if combined with other information, and this larger picture can be used for any number of purposes.

Until a few decades ago there was no privacy concern or anything alarming about the use and handling of medical data, because this use and exchange happened within a fiduciary relationship – that between patient and physician, especially the family doctor – and because most of the recording happened in paper form or even by working from memory.

This all changed when information technology came into wide use for purposes such as prevention, diagnosis, treatment, and medical emergency from a remote location: this new way of delivering health care brought out the need to work out legal protections against the misuse of medical information.

2.1 Managing Personal Information

European Union and international law have responded with legislation setting forth a general prohibition against processing data suited to revealing the data-subject's state of health or sexual orientation or life, and the domestic legislation internal to different states may provide for additional security measures.

As early as 1981, the Strasbourg Convention (no. 108 of 28 Nov. 1981) stated the need to protect people from automated processing of personal data, and the signatory states agreed that such processing must not encroach on the right to privacy or on any other basic right, and that this guarantee applies to everyone regardless of nationality or residence. The convention also states that 'personal data concerning health or sexual life may not be processed automatically unless domestic law provides appropriate safeguards'.

Directive 95/46/EC of 24 October 1995 is based on the assumption that integration among member states requires considerable exchange of information among such states, and so makes it necessary to set out common Europe-wide rules and criteria for the processing of personal information. Under this directive, all member states must pass

legislation guaranteeing a level of protection at least as strong as that required under European Union legislation, and transposition of this directive was to take place no later than 25 October 1998. This deadline gave new momentum to our own lawmaking process in Italy, a process that had already been underway since the 1980s with the Mirabelli Commission and was then carried to completion with Law no. 675/96.

Under Art. 8.1 of Directive 95/46/EC, sensitive data gives rise to a special category of data and so must be held to a tougher standard of protection than is personal data. This places a general prohibition on the processing of sensitive data unless the data subject has consented, and even where no such consent is available, sensitive data may still be processed to protect a 'substantial public interest' or the 'vital interests of the data subject or of another person', or for health purposes.

The consent referred to under Art. 2 (h) of Directive 95/46/EC will have to be free, voluntary, specific, and informed. So the exceptions to consent provided for under this directive will have to be accompanied by measures guaranteeing the protection of basic individual rights, including the right to privacy.

Data subjects are entitled to rights giving them control over their own data, and these rights are enforced by way of corresponding duties of third parties processing the same data. Thus, the data subject has a right to have full disclosure about who the data controller is (whether a natural or a legal person) and about the purposes for which the data has been collected, this to enable the data subject to access the same data and have it rectified, erased, or blocked.

Directive 95/46/EC therefore follows the European Council in its general prohibition against processing of sensitive data, but it also provides for an exception to this prohibition in case the data is processed (a) by a health professional bound by national law to an obligation of professional secrecy and (b) for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services.

This balancing of interests – protecting privacy as against delivering effective health care – informs Italian Law no. 675 of 1996 as well as

the Italian Code on Privacy of 2003,[4] under which medical data may be processed for the purpose of health protection, in such a way that the patient's privacy is protected quite independently of the health-care provider's duty of professional secrecy, as had traditionally been the case. So, too, the Italian Code on Privacy has brought the matter under the purview of statutory law, in contrast to its previous regulation under administrative law.

As an essentially delocalized and transnational practice, telemedicine involves the movement of medical data across national boundaries, primarily for the purpose of providing the data subject with appropriate health care, and this movement poses a problem of uniformity in data-protection regulation as we pass from one country's law to that of another. In fact differences among legal systems may act as a hindrance to the movement of medical information, especially when moving such information from the European system of law to other systems whose forms of protection are much less exacting.

2.2 The I-Care project

In Italy, an e-Government and e-Health project called I-Care has been launched framed in keeping with the social-welfare guidelines set forth in the 2003–05 National Health Plan, among whose objectives is that of setting up an integrated network of social and health services for the chronically ill, the elderly, and the disabled. I-Care is a EU-funded research program promoted by Emilia-Romagna Region under 2005 1.1 initiative of the Regional ITC Plan, in accordance with the 2005–07 Social and Health Plan, which called for joint initiatives by universities and industry aimed at conducting research for the development of new technologies applicable in health care, working out criteria for assessing the impact of such technologies, and experimenting their adoption by health-care providers, all the while monitoring the process in its early stages.

---

4 Legislative Decree no. 196 of 30 June 2003, with the title *Personal Data Protection Code*.

I-Care – a collaborative project conducted university research centres, local government bodies, and private enterprise – is aimed at creating a system based on the use of ICT's to deliver health and social services and enable the service providers within the network to easily exchange the data deeded for these services. The technological infrastructure in question is mainly designed to support organizational processes by which to provide at-home social and health care for the elderly, collect and evaluate service requests, plan for the delivery of service requests, and balance accounts on such service provisions.

The platform for the project will consist of wireless devices, Web technologies, and regional broadband infrastructures to support tracking, planning, and management of the services provided.

The core technological objective was to develop a system named S2I – an Italian initialism for Socio-Sanitario Integrato, meaning integrated social and health services – based on an architecture that models the relationship among the different subjects involved in the project.

This architecture is made up of three main components as follows:[5]

(1) S2I-Manager. This is the information system supporting organization and management activity, and it enables the following functions: recording and validating service requests; collecting and consolidating the information relevant to each service request and to the service provided for it; extracting, interpreting, and loading information relative to all the activities recorded by the associated S2I-Field systems; doing bookkeeping and balancing of accounts on all the services provided, as well as auditing and managing these services; reconstructing each patient's medical and social-service history; and compiling statistics about the service and working out standards and parameters for it;

(2) S2I-Field. This system supports the back-office and fieldwork activities carried out by the service providers and their agents

5 Summary of the technical document *Progetto I-Care: Sviluppo e validazione del sistema S2I, revision 1.0.* (Rif. 3442/P-RC/ec, Forlì, 8 June 2004) published as an annex to the general I-Care participants agreement.

(whose work in the field is supported by user-friendly computing equipment such as Personal Digital Assistants and tablet PCs). The system enables the following functions: allocating resources for optimal service provision; managing interaction for management of unforeseen events; achieving scalability with growing amounts of data; using the computing devices just mentioned to automate record and time keeping for all treatments, materials, and results; enabling all practitioners to access clinical data on request; enabling on-request access to service; and compiling statistics for all organization activities as well as monitoring and managing these activities;

(3) S2I-Integrator. This is an Enterprise Application Integration (EAI)[6] component specifically tailored to meet the needs of health-care provision. It coordinates and certifies the flow of information between multiple components (S2I-Manager, S2I-Field, and other external systems) in such a way as to enable the following: integrity of information in the course of synchronous and asynchronous exchange alike; security, as by using authentication and cryptography to ensure privacy; mapping of communication protocols, formats, and classes in the course of interchange with external systems; and management of the Health Level 7 (HL7)[7] communication protocol in connection with the S2I-Manager and S2I-Field components.

---

6 Enterprise Application Integration (EAI) is the set of projects, methods, and tools for connecting and coordinating a business's software applications and their data so as to achieve an integrated, consolidated, expansible system. An EAI will take up all of a business's applications (including ones dating from earlier periods, so-called legacy applications) and the databases associated with them and gets them to communicate through Web interfacing, thus breaking down the barriers owed to differing technological approaches, formats, and standards. This way, a business can continue to use applications vertically on different technological platforms (mainframe, client server, Web, etc.) all the while maintaining a modern integrated view of its ICT system.

7 Health Level 7 is an international body set up to develop an XML standard for sharing, managing, and integrating data in support of the patient's clinical treatment, and for managing, delivering, and assessing medical services. HL7 seeks to become the standard for a universal language on which basis to build digital clinical records and bring into direct relation the applications and services by which patients can be accepted and their treatment managed, including from an administrative point of view.

Following are the basic concepts involved in implementing this architecture:

— in a typical application running in the field, there are as many S2I-Field instances as there are participating service providers. Instead, there is a single instance of S2I-Manager and S2I-Integrator. S2I-Manager and S2I-Integrator instances can operate on the same server, on which multiple S2I-Instances can be run. All the systems communicate through an Extranet, and if necessary, through the Internet. At any rate, communication is based on IP protocols;

— communication between S2I-Manager and all S2I-Field instances as well as communication between the S2I-Manager and external legacy systems are mediated by S2I-Integrator, which ensures that rules are followed and that communication is valid. The information exchange among the S2I modules take place whenever possible through web service;[8]

— the external legacy systems are typically: municipal register of births and deaths, the personal record of the local health centre, the information system by which participating hospitals manage admittances, dismissals and transfers (a.k.a. ADT module). Information exchanges with external systems go through web services. A specifically designed S2I-Integrator software tool makes it possible to generate such web services easily using the Application Program Interfaces of the host system or, otherwise, emulating user transactions of the system itself;

— the S2I-Manager and the S2I-Integrator present to their users a pure Web interface. S2I-Field is independent of other components and can be used as such by a service provider.

---

8 Web service is a software system designed to support interoperable computer to computer interaction over a network. They are frequently Application Program Interfaces that can be accessed over a network such as the Internet, and executed on a remote system hosting the requested services.

3 Privacy Issues

An important part of the I-Care project has consisted in analyzing the legal issues connected with delivering e-Health services across an open network, and especially those issues that concern information security and data privacy.

It should be pointed out that the issues involved in the processing of personal data have affected all of the main relationship analyzed in the project.

3.1 I-Care and Privacy

One important privacy area is that of interpersonal (so-called micro/micro) relationship, which concern patients in their relationship not with physicians, health practitioners, and social workers, but also with any other caregiver, including family and friends. Given this broader range of application in which privacy has a role, the caregiver will have to be especially careful in processing data pertaining to the cared for, complying with all applicable law and deontological codes.

Likewise, health practitioners will have to undergo training qualifying them to make sure that the patients' data is processed properly and respecting confidentiality before family and friends. And we must also take into account the relationship between the cared for and the institutional health provider: this involves the use of medical data, a use extensively regulated by law, and data processor is therefore required to give privacy notices to the data subjects and to obtain the latter's consent. Specific forms have thus been prepared in compliance with the law, these including the privacy notices and the consent form.

A second important privacy area is that of the (micro/macro) relationship that service personnel have with service providers (hospital and field nursing staff, social co-operatives, service sector institutions) and with service managers (municipality and local health authorities). Privacy requires here that practitioners be identified or authenticated and that they go through the appropriate access authorization profiling depending on the kind of practitioner involved, on the kind of institutional function he or she is entrusted with.

There is also a third privacy area, this being the (macro/macro) relationship between agencies, and this too has been a point of legal analysis. In fact, we have had to make sure that each agency was compliant with privacy law, especially as the new Italian Code on Privacy of 2003 introduced several important innovation. The major innovation has consisted in regulating information flows among agencies, a process that has hitherto taken place in paper form and is now in digital. The reason why European and Italian legislation has focused on information exchange by way of ICTs, is that this poses a greater risk to privacy and carries a greater likelihood of data misuse, which may come to light only subsequently, when different pieces of data are cross-checked.

For the I-Care project we first classified the data to be processed and services to be provided, and then built this classification into the ICT model for interaction between citizen and service provider, and this made it possible to single out the main privacy issues involved in processing personal, sensitive and health data along with the security measures to be adopted to this end. Our focus with respect to health and social practitioner was on the obligations to provide privacy notices and obtain the citizens' consent before processing their medical data. The classification of data made it possible to process it according to appropriate rules and procedures in compliance with the law.

Data was classified into three groups: health, sensitive and personal data. Also, we had to focus on the legal status of practitioners. Indeed, Italian law requires that processing be carried out by public health providers and medical professionals,[9] a group that does not include social workers. This made it necessary to use two different privacy standard depending on whether at-home service to the cared for is

9 Under the Italian Code on Privacy, section 4(d), sensitive data means any personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as data disclosing health and sex life. In this last respect, section 76 and ff. classify health data as sensitive, requiring that it be processes as such and only by qualified operators and health-care professionals.

carried out by a health professional or by a social worker. Thus legislative decree no. 196/2003 section 34, and annex B, single out different authorization levels ranked according to classes of practitioners (e.g. specialized physicians, general practitioners, nurses, social workers – seventeen classes in all): accordingly, we have had to work out different forms of authentication and authorization that different practitioners need in order to access different services.

Another problem was that of using personal records – as well as health and sensitive data – to see if the S2I software modules could be used outside the control of the institutions legally competent to store and use the same data. Indeed, when a governmental institution builds a digital archive using data coming from other agencies, the data processor at this agency will have to comply with the rules established by the Privacy Authority for such communication, and will also have to offer a reason or justification based on the institutional role of the receiving agency. Personal records are subject to specific rules thus Italian law (DPR 223/1989) requires that personal records be viewed and extracted exclusively by the municipal officials specifically designated to that purpose. This requirement have been implemented into the I-Care platform by making it impossible to anyone except for the municipal records official to access the data used for the project; therefore I-Care software components filter medical records accordingly.

3.2 Identity management

The I-Care project manages identities in compliance with applicable law by regulating access according to different level of authorization; thus, for each identified user (for each authentication), a corresponding role has been defined for access to the system.

Each role has been associated with a group of authorizations; by authorization is meant a privilege by which a user can access a finite set of system resources (i.e. functions or data the system makes available) depending on the user's role, and in such a way that users in other roles cannot do. It is the system administrator's job to manage roles for each of the system's users.

The system administrator assigns to each user one or more roles through which the user can access only those system resources necessary for his or her role. The system administrator uses the system's authorization-management function to enable or disable roles for any user.

The set of roles in which a user accesses the system defines that user's authorization, and so is called in the law.

Thus, I-Care implements an authorization configuration system specifying (a) who can access the system, (b) the functions and actions each user can take, (c) the kind of data on which these actions and functions can be performed.

By function is meant the operations that can be called up from a menu or from other interface elements. By action is meant the basic operation a user can carry out on each of the system's function (e.g. insertion, updating, deleting). By domain of visibility is meant the range transaction types (e.g. request, admission, medical treatment) the organization sets up for access to it. Following are the access options available:

— personnel-specific, the user can access only transactions attributed to him or her specifically;
— unit-specific, the user can access transactions attributed to his or her operational unit;
— service-specific, the user can access transactions attributed to all the operational units providing the service the user is entrusted to;
— unrestricted, the user can access all transactions.

This ranking has made it possible to accurately configure the authorization available for each role – for each person who accesses the system. Each person looking to operate must log in as a user: this authentication requires the person provide a pair of personal keys, at which point the user enters the system as a user with all the information relative to his or her operational units and roles.

The user groups defined for the I-Care experiment has been singled out taking into account the operational skills that each user has within the service he or she is providing.

A practitioner who resigns will no longer have any placement within any operational units, and so will no longer be able to access the system.

In managing identities, the I-Care project has had to also take into account section 22.2 of the Italian Code on Privacy, under which electronically processed sensitive and health data stored in databases must be processed using cryptography or identification codes or other solutions that make such data temporarily unintelligible even to those authorized to access it, in such a way that the data subject can be identified only in case of strict necessity.

Section 22.7 specifies in addiction that data revealing a subject's health or sexual life be stored separately from other personal data processed for purposes for which such data is not needed.

Sections 33 and 34 of the Italian Code on Privacy set out minimum security measures, accompanied by corresponding criminal penalties. Section 34 establishes that no health organization can process data revealing a subject's health or sexual life unless cryptographic techniques and identification codes are used for such processes.

Sections 22 and 34 combined therefore require that databases storing health be built using cryptography or identification code and keeping health data separate from data identifying the patient, so that even an authorized health practitioner will be prevented from immediately recognizing the patient. Indeed, only upon a decrypting operation or entering an identification code will it be possible to couple the patient's identity with his or her health data – this in accordance with minimum security measures as set forth in chapter II (in particular, section 34.g) and in annex B of the Italian Code on Privacy which, under section 19.8, requires that the Security Policy Document comply with these two security requisites.

The separation of data must also be implemented in the information system and the matching between the two sets of data will have to occur by way of a unique and secure patient identification code.

Identification data is encrypted into the database using advanced cryptography techniques: this will make it possible to render

anonymous any data revealing the patient's health in case should anyone access the database without authorization.

If identification data is to be temporarily unintelligible even to those authorized to access it, making identification possible only when necessary (section 22.6), the graphical user interface must make it possible to display in anonymous form the data revealing the subject's health: identification data are visualized in an encrypted form and are therefore unintelligible to everyone except for personnel authorized to view such data.

3.3 Business Process Reengineering and Implementation

As we have seen, I-Care is a complex project involving organizational, technological and legislative aspects: the corresponding process analysis, based on the method known as Business Process Reengineering (BPR)[10] was accordingly developed taking different aspects into account, thus analyzing (a) the source of the services provided at home, (b) the functions and the flows of information circulating through the system as is (as-is analysis) and (c) as-is practices with respect to the applicable law, and how such practices should be changed to achieve compliance.

This analysis was carried out in the course in meetings with the people running the organizational units and with the practitioners in the field.

Every micro process was for compliance with (a) legislative requirements on the the protection of personal data and on security measures and (b) transparency in the administrative procedure, and attention was paid as well as to access to the procedure and to the task of translating paper procedures into digital ones.

---

10 BPR is an accredited method first developed in the 1990s – M. Hammer, *The Reengineering Revolution* (NewYork, Harper Collins, 1995) – which sets out three phases, a first one in which a process's range of application is defined; a second one assessing the situation as is, in such a way as to single out areas for possible improvement; and a third one in which the actual reengineering is undertaken, by modelling processes designed to address the problem areas that came to light in the diagnostic phase.

At a second stage (to-be phase) we redefined the administrative procedure on the basis of the BPR and singled out the changes that needed to be brought to the ICT system. All health and social services provided to the citizens had to be compliant with the law, and especially with the rules on administrative procedure, on document digitizing, and on privacy.

Privacy issues are especially important when dealing as with relatives who mediate between the care-for and the service provider; this raises an issue with regard (a) choosing of service, (b) timing the service request, and (c) expressing the options set forth in the Italian Code on Privacy. In fact the service request is fragmented over time and so is difficult to satisfy, for it rarely seems to coincide with the formal acceptance process. Administrative procedure thus becomes more difficult to make transparent for citizens looking to find out how long a procedure will take or having to revoke a service request or access the documents pertaining to the procedure.[11]

Especially critical – when it comes to justifying a request for service revocation or for access to documents – is the fragmented situation that one faces having to deal with paper documents stored in separate archives and in separate offices run by different people. This makes it difficult to find the person in charge of the process and capable of carrying it through.

In the effort to achieve a seamless flow of document exchange (in keeping with BPR guidelines) a difficulty comes up owing to the

11 There is a rough division of responsibilities in Italy's institutional setting, with social services being handled mainly by municipalities and medical services by Local Health Centres. Framework Law 328/2000 calls instead for a unified service more responsive to the needs of recipients. A program based on this idea has thus been set up called ADI (Assistenza Domiciliare Integrata, or 'integrated at-home care'), a set of social, health, nursing, and rehabilitation services delivered at home in keeping with minimum standards for integrated service and with individual service plans drawn up with the help of professionals familiar with the case at hand. The general practitioner plays a central role in providing at-home care for the elderly and the disabled and is competent to take decisions for treatment both at home and in the hospital as well as to carry out and evaluate the individual treatment plan recommended by the Geriatrics Operational Unit.

fragmentation referred to, with the procedure broken up, and documents being scattered around and exchanged through different channels – sometimes in digital form other times in paper form – and communication taking place on an informal basis (over telephone or e-mail) and filing being carried out mainly in paper form.

When health organizations or practitioners are involved, the problem becomes obtaining consent for processing of data, giving the relative privacy notice, naming the family members authorized to come into possession of the patient's health data, and communicating the patient's health data through the physician or other medical practitioner chosen by the patients themselves.

These operation must be carried out as soon as possible, so as to avoid processing of data without consent or without the mandatory privacy notice, as well as to prevent the same data from being communicated to unauthorized third parties.

In I-Care, it was decided to unify the different methods in use for placing a request (through a family member or hospital doctor or a general practitioner, or the patients): whatever method is used to place a service request, service recipients must themselves be formally present (if capable) when the request is made.

The patient's consent, the privacy notice, and any other request (e.g. selecting the doctor who will communicate health data and the persons to whom such data may be communicated) must happen when first making contact with a practitioner: this way all the information and choices made enter the procedure and information system from the start.

Before the BPR analysis, by contrast, these different requests and procedures could take place at any time, and especially did not have to be concurrent.

Therefore, the municipal official in charge of the process must now provide two forms: the privacy notice relating to data collected by the municipality itself and the informed consent for processing such data, so that this consent flows into the administrative process from the start.

Therefore, in agreement with the agencies involved, we prepared the necessary forms for adopting this experimental solution.

In the digitized document flow, the data-collection moment has been made to coincide with the service request that initiates the relative administrative procedure.

The single contact moment is clearly called for in the BPR analysis and consists in the service request made to the competent office (e.g. elderly care unit), at which point the administrative procedure enters its digitized ICT mode and must therefore be properly protocolled from this point onward; so, too, the service recipient's consent will be on the record for the outset, expressed once and for all (and digitally recorded) for the entire service period that follows, whatever form such service takes.

This integrated form of social and health system, with the municipality and the local health centre working together, is fully compliant with e-Government guidelines as state in Europe and Italy alike, which single out the public administration as the primary provider of service to the citizen, who will then have to turn to the front-office, receiving appropriate feed-back, without having to know the internal intricacies of back-office organization.

The automated protocolling of a service request, concurrently with the request itself, will make it possible for the citizen to find out when the procedure began and hence how long it will last. The citizen will therefore be able to find out whether a request has been rejected and therefore to inquire into the reason for such rejection, as he or she is entitled to do.

From a broader perspective, ICTs make it possible to ensure transparency in administrative procedure, a standard requiring that the citizen, and anyone legally empowered to protect the citizen's data, be able to access the procedure and view the relevant documents.

4 Conclusions

As we have seen, in order for service delivering through ICTs to be successful, there will have to be a preliminary step in which the service providing agencies rationalize and reengineer overall administrative workflow, so as to weed out redundant information and procedures.

Indeed, e-Government involves not only applying ICTs to the administrative function but also using them in a broader process by which to change the public administration relationship to the citizenry at large, not only by undergoing internal reorganization but also by improving the points of contact between the two sides of the exchange.

However the public sector clearly does not make as easy to reinvent services, activities and structures as is instead generally possible in the private sector.

The public organization's mission and activity must comply with a detailed legislative framework and is subject to management and supervision on the part of policy makers and oversight bodies.

It follows that while any reengineering of the public sector comes under legislative restriction, it may also advance initiatives and proposals for legislative change with a view to achieving administrative simplification.

Hence, understanding administrative organizations and working out solutions by which to improve it will involve not a mechanical carrying out of sequences of action but a close collaboration among analysts, legal practitioners, administrative staff, and all personnel working to deliver the service.

The I-Care project showed us that in setting up an e-Health system two key aspects must be taken into account, the first being a legal analysis and the second a BPR analysis capable of handle multiple factors and variables such as the specificity of the service delivered, the centrality of the citizen-as-patient in distinction to the multiple private and public agencies involved in delivering e-Services, the necessary role of the public administrations and of health organizations, the role of private enterprise and social cooperative, and the different ICT platform serving as a technological foundation for the services.

Key areas of that legislation are being rewritten in a continuing effort to keep pace with the changing environment that is shaping up with the information society, and health data has become a focus of attention, so much so that international and Community laws have set out a general prohibition against processing data suited to revealing a person's state of health, a prohibition subject only to exceptions framed

to allow national law to provide for adequate security measures and data access authentication.

In I-Care we addressed three questions in the regard of issue of the privacy of medical data:

— the question of the right to privacy. Here it was necessary to publish a legal notice setting out the responsibilities and obligations of those in charge of processing the data and obtaining the user's consent to go ahead with such processing. Because the project was designed for delivery of both medical and social services, we accordingly had to process two types of personal data – medical and nonmedical – and set up two standards, a double set of regulations according as the data to be processed is classified as medical (under the Italian Code on Privacy) or otherwise;

— the question of data-processing techniques. Here it was necessary to set out requirement for cryptography and digital signatures, along with the signer's responsibilities;

— the question of authenticating the system operators. Here we needed access codes and digital signatures for all documents needing to be underwritten for administrative purposes.

References

S. Dawes and L. Prefontaine, 'Delivering government services' (2003), *Communications of the ACM*, v. 46, n. 1.

K. Dean (ed.), *Connected Health* (Premium Publishing: London, 2003).

P. Di Giacomo and F. L. Ricci, 'Agent-based workflow processing for functional integration and process re-engineering in the healthcare domain', in *Proceedings AICA Congress 2005* (AICA: Milan, 2005).

M. Hammer, *The reengineering revolution* (Harper Collins: New York, 1995).

'I-Care project' in <http://www.regionedigitale.net/wem/erdigitale/pagine/res/paginaprogetti/Scheda_I%Care.pdf> (visited June 13, 2007).

'i2010, a European Information Society for growth and employment' in <ec.europa.eu/information_society/eeurope/i2010/index_en.htm> (visited June 11, 2007).

C. Maioli and C. Rabbito, 'Promoting e-Participation to qualify territorial e-Government policies', in S. Flogatis, U. Karpe and A. Masucci (eds.), *e-Government and e-Democracy* (Esperia: London, 2006).

C. Maioli, 'e-Governance for local systems', in K. Lenk and R. Traunmuller (eds.), *Electronic Government* (Springer: Berlin, 2002).

J. Monducci and G. Sartor (eds.), *The Italian Code on Privacy: systematic comments* (in Italian) (Cedam: Padua, 2004).

A. Rossi Mori and G. Freriks, 'A European Perspective on the Cultural and Political Context for Deploying the Electronic Health Record', in J. E. Demetriades et al. (eds.), *Person Centered Health Records* (Springer Science: New York, 2005).

THE RIGHT TO BE LEFT ALONE IN THE WORKPLACE. TENSIONS BETWEEN RIGHTS AND OBLIGATIONS

Ahti Saarenpää

1 The individual, privacy and data protection

The right to privacy – the right to be left alone – is a basic human right, one of the most important. In a democracy, privacy is closely linked to our right to self-determination, and this is the inevitable starting point even when speaking about our right to be left alone in the workplace. Everything that I have said above with regard to privacy essentially applies to privacy in the workplace as well. We do not leave our privacy at the office door or the factory gate, at least not all of it.

As a fundamental right, privacy cases belong in partice often to so called hard cases: it is hard to regulate and to realise. We do not always acknowledge – or want to – that privacy is a tumult of conflicting aims. Yet the right to privacy is always there to a certain extent: it does not vanish when we step into public service or into the public eye. At the end of the day, our private lives enjoy very strong protection. Everyone from the Prime Minister to the man or woman in the street should have a right to privacy – be it divided or indivisible.

> In Finland a woman who was dating the Prime Minister recently published a book about their relationship. This was no doubt contrary to good practice but, as one of the parties involved, she has the right to tell about her experiences. In contrast, in covering the story, the media may well have invaded the Prime Minister's privacy.[1]

---

1 At this writing – autumn of 2007 – court proceedings are pending to determine whether publication of the book violated the Primer Minister's right to privacy. Media

The right to personal data protection is also a basic human and fundamental right. Today, it is an important part of the protection of privacy. We can and should talk about the family of privacy. There are many different forms of privacy; it cannot be precisely defined. Privacy must always be viewed in relation to something else.[2] The recognition of the relevant relations is an everyday part of our juridical, legal life.

Ignorance and inexperience are the most common barriers to our coming to terms with data protection. People do not know what is right, and do not recognise what kind of legal regulations should be observed in a given case. The increasing complexity of technology has of course done nothing to reduce problems. In the words of Reijo Aarnio, the Finnish Data Ombudsman, what we are dealing with is a significant deficiency in social and legal skills.[3] Legal education has never really been able to address this shortcoming. And this is really a global problem.

Working life is an area fraught with particular tensions where the development and realisation of data protection are concerned. The idea that an employer has the right to control what is done in the workplace and how is hard to reconcile with the development of the rights of the individual in labour law, except in their traditional sense.

Today the same problems affect not only the processing of personal data but the protection of privacy in the workplace more generally. The increase in different forms of supervision is more than a mere technical consideration: all of them – from building access to the use of information networks – entail new legal challenges. What we see increasingly are measures infringing people's right to privacy that, in a constitutional state, must be set out in the law.

To our knowledge, Finland was the first country in the world to enact a separate law on privacy in working life. The first version of this

---

is all the time eager to say, that Prime Minister can not have a private life. I my self have an opposite opinion.

2 See my introductory article to this volume.

3 See also his article in this volume.

legislation came into force in 2001. A mere three years later, a new, extensively amended version of the law was passed. I will now briefly sketch the development of this legislation and take up the content of the present law and the practices accompanying it.[4]

I can of course only deal in passing with the important consideration that, in addition to having certain international elements, every law dealing with working life has very strong links via the legal culture to the labour market in the country where it is enacted and the particular history and functionality of that market.

2 Data protection and privacy in working life

Throughout the European history of data protection legislation, working life has been a problem in the implementation of personal data protection and privacy in the workplace. Finland made attempts to introduce data protection legislation back in the early 1970s, and representatives of labour market organisations were involved in the preparatory work. These preparations did not bear fruit, however, one of the key reasons being a complete difference of opinions between the labour market organisations about the goals and implementation of data protection. When this was combined with corresponding political differences of opinion, the legislation in Finland – when comparing it to Sweden – was delayed for more than ten years.

Finland's first data protection act – the Personal Data File Act – was a so called second-generation act from the 1980s;[5] it came into force in 1988. This act was a general act which could also be applied to data protection in working life. Labour market organisations were duly consulted when the law was being drafted.

---

4 When an act is the first of its kind, it can be described as a first-generation act in the field. Its importance from a comparative standpoint is greater than usual.

5 It is important to note that we can and should distinguish several generations in European data protection legislation. For a detailed treatment of this issue, see, e.g., Saarenpää, *Europa y la Protección de los Datos Personales, Revista Chilena de Derecho Informático*, no. 3, December 2003, p. 15.

After the EU Personal Data Directive was implemented in 1999, we thought that working life did not necessarily need data protection legislation of its own. Neither was the involvement of representatives from labour market organisations required in drafting the implementing act.[6] The situation changed rapidly, however. The Ministry of Labour was activated and, at its urging, work began to prepare a special act on privacy in the workplace. We had prepared the general act at the behest of the Ministry of Justice and the early drafting work had taken place under the auspices of that same ministry.

> Enacting legislation on privacy and data protection is not easy. Drafting such legislation requires special skills, as the Ministry of Labour found out when Parliament sent the first bill back for failing to meet its standards. Later on, in 2001, with all its deficiencies, the first act on Privacy in Working Life came into force, just three years before it was to be significant amended. The current act came into force in October 2004.

So why did we go down this road of passing a special act? As far as I know, there were many reasons having to do with politics and labour market policy, but this is insider information. To my understanding, there were three other realistic explanations.

Firstly, the current special act is more extensive than the Personal Data Act. Its key element is the processing of personal data, but it also covers other concerns, for example, the procedure involved in introducing and using different surveillance systems in the workplace. So, in many ways, it is also a special labour law act. There is a long history of cooperation between the state and the labour market organisations in drafting such legislation, and the Ministry of Labour did not want to abandon this tradition.

The second reason concerns the dramatic increase in the use of data networks and e-mail in the workplace since the end of the 1990s. In the preparation of the general act, these issues were only dealt with briefly.

---

6 I my self was a member of the committee appointed by the Ministry of Justice to draft the act implementing the Directive. The committee included experts who were representatives of labour market organisations.

We trusted in the power of an abstract general law. As e-mail in particular had been introduced in an unrestricted way, with no one anticipating the related legal problems and risks, the aim was to correct mistakes seen in practice by regulating its use through a more detailed act.

The third reason has to do with the development of different tests and testing methods. In particular, the proliferation of drug tests and the prospect of genetic testing have increased the need for legislation. We have already moved into the age of genome, and the issues involved are something other than the mere processing of personal data. Thus the name of the act – the Act on the Protection of Privacy in Working Life – was a most appropriate choice.

To my understanding, the main solutions to almost all the aforementioned questions can also be found in the Personal Data Act and its related regulations. At least with very minor amendments the matter could have been taken care of by a general law. In Finland, as I mentioned earlier, the labour market organisations have a long tradition in controlling the development of legislation in working life. This is how things are done in the digital operating environment of the Internet community. But as we have already seen, a lack of special skills in the field may cause problems. The path of data from its establishment to its archiving or destruction is difficult to monitor. And the legal problems connected to this path are sometimes difficult to understand.

Lest I give the wrong picture of the competence of the Finnish Ministry of Labour in the area of data protection, let me point out that when we were drafting the general law we did not pay enough attention to the need for special laws and for the drafting involved in them. We failed to realise that the enactment of special laws might well convey a different message than heretofore concerning the purpose of and need for data protection.

This seems to have happened in many cases. Where the protection of fundamental rights is the leading, pronounced aim of the Personal Data Act, many special laws and provisions consider the protection of personal data no more than a necessary evil. Such provisions are included because they have to be, but the issue is considered rather less

important and tends to be shadowed by the aims pursued in the specific area of the law in question.

I will now go on to look at the scope of application of the law on privacy in the workplace. This scope is – of course – particularly crucial in all data protection legislation.

3 Scope of the law

From a legislative point of view, acts can be divided into general and special. General acts are usually interpreted broadly, special acts more narrowly. However, this basic distinction can by no means be maintained as consistently or as often as one might like. The Act on the Protection of Privacy in Working Life[7] is at the same time both a general and a special act. This brings problems in practical interpretation, but then again, this is not always noticed. In practical legal life a special act is often thought to be more comprehensive than it actually is.

As a special act for the protection of personal data, the Finnish Act on the Protection of Privacy in Working Life is secondary in relation to the Personal Data Act. It is more specific and modifies the application of the Personal Data Act only in the particulars that are expressly enacted in the law.[8] While the new special act is comparatively concise factually and quantitatively – it has just 26 sections compared to the 51 of the Finnish Personal Data Act – the Personal Data Act is both in principle and in practice still the key piece of legislation for data protection. If people in the workplace try only to use the Act on the Protection of Privacy in Working Life, they will get an inadequate and perhaps flawed picture of what is correct.

An illustrative example of the relation between the general act and the special act is testing for alcohol in the workplace. As yet there are no

---

7 You can find the act in English in the Finnish official Data Bank FINLEX at the following address: <http://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf>.

8 The Personal Data Act is a general act. It is always applied when there is no provision elsewhere in the law governing the matter at issue. At this writing, Finland does not have any legislation that would wholly supersede the Personal Data Act.

provisions for this in the Act on the Protection of Privacy in Working Life. As alcohol testing means invading a person's privacy and processing information related to it, in the light of the Constitution and the Personal Data Act testing is not permitted without the consent of the employee or the operation of some special legal rule. On their own, the management and supervision rights of the employer do not provide the right to make test, contrary to what employers have often thought.

> An insightful example in Finland was the case where the headmaster of a school took a teacher who had dropped by the school while on sick leave to the local health-care centre to be tested for alcohol. The Parliamentary Ombudsman issued a reprimand to the headmaster and the doctor for invading the teacher's privacy.

Then again, the Act on the Protection of Privacy in Working Life is also a general act. Firstly, it concerns the whole of working life, both the private and the public sector. Secondly, its influence even extends to job applications. It could not be any other way: information about job applicants is valuable to the labour market.

But general acts are often limited and the Act on the Protection of Privacy in Working Life is no exception. The crux of the matter is privacy in working life. Other legislation contains a significant number of regulations influencing the processing of individual employees' personal data, either directly or indirectly. An example of this is the question of employees' salaries.

> According to the Personal Data Directive, salary information is already a matter of privacy. Salary data is personal data. With reference to the principles of Nordic openness, however, Finland has legislated differently, whereby information on the salaries of all public sector employees and the bases for their salaries are in the public domain. This matter is regulated in the Act on Personal Files. It separately defines data gathered about public sector employees and its processing. As a special law, the Act on Personal Files disregards the Act on the Protection of Privacy in Working Life as far as matters such as salary information are concerned.

Furthermore, the privacy of salary information is restricted by the Act on the Public Disclosure and Confidentiality of Tax Information. According to this act, information on everybody's taxable income and

property ownership, including those working in the private sector, is in the public domain. This legislation, too, is based on the openness principle.

> In individual cases, the confidentiality of salary information can be denied on the basis of the Equality Act. When looking into possible cases of discrimination, the salary information of individual persons can be compared to that of others. The principle at work here is maintaining a balance of information.

4 Key content of the Act on the Protection of Privacy in Working Life

The general aim of the act is the protection of basic rights concerning privacy. The method of regulation is borrowed directly from the Personal Data Act. Attention is paid to the definition of basic, fundamental rights.

> Section 1 – Purpose of the Act
> The purpose of this Act is to promote the protection of privacy and other basic rights safeguarding the protection of privacy in working life.

The European Personal Data Directive is more comprehensive. Its purpose is to protect all basic rights in the processing of personal data. By comparison, Finnish data protection legislation is, unfortunately, narrower, and can even be described as contrary to the Directive.

The law is enacted in four different categories, beginning with general requirements for the processing of personal data and ending with technical surveillance in the workplace. I shall now examine each of these categories briefly.

4.1 Requirements for the processing of personal data

The most basic starting point in the processing of all personal data – both in working life and elsewhere – is consent by the individual, that is, our own conscious consent. Our information belongs in principle to

us and to nobody else. The personal identity number, in those countries where it is used, is also part of one's identity. The government may create it for us, but we as citizens 'own' it.

When our data is processed in the workplace, even our consent is not enough. An employer may only ever process data required for the job. The legislator does not trust the employer. It is a question of regulation of the relationship between the weaker and the stronger.

The data must truly be necessary for the implementation of our rights, obligations and benefits. In principle our private life has nothing to do with our employer. That is why no exceptions can be made to the necessity requirement, even with the employee's consent. This is a crucial restriction on the rights of the employer but one that is very difficult to enforce. It has been a tradition, for example, in interviews and aptitude tests, to ask applicants about their private lives, and even rather extensively.

Moreover, as we usually decide about our data ourselves, it should also be primarily collected from us. Employment cannot survive on rumours and secret information sources. So generally our employer must obtain our consent in order to acquire our data from elsewhere. Exceptions are credit data and official public information, although even the use of such data must be reported to the employee or job applicant before it is used. There is an openness principle steering the accepted collection of personal data too.

As the law applies to job-seekers as well, searching on networks for information on applicants is prohibited without their express consent. This prohibition, which is impossible to enforce, has created a great deal of confusion in practice. But the idea is very clear. We have different identities. By collecting information from the Internet, an employer may see us in false light too.

Nowadays, the confidentiality of employees is felt to be more important than ever. On the other hand, we increasingly find ourselves in a risk society, where the reliability of staff is essential. To this end, the Act on Background Checks allows employers to have the police carry out background checks when, for example, recruiting personnel for critical

tasks relating to corporate secrets or information security. Similarly, screening is required to determine if those planning to work with children have a criminal background. In both cases, however, the starting point is the consent of the party involved. An employer may only request a background check based on the consent of the person involved, and those wanting to work with children must obtain an extract from the criminal register themselves.

> There are three kinds of background checks. The most limited kind are based on local police records. The more extensive ones are carried out by the Finnish Security Police. In addition to these are background checks conducted by the Defence Forces, which are drawn up by the Defence Staff.

The traditional bone of contention has been the processing of an employee's health records. According to the Personal Data Act, information relating to health is always sensitive information. Processing such information is more restricted than that of any other kind of personal data. In the workplace, however, such information is sometimes processed even more extensively than other types, because it is information on health, above all, that affects the payment and monitoring of sickness and other social benefits.

The processing of health data is guided by four important rules. Firstly, (1) the demand of necessity is emphasised in the content of the medical certificate. The need for the employer to receive information on health is limited to what it really needs to know. Unfortunately doctors in Finland do not always remember this themselves, when writing out the certificate. The second rule is that (2) when an employee gives his or her consent for the acquisition of data from elsewhere, for the sake of evidence, this consent must be in written form. Furthermore, (3) the workplace must expressly specify in advance the person or persons who have the right to process health data. Lastly, (4) the data must be stored separately from other personal data.

Typically, information on an employee's state of health is needed when he or she has been absent from work due to illness. In such cases it is important for the employer to know the reason for the absence with a sufficient degree of accuracy. The problem that comes up in practice is

whether the diagnosis also divulges other information about the employee or conditions in the workplace.

To avoid data and information security risks, the data may not under any circumstances be stored in any equipment connected to the Internet; and the same generally goes for other personal data. We can trace this principle to the data security regulations in the Personal Data Act. Due to the typically poor level of information security, connecting to an open information network is very risky indeed; unfortunately, in practice most computers, especially in offices, are connected to the Internet without high-quality security solutions.

4.2 Testing employees

Genetic tests are also connected to our health. Employers have no permission to request these. In fact, it is forbidden even to demand information on whether or not a person has undergone a genetic test. In many situations, answers to this question could tell almost as much as test results.

The reason for this kind of regulation is simple. Our genes are still very much a part of our privacy. This is one of the key elements of our self determination in modern democracy. At present the issue has been decided unequivocally in favour of the employee's privacy. Yet, it can be assumed that genetic testing will eventually have to be considered in at least some risk occupations. The prohibition against asking about testing is part of the respect for the human being under the law of personality.

Drug use is also basically a private matter, although the legality of it varies from country to country. But the risk of drug use is also a significant question in labour law. Therefore, drug tests have already become an important aspect of working life.[9]

Our right to integrity prevents the use of drug tests without legal justification. However, the Act on the Protection of Privacy in Working Life opens the way for limited drug testing. The starting point again is

9 An overview of drug regulation in different European countries can be found in the European Legal Database on Drugs – ELDD at <www.eldd.emcdda.europa.eu>.

simply that we have our rights. Demanding a drug test of an employee is an exception to the general rule. It requires risk analysis. Typical factors that could justify testing are traffic safety, environmental safety and other threats to employee safety. In such cases, the employer must also report the requirement of a drug test as part of the application procedure.

The employer can demand test results as one's employment continues. In such cases the permissibility of the testing has a three-stage process of consideration behind it. The general criterion is based on the suspicion of a person's drug dependency or an employee carrying out his or her responsibilities in the workplace under the influence of drugs. The second criterion for testing concerns the nature of the work. It must require special accuracy, reliability, independent judgement or quick reactions. The third criterion is an evaluation of the consequences. Not until the use of drugs seriously endangers individual safety, data security, the environment or, for example, corporate secrets does the employer have the right to demand a drug test of an employee during his or her employment.

> In 2005, many public offices and big companies decided to begin drug tests. The interest in random testing seems to be growing considerably. Any move towards testing requires that there be a substance abuse programme in each workplace. In practice the tests are governed by guidelines in the Government Decree on Drug Tests, which was enacted in 2005.

The most common types of test, however, are aptitude tests. In the job market, employers are looking for different skills and carrying out psychological and aptitude tests to identify the most promising applicants. Particularly in the Finnish public sector, aptitude tests have become something of a fad. For any higher-than-average posts, short-listed applicants are sent for testing.[10] The private sector – where this craze, shall we say, in fact began – has been quick to follow suit.

Aptitude tests are not obligatory. In connection with job applications and during employment, they can only be administered with the

10 For example, persons applying for senior judgeships are tested.

consent of the individual concerned. The law says nothing about the detrimental consequences for the applicant who refuses to take them.

An aptitude test in itself is not a negative thing. It is a way of indicating professional skill. What is problematic is how to perform the test, how to interpret it and what its credibility actually is. In practice, problems have sprung up in relation to all these issues. Because of this, an employer is legally obliged to ensure the quality of the tests and the competence of those who conduct them. Nowadays there are for example a large number of questions concerning the applicant's family and family life. These should not be allowed. But many test companies still continue the old tradition.

> In his decision, handed down in 2005, the Chancellor of Justice considered it improper to ask applicants for a nurse's position about the following: a) their background, family and hobbies (question 1); what their state of health is like (question 2); and what their expectations for the future are (question 3). Information on their health is relevant but it must be connected with their anticipated duties.

In Finland, the rules on testing have remained open in a peculiar way. According to the rules, the employee must receive a written test report free of charge, the aim being to avoid the creation and exploitation of confidential information. Yet, at the same time the law also allows the use of verbal information; i.e., the report can be given by word of mouth. It must be told to the employee, but the message might change en route…

4.3 Technical surveillance

The development of technology has enabled the use of different surveillance systems in the workplace and systems that can be adapted for different purposes. Some of these target employees directly or indirectly. Accordingly, the Act on the Protection of Privacy in Working Life defines technical surveillance as falling under what is know as the workplace co-operation procedure. Even if a company is too small for the legislation on the codetermination procedure to apply to it, its employees must be heard before the introduction of surveillance. In this

way, we can try to prevent clandestine surveillance, which has occurred in practice.

Only video surveillance is today regulated in any detail by law. Constant filming is one of the most blatant violations of our privacy, but is widely used. In this connection, it can be said that the Act on the Protection of Privacy in Working Life complements the spying and eavesdropping regulations in the penal code and demands openness and discretion in filming.

Video surveillance is restricted both in terms of location and with respect to individuals. Surveillance cannot be targeted at the working room, rest, toilet or other areas used by an individual employee. Moreover, it is important to observe that, as a general rule, no permission exists for the use of constant surveillance by camera of an individual employee unless it is essential for the employee's safety or the prevention of a significant act of theft. Furthermore, surveillance can be agreed on the initiative of the employee.

It is worth pointing out that video surveillance is also governed by the provisions of the criminal law on illicit viewing. Here the law says that fitting booths in stores, for example, are areas that fall within the privacy of the customer.[11]

As a basic rule, video recordings can only be used for the purpose for which they are made. But – and this is a 'but' derived from working life – it is also permitted to use them for termination of employment, proof of harassment or molestation and accident investigation. These are, however, extreme situations.

It should separately be noted that video surveillance is by no means an automatic solution when arranging surveillance. Before it is introduced, the employer must look into the possibilities for using other kinds of surveillance. Neither can recordings be kept and used permanently. As a general rule, they must be destroyed as soon as their use becomes unnecessary and, at the latest, within one year of being made, unless there is some unresolved matter for which they are needed.

---

11 It is worth pointing out that general data protection legislation also applies to video recordings. Our picture, figure and voice are personal data.

4.4 Employee's e-mail

In the transition to the network society, e-mail rapidly became a general tool in the workplace. Technically, its introduction was a great success. Employees were given personal e-mail addresses. Then again, from a legal point of view, its introduction was generally a dismal failure. That e-mail was a form of confidential communication was generally not obvious. Employers thought that they could monitor their employees' e-mail messages. Anarchy ruled.

The new act aims to specify the framework and the procedure, which, in extreme situations, allow an employer to search for and, as a last resort, to open an e-mail that has been received or sent by an employee. In Finland, the general rule is still the confidentiality of e-mail. E-mail in the employee's own name in the workplace information system is primarily under his or her control. It is a tool but a personal one.

In a normal working situation, the employer does not have the right to search for or open e-mail. An exception to this is where the employee is absent. Even then, certain quality requirements must first be set for the e-mail system. The search for and opening of mail is permitted only if the employee has had the chance to report his absence within the system or to transfer his or her mail to another person. Unless the employer has taken care of this in accordance with its duty of care, the messages must remain confidential. Here the aim is to develop an e-mail culture indirectly.

Even when the system meets the quality requirements, searching and opening are closely regulated. E-mails may not be freely scanned by the employer. They can only be searched for and opened when it is a question of e-mails arriving while the employee is absent or messages he or she has sent just before his absence began, or if the consent of the employee is not received within a reasonable time. And even then, it can only involve messages concerning tasks which the employee has handled independently, as deemed necessary by the employer. In other words, in Finland, as long as employees are performing their tasks adequately, an employer may not touch their e-mail.

Searching for and opening e-mail are completely different things. Searching means looking for e-mails, with the aid of the main user of the information system, that the employer deems necessary on the basis of the sender, recipient or subject. Opening them is only possible if no contact can be made with the external sender or recipient of the message.

The regulation of e-mail in the Act on the Protection of Privacy in Working Life only deals with the search for and possible opening of e-mail in the data system. Other aspects of the monitoring of e-mail traffic are mainly dealt with in the Act on the Protection of Privacy in Electronic Communications. E-mail addressed to an individual person is always confidential communication. Therefore, provision on screening junk mail, for example, are set out separately in the Act on the Protection of Privacy in Electronic Communications. The employer already has a far-reaching data security obligation in relation to its data system pursuant to the Personal Data Act.

> Of particular interest is a local court case dealing with the email of a former employee. The employer and employee had agreed that the employer could monitor any email traffic related to uncompleted projects. However, he had opened another email and, despite a request, failed to discontinue the employee's email address. The employer was sentenced for message interception (opening the email) and a data protection offence (keeping the email address active).

A striking contrast to the above is the case where the Ministry of Transport and Communications was drafting a bill in 2006 at the request of the Government that would have increased the employers' opportunities to monitor employees' communication. This was justified in terms of preserving trade secrets. Drafting was discontinued when the Chancellor of Justice intervened, emphasising the importance of basic rights. Nevertheless, a bill to essentially the same effect will be brought before Parliament at the end of 2007.[12]

---

12 The bill has generated a great deal of debate and experts consider it damaging to Finland's reputation as the country with the most advanced legislation on privacy in the workplace.

4.5 Procedures in the workplace

Unlike many other countries, Finland has not had a regional or workplace-specific data protection ombudsman. The Act on the Protection of Privacy in Working Life brought an essential change in this in its first version in 2001. Together with the national Data Protection Ombudsman, the occupational safety authorities started to monitor the implementation of data protection in the workplace. As the occupational safety officer elected by the employees in the workplace is an important part of the monitoring of data protection, a new level of workplace-oriented data protection monitoring was actually created.

The law separately regulates codetermination procedures in relation to technical surveillance. The starting point is that, apart from knowing about surveillance, employees must also be able to express their opinions about its introduction in advance.

5 Conclusion

In a modern European constitutional state, our right to self-determination is stronger than ever. The strengthening of our privacy is linked to this. Correspondingly, in one way or other, those who encroach upon our privacy by supervising us or processing our personal data have to choose the least invasive means. This is also a principal rule in the organisation of privacy in working life. Employment takes place under the direction and monitoring of the employer but with due respect for the privacy of the employee.

As the workplace increasingly becomes to a digital operating environment, the fact that data processing is no longer merely an aid to office automation has generally gone unnoticed. Each time that we process personal data, at the same time it is a question of processing basic rights. In the light of both the European Convention on Human Rights and the European Directive on Personal Data, this requires the judicial planning and legal assessment of data systems, including the relevant risk analysis.

Attention must also be paid to the demand for a balance of information between the employee and the employer. The data system must serve the exercise of the rights and obligations of both parties and the judicial study of procedures. In recent years, these have been the stumbling blocks and basic questions causing considerable expenditure for privacy and data protection in working life. In Finland, the legislative procedure for the Act on the Protection of Privacy in Working Life did not take sufficient account of this.

In the public sector, a new threat to proper development is being created by the development of administration. To a large extent, Europe has introduced what is called new public management. This targets such things as efficiency, rationality and, in many cases, outsourcing. These goals – especially outsourcing – endanger data security and, with it, the level of data protection.

The third basic problem for privacy in working life concerns the legal information connected with it. In Finland, we have already been able to see that informative material on the matter, particularly commentaries, has been published by labour market organisations and from a very one-sided perspective. The ideas easily differ from the general principles of protection of privacy and data protection, and in fact have very little in common with those principles at all.

One possibility to partially combat this problem is the wider introduction of codes of conduct. A well-formulated code of conduct as a commonly approved way of reading the law has proven to be a good legislative solution in the field of data protection, at least in Finland. We can feel that it is our own law!

Plans are currently in the works for including the Population Register offices among the authorities that must inform citizens about data protection. This might be favourable for employees, too.

DATA PROTECTION HERE AND NOW

Reijo Aarnio[1]

1 Tasks and status

In his 2002 study, which also corresponds to Finnish reality, the American professor Colin J. Bennet described a data protection ombudsman as being each of the following: 1) auditor, 2) inspector, 3) consultant, 4) educator, 5) policy adviser, 6) negotiator, 7) enforcer, and 8) international ambassador. I would also add acting as the head of an agency.[2] In a report published during the year under review, the National Research Institute of Legal Policy, OPTULA, studied data protection from the citizens' perspective.[3]

According to the study, the structure of Finnish data protection legislation conforms to the European model, which is characterised by a regulation strategy based on comprehensive general legislation and national data protection authorities, which monitor the implementation of the legislation. According to OPTULA, data protection regulation contains conflicting interests because it has to simultaneously cater for citizens' rights and also register controllers' interests.

Internationally, data protection legislation has expanded and the rights of data subjects have improved over the past few decades. The following

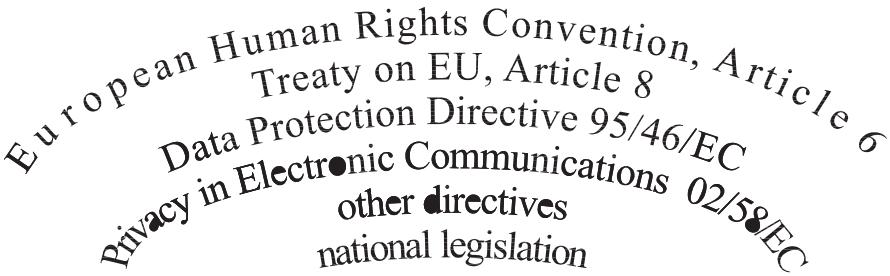
---

1 Mr. Aarnio is the Finish Data Protection Ombudsman (e-mail: <reijo.aarnio@om.fi>). The first parts of this paper are based on his annual report 2006.

2 See Colin J. Bennet (2002).

3 Vesa Muttilainen, National Research Institute of Legal Policy, *Finns and Data Protection*. Data based on Surveys and Statistical Data covering the 1990s and early 2000. Helsinki, 2006, no. 218.

figure describes the umbrella of data protection, although not exhaustively.



Now data protection is expanding also to cover the Pillar III.

Finnish data protection was also evaluated internationally. In the e-Protdat survey financed by the European Commission, Finland ranked third after Germany and Austria.

I will once again refer to OPTULA study. According to it, a relatively smaller proportion of Finns have doubts about the protection of their personal data than in the European Union in general. However, in Finland, the share of those expressing doubts has increased, whereas elsewhere in the EU it has remained the same. This development is naturally regrettable and register controllers should immediately respond to it by taking measures that increase confidence.

Approximately one in three Finns feels that they have had to disclose too much information to registers controlled by the authorities or various companies. As far as I can see, there can be at least two reasons for this: First of all, the data systems may be designed poorly and, thus, cause unnecessary actions or even costs to both data subjects and controllers. On the other hand, the results suggest a besetting sin so characteristic of Finns, namely that controllers do not openly state the reasons for collecting data (the right to be informed).

A third observation in the OPTULA study is that the number of cases referred by citizens to the Office of the Data Protection Ombudsman has doubled in ten years. According to our statistics, there is also a shift from cases concerning the authorities towards those involving the

private sector.[4] I believe the reason for this is that the public sector has more centralised supervision, strongly supported by legislation, that the processing of personal data is more clearly based on law or tasks arising from the law, that there is tighter official supervision, and, on the other hand, the business culture in the private sector has changed quite rapidly. Perhaps there is a touch of testing the boundaries. Both sectors still suffer from a shortage of know-how in data protection matters.

The OPTULA report also reveals that people's views of data protection vary relatively little between different demographic groups. I find this result pleasing because the protection of personal data is part of the Finnish and European system of civil rights and, as such, is generally acceptable.

While crimes violating people's data rights are slowly but steadily increasing so too are the detection rates of such crimes. Increased awareness, better protection systems that increase the risk of getting caught, and improved know-how among those who investigate crime probably explain this development.[5] Finally, the OPTULA report calls for more research on a more regular basis. It is easy for me to agree with this. I have stressed the need to include data protection in the national information society barometer.

2 International affairs

During its 19th year of our operation – 2006 – the Office of the Data Protection Ombudsman was kept particularly busy by international data protection issues. Finland held the EU Presidency during the latter half of the year. The term was associated with many other meetings, the largest and most prominent being the Asia–Europe Meeting (ASEM). The aftermath of the demonstration organised in connection with the

4 Simultaneously the human resources available to us have increased only a little bit.

5 During the year under review, the Finnish Prosecution Service and the Office of the Data Protection Ombudsman and co-operation partners organised education on the matter.

ASEM and the subsequent police operation is still being dealt with, by the police as well as by the Parliamentary Ombudsman and the Data Protection Ombudsman. My concern in the matter is that no data on those who were arrested that could later prevent them getting a job or a study place should be recorded without a justified cause (fundamental social rights).

The Finnish presidency saw many significant pan-European data protection matters being raised. Helped by the Commission, Finland led the negotiations on the new agreement on the transferral of airline passenger data to the authorities in the United States. The agreement will, at least temporarily, remove the legal uncertainty that airlines have had to face.

Even before this agreement, it became known that the SWIFT co-operative, which deals with international financial transactions, had been forced by US authorities to submit related data to the US. Based on an enquiry we made to the Finnish Bankers' Association, it seems that Finnish banks, and their customers, were not aware of this practice. The matter is still being examined.

The Finnish Presidency also saw the signing of the Eurojust agreement on judicial co-operation between the EU and the US.

EU action to fight terrorism and serious crime rests on four basic documents. The first is The Hague Programme, which follows the Tampere Programme begun during the previous Finnish Presidency of the EU, and which creates an umbrella for the co-operation. The second significant initiative is the Pillar III data protection principles based on the Commission proposal of 4 October 2005, which has just recently started to move forward. Furthermore, the proposal is still open on the accessibility principle, which would grant authorities from other countries access to Finnish databases. The fourth instrument that has been used is the Prüm Agreement, which Finland also signed and which has since become part of European law. I feel that the overall picture is alarmingly fragmented as each of the aforementioned instruments can lead to significant pressure to change our national legislation. On the other hand, it is necessary to urgently organise

comprehensive supervision of these forms of co-operation and of the processing of personal data across Europe.

The Commission also regularly assesses the functioning of the general Data Protection Directive. In this context, it has confirmed its commitment to the harmonisation of data protection and urged the Article 29 Data Protection Working Party to engage in closer co-operation.[6] As a result, the Working Party began preparing the first pan-European inspection, which targeted private companies offering voluntary social insurance. For Finland, the inspection went well. The London initiative accepted at the Privacy Conference in London also supports this pursuit.

As the ten new Member States joined the EU, they also signed the Schengen Convention. As a consequence, I participated in data protection inspections in five of the ten countries as a member of the inspection group and directed the inspection group in the five remaining countries. The land, air and sea border controls and data protection of all new Schengen Convention signatories are inspected. This emphasises the importance of data protection. Three Member States faced re-inspections as regards data protection.

3 Developments in Finland

During the year 2006, I participated in the work of the steering committee for the planning of a national information society strategy. The work, entitled Kiinailmiöstä Suomi-ilmiöön, aims at taking civil rights and data protection into account in our information society.

The Ministry of Transport and Communications commissioned the Helsinki Institute of Information Technology (HIIT) to write a report on the benefits, drawbacks, challenges and risks of the ubiquitous society. It was made clear that data protection and our right to privacy

6 The Commission also states that data protection does not pose a problem in the internal market and that self-regulation by register controllers should be supported (COM (2007) 87 final).

in particular will face major challenges. I am delighted that already at this point in the process data protection is being given the attention it deserves. Time will tell us to what the trend will be in this ubiquitous computing sector.

A beautiful example of well-functioning co-operation between the public and private sectors was provided by the third national Information Security Day in February. The main target groups of the day and its many events were schools and small and medium-sized enterprises. I think this choice was very successful, but I would also like to emphasise that data protection work and measures to increase public awareness must be continuous and as comprehensive as possible.

During the year under review, a proposal to amend the data protection law on electronic communications, prepared by labour market organisations, received wide attention. It would have given employers the right, at least to a certain extent, to monitor their employees' e-mail communications and even message contents. My view on the matter was that the primary need for protecting business and professional secrets should be implemented before the communication stage. After the Chancellor of Justice issued his statement, the matter was returned for further consideration. The ECHR decision of 3 April 2007 in Copeland vs. UK was carefully taken into account in this further consideration. Finland also expressed its provision on the bringing into force of the Data Retention Directive (2006/24/EC).

Parliament passed a bill on the reform of municipal and service structures. During the transition period, it will cause considerable changes in service production and their supportive data systems. Another major project is the health-care reform. The adoption of an electronic health-record system and electronic prescriptions and the role of the Social Insurance Institution of Finland, KELA, in the matter as a national body will probably clarify the situation and increase the transparency of the system. Challenges to data protection are great.

Various identification and online transaction services have constituted a separate group of problems. It has become apparent that the verification of customers by some mobile phone instant loan providers

has been deficient such that identity thefts have occurred. The Office of the Data Protection Ombudsman began to investigate the matter. It is probably partly due to this that some of the companies in the field have now drawn up ethical guidelines for the sector. Lively debate about the electronic transaction identity code created for and recorded in the population register system continued. Existing and potential actors in the field would like to gain access to the population register system's SATU code. These demands have been justified by the existing infrastructure, compatibility and general competition legislative aspects. The Population Register Centre, however, declined to make the SATU codes available because it deemed that legislation prescribes them to be used exclusively in the government's HST certificates. I felt that this debate needed a genuine risk analysis because I feel that it would be problematic to put all the eggs in one basket regarding this matter, especially since an estimated 25 per cent of the turnover of Finnish teleoperators is gained by foreign ownership. These companies are not always even based in EU countries. It is also problematic from the legislative perspective because the Data Protection Directive (95/46/EC) decrees that personal identification codes in general use should be regulated by data protection legislation. Liability issues and perhaps also the competition legislation aspect still need further investigation.

At the same time, electronic transaction codes are being replaced by biometric identification. The first experiences of the uses – and threats – of radio frequency technology and biometric identification are already in place. A law on biometric identification is being prepared and a committee on biobanks has also been established.

4 Social impact

The main mission of our office is to prevent rights violations related to data protection. According to our working hours monitoring system, we spend nowadays only about a fifth of our working hours on resolving actual practical complaints. The office can not be only working with different kind occasional complaints. We have sought to bring about an

effective social impact of modern data protection by integrating into different working groups, committees, etc.

5 What's next?

A great deal is evidently going on in data protection. Yet we also have to face the future. This is due to many things, such as the data life cycle management (storage and deletion times) required by law and the need for diligence and planning. How can we anticipate what is to come?

The government proposal concerning the Personal Data Act implemented back in 1987 commented on the quality of data (necessity requirement), shall I say, in a rather amusing way: 'When assessing the necessity requirement, the controller's own assessment must not be used as the only standard. The Bill is based on the idea that keeping a personal data file and the personal data entered into the file have to be justified as regards the management and operations of the controller and according to general standards. This means, for example, that the operation of the controller is compared with the practices adopted by other controllers with similar operations'.

This would sometimes be interpreted in such extreme ways that the competitors of the controller (a business owner) ended up defining the necessity of personal data management. Perhaps this now outmoded way of thinking sometimes led to data protection authorities being cautious about innovations. It is easier to be reserved than courageously speak out!

The implementation of the Data Protection Directive changed things dramatically. Today, national actors are controlled by the work done in the UN, OECD, Council of Europe, EU and other multinational organisations, the impact of which is often being realised at the national level as well. Furthermore, technology develops at a dizzying speed. The central idea regarding this is detailed in Item 2 of the recitals of the Directive: '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 wellbeing of individuals'. My interpretation is that there is an obligation in new situations to integrate data protection as part of the renewal of systems, services and processes. But when assessing the acceptability of a change, other factors besides data protection must also be accommodated. Parliament is the most important data protection authority.

The EU Commission was very straightforward when introducing its views on the transition from the Fifth Framework Programme to the Sixth. The Commission stated that data protection should be an active part of system planning, the basics of data protection should be made a basic element of business processes, new online data protection models must be developed, and business models must be reformed with data protection. I also wish to point out that the Commission recently stated that data protection principles as such have worked well and need no reform.

6 PIA (Privacy Impact Assessment)

I presented above Colin J. Bennet's definition of the various roles of data protection authorities. We work as auditors, educators, consultants, and so forth. The work can be hectic, and we always have to be prepared to comment quickly on new phenomena in the world. The public and the media are very interested in data protection.

This is a challenge to the Legal Framework for the Information Society (LEFIS): we need a tool to assess the impact of privacy protection. What could it be like?

The Maltese physician and philosopher Edward de Bono has developed 'a water logic model', where he urges us to ask the question: what does this (new thing, etc.) lead to? In his book *Six Thinking Hats*, he advices decision makers to review matters from six different angles: factual (a white thinking hat), emotional (a red hat), critical (a black hat), positive (a yellow hat) and creative (a green hat). The sixth angle is always to view matters from a helicopter perspective, to see the big picture (a blue hat).

Certain data protection principles can be placed in this conceptual framework. The white hat could represent the 'identify the phenomenon' thinking; in other words, identify the appropriate justification for personal data processing, which is not always easy. The red hat could be the relativity principle, the necessity requirement, while the black hat could stand for the analysis of legal risk and legality. The yellow hat would be Item 2 in the recitals I mentioned above, the integration of data protection as a positive success factor; and the green hat would be the requirement for carefulness and planning. Finally, the blue hat would stand for the entire data protection legislation as a set of norms. By this time at the very latest, we must assess the impact of substance legislation and matters such as rules of jurisdiction for authorities. Am I therefore making a circular argument by demanding a PIA tool while admitting that the current legislation already has this for the future?

As regards the operations of the data protection ombudsman, the law is the minimum level of law enforcement. According to a decision made by the Supreme Administrative Court, when considering sanctions, the data protection ombudsman must always be able to show where the controller is allegedly breaking the law. In such a case, the ever-changing, not-so-harmonised substance legislation is in a key position. As far as I know, a high level of data protection also creates added value to support the controller's operations. The Information Society Programme of the previous Finnish Government stated that the confidence of citizens and companies in the services of the information society is to be improved by enhancing data security and data protection. In other words, data protection is a positive success factor that must be integrated into the transient world. Furthermore, as it is generally understood that new technologies often include hidden functions and the application possibilities of technologies supporting data protection (PET technology) are not always identified, I still think that we need a PIA tool.

As it is, we are currently developing a PIA model, partly in cooperation with other authorities. At the start of the project, we collected information on currently-used models and used benchmarking because we can

learn a great deal from methods such as the Environmental Impact Assessment.

In the United States, PIA is defined as an analysis of how to collect, store, protect and deliver the data concerning identifiable people and how this process is managed to ensure that the owners and developers of the system consciously integrate data protection as a comprehensive part of the life cycle of the entire system. Similar definitions have come from Australia, Canada, Hong Kong and New Zealand. Is Europe lagging behind in this development?

However, it is my understanding that these models are not good enough, since they concentrate too much on the analysis of the present, and because we require something quite different to a tool for the analysis of mere legalities.

In our Finnish model, we regard data protection as part of the fundamental rights system, which is why we always have to assess data protection against certain other fundamental rights (e.g. property protection). Correspondingly, we bear in mind that every data system and service produced with it should be assessed from an ethical point of view; each one has an impact on our social relations, and even our security. Yet we also want to see data protection as a set of rights that extends further than the traditional concept of privacy.[7]

The cost efficiency of the new systems is quite a challenge. Of course, it is practical to use a method of single identification, but will it result in data accumulating in only one place, and customers possibly starting to use some other system? And is it acceptable to require fingerprint identification where a lock and key would be enough? Investments already made, and perhaps working against the relativity principle, may be wasted.

As data protection authorities we should also be innovative! Our customers often expect guidance and counselling instead of just a legal

7 As far as I know, nobody has so far been able to exhaustively define the concept of privacy. It is not included in the Finnish Personal Data Act, either.

assessment. Guiding them to use PET technologies is a good example of this.

Finally, an assessment of legal issues is, of course, always needed. This is why data protection authorities are often granted the power to make initiatives to change legislation.

CHAPTER 5
CRISIS MANAGEMENT

LIMITATION OF THE RIGHT TO ANONYMITY AS A PART OF THE RIGHT TO PRIVACY IN CYBERSPACE FOR THE SUPPRESSION OF TERRORISM IN THE REPUBLIC OF LITHUANIA

Rimantas Petrauskas and Kristina Spalveters[1]

1 Introduction

The right to anonymity[2] is not absolute and it does not include an absolute right to act anonymously in cyberspace. Article 22 of the Constitution of the Republic of Lithuania and part 2 of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms establish that under certain conditions this right can be limited. The Constitution specifies that information on private life can be collected only by a reasoned Court decision and only in accordance with the law.[3] The Convention for the Protection of Human Rights and Fundamental Freedoms establishes that public institutions have no

---

1 Prof. Dr. Rimantas Petrauskas and Ph.D. student Kristina Spalveters are working in the Mykolas Romeris University, Vilnius. E-mail: <rpetraus@mruni.lt> and: <kristina@lukrecija.lt>.

2 On a scientific level right to anonymity is determined as a dimention of privacy. Privacy determinates as an interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. Privacy has several dimensions one of these is information privacy: individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. Information privacy includes right to anonymity: the desire not to be identified.

3 Constitution of the Republic of Lithuania, *The State Gazette*, 1992, no. 31–953.

right to restrict this right, except for the cases specified by the laws and when it is necessary for the State and public security or economic welfare of the country; to prevent violations of public order or criminal offences; and when it is necessary for the protection of people's health or morality or other human rights and freedoms.[4] It is obvious that a precondition for the restriction of a person's right to anonymity in respect to public interest requires that a restriction of any type be proportionate to the legal purpose. The restriction of the right to the inviolability of private life should be based on certain principles formulated by the European Court of Human Rights in the cases Amann vs Switzerland, Armstrong vs UK, Khan vs UK and others:[5]

1) legitimacy clause to the effect that restrictions may only be imposed by a publicly declared and explicitly formulated law;
2) necessity clause to the effect that restrictions may only be imposed where these are necessary for the democratic society.

During the period of the spread of electronic means of communication, use of the Internet for organized crime, terrorist communications and organization of attacks, pursuit of the protection of a person's right to anonymity in cyberspace is restricted by the pursuit of the protection of public interests. Criminals try to justify their electronic communication through the protection of human rights; however, protection of the State and public security is the priority in this case. Therefore, protection of the right to remain absolutely anonymous in cyberspace becomes impossible.

The La Gomera Declaration adopted in 1995 states that terrorism is one of the major violations of democracy and superiority of law.[6] The European Security Strategy of 12 December 2003 names terrorism as one of the biggest threats of this century.

In the 21th century terrorism has become more and more dangerous to the safety of the World Community. The events of 11 September

---

4 The Convention for the Protection of Human Rights and Fundamental Freedoms, *The State Gazette*, 2000, no. 96–3016.

5 Internet address <http://www.echr.coe.int>.

6 EU Council Framework Decision on Combating Terrorism, 2002/475/TVR.

2001 in the United States, the terrorist act of 11 March 2004 in Madrid, and the attacks in July 2005 in London highlight one of the greatest challenges of today: How to ensure safety and prevent terrorism while at the same time respecting fundamental human rights and freedoms in strengthening democracy and the legal State.

2 Legal assessment of the suppression of terrorism

The phenomenon of terrorism has been known since the first century (a.d. 66–73), when the Jewish Zealot sect carried out attacks against the Romans in Judah. Members of this terrorist group acted in cities ruled by the Romans. They even murdered their compatriots – the Jews. Although terrorism started in the first century, theories about terrorism appeared only in the twentieth century.[7]

Until now the world has no general, unanimously recognized concept of terrorism. The European Convention on the Suppression of Terrorism of 27 January 1977 does not give a clear definition of terrorism. It simply defines traits and types of terrorist acts.[8] The European Parliament Recommendation on the Role of the European Union in Combating Terrorism of 5 September 2001 defines terrorism as any action executed by a single person or a group of persons who use violence or threaten to use violence against the State, its institutions, its citizens in general or certain persons, and who due to their separatist purposes, extreme ideological beliefs, religious fanaticism or pursuit of benefit seek to arouse fear among the authorities, certain persons, societal groups or in the society itself.[9]

The above-mentioned documents are not obligatory. They present only guidelines for the member states of the European Union in adopting

---

7 W. Laqueur, *Terrorism*, Boston: Little, Brown and Co., 1977. Franklin L. Ford, *Political Murder: From Tyrannicide to Terrorism*, Cambridge: Harvard University Press, 1985.

8 European Convention on the Suppression of Terrorism, *The State Gazette*, 1997, no. 7–116.

9 European Parliament Recommendation on the role of the European Union in combating terrorism 2001/2016 (INI), *Official Journal* C 72 E, 2002.

legal acts on the suppression of terrorism. The EU Anti-terrorism Action Plan highlights the objective to adopt a global definition of terrorism and Global Convention on International Terrorism.[10] However, the absence of a common definition of terrorism results in the situation where the fight against terrorism, as an undefined phenomenon, is used for illegal purposes and violates generally accepted human rights.

The Criminal Code of the Republic of Lithuania provides for criminal responsibility for terrorist acts[11] and provocation of terrorism.[12] Criminal offences listed in the Criminal Code are also defined in conventions ratified by the Republic of Lithuania, which specify principles of the suppression of terrorism.[13] Article 7 of the Criminal Code of the Republic of Lithuania establishes that individuals can be prosecuted for their criminal offences irrespective of their citizenship, place of residence, place of the crime, and regardless of whether a person should be punished for the crime according to the laws of the place of the crime, when responsibility for the committed crimes is provided for by international agreements.

The norm on a terrorist act defined in the Criminal Code of the Republic of Lithuania lists only criminal actions, however not always specifying when and where terrorism begins and ends: 1) explosives laid in dwelling, work or public areas with the intent to cause an explosion, explosion or fire-raising; 2) explosives laid in dwelling, work or public areas with the intent to cause an explosion, explosion or firing, if it

---

10 European Parliament Recommendation to the European Council and the Council on the EU Anti-terrorism Action Plan 2004/2214 (INI), *Official Journal* C 124 E, 2006.

11 Criminal Code of the Republic of Lithuania, Article 250, *The State Gazette*, 2000, no. 89–2741.

12 Criminal Code of the Republic of Lithuania, Article 250[1], *The State Gazette*, 2000, no. 89–2741.

13 European Convention on the Suppression of Terrorism of 27 January 1977, ratified by the Seimas of the Republic of Lithuania on 14 January 1999. International Convention for the Suppression of the Financing of Terrorism of 9 December 1999, ratified by the Seimas of the Republic of Lithuania on 3 December 2002. International Convention on Combating Terrorist Bombings of 15 December 1997, ratified by the Seimas of the Republic of Lithuania on 9 December 2003.

disturbed another person's health or destroyed or damaged a vehicle or a building or equipment that was in the building; 3) explosion, firing or other destruction or damage of a building or erection, if it caused danger to people's lives or health; or the spread of biological or chemical hazardous materials, preparations or micro-organisms; 4) explosion, firing or other destruction or damage of a building or erection, if it caused danger to people's lives or health; or the spread of biological or chemical hazardous materials, preparations or micro-organisms, if all this was directed against a strategic object or caused severe consequences; 5) initiation of an organized group of collaborates for execution of the above listed actions or participation in the activity of such groups, financing of such groups or material or other support to such groups; 6) formation of a terrorist group aimed at using the above-mentioned actions to frighten people or illegally demand the State, its institutions or international organizations to perform certain actions or to restrain from certain actions; or participation in the activity of such group, or material or other support to such group;[14] provocation of terrorist acts or other terrorist crimes or humiliation of the victims of terrorism through oral or written public announcements or via mass media.[15] Analysis of the above-mentioned norm allows the conclusion that actions, which cause danger to public safety and are equal to other crimes or criminal offences specified by the Criminal Code of the Republic of Lithuania, can be equated to terrorism.

When talking about restriction of the right to anonymity in cyberspace to prevent terrorism, the absence of a precise definition of terrorism and insufficient specification of terrorism as criminal action in the Criminal Code of the Republic of Lithuania impede implementation of a proportionate and fair restriction of the right to anonymity in cyberspace.

---

14 Criminal Code of the Republic of Lithuania, Article 250, *The State Gazette*, 2000, no. 89–2741.

15 Criminal Code of the Republic of Lithuania, Article 250[1], *The State Gazette*, 2000, no. 89–2741.

3 Restriction of the right to anonymity for the investigation of terrorism as a crime

Institutions of the European Union highlight the necessity to maintain balance when strengthening freedom, safety and justice so as not to violate fundamental values (human rights and freedoms of the citizens) and democracy principles of the European Union (principle of a legal State). They also stress that freedom should not be less important than safety and that protection of fundamental human rights is the most important value.[16]

European Union Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector requires that: 'Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. Listening, recording, collecting or other takeover and control of traffic data flows without the related user's consent is prohibited. They shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned'.[17] 'Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication'.[18] However, the right to anonymity may be restricted 'if such restriction constitutes a necessary, appropriate and proportionate

16 The European Union Agreement, summary edition, *Official Journal* C 321, 2006; The Hague Programme for strengthening freedom, security and justice in the European Union, *Official Journal* C 53/01, 2005; Opinion of the European Economic and Social Committee on the Communiqué to the Council and the European Parliament on The Hague Programme: ten priorities for the forthcoming five years, *Official Journal* C 65, 2006.

17 European Union Directive EC/58/2002 on the processing of personal data and privacy protection in electronic communication. EC/58/2002 [2002] OJ L. 201.

18 The same.

measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system'.[19]

In the context of terrorism preventing, competent institutions may restrict the right to private life by collecting and processing personal data for the purpose of State security[20] only if such collection and processing of personal data: 1) is regulated by appropriate legal acts; 2) is proportionate to the purpose of such collection and processing; 3) may be supervised by an independent outside institution.[21]

Means for the restriction of anonymity (overhearing using special devices, overhearing of telephone conversations, control of messages and employment of secret agents) used for terrorism prevention should be specified by the law.[22]

In the Council of the Europe's Convention on Cyber crime adopted in 2001,[23] in addition to ordinary procedures of cyberspace, such as search and seizure, new measures were introduced regarding operational retention of data, which should insure that ordinary measures for the collection of evidence were also effective in cyberspace. Ordinary procedures of the collection of evidence in

---

19 The same.

20 The right to anonymity can be restricted as well: many authors agree that guaranteed right to privacy guarantees the right to anonymity. The right to anonymity derives from the right to the privacy of information as an exceptional possibility to preserve personal data inaccessible to third parties. J. Cohan, 'A Right to Read Anonymously: A closer Look at Copyright Management in Cyberspace' (1996), *Conn. L. Rev.*, 98; J. Litman, 'Information Privacy, Information Property' (2000), *Stanford Law Review*, 1283.

21 Recommendation of the European Parliament to the European Leaders Council and the Council on the fight against terrorism: exchange of information and intelligence concerning terrorist offences, *Official Journal* C 124, 2006.

22 Recommendation to the European Leaders Council and the Council on the fight against terrorism: exchange of information and intelligence concerning terrorist offences 2005/2046(INI), *Official Journal* C 124 E, 2006.

23 Convention on Cybercrime, *The State Gazette*, 07-03-2004, no. 36–1188. Convention on Cybercrime of the Republic of Lithuania ratified on 07-03-2004 by Order on the Ratification of the Convention on Cybercrime, *The State Gazette*, 07-03-2004, no. 36–1178.

communications, such as collection of data flow in real time and takeover of data content, are applied in order to enable collection of data during the process of transfer of information.

Article 154 of the Criminal Code of the Republic of Lithuania provides for the possibility to control information transferred in cyberspace and record it for the purposes of pre-trial investigation.[24]

Following the Law on Operational Activities of the Republic of Lithuania, data on accomplished electronic communication necessary for operational investigation can be obtained by the subjects of operational activity from electronic communication operators and service providers only by a reasoned Court decision adopted on the basis of reasoned offerings of the authorities of the subjects of operational activity.[25] Law on Operational Activities of the Republic of Lithuania determines: 'Undertakings providing electronic communications networks and/or services must submit, in accordance with the procedure established by the law, to operational investigation services, pre-trial investigation institutions, prosecutors, courts or judges information which is available to them and which is necessary to prevent, investigate and detect criminal acts'.[26]

Law on Operational Activities of the Republic of Lithuania obliges electronic communications operators and service providers to ensure technical possibilities to exercise control over the content of information transmitted by electronic communications networks.[27]

Law on Electronic Communications of the Republic of Lithuania provides that: there is a reasoned court ruling, undertakings providing electronic communications networks and/or services must provide operational investigation services, in accordance with the procedure

---

24 Criminal Code of the Republic of Lithuania, *The State Gazette*, 2000, no. 89–2741.

25 Law on Operational Activities of the Republic of Lithuania, Article 10, part 12, *The State Gazette*, 2002, no. 65–2633.

26 Law on Electronic Communications of the Republic of Lithuania, Article 77, part 2, *The State Gazette*, 2004, no. 69–2382.

27 Law on Operational Activities of the Republic of Lithuania, Article 10, part 10, *The State Gazette*, 2002, no. 65–2633.

established by the law and pre-trial investigation institutions, in accordance with the procedure established by the Code of Criminal Procedure, with technical possibilities to exercise control over the content of information transmitted by electronic communications networks.[28]

The established restrictions limit a person's right to remain anonymous in cyberspace; collection of personal information, disclosure of personal identity seeking to disclose criminal offences is allowed.

Seeking to restrict the right to anonymity in cyberspace for the purpose of terrorism prevention, on 15 March 2006 the European Parliament and the Council adopted Directive 2006/24/EC 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 amended Directive 2002/58/EC,[29] the aim of which is to harmonize regulations of the member states on the obligations of the providers of electronic communications to retain certain data which they generate and process, and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crimes,[30] as defined by each Member State in its national law and to legalize restrictions of the right to anonymity in cyberspace.

The Directive expands possibilities for the collection of personal data for the purpose of the prevention and investigation of serious crimes. The Directive will make an important impact for the control of the past traffic data whereby the providers of electronic communications shall be obliged to gather and keep information about the traffic data stored from 6 months to 2 years from the moment it has been recorded for the benefit of law enforcement institutions. To this end, the practice shows that, seeking to ensure economic activities, providers of electronic

---

28 Law on Electronic Communications of the Republic of Lithuania, Article 77, part 3, *The State Gazette*, 2004, no. 69–2382.

29 The Republic of Lithuania postponed application of Directive 2006/24/EC to communication data related to Internet access, Internet telephones and electronic mail transferred via Internet until 15 September 2009.

30 Criminal Code of the Republic of Lithuania, Article 11, Article 250, *The State Gazette*, 2000, no. 89–2741.

communications services tend to store information about the traffic data for as long as a few months; therefore, the requirement to keep information for up to 2 years would mean that the information about private life would be stored for law enforcement purposes for a certain period without the permission of the court.

As it has already been mentioned, according to Article 22 of the Constitution of the Republic of Lithuania, information about private life can be collected subject to a reasoned decision of the court and only in case it is provided for in the law. The Constitutional Court of the Republic of Lithuania gave already its opinion regarding this issue. Therefore, such obligation to store information longer than it is necessary for the economic activities without a reasoned decision of the court can constitute a breach of the right to private life (rights to anonymity) and is, thus, inconsistent with the provisions of Article 22 of the Constitution. A legislator in Lithuania should estimate the impact of the Directive and its relation with the Constitution of the Republic of Lithuania and be prepared to carry out some actions (including legislative amendments), which would help to avoid the inconsistence between the provisions of the Directive and those of the Constitution of the Republic of Lithuania.

4 Conclusions

The defined measures for the collection of personal data and restriction of the right to anonymity in cyberspace aimed at the protection of the State and the society, in most cases – from terrorism as a major threat, may precondition unreasoned restriction of a person's right to anonymity. In the absence of the generally accepted notion of terrorism and clear distinction of terrorism from other criminal offences in the Criminal Code of the Republic of Lithuania, there is a threat that provisions of legal acts providing for the possibility to restrict a person's right to anonymity can be used by violating fundamental principles of democracy and protection of human rights.

The EU directive on the retention of communications can make a great impact on the period of retention of the traffic data administered by

providers of electronic communications services. The provisions of the Directive are possibly inconsistent with those of the Constitution of the Republic of Lithuanian as far as it concerns the requirement to store information about the traffic data longer than it is needed to ensure economical activities. Competent institutions should take all necessary measures to evaluate this possible inconsistence upon implementing the Directive.

List of references

Constitution of the Republic of Lithuania, *The State Gazette*, 1992, no. 31–953.

Convention for the Protection of Human Rights and Fundamental Freedoms, *The State Gazette*, 2000, no. 96–3016.

European Convention on the Suppression of Terrorism, *The State Gazette*, 1997, no. 7–116.

Convention on Cybercrime, *The State Gazette*, 07-03-2004, no. 36–1188.

The European Union Agreement, summary edition, *Official Journal* C 321, 2006.

European Union Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector. 2002/58/EC (2002), *Official Journal* L 201.

Directive 2006/24/EC 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. 2006/24/EC (2006), *Official Journal* L 105–54.

EU Council Framework Decision on Combating Terrorism, 2002/475/TVR, *Official Journal* L 164, 2002.

European Parliament Recommendation on the role of the European Union in combating terrorism 2001/2016 (INI), *Official Journal* C 72 E, 2002.

European Parliament Recommendation to the European Council and the Council on the EU Anti-terrorism Action Plan 2004/2214 (INI), *Official Journal* C 124 E, 2006.

The Hague Programme for strengthening freedom, security and justice in the European Union, *Official Journal* C 53/01, 2005; Opinion of the European Economic and Social Committee on the Communiqué to the Council and the European Parliament on The Hague Programme: ten priorities for the forthcoming five years, *Official Journal* C 65, 2006.

Criminal Code of the Republic of Lithuania, *The State Gazette*, 2000, no. 89–2741.

Law on Operational Activities of the Republic of Lithuania, *The State Gazette*, 2002, no. 65–2633.

Law on Electronic Communications of the Republic of Lithuania, *The State Gazette*, 2004, no. 69–2382.

J. Cohan, 'A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace' (1996), *Conn. L. Rev*, 98.

Franklin L. Ford, *Political Murder: From Tyrannicide to Terrorism* (Harvard University Press: Cambridge, 1985).

W. Laqueur, *Terrorism* (Little, Brown and Co.: Boston, 1977).

J. Litman, 'Information Privacy, Information Property' (2000), *Stanford Law Rev*, 1283.

NAME INDEX