arsboni

The right to privacy applied to problems of data protection

Laura GEIGER
Yevgeniya RYSINA
Sara SCOMBUSSOLO
Lilla SZAKÁCS

Tanulmány az ars boni jogi folyóiratból. arsboni.hu - 2012.

Laura GEIGER
Yevgeniya RYSINA
Sara SCOMBUSSOLO
Lilla SZAKÁCS

The right to privacy applied to problems of data protection

A tanulmány eredetileg a University of Luxembourg, Faculty of Law, Economics and Finance Master in European Law program keretében Dr. Stefan BRAUM (Institutions and Practice of European Criminal Law) konzulenshez készült a 2010/2011-es évben.

A tanulmány az ars boni jogi folyóiratban jelent meg, eredeti formájában szabadon terjeszthető és tudományos célra felhasználható.

Az ars boni jogi folyóirat a Stádium Intézet Alapítvány kiadványa.

Design: G. Szabó Dániel

facebook.com/arsboni • arsboni.hu • info@arsboni.hu

facebook.com/stadiumintezet • stadiumintezet.hu • info@stadiumintezet.hu

TARTALOMJEGYZÉK

INTRODUCTION

When did the concept of 'human rights' have birth? Certain popular quotations are well-known concerning the universal dimension of human rights, as for example: 'all men are born equally free and independent'[11], 'all men are created equal,... they are endowed by their Creator with certain unalienable Rights[22]'. In Europe: 'men are free and equal in rights', and this is a 'sacred and inalienable right[33]'.

Most probably, the declarations cited above are the heirs of European Enlightenment, belong to the intellectual development of Europe, from 'Locke' to 'Rousseau' and 'Kant'. Thus, Europe is the birthplace of the theory of human rights, but this theory remained long disregarded in its homeland.

It is only recently, since 1945 and even 1970, that protection of human rights has become an essential element in the legal systems of western European countries.

The first real source of protection of human rights is the '***European Convention on Human Rights***' (ECHR), which was intended by the authors to be the first embodiment in actual law of the Universal Declaration of Human Rights (1948)[4]4. The EConvHR (formally the 'Convention for the Protection of Human Rights and Fundamental Freedoms') was drafted in 1950 and entered into force on **3 September 1953**.

On 4 November 1950 was signed the European Convention on Human Rights which laid the 'foundations for the new Europe which they hoped to build on the ruins of a continent ravaged by a war of unparalleled atrocity'. Today, the success of this Convention is really apparent because it is the most developed and the best observed. The institution which supervises the Convention is the new European Court of Human Rights in Strasbourg (initially it was supervised by the European Commission and the Court of Human Rights).

The aim of the Convention is to **protect human rights** as well as **human dignity**. One of the rights protected by this 58 years old Convention is especially the right of every human being to **respect to privacy**.

EU institutions, as well as Non- EU institutions such as the UN, OECD (Organization for Economic Co-operation and Development), Berlin group (International Working Group on Data Protection in Telecommunication, formed at the initiative of the Berlin data protection commissioner) and the Council of Europe (intergovernmental institution headquarter in Strasbourg, which often works together with the EU institutions in a number of areas, including data protection).

Let's consider, in a first step, what were the origins of the concept of 'right to privacy', in what direction it evolved, and why its protection is of fundamental importance in today's modern era, where technology might represent a real danger for human privacy, especially in matters of data

1Virginia Declaration of Rights, June 1776
2Declaration of Independence of te United States of America, July 1776
3France, 1789
4Adopted and proclaimed by the General Assembly of the United States on December 10, 1948

protection. Then, in a second step, we'll analyze how these rights are protected in practice by the EU Member States and the European Courts.

I. FROM A RIGHT TO PRIVACY TO DATA PROTECTION

A. The concept of 'Right of Privacy'

Article 8 of the European Convention on Human Rights provides the legitimate right for everyone 'to respect for private and family life, his home and his correspondence', and (in Article 8(2)) that '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 rights and freedoms of others'.

The 1st paragraph is based on Article 12 of the Universal Declaration.

The 2nd paragraph nevertheless sets out the limitations that may exist to the right proclaimed in the 1st paragraph of the article. The different issues that may arise in relation to Article 8 are the four headings of privacy, family, life, home and correspondence. Today we will deal about the right to privacy regarding data protection.

a. *The origin of the concept of ‹right to privacy›*

i. *The original meaning and the evolution of the word ‹privacy›*

The English word 'privacy' comes from the Latin 'private', to deprive. The sense was very near of 'privation'. A 'private' person was 'deprived of official position or rank'. But in the 16th century, the word 'private' began to be used in a positive way: to denote a privilege, privileged access (private property) or privileged relations (private friends). It became associated with 'independence, exclusivity, intimacy'.

In the 18th and 19th century the word 'privacy' approached the meaning of the todays protected right: it came to denote the value of a 'quiet life, the seclusion of the home, the comfort of family and friends'.

The right to privacy is legally protected in many national jurisdictions and it receives international legal protection as a human right.

The idea that privacy should be a legally protected right can be traced to the late 19th century United States and more precisely in an article by Louis Brandeis and Samuel Warren which title was 'The Right to Privacy'. The impetus for that article may be the unwelcome publicity at that time surrounding the wedding of celebrities.

The reason driving the right to privacy in this early period was 'the unauthorized observation and/or the unauthorized publication of images of powerful or famous people'7.

In these cases, the threat to privacy came from individuals, newspapers or other agents within society. But afterwards, privacy began to encompass an interest in protection from over intrusive state power: this served to democratize privacy to a degree that ordinary people were affected as well as powerful and privileged people.

In the late 20th and 21st century, a key preoccupation arised in relation with the concept of right to privacy: the impact of the so-called 'information-age'.

Thus, the right to privacy in international human rights law is the idea of protecting private life from unjustified interference. This concept of privacy is associated with independence, exclusivity, and intimacy.

ii. *The concept of private life*

Private life is a broad term and there has been no real attempt to define it comprehensively. 'An interference with privacy is not even like the elephant, of which it can be said it is at least easy to recognise if not to define'. In this case, a more comprehensive definition had been attempted: 'The privacy of a human being denotes at the same time the personal space in which the individual is free to be itself, and also the carapace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from intrusion. An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate'. It covers 'all aspects of a person's physical identity and thus freedom to live life as he or she chooses.

b. *T*he ECHR›s attempt to define the ‹right to privacy›

i. *The notion›s multiple definitions*

The Convention does not attempt the notion of privacy, which is very hard to do. The complexity of this notion can be indicated with the several definitions:

- 'Protection of the individual's physical and mental inviolability and a person's moral and intellectual freedom'
- 'Protection against attacks on a individual's honor or reputation and assimilated torts'
- 'Protection of an individual's name, identity or likeness against unauthorized use'
- 'Protection of the individual against being spied on, watched or harassed'
- 'Protection against disclosure of information covered by the duty of professional secrecy'

The Commission's definition was 'the right to live, as far as one wishes, protected from publicity' considered together with another part of definition: 'to a certain degree, the right to

establish and develop relationships with other human beings especially in the emotional field, for the development and fulfillment of one's own personality'.

ii. *The ECHR's 'definition' of right to privacy*

There's a clear interference in the right to respect for private life if an individual is kept under surveillance by the authorities: for example tap his telephone, control his activities, and investigate in his financial affairs. These are also interferences in the right to respect for the home and correspondence.

Let's take a look on some cases dealing with that concept:

The right to privacy (or the right to private life), is 'at the heart of individual freedom' and it's also the right to be free from arbitrary state interference.

Traditionally, the right to privacy represented the right to be let alone and the right to enjoy one's individual space. This includes: the right to enjoy one's property, being free from physical interference. This makes it possible to an individual to enjoy an individual and private existence within a state.

'Privacy' and 'private life' are very important to honor the 'social contract'. The right to privacy also implies one's right to make choices about one's life (free choice about medical treatment, who you marry, the right or not to die. It concerns also the fact to be free from inhuman or degrading treatment and thus protect a person's dignitiy.

It also implies the right to choose one's sexual orientation 'free from undue interference or proscription by the state'.

iii. *The ECHR's definition of right to privacy related to data protection*

Most important for the matters of this subject: The right to privacy is also the right to withhold, or access, personal information.

The right to privacy goes even further than protecting an individual's right to 'family life, home and correspondence'; the concept of 'privacy' also covers privacy issues relating to 'access to personal information'.

In a case such as 'Peck', the European Convention recognizes the right of privacy, in particular the individual's right to control information relating to his personal life or image. The ECHR has, according to this, recognized not only the 'necessity of not only regulating other's people access to information, but also of allowing the individual's to access such personal information'. Thus, in Gaskin v United Kingdom (mentioned already), the Court considered that ' a system that denied a person's access to information relating to his upbringing was an unnecessary restriction on the right to private life'.

European data protection law is also of fundamental importance for any company doing business in the global networked economy:

- the free flow of information has become the life blood of the world economy – any

restriction of this flow might have crucial implications for companies doing business internationally

- EU data protection regulation can have an effect on a company's success, Europe being one of the largest markets for goods and services

c. *Right to privacy and Democracy*

i. *The interdependence between the two concepts*

'Democracy assures participation, whereas rights protect dignity'. But Democracy and human rights are interdependent because 'true democracy isn't possible without the recognition and protection of individual dignity'.

So we can say that rights are the foundation of the 'modern democracy'. Human rights are equal for everyone regardless of distinctions of sex, race, wealth, hierarchy, and so on. Democracy makes it possible to guarantee such equality because the democratic system of government should have a control over those who 'exercise power'. Individual rights protect a person against the will of a majority, or when this majority trespasses on the rights of individuals. If an individual is in a weaker position than the state body or the official who violates her rights, this individual should be able to seek the state's help (in the guise of courts, police and prosecutors, etc) against abuses by state officials. The protection of rights requires a strong effective state divides in 'protective powers' , which should be accessible to individuals and minorities.

A very important instrument of Member States to protect such human rights is the Constitution. Let's see how the right to privacy concerning 'data protection' is protected by national Constitutions in the European Union.

ii. *The protection of the right to privacy by EU Member States*

Each state has the task to ensure that an individual's right to privacy or private life is protected by its national jurisdictions, because article 8 of the European Convention clearly provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. Article 8(2) continues saying that there 'there may be no interference with the exercise of those rights by a public authority, unless the restrictions are in accordance with law and necessary in a democratic society, for the purpose of achieving legitimate aims such as the prevention of disorder or crime or the protection of health or morals'.

In the area such as 'private life', there's an important scope for the balancing of the rights of society as a whole against the rights of the individual. In these cases, the national legal order which addresses this balance is needed if any interference is to be regarded as being necessary in a democratic society. There's an increasing volume of case law concerned with the positive obligations of the State.

Let's consider now how the provisions contained in the national Constitutions of the Member States of the EU try to protect the individual's right to privacy, in particular the context of data protection and why this protection has to be harmonized by the EU to allow a successful protection of individual's personal data.

Before explaining how personal data is protected by the Member States and the European Union, we have first to explain what the protection of personal data means and why instruments of the protection of privacy are today not more enough to protect also individual's personal data.

B. The right to privacy applied to personal data

In our society which is today based on computers and technology, information concerning individuals, called "personal data", is collected and used in many aspects of everyday life. This personal data is part of our private life and must be protected by the right to private life.

Personal data means "any data relating directly or indirectly to a living individual, such that it is possible and practical to ascertain the identity of the individual from the said data. The data must be represented in a recorded form and be capable of being reproduced". [5]

The legal definition of personal data can be found in section 2 of the Personal Data (Privacy) Ordinance: ""personal data" means any data—

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable;[6]

A similar definition is contained in the EU Data Protection Directive (95/46/EC): ""personal data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

This definition is a very broad but in principle, personal data covers any information that relates to an identifiable, living individual.

This information can include for example the name, identity card number, telephone number, address, sex, age, occupation, salary, nationality, photos and medical records of an individual. All this information is part of our daily life and especially our private life.

Today there are a numerous institutions and organizations collecting more and more information about individuals and by consequent use this personal data in many ways. We give information about ourselves in many situations of our daily life like for example when we register for a library card, sign up for a gym membership or open a bank account. In this way,

5 CLIC – Personal Data Privacy
6 Personal Data (Privacy) Ordinance 1995

our personal data circulates around more and more places and can be used for other purposes and shared with other people.

Because of the development in computer technology and new communication networks, such as Facebook and Twitter, personal data can cross borders so that it can also be used in other Member States of the EU and can not only be used by public authorities but also companies, professionals, clubs and associations.

First this data, as part of our private life, was protected through the right to privacy under article 8 of the European Convention on Human Rights which was adopted in 1950. This article concerns the respect for private and family life and provides that: "Everyone has the right to respect for his or her private and family life, home and correspondence." [7]

When this article was adopted technology was not as developed and the possibility of process of data was less common in daily life, so that the ECHR was enough to protect individual's data.

But today personal data is collected and exchanged more frequently and the protection of individual's data by the right to private life is not more enough and regulation on data transfers became necessary.

The adopted regulations have not been developed to protect us from data processing but to avoid unlawful and disproportionate data processing.

The loss of control over our personal data and the intrusion into our private life makes it necessary to develop regulations which protect citizens against unjustified collection, storage, use and dissemination of their personal details. [8] This includes the obligation to process data fairly and in a secure manner and to use personal data for explicit and legitimate purposes.

a. The need for a broader protection of personal data

i. *The larger scope of data protection*

The existing legislation concerning the right to privacy, especially article 8 of the ECHT, is today no longer enough to protect personal data. The right to private life does not necessary include all personal data and so there was the question if this legislation would be sufficient to protect our data.

Technology and data processing has moved on since the ECHR was written so that there is now an important processing of personal information through the internet which has become a considerable tool for processing personal data for commercial and public purposes. [9]

By consequence data protection has a broader aim then just to protect private life. The right to privacy outlined in article 8 of the ECHR refers mainly to the right to private and family life,

7 Cf. ECHR, article 8(1)
8 P.J. Hustinx, « Data protection in the European Union », Privacy and Informatie, 2005, No 2, p 62
9 EU data protection : the development of a new right of privacy in Europe

respect of private home and private correspondents. It is clear that the right of privacy is part of the protection of personal data but data protection is not limited to private issues.

Data protection is used not only to protect privacy and family life but also other fundamental rights and freedoms concerning the processing of information relating to individual's, such as the origin, political opinions, religious believes, his health or sexual life.

The difference between those two fundamental rights is also mentioned in Article 1 of the Convention 108 which considered for the first time the distinction between the right to privacy and the protection of personal data:

"The purpose of this Convention is to secure [...] for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). " [10]

Furthermore the protection of other fundamental rights by the protection of data is mentioned in the Convention's explanatory statement: "The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms. Moreover, it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit). It is in order to maintain a just balance between the different rights and interests of individuals that the convention sets out certain conditions or restrictions with regard to the processing of information. No other motives could justify the rules which the Contracting States undertake to apply in this field."

ii. *Data protection, another fundamental right beside the right to privacy. A constitutional approach to data protection*

The right to privacy, and the associated right of protection of personal data, is a general, fundamental right, recognized by law and directly enforceable. They have the same status as other fundamental rights such as freedom of expression or freedom of information. Furthermore they have a horizontal application which means that they are also applicable between private persons.

The fundamental rights, such as right to privacy and protection of personal data, recognized in the ECHR and the Charter on fundamental rights are considered as quasi- constitutional statutes and as "general principles of the Community law". [11] Article 6 of the Treaty on European Union states: "The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection on Human rights and fundamental freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law". [12]

10 Cf. Article 1 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

11 Fipr : Foundation for Information Policy research, UK Information Commissioner Study Project: Paper N°4 of 2004: the legal framework

12 Cf. Article 6 of the Treaty on European Union

Today with the Treaty of Lisbon data protection as a fundamental right becomes binding to all member States.

b. The history of data protection and the need of harmonization within the EU

Because the protection of data by the tool of the right to a private life, recognized by article 8 of the European Convention for the protection of human rights and fundamental freedoms, adopted in 1950, was not more enough in the light of new developments in the area of information technology and the internet there was a need in the European Union to adopt separate regulations which go beyond the restricted scope of the protection of private life.

As a consequence, in 1981 the Council of Europe adopted for the first time a separate Convention on Data protection dealing with data protection as a fundamental right of the citizens. This Convention also known as Convention 108 is named Convention for the Protection of Individuals with regard to automatic processing of personal data. [13]

This Convention did not directly confer rights to the EU citizens; it was only addressed to the Member States of the Council of Europe. Its main function was to encourage the Member States to establish data protection on national level but on the same time it allowed them to exclude some categories of data from the scope of this protection.[14]

i. *National legislations*

In some countries like Germany, France, Italy and the Netherlands, data protection has a constitutional basis and in others it is only indirectly protected by the constitution.[15] To give an example of the different national legislations I will confine me on the legislation of Luxemburg and its neighbor countries.

-Luxemburg's first personal data protection regulation was the Act concerning the use of Nominal Data in Computer Processing of 1979. The law regulates individually identifiable automated personal records in both public and private computer files. All databanks including personal data have to be authorized, and data subjects have the right to correct their personal data and correct them if inaccurate. The law also requires licensing of systems used for the processing of personal data. [16]

- In France there has been full protection of personal data since 1978 with the law Nr. 79-17 of 6 January 1978. [17]

13 Reinventing data protection? Serge Gutwirth, Yves Poulett, Paul de Hert, Cécile de Terwangne et Sjaak Nouwt

14 European data protection supervisor: public access to documents and data protection, European Communities, July 2005

15 Fipr : Foundation for Information Policy research, UK Information Commissioner Study Project: Paper N°4 of 2004: the legal framework

16 www.privacyinternational.org

17 Sensitive Data protection in the EU by Anne Cammilleri-Subrenat and Claire Levallois-Barth

- The first regulation concerning data protection in Germany was the "Telecommunications Act" (1996) and the "Information and Communications Services Act" (1997) "which protect the users of modern electronic media from the curiosity of network and service providers about their conduct and preferences". [18]

Then since 1970 the individual Länder have created their own data protection acts, which primarily set limits on the dealings of government offices with personal data. There has been a "Federal Data Protection Act" since 1978. It was amended for the first time in 1990 and for the second time in 2001. The purpose of this Act is to protect the individual against his right to privacy being impaired through the handling of his personal data. [19]

- In Belgium it was the law of December 8 1992 on the protection of privacy in relation to the processing of personal data which protects personal data. Its article 2 states that: "Any natural person shall be entitled to the protection of his fundamental rights and freedoms, in particular the protection of his privacy, with regard to the processing of personal data relating to him." [20]

ii. *The need of a common protection of personal data*

The flexibility offered to the different Member States, to adopt regulations concerning data protection, lead to the inconsistency between national regulatory systems and produced a different level of data protection in the Member States. Although national laws on data protection want to guarantee the same rights, some differences existed. These existing differences at the national level could create potential obstacles to the free flow of information in the European Community and produced a need of harmonization of the national provisions.

Additionally, there were some Member States which did not have laws on data protection.

The main purpose of the Europe Union was to develop a framework which on the one side prevents barriers to the free flow of personal data within the EU and on the other side to protect the individual's right of privacy and the process of their personal data. [21]

For these reasons, there was a need for action at European level, and this took the form of different directives and regulations.

In order to remove the obstacles to the free movement of data and to protect the fundamental rights of the citizens the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was developed to harmonize national provisions in this field. "In accordance with the 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".

18 www.goethe.de
19 FEDERAL DATA PROTECTION ACT of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)
20Cf. Article 2 of the law of December 8, 1992 on the protection on privacy in relation to the processing of personal data
21 Article 1 of the Directive 95/46/EC

As a result, the personal data of all citizens will have equivalent protection across the Union. This directive has been implemented into the law of all EU and EEA States. The directive has more effect then the Convention 108 because of the obligation of the Member States to implement the directive into national legislation.

In Luxemburg the directive has been implemented by the law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data. The new law goes even beyond the framework of the Directive by covering not only natural, but also moral, persons; it contains specific provisions on the processing of medical data by health services, the processing of personal data for surveillance purposes and in the workplace".[22]

In France it was the law 2004-801 of August 2004 modifying the law of 1978 relating to the Protection of Data Subjects as Regards the Processing of Personal Data which implemented the directive. In Germany the law of 1978 was modified by the federal data protection Act 2001 which implemented the directive in the German national legislation.

And finally in Belgium the Directive 95/46/EC was implemented through the law of 11 December 1998.

This directive was a first step of harmonization of data protection in the EU but today there exists still a lack of complete harmonization because the Member States have implemented this Directive in divergent and sometimes, contradictory ways.

In addition the EU Parliament and the Council adopted a separate Directive, Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector which is afterwards replaced by the Directive 2002/58 on privacy and electronic communication. These two directives deal with the protection of privacy in telecommunications and oblige the Member States to guarantee the confidentiality of communication through national regulations.

Another important regulation is adopted in 2001 by the EU Parliament and the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and in the free movement of such data.

At the constitutional level, the right to data protection is recognized by Article 8 in the Charter of Fundamental Rights of the European Union: "Protection of personal data:

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

With the treaty of Lisbon the EU Charter on Fundamental rights, with Article 8, became legally binding for the Member States when acting in the scope of EU law. Additionally article 16(1) TFEU (formerly Article 286 EC) proclaims that "everyone has the right to the protection of personal data concerning them".

22 Art. 7, 10, 11, Data Protection Act of 2002

c. Possible justifications to infringe into the protection of personal data

i. *The principles for a lawful collecting and processing of personal data*

Data protection means the right of a person to know which data concerning him or she is collected, how this data is used, and where his data is transmitted.[23] Any person or organization collecting, holding, processing or using personal data must comply with different principles established by law to protect individuals from unlawful and disproportionate use of their data.

First there is a principle of legitimacy. The process of personal data is only allowed if there are legitimate reasons to do so and if you have the consent of the person concerned. In all cases, the person concerned has to give his consent when his data is used by private persons, the government or companies. The concerned person has a right to exercise personal control which means that anyone who wants to process personal data must notify it to this person so that he can allow it or decide that certain data will not be processed.

The individual's consent for processing his or her personal data should be "a freely given specific and informed indication" of his or her wishes by which the individual signifies his or her agreement to this data processing. [24]

Then there is a principle of purpose. The use of personal data must be confined to a purpose which has been determined beforehand. "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes". [25]When personal data are collected from an individual that person must be informed of the purpose for which the data are to be used and the collection is only allowed in relation with this purpose.

Another principle is the principle of necessity and proportionality. Personal data may be processed only insofar as it is "adequate, relevant and not excessive in relation to the purposes for which they are processed". [26]The processing of data must be in direct connection with the initial purpose. Furthermore this processing must be necessary and not excessive in relation to the purpose pursued.

Finally there is a principle of transparency which is necessary to ensure effective protection of personal data.[27] This principle means that individuals must be well and clearly informed, in a transparency way, about how and by whom their data are collected and processed, for what reason and for how long their data are collected. Additionally every person as a data subject has the right to access, to rectify and to delete his own data.

If these principles have been respected by the person or organization processing once data, this processing is considered as lawful and can produce its effects.

23 EU date protection : the development of a new right of privacy in Europe
24 Cf. Article 2(h) of Directive 95/46/EC
25 Data protection act 1998, Schedule 1: the data protection principles
26 Id. 20
27 European Commission : Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Region, Brussels, 4.11.2010

ii. *The different rights concerning data protection and the right of informational self-determination*

Beside these principles of lawful processing and storage of personal data there exists also a right of the individuals to have control over their own data. Everybody has the right to use his data, to modify it and to rectify it. Article 8(2) of the Charter on fundamental rights state that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".[28] Everyone has the right to access, rectify, delete and block data concerning him or her. The individual has to be informed about the collection of the data and the processing and has the right of access which means the right to know which information is collected.

Furthermore there is a more specific protection for sensitive data. The processing of sensitive data, which is data concerning racial or ethnic origin, religious believe, political opinion, health or sex life, is generally prohibited. [29]

Another meaning of data protection is the right of informational self-determination which is "the right of the individual to have a basic decision over the rendition and use of his personal data."[30] This principle has been developed by the decision of 15th December 1983 of the German Federal Constitutional Court, the so called "Volkszählungsurteil". This judgment had an important impact on the future decisions of the EU courts, such as the ECHR and the ECJ.

In 1983, the German federal government planned to conduct a general population census. This census was however refused by the German population because its fears that this statistic census will increase the surveillance and constitutes an unjust invasion of privacy.[31] For the peoples there existed a data protection risk because there was a risk that the data could be linked back to the individuals because of the numerous questions they had to answer.

These feelings led then to a public debate, and finally to a decision of the Bundesverfassungsgericht which decided that the Population Census Act was partly unconstitutional and that further procedural and organizational safeguards were necessary to protect citizens' fundamental rights.

The Court ruled that: "Who cannot certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situations knows about them.

[...] in the context of modern data processing, the protections of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German Constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal

28 Cf. Article 8(2) CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01)
29 Cf. Article 8 of directive 95/46/EC
30 www.dataprotection.eu
31 J. Taeger, *Die Volkszählung*, 1983

data. Limitations to this informational self-determination are allowed only in case of overriding public interest."

This decision contains 2 important elements: one the one side it creates an individual right of everyone to know which data of them is collected and processed. Looking at the big amount of data exchanged, it is important to know where our data is and to have the possibility to control this data. There must be an individual right to have power on your own data.

On the other side the Court held that there is not just an individual right but the right to self-determination constitutes a principle of democracy. This right has to be protected that democracy can exist. "If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom" and cannot take part in democracy. [32]

Later one this decision had an important impact both in Germany and abroad. The principle developed by the court appeared in the state data protection acts the following years, as well as in the General Amendment to the German Federal Data Protection Act of 1990. It also influenced the Austrian data protection act, as well as the Norwegian, Finnish and Dutch acts.

This principle of self-determination can be compared to the above mentioned principles concerning lawful storage and processing of personal data. The conditions of processing of data are the consent and the information of the individual which is concerned of it. This means that the individual must be involved in the process and must give his decision over the use of his personal data. This obligation has already been developed by the German Federal Court in its decision of 1983.

II. DATA PROTECTION IN PRACTICE

In the **first Chapter** we will see briefly the practical side of data protection and in the **second Chapter** the case-law relating to resolution of the problems of data protection.

A. The practical side of data protection (Lilla SZAKÁCS)

In the pages above we stated the connection between right to privacy and data protection, we discussed the 'birth' of data protection and we outlined the regulation connected to data protection and right to privacy, as well as we drafted the main problems of common protection of personal data and its harmonization.

This part describes the practical side of data protection. What would the European Union like to achieve in the field of data protection regarding technological developments? What are the challenges, changes and risks connected to data protection? What kind of technologies do exist nowadays? I try to answer these questions in the following pages.

32 Computer Law & Security Report, Volume 25, Issue 1, 2009

1. Changes and challenges in the field of data protection

„The undeniable fact that our lives are now becoming a continuous exchange of information, and that we live in a continuous stream of data, means that data protection is gaining importance and moving to the centre of the political and institutional system."[33] Data protection is a fluid and evermoving subject, individual's personal information can easily be stored and multiplied on the World Wide Web. In the Information Society new risks call for better legal and technical remedies.

Since in this 'electronic-based' society in a few minutes you can find, collect, computerize and store stranger's personal data for free and usually without the knowledge of the 'target' a new phenomenon has become frequent, namely the 'profiling'. Employers, banks, business companies, publicity agencies (for example: behavioural targeting/advertising) use more and more often profiling in order to present more personalized offers as part of their business strategy or to facilitate a decision about an individual. „Yahoo, AOL, Google and Microsoft, the big four on the worldwide web have already invested in advertising firms because they are convinced there is a lot of money to be made by tracking users' behaviour."[34] Google scans Gmail users' e-mail in order to offer them targeted advertising based on their personal e-mail correspondence. As the Commission stated: „the use of sophisticated tools allows economic operators to better target individuals thanks to the monitoring of their behaviour."[35] Obviously on the one hand these profiles can be very helpful and improve efficiency, however on the other hand they can also govern negative decisions about an individual's access to services such as credit or an employment position.

Individuals need to be able to maintain control over their data and keep their autonomy, but to achieve this goal they should be aware the possible threats and the different ways and methods to protect these personal information. Sometimes people can be careless with their own privacy or trade privacy for possible benefits. Millions of people are members of social networking sites, write their own blogs or twitter his every single moves across the globe. With the improvement of so-called 'Web 2.0', computer users have moved „from being recipients of mediated *content to being active producers of self-generated content*."[36]

As the Commission stated „to a large extent, the raw material for interactions in cyberspace is the personal data of individuals moving around in it when they purchase goods and services, establish or maintain contact with others or communicate their ideas on the world wide web. Alongside the benefits brought about by these developments, new risks also arise for the individual, such as identity theft, discriminatory profiling, continuous surveillance or fraud."[37]

33 European Union Agency for Fundamental Rights: Data Protection in the European Union: The role of National Data Protection Authorities - Strengthening the fundamental rights architecture in the EU II - 2010

34 http://www.business-standard.com/india/news/every-move-you-make-google-will-be-watching-you/57071/on

35 Communication from the Commission to the European Parliament, the Council, the Economic, and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union

36 Christopher Kuner: European Data Protection Law – Corporate Compliance and Regulation – Second Edition-2007

37 Communication from the Commission to the European Parliament and Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) - Brussels, 2.5.2007 – Introduction

The European Commission's Communication[38] identifies the main problems and challenges in the field of data protection in the European Union. One of these challenges is the so-called 'cloud computing'- „i.e., Internet-based computing whereby software, shared resources and information are on remote servers ('in the cloud')", this cloud computing can cause the loss of individuals' control over their personal data when they store their information with programs hosted on someone else's hardware. If cloud services located in different geographies, users' personal data travel across jurisdictions causing regulatory challenges.

The other problematic issue in this field is that the „ways of collecting personal data have become increasingly elaborated and less easily detectable." The Communication gave some examples for the better understanding of the difficulties: „... the growing use of procedures allowing automatic data collection, such as electronic transport ticketing, road toll collecting, or of geo-location devices make it easier to determine the location of individuals simply because they use a mobile device. Public authorities also use more and more personal data for various purposes, such as tracing individuals in the event of an outbreak of a communicable disease, for preventing and fighting terrorism and crime more effectively, to administer social security schemes or for taxation purposes, as part of their e-government applications etc."

In the fight against terrorism direct surveillance is a new technological weapon. The European Parliament stated some examples for direct surveillance. These are the followings: "Closed Circuit Television (CCTV), combined with face recognition software; motorway cameras that can read car licence plates and track selected cars; technologies to monitor, screen and analyse billions of telephone and email communications simultaneously, in real time; virtually undetectable "bugs" and tracing technologies."[39]

The phenomenon of global online insecurity is experienced first hand in the phenomenon of identity theft and forms of criminality associated with the misuse of personal information, personal identity codes and personal networks (from the theft of banking codes to more insidious forms of hacking, malicious spyware that 'seed' remote code execution programs and pre-installed key logging devices, and cyberstalking) „the electronic risk to privacy has moved on from the isolated attacks of 'lonely hackers' and the physical theft of credit cards to the world of organised criminal rings simultaneously attacking multiple networks from anonymous sites in cyberspace."[40] Nowadays people are more anxious about having their online identities compromised than they are of being mugged. „The current practices on electronic information networks undermine individuals' trust and threaten critical domains like mobility, healthcare, and the exercise of democracy."[41]

The Communication detailed the problematic issues as the followings[42]:

38 Communication from the Commission to the European Parliament, the Council, the Economic, and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union – page 2

39 http://www.europarl.europa.eu/parliament/expert/displayFtu.do?language=en&id=73&ftuId=FTU_4.12.8.html

40 Barry Sandywell: On the globalisation of crime: the Internet and new criminality – Handbook of internet crime

41 Privacy and Identity Management for Europe – White Paper – 18 July 2005 – PRIME project

42 Communication from the Commission to the European Parliament, the Council, the Economic, and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection

- *Addressing the impact of new technologies*
- *Enhancing the internal market dimension of data protection*
- *Addressing globalisation and improving international data transfers*
- *Providing a stronger institutional arrangement for the effective enforcement of data protection rules*
- *Improving the coherence of the data protection legal framework*

2. Need for technologies

a. Background

Public authorities /national and international as well/ and private sector organisations realize more and more that the most effective way to reach the aims of data protection and protection of privacy is via technological improvements. The Commission of the European Communities considered „that the use of appropriate **technological measures** is an **essential complement to legal means** and **should be an integral part** in any efforts to achieve a sufficient level of privacy protection."[43] As the Article 29 Data Protection Working Party and the Working Party on Police and Justice stated in its contribution „the idea of incorporating technological data protection safeguards in information and communication technologies (ICT) is not completely new."[44] Data Protection Directive[45] already contains several provisions which expressly call for data controllers to implement technology safeguards in the design and operation of ICT.

Article 17 (Security of processing) of Data Protection Directive :

„*Member States shall provide that* ***the controller must implement appropriate technical*** *and organizational* ***measures*** *to protect personal data against ... unlawful forms of processing."*

Recital 46 of Data Protection Directive 95/46/EC:

„*Whereas 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.****... particularly in order to maintain security and thereby to prevent any unauthorized processing"*

The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive[46].

in the European Union – page 3-4

43 Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC) Brussels, 15.5.2003 COM(2003) 265 final

44 Article 29 Data Protection Working Party – Working Party on Police and Justice – 02356/09/EN WP 168 The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data - Adopted on 01 December 2009

45 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

46 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the pro-

Article 14 (3) of ePrivacy Directive:

„*Where required,* ***measures may be adopted*** *to ensure that terminal equipment is constructed in a way that is compatible with the right of users* ***to protect and control the use of their personal data.***"

Recital 46 of ePrivacy Directive:

„*It may therefore be* ***necessary to adopt measures*** *requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected.*"

b. The appropriate technology - Privacy Enhancing Technologies

This appropriate technological measure is the so-called Privacy Enhancing Technologies (PETs), which is the production of Information and Communication Technologies (ICT).

Privacy-Enhancing Technologies *„is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."*[47]

„A further step to pursue the aim of the legal framework, whose objective is to minimise the processing of personal data and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult."[48]

The goal of PETs is complex. With using PETs individuals can increase their control over their personal information (enhancing their self-determination), minimise the amount of collected personal data, PETs is able to make more difficult to break data protection rules and in case of a breach to detect it more effectively.

Data protection authorities, business associations and consumer advocacy groups are in agreement that:

- the risks associated with the use of personal data in electronic form is recognised as serious and growing;
- consumer awareness of these risks is seen as low; and
- PETs are an effective means of protection against these risks.[49]

Some examples for existing PETs:

---

cessing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07. 2002

47 G.W. van Blarkom; J.J. Borking; J.G.E. Olk : Handbook of Privacy and Privacy-Enhancing Technologies -The case of Intelligent Software Agents – PISA Consortium - The Hague, 2003

48 Communication from the Commission to the European Parliament and Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) - Brussels, 2.5.2007 – Introduction

49 Study on the economic benefits of privacy enhancing technologies – page 14 http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

- Automatic anonymisation of data after a certain lapse of time
- Encryption tools- protect data transmission via Internet
- Cookie-cutters – blocking illegal cookies on user's PC
- Platform for Privacy Preferences – internet users can analyze the privacy policies of websites

3. Threats and risks regarding data protection

a. Privacy and identity management[50]

In everyday life most people use identity management without being completely conscious about it. Every human being has an identity, which distinguish this person from other people.

„An identity is any subset of attributes of a person which uniquely characterises this person within a set of persons."[51]

A possible subset of attributes (e.g.: name, appearance, hobbies, characteristic properties, financial status...etc.) forming an identity, but it's only a specific ***partial identity*** of this person, since no one (not even the person itself) can build up a complete view of all attributes of a person (*'complete identity'*). This partial identity does not necessarily identify a person, but only characterise him. For example the partial identity a superior knows of one of his employees is typically different from the partial identity known by the employee's wife.

The partial identities we are using when we interact with governmental authorities or the identities these governmental authorities assign to us called ***civil identities*** -e.g.: the combination of name and date of birth, or a passport or Social Security number. We use them to identify us for government facilities, such as a registry office, or for services of other organisations like a bank. Let's take an example about using of our passport/ID as an identifying and authenticating document. We can use it in different situations. In some countries, we must show our passport/ID at the hotel's check-in desk before we book a room. Or if we want to assure an officer, a salesman or just a bartender about our age the easiest way is to show our passport/ID. However in this case they only should know our age, we've already gave them much more personal data without recognising it.

Every single day when we interact with our environment, we leave different personal information (so-called *'data traces'*) that are noticeable by others. In order to protect our privacy, we should always be aware of disclosure of our personal data and then decide accordingly concerning its handling.

50 This part is written by using the Tutorials (General ~ and Advanced ~) of PRIME- Privacy and Identity Management for Europe - project (funded by the European Community's Sixth Framework Programme). https://www.prime-project.eu/

51 Privacy and Identity Management for Europe – General Public Tutorial

In the digital world, identifiably depends typically on addresses and other identifiers such as IP addresses, e-mail addresses and additional identifiers e.g.: cookies. Many Internet users believe that they act in an unidentifiable way over the Internet when they browse web sites. Unfortunately they don't know that their activities can be easily logged (according to their IP addresses) not just by the Internet access providers but also by many service providers (e.g.: online shopping). If we link these logged data with the data logged by the Internet access provider, we can link the activities on a website to the personal data of this user .

b. **Unlinkability and pseudonymity**

Most of us own a bonus/fidelity card (e.g.: IKEA card, Cactus card, dm card.....etc.) offered by chain stores, petrol stations or other service provider companies. However only a few of us are aware of the consequences concerning our personal data. We use these cards in the off-line world, but the collected information is processed and evaluated digitally, therefore these data transactions are unforgettable and combine the off-line and the online world as well. When a bonus/fidelity card is brought into action paying for goods, a series of personal data is transmitted (e.g.: the personal purchase pattern, a list of products bought, the address of the customer etc.) in order to get a detailed profile of the user (e.g. for user- specific advertisements).

„*Two sets of data (i.e., digital partial identities) are* ***unlinkable*** *if no one (with the possible exception of the person concerned) can relate them to each other by technical means."*[52]

In the digital world we have to identify ourselves to get access to a service (e.g.: digital communication systems, e-mail account, chat rooms; online shopping sites;...etc.). When we register ourself on websites, we should use different names or character strings as identifier instead of our real name to prevent that service providers link our personal data with other detailed personal information which we transmitted in different situations (e.g.: to buy a concert ticket online). These names are our nicknames or pseudonyms, which hide our real (complete) identity and make more difficult to discover who we really are (only what we do is known). **Pseudonyms** do not contain any personal data, so they realise unlinkability within the online world.

c. ***Privacy and data protection risks***

Identity is „the new money"[53]. Criminals in the twenty-first century look to identity as a new source of wealth. The advent of ICT provided a rich source of personal information to steal. „Owing to the often lax security measures present in organisations to protect electronic data, the theft of personal information by criminals is relatively easy."[54] There are two types of personal information at risk of misuse by identity criminals. First is the life history information such as a person's name, sex, age, address, and a variety of numbers used as identifiers when dealing with government agencies and businesses. Second is the financial information such as bank

52 PRIME project : General Public Tutorial
53 J. Crosby: Challenges and Opportunities in Identity Assurance – 2008, London: HM Treasury
54 Russell G. Smith: Identity theft and fraud – Handbook of Internet Crime - 2010

account names, numbers, commencement and expiry dates; secure numbers and passwords used to conduct secure electronic transactions. In addition, biometric data such as that obtained from fingerprint or facial scans, is a form of personal information that can be misused for the commission of identity crime.

Personal identification data can be obtained from a variety of sources including accidental data leakage from government or business networks, deliberate harvesting of data through the use of computer hacking or by gathering documents that contain personal information, or by social engineering in which individuals are persuaded or tricked into disclosing personal information to individuals for use in criminal activities.

In recent years, the use of electronic transactions has increased considerably and electronic payment systems are an increasingly important part of the retail and commercial sectors. In the past, identity thieves were required to counterfeit or alter cheques in order to commit financial transaction-based identity fraud. Nowadays, all that is required is the ability to gain access to a network using a stolen login and password and money can be transferred seamlessly and instantaneously.

Identity crime facilitated through the Internet is also beginning to be perpetrated through wireless communication systems such as third- and fourth-generation mobile phones PDAs with GSM/GPRS. Wireless networks create a number of risks regarding to identity crime. Of particular concern is the potential for users who have created an insecure, and unencrypted network to have their network used by nearby users within wireless range of the available computer. The most important problem with this so-called **'war-driving'** is that the 'war-driver' can easily get access to the personal data of the incautious wireless network users.

i. *Selected examples:*

Sniffing

When we transmit data over the Internet, our message is cut into small packets, so actually we send packets of data forwarded by multiple computers until it reaches its final destination, the computer addressed. „A sniffer is an application on one of the computers which listens to all packets on the network in order to log and analyse the traffic of these packets."[55] If we use encryption we can prevent sniffing by hiding our data.

Man-in-the-middle attacks

In this case an „attacker located between two communication partners, where he has complete control over the data traffic, i.e., he is able to read, insert and modify messages between the sender and the receiver. The attacker can manipulate the traffic between user and service or requests to or answers from the web service in order to gain something from either or both unsuspecting parties."[56] This attack can be prevented by using the encryption protocol SSL (secure socket layer), which provides end-to-end authentication and communications privacy over the Internet.

55 PRIME project : General Public Tutorial
56 Ibid

Identity theft by phishing

Identity theft may be implemented by hoax e-mails. Phishing is the fraudulent practice of sending emails to individuals that purport to come from a legitimate Internet retailer or financial service. The aim is to persuade the victim to voluntarily disclose data (e.g.: date of birth, bank account and credit card details...etc.) which can then be exploited to defraud the individual concerned.[57]

Identity theft by pharming

A pharming attacker redirects a website's visitors (especially in case of e-commerce or online banking) from the legitimate website (e.g.: amazon.com or e-Buy) to a faked one, a facsimile, where the victims will unknowingly surrender personal data (e.g.: account passwords, credit card numbers, bank details...etc.).

Identity theft by skimming

In case of skimming personal data are extracted from the magnetic stripe on credit cards. „The skimmer is a small device that scans a credit card and stored the information contained in the magnetic strip."[58] This crime can be committed during a legitimate transaction (e.g.: when you try to pay the bill in a restaurant with your credit card).

B. The case-law relating to data protection (Yevgeniya RYSINA)

As will be seen in this Chapter, both the European Court of Human Rights (Section 1) and the European Court of Justice (Section 2) have "constitutional approach" to data protection.

1. The principles established by the European Court of Human Rights

The European Court of Human Rights has recognized a number of important principles covering data protection (§§ 2-7). The main principle is that the interference with the right to respect for private life is prohibited (§ 1).

a. *General rule: prohibition of interference with the right to respect for private life within the meaning of the Article 8 ECHR*

In order to understand the meaning of the first principle, we will see briefly its scope (A) and exception (B).

57 Yvonne Jewkes and Majid Jar: Handbook of Internet Crime - 2010
58 http://www.investopedia.com/terms/s/skimming.asp

i. *Scope of the rule*

The Court of Strasbourg case-law relating to the data protection has developed very slowly. Generally, it is based on the Article 8 of the Convention. It should be noted that the Court has refused to protect personal data under Article 10 ECHR, which guarantees "freedom to receive and impart information"[59]. The **concept of "private life"** used by this Article 8 ECHR is **interpreted by the Court broadly**. This appears, for example, in the case ***Niemitz v. Germany*** of 16 December 1992[60], where the Court said: "it would be too restrictive to limit the notion (of private life) to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationship with other human beings".

In addition, the Court considers that the **term of "private life" covers a range of more particular interests**, such as the freedom of individuals to associate with others, the freedom to engage in sexual activities, the physical and moral integrity of the person[61] and protection of the human identity[62]. In general, all these interests are limited to natural person. Nonetheless, in *Niemietz v. Germany*, the ECtHR held that the relations in a business context could also be covered by the concept of "private life".

ii. *Exception to the rule*

The Article 8 ECHR is subject to an exception clause, which can be found in the **second paragraph** of the article. It explains that the **interference** with the rights protected by the first paragraph **can be justified if** the interference is **"in accordance with law"[63] and "necessary in a democratic society"** for the protection of important public interests or for the protection of the rights and freedoms of others. Thus, in ***Klass and Others v. Germany***, the Court of Strasbourg found no violation of Article 8 because the law challenged by the applicants was necessary in a democratic society in the interests of national security and for the prevention of crime[64].

59 See, ECtHR, *Leander v Sweden, Judgment of 26 March 1987, A-116;* ECtHR, *Gaskin v. the United Kingdom*, Judgment of 7 July 1989, A-160.

60 *ECtHR, Niemietz v. Germany, Judgment of 16 December 1992.*

61 *As for example, protection from sexual assault and corporal punishment.*

62 *See, to this extent, ECtHR, Pretty v. the United Kingdom, Judgment of 29 April 2002, § 61: "(…) Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (…). Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world. Though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees".*

63 *It may be noted that the ECtHR gives a particular importance to the quality of the law. For the Court, the phrase "in accordance with law" implies the existence of legal basis in domestic law and requires that legal basis be "accessible" and "foreseeable". "A rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct" (ECtHR, Malon v. the United Kingdom, Judgment of 2 August 1984, Series A no. 82, pp. 31-32, § 66).*

64 *ECtHR, Klass v. Germany, Judgment of 6 September 1978 (see, further, ECtHR, Leander v Sweden, Judgment of 26 March 1987; ECtHR, Segerstedt-Wiberg and Others v. Sweden, Judgment of 6 June 2006).*

b. *Decisions with regard to collecting, storing and use of personal information*

One of the most important applications of notion of "private life" is certainly in the matter concerning collecting, storing and use of personal data and files. However, in this area the jurisprudence has developed only slowly. The first case to be noted is ***X v. Federal Republic of Germany*** of 1973, where the European Commission of Human Rights stated that "the collecting and storing of information by the police did not, as such, conflict with Article 8 – even when the data subject had no criminal record[65]".

In ***Leander v. Sweden*** case, the ECtHR recognized for the **first time** that a **registering of personal information could interfere with a concept of "private life"**: "It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1"[66]. The next authoritative case is ***Rotaru v. Romania***[67], where the Court held that "both the storing of (the information on the applicant) and the use of it, which were coupled with a refusal to allow the applicant an opportunity to refute it, amounted to interference with his right to respect for his private life as guaranteed by Article 8 § 1". Another important case concerning access to data is ***Gaskin v. the United Kingdom*** of 7 July 1989. In this case, the applicant, who had been taken into care as a child, wished to find out about his past, but he was refused access to his file because it contained confidential information. The Court of Strasbourg held that it is contrary to the Article 8 ECHR because the decision following the denial of access to Mr Gaskin's had not been taken by an independent authority.

c. *Decisions concerning surveillance methods*

Another important matter covered by Article 8 is the use of the surveillance methods. The first case to be noted here is ***Peck v. the United Kingdom***[68] of 2003. In this case the Court found violation of Article 8 on account of the disclosure to the media of footage filmed in a public road by a closed-circuit television camera operated by UK local council, showing the applicant cutting his wrists.

Concerning the monitoring of an individual in a public place by the use of photographic equipment which does not record the visual data, according to the Court, it does not give rise to an interference with the applicant's private life[69]. But in ***Rotaru***[70] and ***Amann***[71] cases, the Court of Strasbourg held that the compilation of data on individuals made by security authorities, even without use of covert "surveillance methods", constituted an interference with the concept of

65 *X v Federal Republic of Germany, Appl. No. 5877/72, YB XVI (1973), p. 328, at 388 (see, also, X v Austria, Appl. No. 8170/78, YB XXIII(1979), p. 308, at. 320-322).*
66 Cf, § 48 of the Judgment.
67 ECtHR, *Rotaru v Romania*, Judgment of 4 Mai 2000, § 16.
68 ECtHR, *Peck v. the United Kingdom*, Judgment of 28 January 2003.
69 See, *Herbecq and Another v. Belgium*, appl. nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-A, p. 92.
70 Cf, §§ 43-44 of the Judgment.
71 Cf, §§ 65-67 of the Judgment.

"private life". While in ***P.G. and J.H.***[72] judgment, the recording of applicants' voices made when they answered questions in police cell, the recording of their voices in further was considered by the Court as the processing of personal data about them amounting to an interference with the term of "private life".

d. *Decision on obstacles to detainees' correspondence*

Frequently, the ECtHR ruled on obstacles to detainees' correspondence. Thus, in some polish cases[73], the Court stated that the practice of stamping "censored" on detainees' letters by domestic authorities, is in a breach of Article 8. But in the recent case ***Bista v. Poland*** of 12 January 2010, the Court of Strasbourg went on to admit that there now was a remedy in Poland for prisoner complaints of censorship of correspondence. Moreover, there are some decisions of the Court concerned **interception of correspondence**, as for example, the case ***Silver and Others v. the United Kingdom***[74]. Other decisions related to the **restrictions on correspondence with the Court**, as appears in ***Campbell v. the United Kingdom***[75], where the ECtHR found a violation of Article 8 on a ground of the opening of the applicant's correspondence with his lawyer and the Commission[76].

e. *Decisions in relation with surveillance of communication*

The case-law of the ECtHR concerning surveillance of communication includes telephone tapping (A) and installation of listening devices in a flat (B).

i. *Tapping and other forms of interception of telephone conversations*

The Court of Strasbourg recognized that "taping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a particularly precise "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"[77]. In the case ***Malone v. the United Kingdom***[78], the Court found a violation of Article 8 because the interception of the applicant's telephone conversations in the context of his trial for handling some stolen goods and registration of the numbers dialed on a

72 Cf, §§ 59-60 of the Judgment.
73 Cf, for example, ECtHR, *Matwiejczuk v. Poland*, Judgment of 2 December 2003.
74 ECtHR, *Silver and Others v. the United Kingdom*, Judgment of 25 Mars 1983.
75 ECtHR, *Campbell v. the United Kingdom*, Judgment of 25 Mars 1992 (see, also, ECtHR, *Cotlet v. Romania*, Judgment of 3 June 2003).
76 See, also, ECtHR, *Wisse v. France*, Judgment of 20 December 2005: concerning the system for **intercepting conversation** that was, according to the Court, in breach of Article 8, because French law did not indicate with sufficient clarity how the authorities were entitled to interfere in detainees' private lives.
77 *See, ECtHR, Kopp v. Switzerland, Judgment of 25 March 1998, § 72 and ECtHR, Amann v. Switzerland, Judgment of 16 February 2000, §§ 55-56.*
78 ECtHR, *Malone v. the United Kingdom, Judgment of 2 August 1984 (see, also, ECtHR, Khan v. the United Kingdom, Judgment of 12 Mai 2000).*

particular telephone, had not been in accordance with the law. Concerning the telephone tapping ordered by a judicial authority, ***Kruslin v. France***[79] of 1990 is the most authoritative example in this regard. Here, the Court considered that the Article 8 ECHR was in breach because French law did not indicate clearly the scope and manner of exercise of the authorities' discretion in this area.

ii. *Installation of listening devices in a flat*

According to the Court's established case-law, bugging of a flat is contrary to Article 8 of the Convention. Thus, in the case ***P.G. and J.H. v. the United Kingdom***[80] of 2001, the Court found a violation of Article 8 because of the police's installation of listening device at a flat used by one of the applicants, which was not in accordance with the law[81].

f. *Decisions relating to protection of medical data*

The Article 8 of the Convention also covers the protection of medical data. For example, the case ***Z. v. Finland***[82], concerned disclosure in court proceedings without the applicant's consent of his health records including his HIV status. Here, the Court held a violation of the Article 8 ECHR on account of the publication of the applicant's identity and medical condition in the judgment of the Court of Appeal. But in ***M. S. v. Sweden***[83] case, where medical record containing information about an abortion performed on the applicant was transmitted to a social-security body, the Court concluded that there was no violation of Article 8.

g. *Decisions on protection of personal data at the workplace*

The ECtHR considers also that it is very important to protect personal data at the workplace. The first example is ***Leander*** case[84], where the applicant had formerly been a member of the Communist Party and after using a secret police file in his recruitment, the commander-in-chief decided not to recruit him. Here, the Court of Strasbourg held that the safeguard contained in the personnel-control system satisfied the requirements of Article 8 and the Swedish Government had been entitled to consider that the interests of national security prevailed over the applicant's

79 ECtHR, *Kruslin v. France, Judgment of 24 April 1990 (see, further, Halford v. the United Kingdom, Judgment of 25 June 1997; ECtHR, Klass and Others v. Germany, Judgment of 6 September 1978; ECtHR, Wisse v. France, Judgment of 20 December 2005, ECtHR,).*

80 ECtHR, *P.G. and J.H. v. the United Kingdom, Judgment of 25 September 2001 (see, to this extent, ECtHR, Vetter v. France, Judgment of 31 Mai 2005).*

81 *See, also, the decisions concerning* **e-mails** *(ECtHR, Copland v. the United Kingdom, Judgment of 3 April 2007) and* **messages** *(ECtHR, Taylor-Sabori v. the United Kingdom, Judgment of 22 October 2002).*

82 ECtHR, *Z. v. Finland, Judgment of 25 February 1997. Similarly, in the case S. and Marper v. the United Kingdom of 4 December 2008, the Court considered that there was a violation of Article 8.*

83 *ECtHR, M.S. v. Sweden, Judgment of 27 August 1997.*

84 ECtHR, *Leander v. Sweden*, Judgment of 23 Mars 1987 (see, further, ECtHR, *Halford v. the United Kingdom*, Judgment of 25 June 1997; ECtHR, *Niemietz v. Germany*, Judgment of 16 December 1992: "There was no reason of principle why the notions of "private life should be taken to exclude professional or business activities, since it was in the course of their working lives that the majority of people had a significant opportunity of developing such relationship".

interests. The second example is the case ***Copland v. the United Kingdom*** of 2007[85]. In this case the Court went on to admit that the e-mails sent from work should be protected under Article 8, as should information derived from the monitoring of personal Internet usage.

2. The principles established by the European Court of Justice

The European Court of Justice (ECJ) has developed an effective legal framework for data protection. It controls the implementation of Directive 95/46/EC[86] in Member States[87]. As will be seen, a number of rules on data protection were established by the ECJ (§§ 2-3). But before discussing these, it is important to consider the substance and scope of data protection under Community law (§ 1).

a. *Substance and scope of data protection under Community law*

A number of judgments have been pronounced by ECJ on the scope of application of Data Protection Directive. Two most authoritative cases in this regard are ***Lindqvist***[88] (A) and ***Österreichischer Rundfunk***[89] (B), because they demonstrate that Directive 95/46/EC have a wide scope and should be applied as a general rule.

i. *Application of Directive 95/46/EC to using personal data on websites*

The case of ***Lindqvist v. Sweden***, makes it clear that **posting personal data on a website constitutes processing for the purposes of national data protection law**. In this case, a woman working for her church had published on the internet some information concerning an illness suffered by another voluntary worker, but she removed these data as soon as some objected. Mrs Lindqvist was charged with criminal violations of Swedish data protection law on following grounds: she had failed to notify the Swedish data protection authority in writing form, she had transferred personal data to third countries without any authorization and she had processed sensitive personal data on health. Before the ECJ, Mrs Lindqvist challenged the applicability of EC Framework Directive on data protection to information published on a website.

The ECJ answered that the principles of Directive of 1995 apply to using personal data on websites and that the act of referring, on an internet page, to various persons and identifying them by name or by other means[90], constituted the processing on "personal data" "wholly or partly by automatic means" within the meaning of Article 3 (1) of Directive[91]. The ECJ accepted that Mrs

85 ECtHR, *Copland v. the United Kingdom*, Judgment of 3 April 2007.
86 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 (EC Framework Directive on data protection).
87 See, for example, the ECJ judgment of 4 October 2001 in case C-450/00, *Commission v. Luxembourg*.
88 ECJ, *Bodil Lindqvist*, 6 November 2003, Case C-101/01.
89 ECJ, *Österreichischer Rundfunk v. Austria*, 20 May 2003, joined Cases C-465/00, C-138/01 and C 139/01.
90 i.e. their phone numbers, information about their hobbies.
91 Cf, § 24 of the Judgment.

Lindqvist activities were mainly charitable and religious and not economic, but held that these are not covered by the exceptions of Article 3 (2). Moreover, according to the Court, referring to the state of health of an individual amounts to processing of data concerning health within the meaning of Directive 95/46[92]. The Court said in addition that the principles of Directive are not contrary to the freedom of expression or other fundamental rights and that the national authorities must ensure a balance between the rights and interests in question[93]. The ECJ noted finally that the Directive lays down rules intended to allow Member States to monitor the transfer of personal data to third countries. The Court decided that EC law did not intend the expression "transfer of data to a third country" to cover the loading of data into an internet page, even if such data are thereby made accessible to persons in third countries[94].

ii. *Data processing in accordance with requirements of necessity and proportionality*

According to Articles 6 and 7 of Directive 95/46/EC, personal data must be processed fairly and lawfully, only so far as is necessary to pursue a lawful purpose. The principle underlying these requirements is the principle of proportionality. It requires that processing must be necessary and appropriate to the aim being pursued. This principle laid down in Article 8 (2) ECHR, was applied by ECJ in the case of ***Österreichischer Rundfunk v. Austria***, which concerned the obligation of public bodies to control by the Rechnungshof (Court of Auditors) to communicate details of the salaries and pensions exceeding a certain threshold, for the purpose of drawing un an annual report to be transmitted to the Nationalrat, the Bundesrat (the two houses of Parliament), the Landtage (provincial parliaments) and also made available to the public. Like several other organizations, Österreichischer Rundfunk (Austrian Radio) refused to disclose the information to Rechnungshof and argued that it would infringe the right to private life of the employees in question, i.e. contrary to Directive 95/46/EC and Article 8 ECHR. The Constitutional Court and the Supreme Court referred two questions to the Court of Justice: is the Austrian law compatible with Community law and if the provisions of Community law are directly applicable?

First of all, the ECJ held that inclusion of data on the salaries paid to individuals in the annual report constitutes the processing of personal data. Secondly, the Court considered that the **provisions of Directive**, "in so far as they **govern the procession of personal data liable to infringe fundamental freedoms**, in particular the right to privacy, **must necessarily be interpreted in the light of fundamental rights**, which (…) form an integral part of the general principles of law whose observance the Court ensures"[95]. Finally, the Court held that, EC Directive 95/46/EC must be interpreted in accordance with the right to private life as protected in Article 8 ECHR and that a breach of the right to privacy implies an unlawful processing in the sense of the Directive[96], i.e. no breach of privacy implies no breach of the Directive. From this, it can be concluded that for the Court of Justice, **personal data must be protected as privacy**[97].

92 Cf, § 50 of the Judgment.
93 Cf, § 90 of the Judgment.
94 Cf, §§ 68-70 of the Judgment.
95 Cf, § 68 of the Judgment.
96 Cf, § 91 of the Judgment.
97 See, ECJ, **Österreichischer Rundfunk v. Austria**, § 91 : « if national courts were to conclude that the national legislation with regard to the processing of personal data is incompatible with Article 8 of the Conven-

b. *Protection of personal data and foreign transfers*

The **scope of article 3 (2) of the Directive 95/46/EC** and the **rules on foreign transfers** - another matter which is of relevance to the present study. The most significant case in this regard is the ***PNR***[98] case, which concerned an action for annulment by European Parliament of Council Decision 2004/496/EC on conclusion of agreement between EU and USA on processing and transfer of Passenger Name Records (PNR) data and on adequacy decision on data transferred to USA. Both agreement and adequacy decision were adopted on the basis of Directive 95/46/CE. Concerning **adequacy decision**, the Court held that transfer of PNR data is processing which concerns public security. The Court noted that it falls within the first indent of Article 3 (2) of Directive, excluding from Directive's scope data protection in the course activities provides form by Titles V and VI of the EU Treaty. Therefore, the Court annulled decision on adequacy. Concerning **agreement**, the Court said that Article 95[99] in conjunction with Article 25 of the Directive[100], do not justify Community competence to conclude Agreement. The ECJ decided therefore that Council decision must be annulated.

c. *Privacy protection in the workplace*

The question if the personal data must be protected at work has been raised already by ECtHR[101]. At Community level, the question to what extent the data protection principles apply where personal information is in a public document subject to the Community rules on public access to documents provided in **Regulation 1049/2001/EC**. This appears in **Article 4 (1) (b)** of Regulation, which states that: "The institutions shall refuse access to a document where disclosure would undermine the protection of (…) (b) privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data". In ***European Commission v. The Bavarian Lager Co. Ltd***[102], the Court of Justice noted that this Article establishes a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public. The Court held also that list of names of participants in meeting is personal data, since persons can be identified and that communication of personal data in response to a request for access to documents constitutes processing.

III. CONCLUSION

THE WAY FORWARD – LILLA SZAKÁCS

tion, that legislation would also be "incapable of satisfying the requirement of proportionality in Articles 6 (1) (c) and 7 (c) or (e) of Directive 95/46".

98 ECJ, *Parliament v. Council and Commission (PNR)*, 30 Mai 2006, joined Cases C-317/04 and C-318/04.

99 On internal market.

100 On transfers to third countries ensuring adequacy.

101 See for example, *ECtHR, Niemietz v. Germany (cited above).*

102 ECJ, *European Commission v. The Bavarian Lager Co. Ltd*, 29 June 2010, Case C-28/08.

When all is said and done we can state that the sufficient and effective protection of individuals' data and privacy require the review of the current legislative arrangements for data protection in order to ensure citizens' control over their own personal information and the limitation of the data controllers' processing in relation to its purposes (data minimisation). Necessary arrangements have already started for the adoption of a new legal framework on data protection. In the followings I specify the major issues in order to outline how to carry on.

The European Data Protection Supervisor (EDPS) set out his opinion[103] for the future framework and drafted the most important driving forces such as:

- The **rights of individuals** (special focus on children's data protection) should be **strengthened**;
- The **responsibility of organisations** needs to be **reinforced**;
- The **inclusion of police and justice cooperation** in the legal framework is a *conditio sine qua non* for effective data protection in future;
- Further harmonisation - Data Protection Directive should be replaced by **a directly applicable regulation**;
- The new legal framework must be formulated in a **technologically neutral** way and must have the ambition to create **legal certainty** for a longer period;
- The enforcement powers of **data protection authorities** should be strengthened and their independence should be better guaranteed across the EU.

In this developing information society **new rights and principles** were born especially in the field of online world such as 'the right to be forgotten', data portability, the principle of accountability and 'the principle of privacy by design'. Since these instruments are strongly supported by the EDPS and their implementation into the new legal framework is presumptive according to the Communication on personal data protection in the EU we detail them a little bit more.

The right to be forgotten such as data portability enhances control over individuals' own data.

According to the Commission's Communication **'the right to be forgotten'** means „the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired." [104]

Data portability means that „providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that

103 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"

104 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union" – page 8

the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers."[105]

The **principle of accountability** means that „data controllers in the public or private sector should pro-actively include new tools in their business processes to ensure compliance with data protection."[106] This principle enhances data controllers' responsibility.

As its developer stated **Privacy by Design** (PbD) approach is „characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize…it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after."[107]

The Communication on personal data protection in the EU deals with 'the principle of privacy by design' as well as the role of Privacy Enhancing Technologies (PETs) within the aim of enhancing data controllers' responsibility. Both of these instruments ensures data security, but 'the principle of privacy by design' is not as evolved as the using of PETs. As the EDPS noted its opinion[108] "this concept is currently developed both for the private and public sector, and therefore must also play an important role in the context of EU internal security and the area of police and justice." He also suggested that there should be a legal obligation for builders and users of information systems to develop and use systems which are in accordance with the principle of 'Privacy by design'.

After development of the World Wide Web the right to privacy and data protection essentially and definitively has changed. In the beginning right to privacy was the only way to achieve the necessary level of data protection, however they soon realized this is far not enough, hence the creation of a legal framework on data protection has begun and it's still not finished. Our privacy is in risk everywhere and in every single moment. Social engineering, malwares, surveillance, eavesdropping…etc. These are just some examples on the challenges of data protection. Technology knows no boundaries, unfortunately legislation does. Our opinion is that the future of privacy and data protection cannot be assured solely by legal frameworks and their compliance. We must build an effective cooperation between the legal and the technological measures in order to prevent the breaches on individuals' privacy.

105 Ibid as footnote 100

106http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-01_Data_protection_reform_strategy_EN.pdf

107 http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

108 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council — 'EU Internal Security Strategy in Action: Five steps towards a more secure Europe' - (2011/C 101/02)

BIBLIOGRAPHY:

JOURNALS AND BOOKS:

J.G. Merrills, A.H. Robertson: Human Rights in Europe - Fourth edition

Paul Gordon Lauren: The Evolution of International Human Rights- Second edition

Philip Alston with Mara Bustelo and James Heenan (editors): The EU and Human Rights

Steve Foster: Human Rights and Civil Liberties- Questions & Answers

Wiktor Osiatynski: Human Rights and Their Limits

Gutwirth S.; Poullet Y.; De Hert P.; De Terwangne C.; Nouwt S.: Reinventing Data Protection ? - Milton Keynes UK- Springer- 2009.

Anne Cammilleri-Subrenat and Claire Levallois-Barth: Sensitive Data protection in the EU

Privacy and Informatie – 2005 - No 2

J. Taeger- Die Volkszählung- 1983

Computer Law & Security Report- Volume 25- Issue 1- 2009

Christopher Kuner: European Data Protection Law – Corporate Compliance and Regulation – Second Edition- 2007

G.W. van Blarkom; J.J. Borking; J.G.E. Olk : Handbook of Privacy and Privacy-Enhancing Technologies -The case of Intelligent Software Agents – PISA Consortium - The Hague, 2003

Yvonne Jewkes and Majid Jar: Handbook of Internet Crime - Willan Publishing – 2010

Ian Walden: Computer Crimes and Digital Investigations – Oxford Publishing- 2007

ARTICLES, STUDIES AND COMMUNICATIONS:

P.J. Hustinx: Data protection in the European Union

Fipr: Foundation for Information Policy research- UK Information Commissioner Study Project- Paper N°4 of 2004: the legal framework

EU data protection : The development of a new right of privacy in Europe

European data protection supervisor: Public access to documents and data protection- European Communities- July 2005

Article 29 Data Protection Working Party– Working Party on Police and Justice – 02356/09/EN WP 168 The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data - Adopted on 01 December 2009

Privacy and Identity Management for Europe- White Paper– 18 July 2005– PRIME project

European Union Agency for Fundamental Rights: Data Protection in the European Union: The role of National Data Protection Authorities- Strengthening the fundamental rights architecture in the EU II– 2010

Barry Sandywell: On the globalisation of crime: the Internet and new criminality

Study on the economic benefits of privacy enhancing technologies

J. Crosby: Challenges and Opportunities in Identity Assurance–2008- London: HM Treasury

Communication from the Commission to the European Parliament, the Council, the Economic, and Social Committee and the Committee of the Regions- A comprehensive approach on personal data protection in the European Union – Brussels, 4.10.2010

Communication from the Commission to the European Parliament and Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) - Brussels, 2.5.2007

Russell G. Smith: Identity theft and fraud -2010

Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC) Brussels, 15.5.2003 COM(2003) 265 final

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions- "A comprehensive approach on personal data protection in the European Union"

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council - 'EU Internal Security Strategy in Action: Five steps towards a more secure Europe' - 2011/C 101/02

CASE-LAW:

WEBSITES:

www.echr.coe.int

www.coe.int

www.ec.europa.eu

www.cnpd.public.lu

www.dataprotection.eu

www.privacyinternational.org

www.goethe.de

www.business-standard.com

www.europarl.europa.eu

www.prime-project.eu

www.investopedia.com

www.edps.europa.eu

www.ipc.on.ca

LEGAL TEXTS:

European Convention on Human Rights

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Treaty on European Union

Charter of fundamental rights of the European Union

Directive 95/46/EC

Federal data protection Act of December 20, 1990 (BGBl.I 1990 S.2954)

The protection on privacy in relation to the processing of personal data - December 8, 1992

Data Protection Act of 2002

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

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, 31.07. 2002

arsboni