The Eclipse of the Legality Principle in the European Union

The Eclipse of the Legality Principle in the European Union

Edited by

Leonard Besselink

Frans Pennings

Sacha Prechal

Wolters Kluwer
Law & Business

Published by:
Kluwer Law International
PO Box 316
2400 AH Alphen aan den Rijn
The Netherlands
Website: www.kluwerlaw.com

Sold and distributed in North, Central and South America by:
Aspen Publishers, Inc.
7201 McKinney Circle
Frederick, MD 21704
United States of America
Email: customer.serivce@aspenpublishers.com

Sold and distributed in all other countries by:
Turpin Distribution Services Ltd.
Stratton Business Park
Pegasus Drive, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom
Email: kluwerlaw@turpin-distribution.com

Printed on acid-free paper.

ISBN 978-90-411-3262-8

Printed in Great Britain.

Summary of Contents

List of Contributors

Leonard Besselink	Professor of European Constitutional Law at Utrecht University
Evelien Brouwer	Assistant Professor of Constitutional and Administrative Law at Utrecht University
Susanne Burri	Associate Professor of Gender and Law at Utrecht University, Europa Institute
Ton Duijkersloot	Assistant Professor in Administrative and Constitutional Law at Utrecht University
Hanneke van Eijken	PhD student in European Law at Utrecht University, Europa Institute
Lyana Francot-Timmermans	Assistant Professor of Legal Theory, Department of Legal Theory, Utrecht University
Teun Jaspers	Emeritus Professor of Labour Law and Social Security Law at Utrecht University, Europa Institute
Gerdy Jurgens	Professor of Administrative Law at Utrecht University
Saskia Lavrijssen	Associate Professor of Public Economic Law at Utrecht University, Europa Institute
Tony Marguery	Assistant professor of European Law, Utrecht University, Europa Institute
Reile Meyers	PhD student in Labour Law at Utrecht University, Europa Institute
Annetje Ottow	Professor of Public Economic Law at the Europa Institute, Utrecht University and Associate Member of the Board of the Dutch Telecommunications Regulator (OPTA).
Frans Pennings	Professor of Labour Law and Social Security Law at Utrecht University, Europa Institute; Professor of International Social Security Law at Tilburg University

Sacha Prechal	Judge in the Court of Justice of the European Union; Professor of European Law, Europa Institute, Utrecht University.
Albertine Veldman	Associate Professor of Labour Law and Social Security Law at Utrecht University, Europa Institute
Maartje Verhoeven	Assistant Professor European and Administrative Law, Utrecht University, Europa Institute
Sybe de Vries	Associate Professor in European Law, Utrecht University, Europa Institute
Ubaldus de Vries	Associate Professor at Department of Legal Theory, Utrecht University and member of the Working Group Reflexive Modernisation and Law.
Rob Widdershoven	Professor of European Administrative Law at Utrecht University
Paulien Willemsen	Assistant Professor of Administrative Law at Utrecht
Aleidus Woltjer	Assistant Professor of Constitutional and Administrative Law, Utrecht University

Chapter 14

Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation

Evelien Brouwer

1. INTRODUCTION

Data protection law regulates the various stages involved in the processing of data or information on individual, physical persons (and sometimes groups and organizations of such persons).[1] One of the core principles of data protection law is purpose limitation. This principle provides that personal data must be collected for specified, explicit and legitimate purposes and must not be further used in a way incompatible with those purposes. Purpose limitation implies different standards data processors should take into account, including time limits for the storage of data and limitations with regard to the quality and relevance of the information being collected or stored. Both at the European union (EU) as at the national level, the principle of purpose limitation seems to be undermined by current developments in the field of data collection and data sharing. Laws establishing new databases or prescribing the exchange of personal data (e.g., PNR data) often

1. L.A. Bygrave & J.P. Berg, 'Reflections on the Rationale for Data Protection Laws, in: *25 Years Anniversary Anthology*, ed. J. Bing & O. Torvund (Tano: Norwegian Research Center For Computers and Law, 1995), 3 ff. See also L.A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2003).

Leonard Besselink, Frans Pennings & Sacha Prechal (eds), *The Eclipse of the Legality Principle in the European Union*, pp. 273–294.

include vague and open criteria on the use of these systems, time limits, and on the authorities having access to these data.

This blurring of purpose limitation, also referred to as 'function creep' seems to be based on the idea that this principle is only a rule of 'soft law'. In this view, purpose limitation should only be dealt with as a guideline for data processing, allowing data owners or data users to derogate when considered necessary.[2] The aim of this contribution is to restate the meaning of purpose limitation by emphasizing its close relation with the principle of legality. In fact, the data protection principle of 'purpose limitation' can be considered an important case study of the meaning of legality within the multilayered legal order of the EU.

In order to clarify the very sense and aim of purpose limitation, the three functions of legality as discussed by others in this volume – legitimation, attribution, and regulation – will be applied to data processing. It will be held that the aim of purpose limitation is comparable to the general aim of the principle of legality: limiting the powers of government. We will see that in dealing with the collection and use of personal information, the legitimation of public powers is not self-evident: what is the legal basis of current measures? What is the role of the European Parliament and national parliaments with regard to the adoption of the EU legislation at stake? With regard to the function of attribution of public authorities, one has to consider the definition of powers and actors in the new rules dealing with data processing and data exchange. Are the powers and actors sufficiently defined? What rules apply to the use of personal information or international databases with regard to the accountability and responsibility of national authorities? Finally, considering the function of regulation of powers, one has to ask whether the rules involved protect individuals from misuse of powers or arbitrariness. What mechanisms are available to control the powers of authorities?

2. SHORT INTRODUCTION TO DATA PROTECTION LAW

2.1. Development of Data Protection Law

Generally, the basic principles of data protection were formulated in the period between 1970 and 1981. During this period, the 'pioneer states' of data protection, including Germany and Sweden, introduced laws including mechanisms of prior control of databases such as prior registration or licensing systems. The second period, between 1981 and 1988, marked the end of an isolated national legislation process. Concerns about data protection on the one hand, and the free flow of information on the other, resulted in the adoption of the Organisation for Economic

2. An example is the report of Commissie Brouwer with the title '*Gewoon doen*' ['Just do it', EB] on the use of data for security purposes. One of its central recommendations is that 'if necessary for the security, authorities should share personal information' without further taking into account data protection law or the right to privacy. Report to the Netherlands Minister of the Interior, January 2009, <www.minbzk.nl>, 1 Jan. 2010.

Co-operation and Development (OECD) Guidelines in 1980 and of the Data Protection Convention of the Council of Europe in 1981. Now, almost thirty years after their adoption, the standards formulated in these instruments have 'stood the test of time' and still can be considered as guiding principles for data protection laws.[3] An important development for the data protection laws of EU Member States was the adoption of the EC Directive 95/46 on the protection of personal data. This Directive was aimed at preventing diverging national data protection laws from hampering the free flow of information between the EU Member States. By offering harmonized rules and emphasizing and developing further the data protection principles of the aforementioned Data Protection Convention, its implications reached much further. Since its adoption, data protection and the protection of individual rights to privacy could no longer be neglected by the EU and national legislatures. The period since 2000–2001 has provided a new era in data protection history. On the one hand, we have seen the introduction of new information technologies, including the use of biometrics, large-scale databases, 'machine-readable documents', and the efforts of national legislatures to respond to these developments. On the other hand, this period has been marked by the recognition of data protection as an independent human right under Article 8 of the Charter on the Fundamental Rights of the EU.[4]

2.2. Objectives and Principles of Data Protection Law

Too often data protection is marginalized to an individual, private interest which, especially in the context of public order and security, must be weighed against more general and public rights and interests. However, when discussing the meaning of data protection law, it is necessary to understand its different objectives, because this clarifies the close relationship of data protection rules with the principle of legality. In my view, one could distinguish three objectives of data protection.[5] The first is the protection of individual rights, and, more specifically, the protection of the right to privacy. This right, protected under Article 8 European Convention on Human Rights (ECHR) and Article 7 of the EU Charter, includes the right to be let alone, the right to liberty and the right to informational self-determination. The second objective of data protection, also referred to in the

3. Richard Thomas, 'Information Commissioner of the United Kingdom', Annual Report 2006–2007.
4. Article 8 of the Charter states:

   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.

5. See also my dissertation, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Leiden/Boston: Martinus Nijhoff Publishers, 2008), 194 ff.

preamble to the Data Protection Convention, is the protection of the rule of law. For this purpose, the concept of the 'rule of law' should be interpreted widely, similar to the German and Dutch concepts of *Rechtsstaat*. In this meaning, the 'rule of law' refers to a legal order in which the powers of the state (and possibly of civil actors) are constrained for the protection of rights and liberties and the equality and legal certainty of individuals.[6] This concept of the rule of law includes the principle of division or balancing of powers, the protection of human rights, and a democratic legal order.[7] By emphasizing this objective separately, it becomes clear that data protection law not only protects the individual, but also the community of individuals as a whole: this has been described as 'the social function' of data protection.[8] A third objective of data protection law concerns the protection of 'good governance' or 'good administration'. This objective protects the interests of both the data subject and the data controller, by guaranteeing the integrity and accuracy of the information being held, and by safeguarding the security of information systems and time limits with regard to the storage of data.

There is no absolute or definitive set of data protection principles. In the relatively young history of data protection law, varying lists have been defined as to what should be considered basic rules of data protection.[9] In general, one could say that the core of data protection law includes the following principles: purpose limitation, purpose specification, data quality, use limitation, security safeguards, openness, individual participation, and accountability.[10]

3. THE PRINCIPLE OF PURPOSE LIMITATION

3.1. General

One of the central principles of data protection is the principle of purpose limitation, or the principle of 'finality'.[11] It not only implies the prior limitation or

6. Ph. Kunig, *Das Rechtsstaatsprinzip: Überlegungen zu seiner Bedeutung für das Verfassungsrecht der Bundesrepublik Deutschland* (Tübingen: Mohr (Siebeck), 1989); M. Burkens et al. *Beginselen van de democratische rechtsstaat* (Alphen aan den Rijn: Kluwer, 2006) and D.J. Elzinga, 'De democratische rechtsstaat als ontwikkelingsperspectief. Over machtsregulering als ontwikkelingslijn', in: *De rechtsstaat herdacht*, ed. J.W.M. Engels & E.M. Middel (Zwolle: W.E.J. Tjeenk Willink, 1989).
7. The explanatory memorandum to this Convention explicitly refers to 'the necessity of data protection as a tool of balancing powers'.
8. Arthur J. Cockfield, 'Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies', *U.B.C. Law Review* 40, no. 1 (May 2007), 41, available at <http://ssrn.com/abstract=1031964>, 1 Jan. 2010.
9. Bennett refers to the six 'core fair information principles': principles of openness, individual access and correction, collection limitation, use limitation, disclosure limitation and security, Bennett (1992), 101 ff.
10. See for example, the European Data Protection Supervisor (EDPS) in his Opinion of 28 Feb. 2006, Brussels: <www.edps.europa.eu>, 1 Jan. 2010.
11. In the German and Dutch language, this principle is referred to as 'Zweckbindung', respectively 'doelbinding'.

definition of the objective of data processing, but also refers to the subsequent use of data. The meaning of purpose limitation may be clarified considering an important provision of one of the oldest legal sources of data protection law: Article 5 of the Council of Europe Data Protection Convention. Under the heading of 'Quality of data', this provides that personal data automatically processed shall be:

(a) obtained and processed fairly and lawfully;
(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;
(d) accurate and, where necessary, kept up to date;
(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

The purpose limitation has been included in Article 6(1)(b) of EC Directive 95/46, providing that personal data must be collected for specified, explicit and legitimate purposes, and may not be further processed in a way incompatible with those purposes.

Considering these provisions in Article 5 DPC and the EC Directive, one can see that purpose limitation includes different layers of protection. Firstly, it prohibits the collection of personal data for unknown or unspecified purposes, referred to as the 'ban on aimless data collection'. Secondly, it implies that the goals of data processing should be legitimate, meaning in accordance with the law and not infringing these laws. Thirdly, it says that the goals must be specified prior to the data collection: purpose specification. Fourthly, any use or disclosure of personal data for goals incompatible to the (specified) goals of the data processing must be considered as unlawful. Finally, purpose limitation implies that data may not be retained longer than necessary for the purposes for which the data are stored: in other words, the data controller should be bound by time limits. These different layers of protection will be explained further in the following sections.

3.2. Ban on Aimless Data Collection

The 'ban on aimless data collection', also described by German scholars as '*Verbot pragmatikloser Datensammlung*', refers to the principle that personal data should not be collected or stored without the prior specification of the objective of this data processing.[12] According to this principle, it is prohibited to collect or gather information just to keep these data 'in stock' for future unspecified purposes. In the Council of Europe Recommendation R (87) on police files, this principle is explicitly included with regard to data processing for criminal investigation procedures. According to principle 2.1 of the Recommendation on police files, the collection of

12. A. Podlech, 'Gesellschaftspolitische Grundlagen des Datenschutzes', in: *Datenschutz und Datensicherung*, ed. Dierstein, Fiedler & Schulz (Köln, 1976), 311. Cited by H.P. Bull (1985), 13.

personal data for police purposes should be limited to such as is necessary 'for the prevention of a real danger or the suppression of a specific criminal offence'. The Recommendation therefore prohibits the general collection of data, unrelated to any specific criminal investigation. The importance of the principle of 'if there is no crime, there is no investigation', was confirmed in the second evaluation of Recommendation R (87) in 1998.[13] This evaluation describes the matching of police data gathered in the course of criminal investigations based on vast numbers of persons, completely unrelated to any crime. According to the conclusions of this evaluation, these general data surveillance checks should be limited to specific cases described in national criminal law *and* be granted on the basis of a specific mandate from the judiciary.

3.3. Legitimacy

The principle of purpose limitation not only requires the availability of a specific purpose for data processing, but also implies the legitimacy of this purpose. This principle of a legitimate purpose is included in Article 5 of the Data Protection Convention. EC Directive 95/46 goes further, with the inclusion of a limitative enumeration of purposes for which personal data may be processed. According to Article 7 of the EC Directive, data processing is legitimate if:

- the data subject has given his consent;
- the data processing is necessary for a contract to which the data subject is a party;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- it is necessary in order to protect the vital interests of the data subject; or
- for the performance of a task in the public interest or in the exercise of an official authority vested in the controller or in a third party to which the data are disclosed and, finally;
- when processing is necessary for the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests are overridden by the fundamental rights and interests of the data subject.

According to these criteria of the EC Directive, it is not always necessary for data processing by public authorities to be explicitly provided for by law. For example, a legal basis is not required if the data subject has given his or her consent, if the data processing is necessary to protect the vital interests of the data subject, or if this is necessary in the public interest or in the exercise of an official authority vested in the controller or in a third party to whom the data are disclosed. The general provision in Article 6(1)(a) of the EC Directive only requires that

13. Report by A. Patijn, CJ-PD expert from the Netherlands, *Data protection and the police. Evaluation of Recommendation* R (87)15, 1998, available at <www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents>, 1 Jan. 2010.

data must be processed fairly and lawfully. This does not mean that data processing must always have a legal basis, but only that it should not be unfair and not be in breach of the applicable law.

3.4. Purpose Specification: Transparency of Data Processing

Purpose limitation is closely related to the principle of 'purpose specification'. This principle secures the transparency of data processing, obliging data owners to inform data subjects on the purposes for which the data may be collected, stored, used or transmitted to other organizations. As we have seen, it is included in Article 5b Data Protection Convention and Article 6(1)(b) of EC Directive 95/46, on the basis of which automatically processed personal data must be stored or collected for specified purposes. According to consideration no. 42 of the explanatory report to the Convention, the reference to 'purposes' in Article 5 indicates that data should not be stored for undefined purposes, however, the way in which the legitimate purpose is specified may vary in accordance with national legislation. Article 10 and 11 of the Directive 95/46 includes the obligations for data controllers to inform the data subjects on the purposes of data processing, the identity of the controllers, and further, on the recipients or categories of recipients and on the existence of the rights of data subjects.

Purpose limitation, in the sense of purpose specification, reflects the idea that data processing should be foreseeable for the data subject and should not go beyond the reasonable expectations of the person concerned.[14] This condition of 'foreseeability' of data processing is closely related to legitimacy as a function of legality. As we will see below, in its case law on the protection of the right to a private life, the ECtHR explicitly emphasized the importance of 'foreseeability' with regard to the processing of personal data by governmental authorities.

3.5. Use or Disclosure Limitation: Informational Division of Powers

The principle of 'use or disclosure limitation' implies that personal data should not be used or transmitted for purposes other than the initial purpose defined at the time of data collection or storage. In general, this purpose limitation principle is not very strictly defined. As we have seen, Article 5(b) of the Data Protection Convention states that data processing must be stored for specified and legitimate purposes and 'not used in a way incompatible with those purposes'. Article 6(1)(b) EC Directive 95/46 allows for the use or disclosure of information for purposes 'which are not incompatible' with the initial purposes. Of course, this criterion can be applied in

14. See D. Elgesem, 'The Structure of Rights in Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data', *Ethics and Information Technology* 1 (1999): 283–293.

various ways. It allows data holders to define very broadly the purposes of their databases or the authorities or users who have access to them. In practice, it will often be difficult for individuals and data protection authorities to enforce or verify the observance of this principle. For example, it is not always easy to establish which use of the information at stake is 'incompatible' with the original purposes.

The old adage 'information is power' relates to an important objective of purpose limitation. In the same way as we expect the functional powers of public authorities to be described in legislative rules, it is also necessary to have rules on which authority may collect or use which information.[15] Closely related to the idea of division of powers within the administration is the concept of informational division of powers or '*Informationelle Gewaltenteilung*'. As predicted by Westin in 1967, new information technologies caused radical changes to the governmental organization: 'All the government agencies concerned with a problem, such as health, employment, education, etc. whatever their level of government, will be part of an integrated information system and will coordinate their information to make decisions'.[16] Therefore, the concept of the informational division of powers was in the first place rooted in the concerns of administrative organizations about the consequences of information technology for their mutual relations. German scholars advocated a more general theory of prohibition to exercise control through the use of information beyond organizational borders.[17] This principle would protect citizens against a concentration of power by the government, by preventing one authority having access to information from other authorities, regardless of organizational boundaries or the purposes for which the information was gathered.[18]

In the *Census* case or *Volkszählungsurteil* of 1983, the German Constitutional Court acknowledged the importance of an informational division of powers.[19] The Court held in this judgment that the public administration does not constitute 'one informational unit' (*Informationseinheit*) in which personal data can be freely exchanged. According to the Court, it is the task of the legislator to provide guarantees against 'alienation of purpose' or *Zweckentfremdung*.[20]

Elsewhere, I have argued that this principle of use or disclosure limitation is closely linked to the prohibition of *détournement de pouvoir* in administrative law.[21] Considering 'good administration' as one of the goals of data protection described above, individuals should have the assurance that in their relations with

15. See on the subject of division of powers within the administration: B. Schlink, *Die Amtshilfe. Ein Beitrag zu einer Lehre von der Gewaltenteilung in der Verwaltung.* (Berlin: Duncker & Humblot, 1982).
16. Westin (1967), 325.
17. A. Podlech, *Gesellschaftspolitischen Grundlagen des Datenschutzes* (1976), cited in Bull (1985), 13.
18. See among others, H.P. Bull, *Datenschutz oder die Angst vor dem Computer* (München-Zürich: Piper, 1984), 113, and A. Roßnagel, *Datenschutz und Datensicherheit (DuD)*, 10/95, 584.
19. BVerfgE 65, 1, paras 46 and 69.
20. S. Simitis (ed.) *Bundesdatenschutzgesetz* (Baden-Baden: Nomos, 2006), 75.
21. See further, Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Leiden/Boston: Martinus Nijhoff Publishers, 2008), 201–202.

governments, information given to one authority is not automatically available to other authorities as well. In other words, this principle should, to a certain extent, safeguard the informational division of powers. I deal further with this subject in section 6.2, below.

3.6. Time Limits

Finally, the principle of purpose limitation prescribes that personal data be retained no longer than necessary for the purpose for which the data are stored or processed. This principle is laid down in the different European instruments of data protection, although these instruments do not include explicit time limits. For example, according to Article 5e of the Data Protection Convention, automatically processed data may not be stored in a form which permits identification of the data subjects for longer than is required for the purpose for which those data are stored. The content of this wording is similar to the (much shorter) wording of Article 6.1 (e) of the EC Directive: 'no longer than is necessary for the purposes for which the data were collected or for which they are further processed'.

More specific criteria have been included in Principle 7 of the Recommendation No. R (87) 15 on police files. According to this provision, the states should ensure that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored. Regarding the decision on whether longer storage is necessary, the following criteria should be taken into account: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular, an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject; and particular categories of data. Furthermore, the Recommendation explicitly requires the adoption of rules aimed at fixing storage periods for the different categories of personal data, and that regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

4. MULTIPLE LEGAL ORDERS WITHIN THE EU: STRENGTHENING PURPOSE LIMITATION OR ENCOURAGING FUNCTION CREEP?

It is very difficult on the basis of the different decisions which have been adopted, to get an overall picture of the EU architecture for the collection and sharing of personal information. EU decision makers gradually extended the use, the functions, and the content of existing and planned databases. In 2004, the European Commission launched the principle of availability and the necessity of interoperability of different EU databases.[22] These principles, together with the creation of

22. This communication was followed by a Commission proposal for a framework decision on the exchange of information under the principle of availability, COM (2005) 490, October 2005. Due to a lack of support by the Member States, it meanwhile has been withdrawn.

large-scale, multipurpose databases such as the Visa Information System (VIS) and SIS II, seem difficult to reconcile with the principle of purpose limitation, including limits on the use and disclosure of personal information. Other developments, such as, for example, the adopted Decision on the access of law enforcement authorities and Europol to VIS,[23] are clear examples of deviation of the original, limited purposes of the databases. This problem has also been addressed by the European Parliament and the European Data Protection Supervisor (EDPS) Mr Hustinx.[24]

A further development eroding the principle of purpose limitation is the adoption of numerous instruments providing for the exchange of personal information between Member States, between Member States and third states, and between Member States and private organizations (e.g., SIS, Prüm, and different agreements on transfer of passenger data to EU Member States and to third countries).[25] Also, the introduction of biometrics in passports and travel documents issued by EU Member States on the basis of Regulation 2205/2004 can lead to unexpected and unforeseen purposes.[26] Once biometrical data and corresponding information are available, the risk of their use for purposes other than the ones they were collected for will undeniably remain present. On the one hand, the use of biometrics enables national governments to secure identity documents against theft or fraud. On the other, it enables national authorities to use different databases, primarily set up for limited and specified purposes, as investigation or intelligence files. The possibility that the data subject will never be aware of such uses and processing of data is realistic as well.[27]

A very clear example of 'function creep' is the proposal of the European Commission to give law enforcement authorities and Europol access to Eurodac, a EU database containing fingerprints of asylum seekers, under certain circumstances.[28] This database became operational in 2003, with the sole purpose of establishing the EU Member State responsible for the asylum application, and to prevent multiple asylum applications within the EU. The proposal to extend the

23. Decision 2008/633 of 23 Jun. 2008 on the access of designated national authorities and Europol to the Visa Information system for the purpose of prevention, detection, and investigation of terrorist offences and other serious criminal offences OJ L 218, 13 Aug. 2008.
24. European Data Protection Supervisor, Opinion of 20 Jan. 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final), <www.edps.eu.int>, 1 Jan. 2010.
25. The meaning (or remains) of purpose limitation in the third pillar has been described by Els de Busser in: Purpose Limitation in the EU-US Data Exchange in Criminal Matters; the Remains of the Day, in: Marc Cools (e.a.) *Readings on Criminal Justice, Criminal Law and Policing. Governance of Security* Research paper series (GofS) vol. 2 (Antwerpen: Apeldoorn: Maklu, 2009), 163–193.
26. Council Regulation of 13 Dec. 2004, OJ L 385, 29 Dec. 2004.
27. See also the reaction of the Art. 29 Data Protection Working Party, *Opinion on Implementing the Council Regulation (EC) No 2252/2004*, 9.
28. COM (2009) 342 and 344, 10.09.09.

current function of Eurodac was criticized by the EDPS in his opinion of 7 October 2009, expressing his serious doubts on the legitimacy of the proposal and the fact that the necessity of the proposal has not been proven.[29] The national data protection authorities, represented in the Working Party on Police and Justice (WPPJ), also stated that the proposal runs counter to fundamental data protection principles such as proportionality of data processing and respect for purpose limitation.[30]

The Data Retention Directive 2006/24 obliges internet providers to store data on their clients for a minimum of six months and a maximum of two years to allow further access and use by national law enforcement authorities.[31] On the basis of Directive 2004/82 on the obligation of carriers to communicate, passenger data carriers can be fined with a maximum of EUR 5,000 and a minimum of EUR 3,000 when they fail to transmit information concerning the passengers at the request of the authorities responsible for border checks. Shortly before the final adoption of this Directive, the strict purpose limitation within the original draft was extended by the Council. In the first place, Member States may derogate from the general rule that data transferred to border authorities must be deleted within twenty-four hours: the data may be stored for a longer period if they are needed later 'for the purposes of exercising the statutory functions of the authorities responsible for the external border checks'. Secondly, a provision has been included on the basis of which Member States also may use the passenger data for law enforcement purposes.

Finally, I refer to the development and adoption of the EU Framework Decision 2008/977 of 27 November 2008 on the protection of personal data in the field of police and judicial cooperation in criminal matters. Its final text establishes the result of continuous and persistent lobbying of European data protection authorities and the EDPS and must be considered as a compromise between the negotiating partners. With regard to principles of lawfulness, proportionality, and purpose limitation, Article 3 provides that personal data may only be collected by the competent authorities for specified, explicit and legitimate purposes in the framework of their tasks, and may be processed only for the same purpose for which the data were collected. Furthermore, processing of the data must be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected. Article 3(2) however permits 'further processing for another purpose' in so far as: 'it is not incompatible with the purposes for which the data were collected; the competent authorities are authorized to process such data for such other purpose in accordance with the applicable legal provisions, and processing is necessary and proportionate to that other purpose. Here, the Framework Directive links the criterion 'compatibility', also referred to in the EC Directive 95/46, to the principle of necessity and proportionality. This leaves the question open as to what is compatible use, and what is necessary and

29. Published on <www.edps.europa.eu>, 1 Jan. 2010.
30. Published on the website of the Dutch Data Protection Authority, CBP, <www.cbpweb.nl>, 1 Jan. 2010.
31. OJ L 105, 13 Apr. 2006.

proportionate. On this question, as we will see in the next session, the case law of the European Court for Human Rights (ECtHR) and the EC Court of Justice provides us with some clues.

5. SETTING STANDARDS: THE CASE LAW OF THE ECtHR AND THE ECJ[32]

5.1. ECtHR and Article 8 ECHR

In its case law, the ECtHR emphasized repeatedly the close relationship between the protection of personal data and the right of privacy: 'the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention'. For our purpose, this case law is especially important, because on the basis of Article 8 (2) ECHR, the ECtHR developed specific criteria underlining the meaning of purpose limitation. According to Article 8 (2) each interference to the right to private life must be in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The criteria as developed by the ECtHR relate to the specification of purpose or transparency of the data processing at stake, limitation of powers, and the necessity of time limits.

5.1.1. Purpose Specification or Transparency of Data Processing

In the *Leander* case on the practice of secret police files, the ECtHR found that it is not sufficient for the interference to have some basis in domestic law: the law in question must be accessible to the individual concerned and its consequences must be predictable. The ECtHR acknowledged that the requirement of predictability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. 'Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security.' Nevertheless, the ECtHR added that in a system applicable to citizens generally, as under the Personnel Control Ordinance, 'the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which, and the conditions on which, the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life'.[33]

32. See also the contribution of Aleidus Woltjer in this volume on the jurisprudence of these courts with regard to the principle of legality.
33. Leander case, 26 Mar. 1987, §§ 50–51.

In *Malone v. UK*, dealing with secret telephone tapping, the ECtHR stated that 'in accordance with the law' refers not only to the availability of domestic law, but also to the 'quality of the law'. Here, the Court explicitly referred to the necessity of the measures being compatible with the rule of law.[34] The requirement of quality of law was further specified in *Huvig and Kruslin v. France*.[35] These cases concerned the claims based on Article 8 ECHR of Mr and Mrs Huvig and Mr Kruslin, whose phones were tapped during criminal proceedings by the French authorities. The question in these cases was not so much whether this telephone tapping constituted an interference with the applicant's right to a private life, but whether the applicable French law was clear and foreseeable. The ECtHR held that, where tapping and other forms of telephone conversation represent a serious interference with private life and correspondence, this must be based accordingly on a law that is, particularly precise. According to the ECtHR, clear, detailed rules on the subject are essential, especially since the technology available for use is continually becoming more sophisticated, as in the case in question. Since the French law at stake, written and unwritten, did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities, the ECtHR found a breach of Article 8 of the Convention.[36]

5.1.2. Limitation of Powers and Time Limits

In the *Huvig and Kruslin* judgments, the ECtHR further defined a set of criteria for lawful telephone tapping that should have been provided for in French law. These criteria included the categories of persons liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order; the lack of an obligation to set a limit on the duration of telephone tapping; the circumstances under which recordings may or must be erased or the tapes destroyed, in particular, when an accused party has been discharged by an investigating judge or acquitted by a court.[37] Interestingly, a comparable list of criteria was given in *Rotaru v. Romania* with regard to the law regulating the collection, recording and the archiving of information in secret files. Assessing the 'quality' of the Romanian law involved, the ECtHR concluded that this law did not include any limits on the exercise of the powers on the storage and use of the information by the Romanian Intelligence Services. Furthermore, Romanian law did not specify which information could be collected or stored, and against which categories of people or under which circumstances these surveillance measures were allowed. Also, there were no limits on the length of time for which the information could be stored.[38] In the view of the ECtHR, the criteria of 'in accordance with the law'

34. Malone case, 2 Aug. 1984, no. 8691/79, *Series A* 82.
35. Both cases of 24 Apr. 1990, no. 11801/95, *Series A* 176A (Kruslin) and no. 11105/84, *Series A* 176B (Huvig).
36. See Kruslin, § 36, and Huvig, § 35.
37. Kruslin § 35, Huvig § 34.
38. *Rotaru v. Romania*, § 41.

and 'quality of law' require supervision procedures and adequate and effective safeguards against abuse of the rule of law.[39] Since the Romanian system did not provide such safeguards or a supervisory mechanism, the ECtHR ruled that the refuted storage and use of information by the intelligence service was not 'in accordance with the law'.

The objective of purpose limitation of protecting individuals against arbitrary interference by national authorities was implicitly underlined by the ECtHR in the judgment *Segerstedt-Wiberg v. Sweden*.[40] In this case, the ECtHR dealt with the storage of personal information in files of the Swedish Security Service on the basis of the Swedish Police Data Act. Assessing whether the interference of the right to a private life was 'in accordance with the law', the ECtHR focussed on the question of whether the Swedish criterion 'special reasons' included 'unfettered powers' for the security agencies. The ECtHR stated that the scope of discretion conferred upon the competent authorities and the manner of its exercise must indicate with 'sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference'.[41]

Also relevant in this context is the judgment in the case *S. and Marper v. the UK*, in which the ECtHR dealt with UK law permitting long-term, systematic storage of fingerprints and DNA samples of individuals, including minors, suspected of having committed criminal offences. The ECtHR found that the applicable UK law violated Article 8 ECHR, particularly on the grounds that these data were stored for indefinite periods and also related to unconvicted persons.[42] In this regard, paragraph 119 is important, in which the ECtHR remarked upon 'the blanket and indiscriminate nature of the power of retention in England and Wales' and the fact that 'the material may be retained irrespective of the nature of gravity of the offence with which the individual was originally suspected or of the age of the suspected offender'. According to the ECtHR, there were only limited ways for the individual to have the data removed from the nationwide database or to have the materials destroyed. Finally, the ECtHR criticized the absence of provisions for independent review of the justification for the retention of data, and the possibility to assess factors such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

---

39. *Rotaru v. Romania*, § 43.
40. *Segerstedt-Wiberg and others v. Sweden*, 6 Jun. 2006, appl. no. 62332/00. Published in *EHRC* (2006): 89 with annotation of Jan Peter Loof.
41. *Segerstedt-Wiberg*, § 79. In this case, the ECtHR found that the Swedish law was sufficiently clear and that the interference was in accordance with the law. Nevertheless, with regard to four of the five applicants, the ECtHR concluded that the continued storage of the information (in one case up to thirty years) constituted a disproportional interference of their right to private life.
42. *S.& Marper v. the UK*, 4 Dec. 2008, appl.no. 30562/04 and 30566/04.

5.2. ECJ and EC Directive 95/46

5.2.1. *Rechnungshof v. Österreichischer Rundfunk*: Broad Interpretation of Data Protection

The *Rechnungshof v. Österreichischer Rundfunk* judgment was the first decision of the ECJ dealing with the interpretation of EC Directive 95/46.[43] It concerned the question of whether the rules of the Austrian Court of Auditors (*Rechnungshof*), on the basis of which organizations and holdings had to disclose information about their employees and pensioners, including names, positions, salaries and their pensions, were in accordance with the provisions of the EC Directive and the Community principles on the protection of privacy. In this judgment, the ECJ confirmed that the scope of the applicability of this Directive has to be interpreted broadly. According to the ECJ, the scope of applicability of the Directive would not be limited to data processing directly linked to the freedoms of free movement as protected in the EC Treaty.[44] The ECJ made it clear that every other interpretation would run the risk of making the boundaries of the Directive's application too uncertain and too vague. Furthermore, it considered that the principles and criteria for legitimate data processing, as laid down in Articles 6 and 7 of the Directive, so including the purpose limitation, have direct effect in the sense that an individual may seek access to a national court in order to prevent the application of national rules contrary to these principles.[45]

In the same judgment, the ECJ explicitly stated that EC Directive 95/46 must be interpreted in accordance with the right to a private life as protected under Article 8 ECHR. According to the ECJ, 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 Convention, 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'.[46] Therefore, exceptions included in Article 13 of that Directive must comply with the requirement of proportionality with respect to the public interest objective being pursued. In the words of the ECJ: 'that provision cannot be interpreted as conferring legitimacy on an interference with the right to respect for private life contrary to Article 8 of the Convention'. This means, that even if the EC Directive 95/46 allows exceptions to a strict purpose limitation, or leaves questions with regard to the interpretation of 'compatible use of data', data processing and the further use of personal information must always meet the criteria of Article 8 (2) ECHR, mentioned above in section 5.2.

---

43. *Rechnungshof v. Österreichischer Rundfunk and Others*, 20 May 2003, Joint Affairs C-465/00, C-138/01 and C-139/01.
44. Paragraph 39–47.
45. Paragraph 100.
46. C-465/00, para. 91.

5.2.2. *Huber v. Germany*: Linking Purpose Limitation to Non-Discrimination

In the judgment *Huber v. Germany*, the ECJ indirectly linked the principle of purpose limitation to the non-discrimination principle of Article 12 EC, and developed further in. This case dealt with the registration of an Austrian citizen, Mr Huber, in the German central aliens administration or AZR.[47] During the procedure before the German courts, Huber argued that his registration as an EU citizen in the AZR constituted an infringement of EC law, in particular, Article 12 EC prohibiting discrimination between EU citizens and EC Directive 2004/38 on the free movement of EU citizens and their family members. The German administrative court (Oberverwaltungsgericht Nordrhein Westfalen) issued preliminary questions on this case to the ECJ. In this case, the ECJ had to assess three different uses of the registered data on aliens: firstly, the use for administrative purposes by the authorities responsible for border and immigration control. Secondly, the ECJ was asked to rule on the lawfulness of the use of the German aliens administration for statistical purposes. Finally, the ECJ was asked whether the use of the data on EU citizens for law enforcement purposes was compatible with EC law.

In its decision, the ECJ firstly concluded that a system for processing personal data relating to Union citizens who are not nationals of the Member State at stake, such as that put in place by German law (*Gesetz über das Ausländerzentralregister*), and having as its object the provision of support to the national authorities responsible for the application of the law relating to the right of residence can be considered to satisfy the requirement of necessity laid down by Article 7(e) of EC Directive 95/46, interpreted in the light of the prohibition on any discrimination on grounds of nationality, as long as:

- it contains only the data which are necessary for the application by those authorities of the legislation on the right to residence, and;
- its centralized nature enables the legislation relating to the right of residence to be more effectively applied as regards Union citizens who are not nationals of that Member State.

In general, the ECJ found that it must be possible for the authorities of Member States to have 'relevant particulars and documents available to it in order to ascertain, within the framework laid down under the applicable Community legislation, whether a right of residence in its territory exists in relation to a national of another Member State and to establish that there are no grounds which would justify a restriction on that right'. It follows that the use of a register such as the AZR for the purpose of providing support to the authorities responsible for the application of the legislation relating to the right of residence is, in principle, legitimate and, having regard to its nature, compatible with the prohibition of discrimination on grounds of nationality laid down by Article 12(1) EC. For this purpose, however, the ECJ concluded that it must be assessed whether the AZR includes no other data

47. C-524/06, 16 Dec. 2008.

than contained in the documents referred to in Articles 8(3) and 27(1) of the Directive 2004/38. Furthermore, the ECJ explicitly referred to the duty of the national authorities of Member States to guarantee the accuracy and relevance of the data being stored 'since a change in the personal situation of a party entitled to a right of residence may have an impact on his status in relation to that right, it is incumbent on the authority responsible for a register such as the AZR to ensure that the data which are stored are, where appropriate, brought up to date so that, first, they reflect the actual situation of the data subjects and, secondly, irrelevant data are removed from that register' (paragraph 60).

Considering the storage and processing of personal data containing *individualised personal information* in a register such as the AZR for statistical purposes, the ECJ found that this cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46 (para 68). According the ECJ, the German authorities could use anonymous data for this purpose.

Finally, with regard to the use of the AZR for law enforcement purposes, the ECJ held that this was not compatible with the prohibition of discrimination as included in Article 12 EC. According to the ECJ, '12(1) EC must be interpreted as meaning that it precludes the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State' (para 52). As in the aforementioned judgment in the case *Rechnungshof v. Österreichischer Rundfunk*, the ECJ in *Huber v. Germany* underlined the necessity of a maximal interpretation of the level of data protection based on the EC Directive. Referring to the eighth and tenth recital in the preamble of the EC Directive 95/46, the ECJ concluded that this Directive is intended to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States, and that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

Furthermore, referring to its conclusion in the earlier *Lindqvist* case, the ECJ emphasized that the harmonization of those national laws should not be limited to minimal harmonization, but 'amounts to harmonization which is generally complete'.[48] More interesting is the fact that in *Huber v. Germany*, the ECJ explicitly clarified that the aim of a harmonized and high level of data protection also applies to the principle of purpose limitation:

> having regard to the objective of ensuring an equivalent level of protection in all Member States, the concept of necessity laid down by Article 7(e) of Directive 95/46, the purpose of which is to delimit precisely one of the situations in which the processing of personal data is lawful, cannot have a meaning which varies between the Member States. It therefore follows that what is at issue is a concept which has its own independent meaning in Community law

48. Case C-101/01 *Lindqvist* [2003] ECR I-12971, para. 96. Referred to by the ECJ in para. 51 of the *Huber* case.

> and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1(1) thereof.[49]

This conclusion is important as it not only applies to the problem of this particular case: non-discrimination rights of EU citizens, but also to the general interpretation of the basic principles of data protection law within the laws of the EC Member States implementing EU law.

6. RESTORING THE PRINCIPLE OF PURPOSE LIMITATION: APPLYING THE FUNCTIONS OF LEGALITY

6.1. Legitimacy

An important function of legality is the legitimation of public authorities. It refers to a classic principle of constitutional law dealing with the relationship between state and citizens: the 'social contract' on the basis of which citizens accept the powers of their government in so far as these powers are considered legitimate and in so far as these powers are not misused. This principle also applies to the informational powers of the state. We accept legislation by which we have to transmit personal data to the government, as long as we are convinced that the government needs this information: tax law, population administration, law enforcement. We also accept the exchange of information between different organizations so long as we understand the connection between these organizations. This requirement of public acceptance of public powers is closely related to the criteria formulated by the ECtHR in its case law on Article 8 ECHR with regard to the 'foreseeability' of the law. For example, mentioned by the House of Commons in the report *A Surveillance Society?*, we may think of the exchange of information between tax authorities and social security as foreseeable for the citizen, however, between tax authorities and the police it is not.[50]

One could wonder whether transparency is not replacing *legitimacy* as the core value of data protection, considering the numerous grounds included in the EC Directive 95/46 and other instruments legitimising data processing, and the special emphasis on transparency and informing the data subject. Or, in the words of De Hert and Guthwirth, 'Legitimate is whatever processing that has been rendered transparent.'[51] However, it should be clear that legitimacy and transparency are not to be considered as alternatives, but as supplements to legality.

---

49. *Huber v. Germany*, para. 52.
50. Report House of Commons, Home Affairs Committee, 'A Surveillance Society?', Fifth Report of session 2007–08, published 8 Jun. 2008 (London: The Stationery Office Limited, 2008), 55, <www.parliament.the-stationery-office.co.uk/> 1 Jan. 2010.
51. P. de Hert, S. Guthwirth, Making sense of privacy and data protection: a prospective overview in the light of the future identity, location-based services and virtual residence, Annex 1 to the report *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Technical Report Series, Institute for Prospective Technological studies, Brussels, July 2003, 146.

The restoration of legitimacy of the information policy is necessary for increasing the involvement of (national and European) parliaments, but especially of the public. This requires more discussion on the aims and objectives of the proposed systems, on the definitions of crimes for which data may be exchanged, on the use of biometric data, including DNA, and the access of governments to data communication of their citizens. An interesting example of public involvement with decisions on the use of personal information is the recent referendum in Switzerland with regard to the biometric passport. Joining EU's travel free zone in 2008, the Swiss government had to decide on the introduction of biometric data in the Swiss passport. The Swiss voters (turnout 38%) accepted by a narrow margin the biometric passport: 50.1% approved, 49.9% rejected the passport.[52] Although one may doubt whether this specific outcome of the referendum is sufficient to legitimize the measure at stake, the instrument as such, can be a useful tool of legitimacy, in the meaning of democratic accountability. That 'legitimacy' in this latter meaning is not synonymous with 'legitimate' meaning lawful or legal, was proven by the outcome of a more recent referendum in Switzerland on the so-called 'minaret ban'.[53] In this referendum of 29 November 2009, 59% of the Swiss voters supported the proposed ban on the further construction of minarets in Switzerland. However, as was held by different commentators (including the Swiss government), the implementation of this ban would be in violation of the Swiss Constitution and international human rights obligations.

Another tool in obtaining (or regaining) legitimacy for measures adopted in the legal framework of the EU could be the use of impact assessment studies by the Commission for important legislative and non-legislative proposals. In the Hague Programme of November 2004, the Member States agreed on the necessity of the 'assessment of added value of new EU databases'. According to this principle, the added value should be established before the setting up of new large scale EU data systems. However, the use of these extended impact assessment studies requires that they are based on transparent and independent research, in which human rights consequences are sufficiently taken into account and not overriden by economical and technical aspects.

6.2. Attribution

In the legal and political debate on data processing and the use of new databases or connection between existing databases, 'legality,' in the sense of strict rules on who receives which powers, receives little or no attention. As I have tried to develop in section 3.5 above, one of the important aims of purpose limitation is the restriction of powers by 'informational division of powers' and to protect individuals against misuse of powers or arbitrariness. Defining in advance the purposes for which personal information may be used prevents that personal

52. Source: <www.swissinfo.ch> visited 17 May 2009.
53. Source: <www.swissinfo.ch> visited 1 Jan. 2010.

information acquired in a specific context under specific conditions will be accessible by other authorities for other purposes or tasks. In this view, purpose limitation is, for example, difficult to reconcile with 'fishing expeditions'.[54] The UK House of Commons, in the aforementioned report of 2008 on surveillance and the use of personal data, emphasized the need of strict purpose limitation, and even advocated a principle of *data minimisation*. According to this report, the principle of restricting the amount of information collected to that what is needed to provide a service should guide the design of any system that involves the collection and storage of personal information.

Furthermore, attribution of powers, when applied to the collection and storage of personal information, requires strict rules on the time limits and the powers of authorities to retain personal information in their files. As we have seen, this has been emphasized by the ECtHR in *Segerstedt Wibergh*, dealing with the storage of information on Swedish citizens by the national security services. What is important to understand when dealing with the storage of personal information is that the longer information is retained, the more likely it is that the information will be out of date and inaccurate. It is precisely for this reason that the ECJ emphasized in the case of *Huber v. Germany* the duty of national authorities to guarantee the accuracy and relevance of data being stored. The need of time limits was also an important conclusion of the 2008 report of the House of Commons:

> Information should only be held as long it is necessary to fulfil the purpose for which it was collected and if information is to be retained for 'secondary purposes' rather than service delivery it should normally be anonymised and retained only for a previously specified purpose.[55]

In other words, not only must the powers to collect personal information be regulated sufficiently clearly, but also the powers of data storage and retention. This requirement of time limits is closely related to 'regularization' of data processing, dealt with in the following final section.

6.3. Regulation

Once powers have been attributed to governmental organizations, the use of these powers needs regulation. Here, I use 'regulation' in the meaning of rules making it possible to control and counterbalance public powers, for example, by offering citizens certain rights, by introducing independent control authorities, or by providing mechanisms by which unlawful use of powers may be sanctioned. This regulatory function has been underlined by the ECtHR in the aforementioned case law. Understanding 'regulation' as such, one may see the direct relation

54. See Colin J. Bennett, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States* (Ithaca and London: Cornell University Press, 1992), 108.
55. Report House of Commons, Home Affairs Committee, 'A Surveillance Society?', Fifth Report of session 2007–08, published 8 Jun. 2008 (London: The Stationery Office Limited, 2008).

between purpose limitation and the other principles of data protection law, for example, individual rights on access, correction, or deletion, the establishment of independent supervisory authorities, or, as mentioned above, time limits on data retention.

One of the current problems of 'regulating' informational powers of governmental authorities is that, although there is a general acceptance of the substance and importance of data protection law, the applicable rules allow for many exceptions under various circumstances. This implies the risk that many provisions of data protection will continue to be considered 'soft law' instead of becoming 'hard law'. The EC Directive 95/46 permits, under certain conditions, limitations on data protection principles, including restriction of participation rights, of the ban on processing sensitive data, and of purpose limitation. If the purpose of data processing and the group of authorities having access to data are defined very widely, purpose limitation as such will not offer any extra safeguard for the persons concerned. The same problem arises with regard to the principle of restricting the storage of data over time. The obligation to apply time limits is only effective as long as these time limits are based on a fair balance between the different interests at stake.

In practice, an important problem remains the ignorance of individuals, not only with regard to their rights, but also with regard to what is happening with their personal information. This can be perceived as a problem of regulation, but also of the legitimacy of informational powers. It requires not only transparency, but also the education and encouragement of persons to use their rights.[56]

7. CONCLUSION

The function of legality is to restrict governmental powers in order to safeguard rights and liberties of citizens. In this contribution, I have tried to establish that the principle of purpose limitation has a similar function with regard to the restriction of informational powers. With regard to the effective meaning of purpose limitation, we saw that Europeanization of law has a double, not to say contradictory, impact. On the one hand European law, and in particular the case law of the ECtHR and the ECJ, reinforced the meaning and importance of purpose limitation, emphasizing its functions of legitimacy, attribution, and regulation. On the other hand, EU policies and legislation tend to undermine the meaning of purpose limitation, by providing vague definitions on the intended use of personal information, the establishment of multifunctional databases, and by extending the use of existing databases for other purposes ('function creep').

---

56. Richard Thomas, Information Commissioner in the UK, in: *A Surveillance Society?* Fifth Report of the House of Commons, Home Affairs Committee, 44. See also Birte Siemen, *Datenschutz als europaïsches Grundrecht* (Berlin: Duncker & Humblot, 2006), 331: *'Damit dieses Recht seine volle Geltung erlangt, muss es von den Bürgern allerdings auch wahrgenommen werden'*.

To regain the legality of the 'EU information network', improvements are to be made at both the level of 'legitimacy', 'attribution', and 'regulation'. This requires in the first place, a legislative process which involves both the European parliament and national parliaments, and which is transparent to the citizens and inhabitants of the EU. Secondly, the attribution of 'informational powers' of governments needs further regulation, including strict rules on the purpose of data processing and the authorities having access to these data, respecting the criteria of necessity and proportionality of such access. Thirdly, further guarantees are to be developed to counterbalance the use and possible misuse of personal information. These guarantees may include the extension of powers for data protection authorities, the strengthening of the individual rights (including the right to financial compensation), and the provision and application of sanctions to the misuse of data.