# A Comparative Analysis in Relation to Informational Self-Determination and Privacy:

The Icelandic Health Sector Database Decision and
The German Census Act Decision

Candidate number: 8003
Supervisor: Dr. Lee A. Bygrave
Deadline for submission: December 1, 2007

Number of words: 17.085 (max. 18.000)

A Thesis Submitted in Partial Fulfilment of the Requirements for the Award of the Degree
Master in Laws in Information and Communication Technology of the University of Oslo

26.11.2007

# Table of Contents

# Acknowledgements

The author thanks Dr. Lee A. Bygrave for his valuable guidance and supervision writing the thesis. The author is also grateful for the assistance of Marta Herkenhoff librarian at the Norwegian Centre for Human Rights and Anne Gunn Bekken librarian at the Norwegian Research Center for Computers and Law. Special thanks to my brother Guðmundur Freyr Úlfarsson for proofreading the thesis and Hlín Lilja Sigfúsdóttir for collecting and sending reference material from Iceland. At last but not least, thanks to my immediate family for all their support and endless patience.

# 1 Introduction

## 1.1 Scope and Aims

The scope of this thesis is an analysis of the Health Sector Database decision[1] by the Icelandic Supreme Court from the year 2003 and a comparison with the twenty years older Census Act decision[2] by the Federal Constitutional Court in Germany. The comparative analysis will be in relation to informational self-determination and privacy.

The reason for this analysis is the author's personal interest in the Icelandic case as a former director of the Monitoring Committee of the Icelandic Health Sector Database. It is interesting to compare the Health Sector Database decision to the Census Act decision because both found a controversial Act unconstitutional and in breach of information privacy.

The Census Act decision has been regarded as a landmark decision in relation to information privacy. The Federal Constitutional Court acknowledged a right to informational self-determination as a constitutional right[3] in Germany in the Census Act Decision. The concept of informational self-determination had been used by scholars some years before like Westin[4] but this term had not been referred to in a court's decision before, to the best of the author's knowledge.

This thesis presents the Courts' reasoning for their decisions. Week points are criticized and attention drawn to interesting questions that perhaps were left unanswered by the courts. Finally, the objective is to seek an answer to the question if a right to

---

[1] Icelandic Supreme Court (ISC), case no. 151/2003, p. 4153-4181.

[2] Judgment of the First Senate of 15 December 1983 - 1 BvR 209/83 et al. Federal Constitutional Court, Karlsruhe.

[3] The Federal Constitutional Court concluded that informational self-determination was a separate right for the citizens, distinct from other rights. The right is drawn from the right to freely develop one's personality and from the right to human dignity of the Basic Law and is therefore a constitutional right. Cf. section 4.2.3.

[4] Cf. section 2. p. 7.

informational self-determination can be regarded as a separate fundamental right in Europe. The answer is based on this analysis of the two previously mentioned decisions and by examining case law from the European Court of Human Rights in Strasbourg.[5] Informational self-determination cannot be regarded as a fundamental right in Europe unless there is some evidence of acknowledgement from the Strasbourg Court in that direction.

First, the thesis presents a brief background of the environment that privacy as a human right has emerged in. Then some background information on the Icelandic Health Sector Database Act is introduced, including a discussion of the facts and conclusion of the Health Sector Database decision, both from the District Court and the Supreme Court of Iceland. The thesis also presents a discussion of the German Census Act and the Census Act decision, facts of the case, and conclusions relevant to this thesis.

This is followed by the comparative analysis of the two decisions. There are some major similarities such as both cases involved a personal data collection and processing from the whole nation based on a controversial and highly political Act. Both decisions were made by each country's high court, where both courts decided there had been a breach of fundamental rights protected by each country's constitution.

## 1.2 Methodological Considerations

This analysis uses the original Icelandic text of the Health Sector Database decision and the Health Sector Database Act. English translations are available on the Internet and those are cited in this thesis. Official translations of the Icelandic Constitution, Health Sector Database Act, Data Protection Act, Freedom of Information Act and the Health Sector Database regulation are available. However, Internet resources make available only an unofficial translation of the Health Sector Database decision itself.

An English translation of the Census Act decision by Riedel is relied upon in this thesis.[6] This translation also includes comments on the Census Act by the judges of the

[5] Cf. European Court of Human Rights at http://www.echr.coe.int/echr/

[6] Riedel: *Federal Constitutional Court, Karlsruhe [FCC, K]*, Human Rights Law Journal [HRLJ], vol. 5, No. 1, 1984, p. 94-116.

Federal Constitutional Court. An English translation of the text of the 1983 Census Act could not be located. A translation of the German Basic Law from the website of the UISCOMP Comparative Law Society, published with permission of the Goethe-Institut Inter-Nationes, is used in this thesis. English translation of the German Data Protection Act and Freedom of Information Act can be found on the website of the German Federal Commissioner for Data Protection and Freedom of Information.

## 1.3 Use of Terms

This thesis refers occasionally to the term constitutional in relation to statutes and rights. A constitution is a written statute, gathering fundamental principles which the state is governed by and basic rights of the people that are governed by that state. Constitution should not be as easily amended as other statutes. Constitutional means that it is allowed by or contained in the constitution. The author chooses to use the term fundamental in relation to the right to privacy and the right to informational self-determination instead of constitutional.[7] That is with reference to the European Convention on Human Rights and Fundamental Freedoms. All 47 member states of the Council of Europe (as of November 2007) have ratified the Convention and agreed on these fundamental human rights.[8] Which fundamental rights are included in the national constitutions varies slightly between countries hence the author does not refer to the term constitutional unless in relation to specific national constitutions.

---

[7] The Treaty establishing a Constitution for Europe, was signed in Rome October 29, 2004 but is not yet in force. The Treaty has been the cause of an on-going and interesting debate on European constitutionalism. The debate is amongst other things about the relationship of national constitutions with an European Union (EU) Constitution and the status of the European Convention on Human Rights in this context. In this debate it is also discussed if the Treaty establishing a Constitution for Europe can even be called a constitution in the traditional sense since the EU is not a state but a union of member states. This discussion is outside the scope of this analysis but is the reason the author uses the term fundamental rather than constitutional. For further information about European constitutionalism see for example: *The European Constitution and National Constitutions: Ratification and Beyond,* Anneli Albi and Jacques Ziller (ed.), 2007; Church and Phinnemore: *Understanding the European Constitution: An Introduction to the EU Constitutional Treaty,* 2006 and *The EU Constitution: The Best Way Forward?,* Deirdre Curtin, Alfred Kellerman and Steven Blockmans (ed.), 2005.

[8] A list of member states that have ratified the Convention can be found at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=&DF=&CL=ENG

It is worth mentioning that the official English translation of Art. 71(1) of the Icelandic Constitution uses the term “privacy” but the original Icelandic text refers to “respect for private life” (is. friðhelgi einkalífs, no. privatlivets fred). The provision is doubtless directly referring to Art. 8 of the European Convention on Human Rights.

Various terms used in this thesis such as personal data, data subject, processing, controller, and processor are used as they are defined in Art. 2 of the European Union (EU) Data Protection Directive 95/46/EC.[9] Data subjects in the thesis are on one hand German citizens that were obligated by law to take part in a census and on the other hand Icelandic citizens that chose not to opt-out of the Health Sector Database. It should be noted that the term processing is a broad term that covers both automatic and manual processing, such as collection, organization, storage, alteration, retrieval, use, transmission, dissemination, erasure or destruction of the personal data.

[9] 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.

## 2 The Fundamental Right to Privacy

In 1946, the United Nations Commission on Human Rights was established and two years later the Universal Declaration of Human Rights was made.[10] It is not legally binding but has a great significance nonetheless. Art. 12 states: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."[11]

The member states of the Council of Europe signed the European Convention on Human Right and Fundamental Freedoms in Rome in 1950. The establishment of the European Court of Human Rights in Strasbourg[12] has given European citizens the opportunity to bring cases against their governments when national remedies have been exhausted.[13] Additional instruments and mechanism have been implemented both by the Council of Europe[14] and the European Union to strengthen human rights protection. Most recent is the Charter of Fundamental Rights of the EU (the Charter),[15] which is included in the Treaty establishing a Constitution for Europe (TCE).[16]

---

[10] Drake and Jørgensen: "Introduction" in *Human Rights in the Global Information Society*, 2006, p. 10-11.

[11] Universal Declaration of Human Rights see: http://www.unhchr.ch/udhr/lang/eng.htm

[12] Originally there were established two bodies, the European Commission of Human Rights and the European Court of Human Rights. This system was revised under protocol no. 11 in 1998 when the two bodies were combined as one body, called the European Court of Human Rights. For more information about background and procedures of the Court see: *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, chapter 1.

[13] Drake and Jørgensen: "Introduction" in *Human Rights in the Global Information Society*, 2006, p. 23.

[14] For example the Committee of Ministers and the Secretary General of the Council of Europe. For more information on these bodies see: *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, p. 44-46.

[15] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, C 364, 18.12.2000. The Charter was signed in Nice December 7, 2000. For further information on the Charter see for example: Polo and den Boer: "The Charter of Fundamental Rights: Novel Method on the Way to the Nice Treaty" in *The Treaty of Nice: Actor Preferences, Bargaining and Institutional Choice*,

The International Covenant on Civil and Political Rights (ICCPR) lays upon member states both negative and positive obligations[17] but there is no legally binding mechanism for individuals to enforce their rights.[18] Art. 17(1) of ICCPR is almost the same as the first sentence of Art. 12 apart from the additional word "unlawful" about interferences and attacks. The latter sentence is the same.

The EU Data Protection Directive gives a harmonized minimum standard for data protection in Europe. Countries that are not member states of the EU, but are members of the European Economic Area (EEA), i.e. Iceland, Norway, and Liechtenstein, have also based their national data protection law on the EU Data Protection Directive.[19]

The right to privacy is protected by Art. 8 of the European Convention on Human Rights, hereafter called the Convention.[20] Art. 8(1) of the Convention states: "Everyone has the right to respect for his private and family life, his home and his correspondence." It is similar to Art. 12 of the Universal Declaration of Human Rights

---

Laursen (ed.), 2006, chapter 24 and Goldsmith: "A Charter of Rights, Freedoms and Principles" in *The Treaty of Nice and Beyond: Enlargement and Constitutional Form*, Andenas and Usher (ed.), 2003, chapter 15.

[16] Treaty establishing a Constitution for Europe, Official Journal of the European Union, C 310, Volume 47, 16 December 2004. The Charter of Fundamental Rights is not legally binding as of now but will be if or when all 27 EU member states (as of November 2007) have ratified the TCE. French voters on May 29, 2005 and Dutch voters on June 1, 2005 rejected the ratification of the TCE in national referendums. See: *The European Constitution and National Constitutions: Ratification and Beyond*, Anneli Albi and Jacques Ziller (ed.), 2007, p. 288. For a list of the 27 member states of the EU cf. http://europa.eu/abc/european_countries/index_en.htm

[17] Negative obligations meaning not violating the rights listed in the ICCPR and positive obligations meaning the state has to implement laws to ensure those rights.

[18] Hosein: "Privacy as Freedom" in *Human Rights in the Global Information Society*, 2006, p. 132

[19] According to the EEA agreement, that came into force on January 1, 1994, the EEA countries must implement directives from certain fields into national law. More information on the EEA agreement can be found at: http://ec.europa.eu/external_relations/eea/index.htm

[20] For more information on Art. 8 of the European Convention on Human Rights see: *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, p. 663-750; Jacobs and White: *The European Convention on Human Rights*, 2006, p. 241-299 and Art. 8 with regard to data protection: Bygrave: *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, vol. 6, 1998, p. 247-284.

but does not use the word privacy and does not refer to attacks on honour and reputation. The European Court of Human Rights has interpreted "private life" broader than one would presume that the word privacy entails.[21] For example in Halford v. United Kingdom it was concluded that the claimant could reasonably expect privacy at her workplace.[22]

The judgments of the European Court of Human Rights show that it has on purpose avoided giving an exhaustive definition of private life. In Pretty v. United Kingdom, for example, the Strasbourg Court stated: "... the concept of 'private life' is a broad term not susceptible to exhaustive definition."[23]

The right to privacy has been analysed and defined in many different ways.[24] The influential definition of Westin[25] is about information privacy, the right to decide what personal information should be communicated to others and under what circumstances, and is quite distinct from the "right to be let alone" as Warren and Brandeis had defined privacy in their article from 1890.[26] Westin's definition of privacy is on the other hand very similar to the German Federal Constitutional Court's definition of the concept of informational self-determination. That is the right to decide for oneself when and within what limits personal information and facts shall be disclosed to others. The concept of informational self-determination will be analysed in more detail in sections 5.10 – 5.12.

---

[21] Wong: "Privacy: Charting its Developments and Prospects" in *Human Rights in the Digital Age*, Klang and Murray (ed.), 2005, p. 152; *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, p. 665.

[22] Halford v. United Kingdom, 1997-III Eur. Ct. H.R, para. 46.

[23] Pretty v. United Kingdom, 2002-IV Eur. Ct. H.R, para. 61.

[24] Bygrave: *Data Protection Law – Approaching Its Rationale, Logic and Limits*, 2002, p. 128-129. Bygrave has gathered four groups of definitions of privacy by various scholars.

[25] Westin: *Privacy and Freedom*, 1967, p. 7. Westin's definition of privacy: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

[26] Warren and Brandeis: *The Right of Privacy*, 4 Harvard Law Review 193, 1890.

Rehm states that the right to privacy includes two aspects.[27] The first aspect refers to the individual's right to keep personal information private and the latter aspect refers to the individual's right to take important decisions. Rehm feels that this separation of privacy is helpful for legal clarification of the concept of privacy in an informational aspect. The author agrees with Rehm especially in the light of the Pretty v. United Kingdom judgment.[28] The author thinks on the other hand that the right to informational self-determination could not be successfully separated into those aspects since it has both elements so closely intertwined.

[27] Rehm: *Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law*, p. 5, 2000. Rehm suggests that: "...legally separating these two interests, instead of lumping them together under the same headline, could help to clarify legal bases, content and limitations of at least the right to privacy in its informational aspect."

[28] Pretty v. United Kingdom, 2002-IV Eur. Ct. H.R. Cf. chapter 6, p. 45-46.

# 3 The Icelandic Health Sector Database Decision (2003)

## 3.1 Background Information

### 3.1.1 Political Disagreement

The first Bill on the Health Sector Database met strong opposition, especially because all Icelanders, living and deceased, were obligated by law to have their health information entered into the database. Later the Bill was changed[29] but many still opposed that the database was to be an opt-out database instead of an opt-in. Opt-out means that if an individual does not want to be in the database then the individual has to opt-out by handing in a signed exclusion form.

### 3.1.2 The Health Sector Database Act No. 139/1998

The Health Sector Database Act was enacted in December 1998. The first chapter is about objective, scope, and term definitions. In Art. 2 it is mentioned that the database excludes bio-samples.

The second chapter is about the operating license. The licensee, who will be the controller in the meaning of Art. 2(d) of the EU Data Protection Directive and a processor, is responsible for the cost of design, making, use, and all monitoring of the Health Sector Database. An operating license is to be given for a period of twelve years. Art. 6 is about a Monitoring Committee concerning the creation and operation of the Health Sector Database.

Chapter three is about collection of information. Art. 7 is about employees of health institutions or self-employed health service workers, who would be processors in the meaning of art 2(e) of the EU Data Protection Directive. They are to prepare medical

[29] Bill on a Health Sector Database , document no. 109, 1998. It says in the comments about Art. 8 that the first Bill did not have opt-out or opt-in options. Since the data was unidentifiable in the opinion of the legislator, explicit consent from the data subjects was believed to be unnecessary by reference to the EU Data Protection Directive. The legislator stated in the final Bill that later was enacted, that it decided to allow an opt-out option.

records for database entry and ensure that personal identification is in encrypted one-way form. The Icelandic Data Protection Authority shall ensure that the encryption process and the data processing comply with necessary privacy standards and data protection. The licensee has the obligation to make working procedures that will fulfil the Data Protection Authority's conditions about data subject's privacy. In Art. 8 there is an opt-out possibility for the patients/data subjects.

Chapter four is about access to the database for the Icelandic Health Ministry and Directorate of Health, which shall be free of charge, for making health reports, planning, policy-making, etc. Then there is one provision, Art. 10, about utilization of data, where the licensee is permitted by law to use the database for financial profit. It allows a merger of the database with databases such as of genetic and genealogic information. Art. 11 is about confidentiality of employees.

Chapter five is about monitoring. It is the Icelandic Data Protection Authority that shall monitor processing of personal data and data protection in the design and later operation of the database. A special Monitoring Committee shall be established and it is responsible for monitoring all other issues, than mentioned above, in the design and later operation of the database. The Committee is for example to monitor all database queries and processing of data from the database and is to regularly send records to the Science Ethics Committee. Then there shall be established an Interdisciplinary Ethics Committee which shall assess studies carried out within the licensee's company and inquiries which are received.

Chapter six is about penalties and the revocation of the license. Finally chapter seven contains various provisions and provisional clauses. Regulation 32/2000 is based on the Act. It contains further information and rules on the Act's provisions, mostly the separation of tasks between each supervising authority.

## 3.2 The Decision in Short

There has been one material judgment from the Supreme Court of Iceland about the Health Sector Database, case 151/2003,[30] where the Supreme Court decided that Art. 71(1) of the Icelandic Constitution had been violated. The provision states: "Everyone shall enjoy freedom from interference with privacy, home, and family life."

[30] Icelandic Supreme Court (ISC), case 151/2003, p. 4153 – 4181.

### 3.2.1 Plaintiff's Claims and Formal Authority

A young woman sent a request to the Icelandic Health Directorate and asked that health information about her late father would not be registered in the Health Sector Database.[31] When her request was denied, on the grounds that she had no authority to make this request for other people than herself, she filed a suit to get that decision invalidated. The District Court in Reykjavík agreed with the defendant that the plaintiff had no authority to make this request and dismissed the case on this lack of formality. The Supreme Court disagreed and said that the plaintiff did have personal interests at stake and should get a material judgment.[32]

### 3.2.2 The Decision of the District Court

The District Court now found that the plaintiff was a rightful party to the case. In Art. 3(6) of the Health Sector Database Act, health information is defined as "information on health of individuals, including genetic information." Art. 10(1) gives permission of merging the Health Sector Database with a database of genealogical data and a database of genetic data. The Court held that the plaintiff had personal interests at stake since it was possible that information concerning her late father could result in implied conclusions about her and her private life.[33]

The District Court stated on the issue of identifiability of data subjects that modern encryption methods were presumed so safe that in general it would be almost impossible to read encrypted information if the encryption code was kept secret.[34] The Court stated there was no reason than to have faith that the Data Protection Authority could fulfil their legitimate purpose of securing the privacy of data subjects. The Court stated that, when assessing if information was identifiable, all possible preventions and safeguards to ensure the privacy of a person had to be considered. That was: The encryption of health information, access control, security claims and supervision by public authorities of the operation of the Health Sector Database, confidentiality of those who design and operate the database, and punishment and sanctions.[35] Finally the

[31] ISC, case 151/2003, p. 4163.

[32] ISC, case 417/2001, p. 3962-3971.

[33] ISC, case 151/2003, p. 4179.

[34] ISC, case 151/2003, p. 4180.

[35] ISC, case 151/2003, p. 4181.

District Court ruled that when all this had been taken into consideration and it was clear that identifiability of the data was not within reasonable expectations without considerable effort, then the data was unidentifiable in the sense of the law. The same applied for the possible merging of the database with databases of genetic and genealogic information. The Court did not think that the Act on the Health Sector Database went against Art. 71(1) of the Icelandic Constitution about protection of privacy, Art. 8 of the Convention, Art. 17 of the ICCPR or European Directives such as 95/46/EC about Data Protection.[36]

The Directorate/defendant was acquitted.

### 3.2.3 The Decision of the Supreme Court

The plaintiff appealed to the Supreme Court.

The District Court, which had a specialist in computer science on board, concluded that one-way-encryption could be done in such a way that it would be almost impossible to read.[37] The Supreme Court pointed out that the Act did not state which information from the medical records had to be encrypted in this way before being added to the Health Sector Database and if certain identifiable information in the medical records should be omitted. Regulation no. 32/200 about the Health Sector Database did not either give any clues on this matter. When looking at the operating license, it seemed that only the data subject's ID numbers should be encrypted, but names and addresses were to be omitted.[38] The Supreme Court went on stating that clearly this information was not the only information that could make a data subject identifiable. Other matters like age, the community where the data subject lives, marital status, education, employment, types of diseases, and other characteristics could alone or combined lead to the identifiability of the data subject.[39]

The Supreme Court also mentioned that Art. 10 of the Health Sector Database Act neither specified what information from the database, which could be used for identification, would appear to those that sent queries to it nor did the Act give any clues as to what could be read into the information with the merging of the three

[36] ISC, case 151/2003, p. 4181.

[37] ISC, case 151/2003, p. 4180.

[38] ISC, case 151/2003, p. 4160.

[39] ISC, case 151/2003, p. 4161.

databases. The regulation based on the Act did not have any specifications on the subject.[40] In various provisions in the Act it was stated that the health information should be unidentifiable but the Act severely lacked information on *how* this should be ensured.[41]

The Court emphasized the importance of Art. 71(1) of the Constitution for protection of people's privacy and said that public monitoring authorities could not do their work sufficiently without having clear legal provisions to support their work. It was insufficient to only include steps for privacy protection in the operating license and working rules that could be changed at any time.[42]

The Supreme Court found that the Health Sector Database Act did not ensure that the health information was in fact unidentifiable and thereby did not ensure the protection of the appellant's privacy as it should, under Art. 71(1) of the Constitution.[43] The Court also referred to common practice of confidentiality about private life and the fact that the Act itself did not prohibit people to opt-out their passed away parents. The decision was in favour of the appellant and the Directorate of Health had to invalidate their decision of refusing the young woman's request.[44]

The reasoning of the Supreme Court is analysed further in chapter 5.

[40] Regulation no. 32/200 about the Health Sector Database.

[41] ISC, case 151/2003, p. 4161.

[42] ISC, case 151/2003, p. 4161.

[43] ISC, case 151/2003, p. 4161.

[44] ISC, case 151/2003, p. 4162.

# 4 The German Census Act Decision (1983)

## 4.1 Background Information

### 4.1.1 Political Disagreement

The Federal Government in Germany wanted a new census from the German nation in the beginning of the 1980's. They needed statistics of "population count, the demographic and social structure of the population, and the economic condition of citizens generally."[45] The Census Act was accepted in both Houses of Parliament in 1983.

The Census Act was controversial and there was a great political debate in German society about the census[46] because it was not just a population count but was also to gather a great amount of personal data such as "data related to job titles, employers and residences."[47] Additionally the Census Act permitted linking and data sharing between federal and local authorities.[48]

### 4.1.2 The Census Act 1983[49]

Sections 1 to 8 of the Act listed in detail what kind of information citizens were obligated to give by the law. For example: Name, address, telephone number, sex, birthday, marital status, religion, nationality, what kind of accommodation, sources of

---

[45] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 95.

[46] Riedel: *New Bearings in German Data Protection*, HRLJ, vol. 5, No. 1, 1984, p. 67.

[47] Jacoby: *Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, 2006, p. 32.

[48] Jacoby: *Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, 2006, p. 32.

[49] The author was not able to locate an English translation of the Census Act like was stated in section 1.2 but has used a translation of the Census Decision by Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 112-116, where the judges comment on the Act.

income, occupation, education, means of transport, time commuting, employment, working hours, status as patients or staff members of institutions, and much more.[50]

Section 9 of the Act permitted a comparison of data from the 1983 Census with the residence registry and the latter could be corrected if necessary. It also permitted anonymous data to be transmitted and shared with other authorities for statistics and community planning or for scientific purposes.

Section 10 of the Act was about the information duty on the citizens. Section 11 had various provisions such as regarding statistical secrecy and the duty of early erasure.[51]

## 4.2 The Census Act Decision in Short

### 4.2.1 The Claims of the Complainants

The complainants had gotten an injunction which suspended the execution of the census.[52] The complainants claimed the Census Act violated several basic rights like the rule of law principle[53] (no. rettssikkerhet, de. Rechtsstaatsprinzip), the norm-clarity and precision principle, and because statistics and administrative actions were combined. They also based their case on the statement that "re-identification of personality-related data under modern conditions of data processing poses no difficulty"[54] and that wide and obscure terms in the Census Act could lead to unconstitutional use of data amongst other things.

### 4.2.2 The Government's Defence

The Federal Government along with some Länder's Governments,[55] hereby called the defendant, claimed amongst other things that the Census Act of 1983 was constitutional and serving statistical purposes. It guaranteed that data collection,

---

[50] Riedel: *FCC,K*, HRLJ, vol. 5, No. 1, 1984, p. 95.

[51] Riedel: *FCC,K*, HRLJ, vol. 5, No. 1, 1984, p. 96.

[52] Injunction by the Federal Constitutional Court from April 13th, 1983, 1 BvR 209,

[53] The rule of law principle involves that governmental and/or public authority can only take their decisions and use their power in accordance with written and published statutes.

[54] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 96.

[55] Germany has had a federal system since 1949 and has a Federal Parliament and Federal Constitutional Court. The country is divided into 16 Länder that each have its own Government and Parliament. Further information can be found in Gunlicks: *The Länder and German Federalism*, 2003.

storage, and transmission were anonymous.[56] The defendant claimed that the legislator had a margin of appreciation and the Census Act did not violate the basic principles the complainants claimed.

### 4.2.3 The Court's Decision

The Court went through all the claims of the complainants and decided that many of the claimed violations were in fact not unconstitutional. For example it was found legitimate to ask for information about the citizen's religion and such a question did not violate the fundamental right of freedom of religious belief.

The Court did find the provisions of Sec. 9(1) – (3) of the Census Act unconstitutional and void. It violated Art. 2(1) in conjunction with Art. 1(1) of the Basic Law (de. Grundgesetz –GG). Art. 2(1) states: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law."[57] Art. 1(1) of the Basic Law states "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority."[58]

The Court concluded that the general right to the free development of one's own personlity or general personality right (de. allgemeines Persönlichkeitsrecht) led to individual self-determination on deciding when actions were to be taken or to be omitted in the informational aspect. In other words, the right to decide for oneself when and within what limits personal information and facts should be disclosed to others, i.e. informational self-determination (de. Informationelle Selbstbestimmung).[59]

The Court limited its discussion of the right to informational self-determination to the applicability and possible utilization of the personal data the Census Act required the German population to give. In that connection the Court examined the purpose of the Act and the possible processing by information technology. The Court stated: "Thereby a particular datum, insignificant on its own, may assume a new order of

[56] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 97.

[57] Translation from the German Basic Law Art. 2(1).

[58] Translation from the German Basic Law Art. 1(1).

[59] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 100.

magnitude; under conditions of automatic data-processing, 'insignificant' data thus no longer exist."[60]

The Court mentioned that data collection and processing for statistical purposes was very important for state policy and planning and could not be too narrowly defined. On the other hand, limitations had to be specified within the given information system.[61] The Court went on and said: "...censuses tend to carry with them the inherent danger of personality-hostile registration and cataloguing of individuals..." and therefore the Court stated there was a need for special provisions to protect the general personality right of those who were obligated to participate in the census, the data subjects.[62]

The Court said that the legislator should consider if the aims of the census, in some circumstances, could be met if the data subjects were anonymous and their identity not traceable. Then it took an example that a warden at a mental hospital could give the necessary statistical information about the patients without identifying them.

It stated that only when suitable safeguards were in place should public authorities be allowed access to the data for the objective of planning.[63]

The Court found that the comparing of the Census to the existing residents registry for correction of the latter in Sec. 9(1) was unconstitutional since it infringed the right to informational self-determination. It found the provision too obscure in content since it was not only for statistical objectives but for administrative action, which was without any purpose limitation.[64]

The Court found that the transmission allowed to other public authorities in Sec. 9(2) also infringed the right to informational self-determination because of obscurity. The provision did not state a clear objective with the transmission and without that, it was hard to predict if the transmission was within the objective's limitations.[65]

The Court found the permission for local authorities to use anonymous personal data for regional planning etc. in Sec. 9(3)1 infringed the right to informational self-

---

[60] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 102.

[61] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 103.

[62] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 104.

[63] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 104.

[64] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 112.

[65] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 113.

determination because of obscurity. The provision did neither state clearly if the personality-related data could also be used for administrative execution, nor did it define clear objectives. Infringement of the right to informational self-determination was also violated with Sec. 9(3)2 of the Census Act. This provision limited local authorities' use of personality-related data to "statistical processing." This expression was found to be too obscure and imprecise also when considering that local authorities usually have additional knowledge that could easily lead to identifiability for individuals.[66]

The transmission of data for scientific purposes to persons in civil service allowed in Sec. 9(4) of the Census Act was on the other hand found to be constitutional. The provision was clear on limitations, names and addresses were to be omitted from the transmission and the objective was specific enough.[67]

[66] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 114.

[67] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 115.

# 5 Comparison of the Health Sector Database and Census Act Decisions

## 5.1 Comparison of Formality

There is a major formality difference in the two cases. The Icelandic case was a private suit, one plaintiff seeking the annulment of the Directorate's decision regarding her affairs. Nevertheless the Court's decision could be relevant for other cases.

The complainants in Germany on the other hand could file a suit directly to the Constitutional Court claiming the Census Act unconstitutional. They did not have to "wait for executive action in subsequent legal redress based upon that statute."[68] The Constitutional Court had the power to nullify provisions that were found to be unconstitutional.

## 5.2 Political Controversy of the Acts

The Census decision was bold at the time. The Federal Government of Germany had spent vast amount of time and finances preparing to carry out the 1983 census.[69] The nation was divided. Many citizens found the census too privacy intrusive but others did not mind assisting the government and public agencies in their collection for statistics.

The Health Sector Database decision was also bold. Vast amount of time and finances had been put into the design of the database and preparation for its operation. The nation was also divided in their opinion. Many citizens found the idea of collecting a whole nation's medical records in a centralized database, operated by a private company for financial profit, controversial. Others were happy to contribute to scientific research that would be advantageous for mankind. The different conclusions of the District Court and the Supreme Court show very well the controversy of the Act.

The criticism of the Health Sector Database Act in the decision had in effect similar impact as in the German decision. The projects became postponed, at least for a while,

---

[68] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 98.

[69] Riedel: *New Bearings in German Data Protection*, HRLJ, vol. 5, No. 1, 1984, p. 68.

because the legal foundation was not solid. The postponement lasted a few years in Germany until a new and improved Census Act was accepted by the parliament in 1987.[70]

The Icelandic Supreme Court's decision came as the final blow and the Health Sector Database never left the designing board.

### 5.3 The Time Factor

The timing of the decisions also deserves consideration. The Census decision was made in 1983 or a number of years before the enormous impact of the Internet. The Federal Constitutional Court of Germany showed precaution and acknowledged possible use and misuse of collected data in the future, especially regarding data transmission to other agencies. The Court emphasized that informational self-determination needed protection because of present and future automatic data processing.[71]

The Health Sector Database decision was made twenty years later when nearly every business and home in Western-Europe had gained Internet access. The possible threats of data collection, transmission, merging, and linking were no longer in the far-fetched future but were real and in the present.

### 5.4 Decisions Based on National Constitutional Rights Only

Both Courts found a breach of fundamental rights protected by their country's constitution. The Icelandic Supreme Court only relied on and referred to the Icelandic Constitution but the District Court mentioned Art. 8 of the Convention, Art. 17 of the ICCPR and the EU Data Protection Directive. Neither the Icelandic nor the German Courts referred to the national Data Protection Act.[72] The German Federal Constitutional Court also relied only on the German Basic Law.

---

[70] Schwartz: *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 1989, p. 700.

[71] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 100.

[72] Icelandic Data Protection Act no. 77/2000 and the Federal Data Protection Act in Germany from November 15, 2006.

The Health Sector Database decision has been criticized for not solving the case with reference to relevant European instruments.[73] It seems to the author that, the Icelandic Court did not feel it was necessary to refer to international instruments since Art. 71(1) of the Constitution applied to the violation at hand. The author thinks it would only have strengthened the Court's decision if it had referred to the case law of the European Court of Human Rights. The Federal Constitutional Court in Germany also relied only on national instruments but one has to keep in mind that in 1983 information privacy case law from Strasbourg was not developed as it is today.

### 5.5 Importance of Correct Information

Another difference between the two cases was how and from whom the personal data was collected. Like has been said before, the Census Act laid upon the German citizens information duty. Everyone had to fill out a detailed questionnaire and was obligated to give correct answers.[74] The Federal Constitutional Court weighed the possibility of data subjects deliberately giving wrong answers, which could be destructive for statistics and the common good of society (de. Gemeinwohl). The Court concluded that obscure purpose provisions especially about future use of the information could make that possibility more likely.[75]

The European Court of Human Rights addressed the importance of information privacy in context to the common good of society in Z v. Finland:[76] "It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community."

In the case of the Icelandic Health Sector Database, personal information was to be collected from health institutions and self-employed health workers and not directly

---

[73] Gertz: *An analysis of the Icelandic Supreme Court judgement on the Health Sector Database Act*, 2004, sections 5.2 and 5.4

[74] Riedel: *FCC, K*,HRLJ, vol. 5, No. 1, 1984, p. 108.

[75] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 105.

[76] Z v. Finland, 1997-I Eur. Ct. H.R, para. 95.

from data subjects. There was greater separation between the data subjects and the database than in the Census case. The data subjects in Iceland were more likely from the beginning to give correct information because the personal data was being collected in relation with the data subject's personal health. Also because there was an opt-out option in the Health Sector Database Act, data subjects could take advantage of it and did not need to withhold information in fear of their data being used in the Health Sector Database. Some people still had doubt, because in fact the whole nation's health data was to be collected. Data for subjects that had opted-out were then to be removed before the data subjects became unidentifiable.

### 5.6 Legitimate Access to the Data

The legitimate access was different in the two cases. The Census Act only allowed access of government and public authorities. The legislator had accepted the Census Act for the purposes of collecting data for governmental and regional statistics and planning. The personal data was not intended to be disclosed to private companies and the census was not intended to give financial profit. The census was being paid for by federal funds.[77]

In Iceland, however, the Health Sector Database Act is first and foremost giving a private company a licence to collect and process personal data. The licensee is permitted by Art. 10(4) to use the Health Sector Database for purposes of financial profit, under conditions laid down in the legislation and the licence. Although Art. 9 of the Health Sector Database Act does ensure the Ministry of Health and the national Directorate of Health access to statistical data for purposes such as policy-making and planning. This access is to be free of charge and is an example of conditions that has to be fulfilled to get and to keep the licence. The making, operation, and monitoring of the Health Sector Database is to be paid for by the licensee according to Art. 4 of the Act.

Has this difference possibly had any effect on the two decisions? The Federal Constitutional Court found it necessary to have clear provisions on content and to have purpose limitations so the government and public agencies had strict guidance to follow.

---

[77] Riedel: *New Bearing in German Data Protection*, HRLJ, vol. 5, No. 1, 1984, p. 74.

There is no reason why data subjects would need less protection of their right to privacy and their right to informational self-determination because the data controller and data processor, is a private firm instead of a public authority, as was the case in the Health Sector Database decision. In the author's view, data subjects would perhaps need even more protection than if the data controller and/or data processor were purely governmental. The reason for this is that it can be even harder to monitor and supervise the actions of private parties. One reason that contributes to this difference is the concept of freedom of information. Many countries around the world have implemented an Act on freedom of information which gives public access to governmental records.[78] A Freedom of Information Act puts pressure on governmental and public bodies to comply with the rule of law at all times. Of course the Data Protection Authority and possibly other monitoring bodies are to monitor and inspect all data controllers and data processors alike, from public and/or private market.

## 5.7 Differentiation of Purpose for Collected Data

The Federal Constitutional Court emphasized the differentiation of data collection for the purpose of statistics versus administrative action. The Court stated that statistics were of great value for state policies and planning and therefore data collected for those purposes could not be too narrow or limited. On the other hand because of difficulty assessing in advance the possible utilization and linkage it was necessary to define unambiguously the processing conditions within the information system.[79] Because of the danger of cataloguing of data subjects that were obligated to take part in the census, data collection and processing for statistical purposes needed special provisions protecting the general personality right and the right to informational self-determination of the data subjects.[80] In the opinion of the Court, the legislator had to investigate if there were ways of meeting the objective of the census while securing unidentifiability of the data subjects.[81] Personal data was identifiable at least at the time of the collection

[78] A German Freedom of Information Act was enacted on January 1, 2006. An Icelandic Freedom of Information Act no. 50/1996 was enacted on January 1, 1997. For more information see www.freedominfo.org

[79] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 103.

[80] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 104.

[81] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 104.

and maybe longer. The Court found suitable safeguards were especially essential with statistical censuses and data had to be made anonymous as soon as possible. Data subjects could not be expected to obey the information duty without suitable safeguards.[82]

The Federal Constitutional Court said that it would infringe the right to informational self-determination if the personal data collected for statistical purposes by law would be identifiable when transmitted and used for administrative action.[83] The Court then went on and stated that different conditions and/or emphasis were of concern when collecting data for statistical purposes versus administrative purposes. Thereby, a statute trying to combine both purposes was unsuitable and unconstitutional. It would lead to obscurity of the norm and involve disproportionality.[84]

In this respect the Health Sector Database decision had similar issues at hand. The Health Sector Database Act was meant to include data collection for the purpose of statistics on the one hand and scientific research on the other. Even though the latter was not administrative action it was a totally different purpose that presumably needed different conditions and/or emphasis to be fulfilled. More procedural mechanisms were needed in the Act to safeguard the right to privacy of the data subjects, in the opinion of the Supreme Court. The merger of the Health Sector Database that was mentioned in Art. 10(2) of the Health Sector Database Act probably influenced what the Supreme Court felt were too obscure purpose provisions which directly led to the infringement of privacy as protected by Art. 71 of the Icelandic Constitution.

## 5.8 The Value of On-line Data Access

The Icelandic Supreme Court advised that legislation should not entail a real risk of unauthorized access to personal information, either to public or private parties.[85] It is interesting that the Court made such a statement without actually going into any depth of the matter. The Court did not answer the question of what is a real risk of unauthorized access.

---

[82] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 104. The concept of suitable safeguards will be discussed further in section 5.12.3.

[83] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 110.

[84] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 111.

[85] ISC, case 151/2003, p. 4160.

In this context it is of relevance to look at Art. 10(4) of the Health Sector Database Act where it says: "The health service database may not be transported out of Iceland, and processing of it may only be carried out here in Iceland." Art. 10(3) of the Health Sector Database Act, says: "The licensee may not grant direct access to data in the database." By reading these provisions, one is inclined to presume that the legislator did not have in mind that the Health Sector Database would be accessible on the Internet. Despite this, the licensee did ask the Icelandic Data Protection Authority for permission of on-line access to the Health Sector Database, later in the designing stage. The first draft of the Bill mentioned the possibility of on-line access to the database.[86] This provision was then abandoned in the final version of the Bill. When questioned by the Data Protection Authority, the Icelandic Health Ministry answered that they did not feel the omission of this clause by the Parliament was an indicator that on-line access was to be forbidden.[87] Then the legislator would have made a clear prohibition on on-line access. The Health Ministry also stated that in their opinion, the provision in article 10(3) where direct access is prohibited, did not cover on-line access. Finally the Ministry concluded that it was up to the Data Protection Authority to decide if the design and procedures complied with the law.[88] This debate was public and covered by the Icelandic press and took place the year before the Supreme Court heard the case.

It is possible that the debate on on-line access of the Health Sector Database had effect on the Icelandic Supreme Court's assessment on what was a real risk. Especially because the Health Sector Database Act permitted merging of the Health Sector Database with a database of genealogical data and a database of genetic data in Art. 10 of the Act. The impact and value of accessibility of data on the Internet should not be underestimated. It makes data retrievable all over the world in seconds and it makes transmission, merging, and linking of data very easy compared to manually collected and stored data. Not to mention possible higher risk of unauthorized access, including hacking.

The permitted merger results in less predictability of future use of the data. Obscure purpose provisions can infringe the right of informational self-determination, like the

---

[86] *Annual Report 2002*, The Icelandic Data Protection Authority, section 3.2.3.

[87] *Annual Report 2002*, The Icelandic Data Protection Authority, section 3.2.4.

[88] *Annual Report 2002*, The Icelandic Data Protection Authority, section 3.2.4.

Census decision showed. Even though there was no debate on on-line access when the Census decision was made the Federal Court showed great deal of precaution and considered possible future threats of automatic processing of data. Transmission of data to other agencies needed clear purpose provisions and could not be unlimited. These precautionary measures were taken at a time when on-line data accessing was not even an issue.

### 5.9 A Right to Refuse Participation

The Census Act Section 5 obligated German citizens to participate in the census.[89] They had to give their personal information or else face punitive sanctions. There was no permission to opt-out. One of the many reasons the census was being done was to register how many voting adults were in each of the Länder.[90] This reason alone gives clarification on why opting-out was not a possibility.

An obligation to participate in a census is an infringement of the right of informational self-determination. The Federal Constitutional Court, on the other hand, found it justifiable and proportionate to the public interests at stake. One can wonder if the lack of an opt-out option for the data subjects had an effect on this decision and if that should lead to a stricter protection. In the author's opinion it should not matter if the personal data was given because of pure obligation, with the free will of those opting-in, or the passivity of those not opting-out. Fundamental rights of the data subjects should always get equal protection.

In the case of the Health Sector Database things were different. In the first Bill all Icelanders, living or deceased, were obligated by law to participate in the database.[91] The Act on the other hand did permit opting-out of the database.[92]

The author doubts that the first draft, without a right to refuse participation, would have been found constitutional. Because even though governmental bodies were to get access to the database for the purpose of statistics and planning, the main function of the Health Sector Database was to be a research tool in the hands of a private company. The licensee bore financial responsibility and was allowed to gain financial profit from

---

[89] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 106.

[90] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 95.

[91] Cf. Bill on a Health Sector Database, document no. 109, 1998, comment on Art. 8.

[92] Health Sector Database Act, Art. 8.

the database. There were no reasons of immediate public interests at stake, such as in the Census case, that could justify such an infringement of the right to informational self-determination. In the author's view that would have failed the balancing test.

Why was there only an opt-out possibility for the data subjects in the Health Sector Database Act and not a provision about opting-in to the database? The case of the Health Sector Database involved almost exclusively health information. Art. 8(1) of the EU Data Protection Directive basically forbids processing on various sensitive information such as health information. Then Art. 8(2) covers exceptions to this rule. Art. 8(2)a specifies that the data subject has to give explicit consent for processing of health information. Is the passivity of those that do not take action by opting-out of the database "explicit consent" enough to be regarded as fulfilling the conditions of Art. 8(2)a? This is an issue that the Icelandic Supreme Court did not address in its decision on the Health Sector Database but is relevant to the question of informational self-determination.[93]

Consent is very much related to a right to informational self-determination. The definition of consent and what is to be interpreted as consent is therefore of relevance. This issue was addressed in a recent working document from the Article 29 Data Protection Working Party, about personal data processing in electronic health records (EHR). Unfortunately the discussion was rather ambiguous. First they state: "...consent in the case of sensitive personal data and therefore in an EHR must be **explicit**. Opt-out solutions will not meet the requirement of being 'explicit'."[94] Then in a chapter about respecting self-determination they say: "The functionality of 'agreeing' in the context of suitable safeguards is different from 'consent' under Article 8(2) of the Directive and therefore needs not meet with all requirements of Article 8(2): e.g. whereas **consent as a legal basis** for processing health data would always have to be 'explicit' according to Article 8(2), **agreement as a safeguard** need not necessarily be given in form of an opt-in – the possibility to express self-determination could – depending on the situation

[93] Cf. Discussion on the issue of consent in Gertz: *An Analysis of the Icelandic Supreme Court Judgment on the Health Sector Database*, 2004, sections 4.2. and 5.1.

[94] Article 29 Data Protection Working Party: *Working document on the processing of personal data relating to health in electronic records (EHR)*, 2007, p. 9.

– also be offered in form of an opt-out/ a right to refuse."[95] Then the Article 29 Data Protection Working Party continues by suggesting that it should be a rule, in an Act covering EHR system, that the data would be "governed by an incremental system of 'opt-in' requirements (especially when processing data, which are potentially extra harmful such as psychiatric data, data about abortion, etc.) and 'opt-out' possibilities for less intrusive data."[96]

The guidance given by Article 29 Data Protection Working Party is not as clear as one had hoped and in the author's view rather contradictory. Many questions are left unanswered such as: How will such filtering be done of "extra harmful" versus "less intrusive" data and who will supervise it?

## 5.10 Informational Self-Determination in the Census Act Decision

The Federal Constitutional Court discussed how the possibilities in automatic data processing could give new meaning to data that before might have been insignificant on its own but when linked with other data collections could give a partial or a complete personality profile (de. Persönlichkeitsbild).[97] If the data subject did not know what data was stored about him/her, when and how it would be used, and by whom, it affected his/her right to decide freely and without pressure which information to give. This would be where self-determination comes in. The Court found it was "...a prerequisite of free development of the personality under modern conditions of data processing, the individual needs protection against unlimited collection, storage, application and transmission of his personal data."[98]

It is interesting in this respect to look at the role the German Federal Constitutional Court is taking. The Court seems to feel it is necessary to protect individuals in this fast-evolving computer age where there is no way of knowing how conditions of data processing will develop. Here the emphasis should be on the word unlimited. The Court found a need for limiting personal data processing by demanding

---

[95] Article 29 Data Protection Working Party: *Working document on the processing of personal data relating to health in electronic records (EHR),* 20007, p. 13-14.

[96] Article 29 Data Protection Working Party: *Working document on the processing of personal data relating to health in electronic records (EHR),* 20007, p. 14.

[97] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 100.

[98] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 101.

unambiguous provisions, clear purpose, and suitable safeguards. The Court was basically using the "in accordance with the law" criterion of the European Court of Human Rights, that is explained further in section 5.12.4.

### 5.10.1 Limitations on the Right of Informational Self-Determination

The Federal Constitutional Court stated that the right to informational self-determination was not without limitations because it needed to be in balance with important public interests.[99] Those interests could be for example necessary statistics for planning purposes such as health care, transportation, education system, national economy, or anything that serves the public common good. According to the Court all limitations had to be in accordance with basic principles such as the rule of law, of clarity and proportionality.[100]

The private interests of the individual for his/her right to informational self-determination are weighed against public interests to find out which are the predominant interests in each case. Even though public interests are found to prevail, certain measures must be taken to keep the infringement of the general personality right and the right to informational self-determination to its minimum or in proportion with the interests at stake. Therefore the legislator has a duty to implement procedural and material safeguards like the Census Act decision showed.[101] The concept of suitable safeguards will be addressed in more detail in section 5.12.3.

This balancing test the Federal Constitutional Court refers to is in fact very similar to the balancing test which is found in Art. 8(2) of the European Convention on Human Rights.[102] The rights that Art. 8(1) of the Convention ensures can only be interfered with if these conditions are fulfilled: a) in accordance with the law, b) necessary in a democratic society and c) one or more certain important public interests that are listed in the Article are in place, such as public safety and prevention of crime. The European Court of Human Rights in Strasbourg always uses this balancing test to

---

[99] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 101.

[100] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 101.

[101] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 102.

[102] More information on human rights limitations can be found for example in Jacobs and White: *The European Convention on Human Rights*, 2006, p. 218-240; Kilkelly: *The Right to Respect for Private and Family Life*, 2001, p. 23-30.

search for justification, when applying Art. 8 in their cases.[103] When evaluating what is necessary in a democratic society, the Court in Strasbourg relies on the principle of proportionality.[104] The Strasbourg Court examines if there has been "a pressing social need" and if the interference has been "proportionate to the legitimate aim pursued" for an interference to be found justifiable by Art. 8(2) of the Convention.[105]

### 5.11 Informational Self-Determination in the Health Sector Database Decision

The Supreme Court, in the Health Sector Database decision, relies solely on Art. 71(1) of the Icelandic Constitution, which is very similar to Art. 8(1) of the European Convention on Human Rights beside the special reference to correspondence, which is in Art. 71(2).[106] The Supreme Court did not directly refer to a violation of a right to informational self-determination.

Extensive amounts of information concerning patients' private life are gathered in most medical records. Some of the information is sensitive data in the meaning of Art. 8(1) of the EU Data Protection Directive.[107] The Icelandic Supreme Court gave general advice to the legislator to be careful that statutes would not result in a real risk of such information getting into the hands of irrelevant third parties.[108] This would be a referral to the necessity of suitable safeguards as in Art. 8(4) of Data Protection Directive.[109]

---

[103] Kilkelly: *The Right to Respect for Private and Family Life*, 2001, p. 9.

[104] *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, p. 747. For more information about the limitations of Art. 8-11 of the Convention see: *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, chapter 5.

[105] Bygrave points out that the necessity/proportionality criterion of the Convention overlaps with the "in accordance with the law/quality of law" criterion in his article: *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, vol. 6, 1998, p. 274. The "in accordance with the law/quality of law" criterion will be addressed in section 5.12.4 about clarity of legal framework.

[106] Art. 71(2) of the Icelandic Constitution: "Bodily or personal search or a search of a person's premises or possessions may only be conducted in accordance with a judicial decision or a statutory law provision. This shall also apply to the examination of documents and mail, communications by telephone and other means, and to any other comparable interference with a person's right to privacy."

[107] Art. 8(1) of Directive 95/46/EC: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

[108] ISC, case 151/2003, p. 4160.

The Supreme Court stated that the legislator had to ensure, as much as possible, that the information was unidentifiable.[110] In the Census Act decision suitable safeguards, such as ensuring unidentifiability were mentioned as a prerequisite of the right to informational self-determination.[111]

In the opinion of the Icelandic Supreme Court, the Health Sector Database Act was obscure on the suitable safeguards the state was obligated to provide the data subjects. The Icelandic Supreme Court emphasized that unidentifiability of the data subjects was not ensured in regards to automatic processing and linking that were authorized in Art. 10(2) of the Health Sector Database Act by permitting the merger of the three databases.[112]

The author presumes the Court could have drawn from this provision a separate right of informational self-determination on the same grounds as the Federal Constitutional Court did. It depends on the definition of privacy used. Informational self-determination should fall within the concept of privacy as for example Westin defined it,[113] just as free development of one's personality and respect for human dignity falls within the concept of private life as the European Court of Human Rights interprets Art. 8 of the Convention.[114] It seems as one of the Icelandic Supreme Court's main arguments was that the data subjects could not be sure that their health data was in fact not traceable to them and what the merger of the Health Sector Database with the two other databases could inflict on their interests. The Supreme Court did not go into the meaning of this for the data subjects in relation to what kind of consent was

---

[109] Art. 8(4) of Directive 95/46/EC: "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."

[110] ISC, case 151/2003, p. 4160.

[111] Riedel: *FCC,K* HRLJ, vol. 5, No. 1, 1984, p. 104.

[112] ISC, case 151/2003, p. 4161.

[113] Westin: *Privacy and Freedom*, 1967, p. 7.

[114] For examples of the European Court of Human Rights acknowledging the right to freely develop one's own personality see: Botta v. Italy, 1998-I Eur. Ct. H.R, para 32; X v. Iceland, Application No. 6825/74, D.R. 5 p. 86, European Commission of H.R.

necessary.[115] Perhaps the Court did not feel that was necessary since the Court concluded it was a breach of the constitutional right to privacy. In the author's view, the risk factor of identifiability could have influenced the citizens' chances of taking a well founded decision when deciding to opt-out or allowing their data to be registered into the Health Sector Database. The fear of identification could even have influenced what patients revealed to their doctors knowing that the information would end in the Health Sector Database. These are also undesirable results for society as a whole, because of increased risk of inaccurate statistics and/or danger to common health for example if a data subject keeps a serious contagious disease a secret. A risk of identifiability is closely connected to informational self-determination.

### 5.11.1 Expanded Right to Informational Self-Determination

It seems that the Health Sector Database decision may have expanded the right to informational self-determination in an interesting and a controversial way. An individual can use it not only for the protection of his own personal data but also personal data of his/her close relatives. The Icelandic Supreme Court mentioned it specifically as an argument that the Health Sector Database Act did not prohibit in so many words that people could opt-out their passed away parents.[116] The Court thereby overlooked what was stated in the preparatory work by the legislator, that opting-out close deceased relatives was not presumed an option.[117] Health data of deceased citizens were anticipated to be stored in the database.

The author presumes what was of relevance in this particular case was the factor of unpredictability for the data subjects with regards to the merging of the Health Sector Database with the databases of genetic information and of genealogical information. The Supreme Court concluded that the Act did not ensure the necessary suitable safeguards.[118] Iceland has a small population of about 300.000[119] and almost everyone is related depending on how far back one looks in the family-trees. The genealogical database consists of all Icelanders living and deceased that have been registered in

---

[115] See discussion on consent in section 5.9.

[116] ISC, case 151/2007, p. 4162.

[117] Cf. Bill on a Health Sector Database, document no. 109, 1998, comment on Art. 8.

[118] ISC, case 151/2007, p. 4160.

[119] Cf. http://www.iceland.is

church books and public records many centuries back. The database of genetic information consists of bio-samples that about 65% of adult Icelanders have donated for research, with informed consent.[120] By the merge of these three databases, in a small society like Iceland, it is a likely reasonable possibility, that even if you opt-out of the Health Sector Database, you might be identifiable as the only "one missing" in the family tree and some conclusions might be drawn about you such as odds of genetic diseases that run in your family. At least that seems to be the conclusion of the Icelandic Supreme Court. The Article 29 Data Protection Working party has said in relation to genetic data: "In this context, questions arise as to whether or not genetic data belong exclusively to the single, specific individual from whom they are collected, and to whether family members have the right to access to such data even in the absence of the individual's consent." The Article 29 Data Protection Working Party suggested that the issued needed to be resolved on a case by case basis, weighing all interests.[121]

The plaintiff in the Health Sector Database decision wanted to opt-out her late father because of such concerns. The risk of this being possible is the same, for the data subject that wants to opt-out, that has all of his/her close relatives alive or if one or all are deceased. It is a statement of this thesis that this is truly an expansion of the individual's right to informational self-determination. Gertz has criticised this as an undesirable result by the Icelandic Supreme Court.[122] Gertz asked if Icelanders are so genetically homogenous as proclaimed then should not the same legal standing be given to every Icelander? Gertz rightly points out, the reasoning of the Court leads to the question if every Icelander can then sue and demand that their living close relatives would opt-out of the Health Sector Database. The Supreme Court did not answer this question but the author presumes it is because of the individual's own right to informational self-determination that those living relatives can decide for themselves if they want to opt-out or not. It would be a personal decision protected by Art. 71(1) of the Icelandic Constitution. Although the results remain that a data subject that has opted-out, when his/her living close relatives have not, is more vulnerable than the data

---

[120] Caplan: *Kari Stefanson,* Time, 2007.

[121] Article 29 Data Protection Working Party, *Working Document on Genetic Data*, 2004, p. 8.

[122] Gertz: *An Analysis of the Icelandic Supreme Court Judgment on the Health Sector Database*, 2004, section 4.1.

subject that has opted-out and used his/her expanded right of informational self-determination to opt-out his/hers deceased close relatives as well.

It seems that the main reason was to find a legal justification for giving the plaintiff a formal status as a rightful party to filing the suit without much thought to the meaning of this reach of a person's right to informational self-determination to the informational sphere of other individuals. It is uncertain if the Icelandic Supreme Court was intentionally expanding a right to informational self-determination but the decision leads to the conclusion that the death of an individual's close relative does seem to give the individual expanded private interests in the relative's health information.

## 5.12 Further Analysis of the Right to Informational Self-Determination

### 5.12.1 Reasonable Expectations of Data Subjects

The Federal Constitutional Court in Germany concluded that a few provisions in the Census Act were lacking objectives and were obscure of content. This infringed the data subjects' right to informational self-determination and was found unconstitutional.[123] Materially this was regarding unclear boundaries between statistics and administrative execution and transmission permission to other public authorities and their utilization of the data.[124] The state had to make sure that the use of the personal data collected for the census was at least within reasonable expectations of the data subjects. The nature of those expectations depends on clear objectives and limitations. Section 5 of the Census Act laid an information duty on the data subjects but the Court pointed out that without the state's assurance of suitable safeguards, such as unidentifiability, the data subjects would not be prepared to give truthful statements.[125] If it was unclear for what purpose the personal data would be used and to what authorities personal data could be transmitted, then the data subjects would not trust the census and perhaps give incorrect answers.

In the case of the Health Sector Database decision the District Court referred to a reasonable expectations test and concluded that the data subjects had reasonable

---

[123] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 112-114.

[124] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 113.

[125] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 105. Importance of correct information was discussed in sesction 5.5.

expectations of unidentifiability in the sense of the law, since it was the assessment of the Court that the health data could not be traced to certain individuals at least without considerable efforts.[126] The Supreme Court still assessed there was a risk of unauthorised access and the data subjects could not be sure of unidentifiability since suitable safeguards were not in place.[127]

The reasonable expectations of data subjects in context to their privacy are always a matter of an assessment in each case.[128] Guidelines and precedence can be found in the case law of the European Court of Human Rights in Strasbourg. The Strasbourg Court seems first to have used the reasonable expectations test for assessing privacy in the case Halford v. United Kingdom from 1997.[129] The case Peck v. United Kingdom concerned personal data processing without the consent of the data subject.[130] The Strasbourg Court concluded that Peck could claim a partial expectation of privacy even though he could not reasonably expect absolute privacy. A recent case is von Hannover v. Germany where the reasonable expectations test seems to have gotten to a stage that it was applied without much explanation. The Strasbourg Court concluded that the photos of von Hannover in her daily life fell within the scope of Art. 8 of the

[126] ISC, case 151/2003, p. 4180.

[127] ISC, case 151/2003, p. 4160.

[128] Detailed discussion on the reasonable expectations test in the case law of the European Court of Human Rights can be found in an article by Gómez-Arostegui: *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, 2005.

[129] Halford v. United Kingdom, 1997-III Eur. Ct. H.R. Halford, the highest ranking female police officer had been repeatedly denied further promotion. She complained about gender discrimination and that her private and work related phone calls in her office had been tapped. The Court concluded she had reasonable expectations of privacy using the telephones in her office. Another more recent decision concludes that an employee should also have reasonable expectations of privacy of e-mail and internet usage as long as no warnings about monitoring have been given, see Copland v. United Kingdom, 2007-IV Eur. Ct. H.R.

[130] Peck v. United Kingdom, 2003-I Eur. Ct. H.R. A video footage from a public-surveillance system, of Peck contemplating suicide on a public bridge, was shown on television and pictures published in newspapers. The court concluded even though Peck could not expect privacy in a public place, these consequences were not reasonably to be expected.

Convention and she should have had a "legitimate expectation of protection of her private life."[131]

### 5.12.2 Data and Identifiability

The Federal Constitutional Court stated that the unpredictable future use of the collected data was a violation of the general personality right and an "informational infringement."[132] However, citizens had to accept this since public interests, statistics for planning purposes etc., outweighed the private interests.[133]

The Court emphasized that collecting personal data for the purpose of statistics and even transmitting it to other authorities was per se not unconstitutional if the data was unidentifiable. The requirement was to remove data subject's identity as soon as possible.[134]

Similar applied to the Health Sector Database decision. The Supreme Court emphasized that the legislator had to address how unidentifiability was to be ensured in the Act itself and not left to be decided later. It was insufficient to give the licensee leeway to develop rules on confidentiality even though the Data Protection Authority should supervise the work.[135] In Art. 10(2) of the Health Sector Database it says: "The licensee shall develop methods and protocols that meet the requirements of the Data Protection Commission in order to ensure confidentiality in connecting data from the Health Sector Database, from a database of genealogical data, and from a database of genetic data." The Court pointed that the Act and regulation did not give any more guidance as to what should be included and how the queries should be processed from the merger of the three databases,[136] apart from the final sentence in Art. 10(2) where it says: "It is not permissible to give information on individuals, and this shall be ensured e.g. by limitation of access."

---

[131] von Hannover v. Germany, 2004 Eur. Ct. H.R, para 78. Informative discussion on the von Hannover decision can be found in Gómez-Arostegui: *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, 2005, p. 171-176.

[132] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 106.

[133]Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 106.

[134] Riedel: *FCC, K*, HRLJ, vol. 5, No. 1, 1984, p. 105.

[135] ISC, case 151/2003, p. 4161.

[136] ISC, case 151/2003, p. 4159.

It can be said with good reasoning that the lack of clear objectives, predictability and safeguards in the Act to ensure unidentifiability, was an infringement of the data subject's right to informational self-determination, just like in the Census decision. The Court was in fact using the "in accordance with the law" criterion of the European Court of Human Rights, that will be elaborated in chapter 5.12.4.

Gertz made a valid and an interesting point that the Supreme Court did not touch upon the question whether a decoding key existed of the supposedly unidentifiable data in the Health Sector Database.[137] Gertz pointed out that if it did exist, it would mean that the Health Sector Database would be in violation with the Health Sector Database Act itself and the EU Data Protection Directive, which Iceland must adhere to as a member of EEA. The Court's conclusion was only based on violation of Art. 71(1) of the Constitution. If sensitive health data is not ensured unidentifiability, explicit consent is required according to Art. 8 of the Data Protection Directive. This issue should have been addressed in the Court's discussion.

In this context, take note of Art. 8(1) of the Health Sector Database Act where it states: "A patient may request at any time that information on him/her not be entered onto the health-sector database. The patient's request may apply to all existing information on him/her or that which may be recorded in the future, or to some specific information." This basically means that existing data in the Health Sector Database partially or in whole is to be retrievable by law if and when the data subject wishes. One can ask how that could be done without an existence of a decoding key, making all data subjects identifiable. It seems like a contradiction in the terms of the Health Sector Database Act since in Art. 7(2) it says: "Personal identification shall be coded one-way, i.e. by coding that cannot be traced using a decoding key."

#### 5.12.2.1 Definition of Identifiability

From the discussion above it is clear that definition of identifiability is of utmost importance in both decisions. Art. 2(a) of the EU Data Protection Directive says: "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,

---

[137] Gertz: *An Analysis of the Icelandic Supreme Court Judgment on the Health Sector Database*, 2004, section 4.3.1.

physiological, mental, economic, cultural or social identity." The same definition is used in Art. 3(2) of the Health Sector Database Act.

The defendants in both the Census case and the Health Sector Database case claimed the relevant Acts guaranteed anonymity and unidentifiability of data subjects. In both cases the Courts decided that the legislators had not taken suitable safeguards to ensure unidentifiability. In the Health Sector Database decision it said that only changing ID-numbers for a pseudonym and omit names and addresses was insufficient because so much other personal data could be indirectly identifying. Especially when taking into consideration the permission of merging the Health Sector Database with a database of genealogical data, which has the name, ID number, address of every Icelander and how they are related, and with a database of genetic data, which includes blood samples and DNA of a large part of the Icelandic population.

#### 5.12.2.2 How to Determine Identifiability

Recital 26 of the EU Protection Directive addresses the topic of how to determine identifiability. It says amongst other things: "... whereas, to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; ..."

Bygrave has analysed the term "likely reasonably" and suggested it might introduce a twofold criteria for identifiability that involved assessment of probability and assessment of difficulty. Bygrave also points out what is of legal essence in the EU Data Protection Directive is the *potential* identifiability rather than actually succeeding in identification.[138] Bygrave states that "likely reasonably" usually can not be inclusive of unauthorised and/or illegal access. Because often "...illegal means will be unexpected or unusual means..."[139] so not to be likely reasonably or expected. Still Bygrave interprets the aim of recital 26 such that "the probability criterion should be given priority over the legality criterion in the event of conflict;"[140] Meaning that if a person has capability and illegal access is probable then that should play a significant part in determining identifiability.

---

[138] Bygrave: *Data Protection Law – Approaching Its Rationale, Logic and Limits*, 2002, p. 44.

[139] Bygrave: *Data Protection Law – Approaching Its Rationale, Logic and Limits*, 2002, p. 45.

[140] Bygrave: *Data Protection Law – Approaching Its Rationale, Logic and Limits*, 2002, p. 45.

An information system is only as strong as its weakest link. A data controller for a valuable and extensive database with sensitive personal information surely must anticipate a possible break-in to the database. It is an assessment to what extent the controller must go in ensuring suitable safeguards for unidentifiability. Recital 26 gives a wide range for determining identifiability by referring to "the controller or *any other* person."

In the Health Sector Database decision, the District Court found that cumulative safeguards as listed in section 3.2.2 were satisfactory to determine that data subjects were unidentifiable in the sense of the law, because it was not reasonably likely, without considerable effort, that the data subjects could be identified. The Supreme Court disagreed with this assessment.

### 5.12.3 Concept of Suitable Safeguards

The concept of suitable safeguards has been mentioned repeatedly in previous sections. It is clear that "suitable safeguards" carried considerable weight in both the Census Act decision and the Health Sector Database decision. The Federal Constitutional Court even went as far as stating that suitable safeguards were a prerequisite to the right to informational self-determination as mentioned in section 5.10. It is more difficult for a data subject to insist there has been an infringement of his/her informational self-determination and/or right to privacy if an Act has clear provisions on unidentifiability and suitable safeguards. If the data subject is ensured of unidentifiability by law, his/her private interests weigh less when using the balancing test.[141] This assurance of unidentifiability can turn out to be a weak link such as was seen in the decision of the Icelandic Supreme Court on the Health Sector Database and was discussed in section 5.11.

The European Court of Human Rights has referred to adequate safeguards as a part of the "in accordance with the law" criterion as will be discussed in section 5.12.4. Suitable safeguards have been one of the fundamentals of European data protection for quite a while and now it has been legalized in the EU Data Protection Directive. Although the concept is not defined in Art. 2 among other definitions, it is mentioned and referred to often both in the recitals and in the provisions. The author chooses to use

[141] The balancing test was explained in section 5.10.1.

the term suitable safeguards because that is the term that is most often used in the EU Data Protection Directive. The terms used vary. For example in Art. 6(1)b and 6(1)e it is "appropriate safeguards", in Art. 8(4) and (5) it is "suitable safeguards", in Art. 13(2) it is "adequate legal safeguards". It is uncertain if any special meaning should be interpreted into this variation of term use. The addition of the term "legal" to the "adequate safeguards" in Art. 13(2) can indicate that in other provisions suitable safeguards are not only referring to legal standards but also organizational and technical standards. In Art. 8(5) the terms used are "suitable specific safeguards." By using "specific" instead of "legal" one might interpret it as it were sufficient to have the safeguards specified somewhere else than in statutes. On the other hand, the fact that it is stated in Art. 8, the provision about processing of sensitive personal data, makes that interpretation doubtful since sensitive data are to be subject to stricter rules than other personal data. The Icelandic Supreme Court emphasized the need that suitable safeguards were addressed in the Act and not in the operation license or easily changeable work rules.[142]

Co-ordinated term use gives a more solid definition so perhaps the authors of the EU Data Protection Directive wanted to have some variation in emphasis. Adding a definition of the concept in Art. 2 is something to think about when revising the Directive.

The EU Data Protection Directive adds "subject to suitable safeguards" when permitting an exemption to a rule. It is each member state's responsibility to decide if safeguards are suitable in each case. Both the Federal Constitutional Court in Germany and the Supreme Court in Iceland decided in the cases that are here for analysis that there was a lack of suitable safeguards by each nation's legislator. Appropriate safeguards are a pre-requisite to further processing of personal data for scientific and statistical purpose according to Art. 6(1)b of the EU Data Protection Directive. If suitable safeguards are not in place, the data subjects' fundamental rights can override legitimate interests of the data controller for processing of personal data.[143]

It says in the recitals: "(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered

[142] ISC, case 151/2003, p. 4161.

[143] Cf. Art. 7(f) of the EU Data Protection Directive.

incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;" This recital gives an important clue as to what should be the main aim of suitable safeguards. Which is to ensure unidentifiability of data subjects so their participation will not affect them in any way and their personal data can not be used against them in separate and unrelated matters.

Art. 29 Data Protection Working Party emphasized the need for transparency in an electronic health record system and suggested that the safeguards of such systems should "preferably be laid down in a special comprehensive legal framework."[144] This supports the decision of the Icelandic Supreme Court that the Health Sector Database Act was too open and lacking clear provisions on necessary suitable safeguards. The utilization of the Health Sector Database was in fact only addressed in one provision, Art. 10 of the Act.

### 5.12.4 Clarity of legal framework

At the end of section 5.10.2 attention is drawn to the limitations that are applicable for Art. 8-11 of the Convention. It is necessary to deliberate further on the expression "in accordance with the law" which is mentioned in Art. 8(2) of the Convention. This criterion is in fact about the "quality of law" and not only about being literally in conformity with the law.[145] The European Court of Human Rights examines a) accessibility, b) predictability, and c) adequate safeguards, when assessing the use of this criterion.[146] Meaning that the law must provide adequate safeguards, be accessible for citizens, and formulated in a way that allows citizens to reasonably foresee the consequences of a given action.[147] The Strasbourg Court stated

---

[144] Article 29 Data Protection Working Party: *Working document on the processing of personal data relating to health in electronic records (EHR),* 20007, p. 13.

[145] *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, p. 336. Cf. for example Olsson (No. 1) v. Sweden, 1988, para. 61.

[146] *Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.], 2006, p. 336-337. Cf. for example Leander v. Sweden, 1987, para. 50-57 about the use of the "in accordance with the law" criterion.

[147] Olsson (No. 1) v. Sweden, 1988, para. 61.

in Olsson (No. 1) v. Sweden, that the "in accordance with the law" expression: "...thus implies that there must be a measure of protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by, inter alia, paragraph 1 of Article 8 (art. 8-1)".[148]

In recital 28 of the EU Data Protection Directive it is stressed that the purpose for personal data processing must be explicit and decided at the time of data collection.[149] Art. 10 of the Health Sector Database Act is a rather open provision, for example by allowing a merger of the Health Sector Database with other databases *such as* databases of genetic and genealogical data. The reason for this is probably that the legislator defined the health data unidentifiable and therefore did not regard it as personal data with strict conditions on explicit consent and purpose. The District Court agreed with the legislator but the Supreme Court disagreed.

The analysis so far has showed that the Courts in both the Health Sector Database decision and the Census Act decision used the "in accordance with the law" criterion when they decided that the legal foundation had to be constitutional, unambiguous in purpose and content, and provide suitable safeguards.

[148] Olsson (No. 1) v. Sweden, 1988, para. 61.

[149] EU Data Protection Directive recital: " (28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;"

# 6 Conclusion

As a part of human dignity and a right to freely develop one's own personality, the Federal Constitutional Court in Germany gave sound reasoning that individuals should have a right to decide for themselves what and when they disclose personal information to others. It is not an unlimited right but needs to undergo a balancing test and weighing of interests similar as in Art. 8(2) of the European Convention on Human Rights about the right to private life. Even though there has been an infringement of an individual's right it can be necessary and justifiable to let certain public interests prevail under certain circumstances.

There is emphasis on the existence of suitable safeguards in the statute at hand. The EU Data Protection Directive gives valuable guidelines for assessing what falls within the suitable safeguards term although the Directive would be even more helpful if it were defined clearly.

Implementing suitable safeguards can be difficult like the Health Sector Database decision shows. One can wonder in how much detail it is reasonable to tackle assurance of unidentifiability in legislation. The Icelandic Supreme Court raised the standard from what the District Court felt was sufficient. Without saying it in so many words, the Health Sector Database decision revealed the necessity of interdisciplinary work of lawyers and technicians for statute preparation. This is something that legislators may have to consider even more than ever nowadays and certainly in the future. The law needs to have room for technical development within its provisions and simultaneously have some minimum standard for protecting the fundamental rights of the data subjects. Letting public interest prevail over private interests should only happen if suitable safeguards, legal and technical, are in place.

Both decisions confirm that in order for a statute to be constitutional in regards to informational self-determination and privacy it is of great importance that the collection and processing of personal data has a specific and unambiguous purpose. That is one of

the main rule of data protection law[150] and is implemented in Art. 8(2) of the Charter of Fundamental Rights of the EU.[151]

Then there is the factor of data subject's reasonable expectation of privacy that can and most likely has great impact on the individual deciding to disclose his/her personal information or not. The European Court of Human Rights in Strasbourg began using the reasonable expectations test only 10 years ago. It has still only been used in a handful of decisions so time will tell how valuable that test will be for determining privacy in the future.

The District Court in Reykjavik, Iceland referred to reasonable expectations and gave a detailed description of their opinion what should be regarded as unidentifiable in the sense of the law.[152] It would have been better if the Icelandic Supreme Court had gone through this reasoning of the District Court to give a more solid ground for their opinion of why this was insufficient. Many questions were left unanswered by the Icelandic Supreme Court, such as what involves a real risk of unauthorized access and what would be sufficient suitable safeguards in the opinion of the Court. The Court did not explore the discrepancy in the Health Sector Database Act about one-way-encryption in Art. 7(2) when Art. 8(1) of the same Act gives the data subjects the right to have their already existing and encrypted data erased.

The bottom-line is that the Supreme Court concluded that there had been a breach of the appellant's information privacy. Even though some would think it was far fetched that an individual can reach his/her private interests into the informational sphere of his/her deceased close relatives. The Article 29 Data Protection Working Party has acknowledged this can be problematic in relation to genetic data. It suggests using the balancing test to weigh interests in relation to the principle of proportionality on a case by case basis.[153]

---

[150] Bygrave: *Data Protection Law – Approaching Its Rationale, Logic and Limits*, 2002, p. 61 for a discussion on the principle of purpose specification.

[151] The first sentence of Art. 8(2) of the Charter states: "Such data must be processed fairly and for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law."

[152] ISC, case 151/2003, p. 4181.

[153] Article 29 Data Protection Working Party, *Working Document on Genetic Data*, 2004, p. 9.

The Icelandic Health Sector Database decision did not refer directly to a right to informational self-determination but such a right is implicit in the application of the right to privacy in the decision.

The Census Act decision gave precedence for individuals having a constitutional right to decide for themselves if, what, and when to disclose their personal information subject to limitations. Important European legal instruments confirm this evolution. Citizens in Europe have now, more than before, the opportunity to decide if they want to become data subjects and have the choice to withdraw their consent. It is this author's thesis that informational self-determination can be regarded to fall within the scope of Art. 8 of the European Convention on Human Rights and should become recognized as a fundamental right in additional European countries besides Germany.

In this research, the author only found cases from the European Court of Human Rights in Strasbourg that support this thesis indirectly. There has not yet been filed a complaint based on a breach of informational self-determination which is claimed to be protected by the above Art. 8 of the Convention. On the other hand the author bases this thesis on various clues in recent decisions and EU development. Such as the Court's intent not to give exhaustive definition of private life[154] and emphasis on the right to freely develop one's own personality.[155] A very important clue is to be found in Pretty v. United Kingdom. The terminally ill applicant wanted to get acknowledged a right to commit suicide with assistance since she was too ill to complete it herself. The applicant argued that a right to self-determination was like "a thread through the Convention as a whole" although especially it was Art. 8 of the Convention that conferred it.[156] The Court stated in relation to this: "Although 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."[157]

---

[154] See for example: Pretty v. United Kingdom, 2002-IV Eur. Ct. H.R, para. 61; X and Y v. the Netherlands, 1985, Series A 91, para. 22.

[155] See for example: Botta v. Italy, 1998-I Eur. Ct. H.R, para. 32; X v. Iceland, Application No. 6825/74, D.R. 5 p. 86, European Commission of H.R.

[156] Pretty v. United Kingdom, 2002-IV Eur. Ct. H.R. para. 17 and 58.

[157] Pretty v. United Kingdom, 2002-IV Eur. Ct. H.R. para. 61.

The Court acknowledged personal autonomy as to fall within the protection of Art. 8 but neither included a right to self-determination nor excluded it. This conclusion of the Court must be interpreted with regards to the special circumstances of the Pretty case. The Court in fact did not address the topic of self-determination beside what was quoted above but focused on if a right to die was protected by Art. 8 of the Convention. This case was more about a right to make decisions on one's own actions instead of personal information or in other words about the decision-making aspect of the right to privacy, according to Rehm.[158] Is there or should there be any difference between the right to self-determination in relation to action on the one hand, or information on the other hand, is debatable and outside the scope of this thesis.

Even though the European Court of Human Rights has not addressed the concept of informational self-determination directly the author feels it is only a matter of time until it will in today's information and technology society. After studying recent case law on Art. 8 of the Convention it would not be surprising that under specific circumstances the Strasbourg Court would recognize this right to fall within the scope of Art. 8 on respect for private life, since it is so closely related to a person's autonomy, human dignity, and free development of one's personality. Of course subject to the the balancing test of Art. 8(2) of the Convention.

It is of interest that the Federal Constitutional Court took such a bold decision based on a futuristic vision of automatic processing in modern society and what impact the Court presumed for example data sharing, merging, and profiling could have. This insight can be summarized in these words of the Federal Constitutional Court of Germany: "Insignificant data thus no longer exist."[159] The author agrees with the Federal Constitutional Court's statement that all information can be of significance in some respect. To build and preserve a society of free development of personality, where individuals have a right to privacy and informational self-determination, it is necessary to have boundaries on personal data processing as the term is defined in Art. 2(b) in the EU Data Protection Directive.

---

[158] Cf. section 2.2.

[159] Riedel: *FCC, K*, HRLJ, vol. 5, No 1, 1984, p. 102.

The right to informational self-determination does not have to be regarded as a separate right as long as it is agreed upon that the fundamental right to privacy includes freedom of deciding if, how, when, and to whom an individual discloses his personal information within certain limitations. Other countries should take Germany's precedence and accept it as a fundamental right. In a fast evolving information society it is of great value to the common European citizen and assists in keeping human right standards and data protection level high.

The importance of data protection is now so recognized that it stands on its own. Data protection is no longer just a part of a right to privacy. There are national data protection laws, the EU Data Protection Directive and Art. 8 of the EU Charter of Fundamental Rights which now is enclosed as part II of the Treaty establishing a Constitution for Europe. This evolution shows also the growing recognition of informational self-determination. In Art. 8(2) of the Charter (Art. II-68(2) of the TCE) it says that data processing must be fair, specific, and based on *consent* or other legitimate basis in law. Art. I-51 of the TCE is also about protection of personal data.[160] Art. II-63 of the TCE is about respect for personal integrity and in paragraph 2 it says: "In the fields of medicine and biology, the following must be respected in particular: a) the free and informed consent of the person concerned, according to the procedures laid down by law;"[161] Consent and therefore informational self-determination, subject to limitation, are regarded as one of the fundamental rights in the Charter and TCE.

A right to informational self-determination is a part of the essence of human dignity in the author's opinion and should at least be regarded as encompassed by the fundamental right to privacy and should even become recognized as a separate right on its own.

---

[160] TCE, Official Journal of the European Union, C 310, Vol. 47, 16.12.2004. p. 36.

[161] TCE, Official Journal of the European Union, C 310, Vol. 47, 16.12.2004, p. 42. Art II-63 of the TCE is the same as Art. 3 of the Charter. Art. II-67 in TCE, about the right to respect for private and family life, is the same as Art. 7 of the Charter. Art. II-61 of the TCE, about the right to human dignity is the same as Art. 1 of the Charter.

## References

### List of Judgements/Decisions

*European Court of Human Rights in Strasbourg:*
Botta v. Italy, Application no. 21439/93, 1998-I Eur. Ct. H.R.
Copland v. United Kingdom, Application no. 62617/00, 2007-IV Eur. Ct. H.R.
Halford v. United Kingdom, Application no. 20605/92, 1997-III Eur. Ct. H.R.
Leander v. Sweden, Application no. 9248/81, 1987, Series A no. 116, Eur. Ct. H.R.
Olsson (No. 1) v. Sweden, Application no. 10465/83, 1988, Series A no. 130, Eur. Ct. H.R.
Peck v. United Kingdom, Application no. 44647/98, 2003-IV Eur. Ct. H.R.
Pretty v. United Kingdom, Application no. 2346/02, 2002-IV Eur. Ct. H.R.
von Hannover v. Germany, Application no. 59320/00, 2004-III Eur. Ct. H.R.
X & Y v. the Netherlands, Application no. 8978/80, 1985 Series A no. 91, Eur. Ct. H.R.
Z v. Finland, Application no. 22009/93, 1997-I Eur. Ct. H.R.
All available at: http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en
[Last visited 13.11.2007]

*Decision of the European Commission of Human Rights:*
X v. Iceland, Application No. 6825/74, D.R. 5 p. 86 (18 May 1976).
Available at: http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en
[Last visited 13.11.2007]

*Germany*
Decision of the First Senate of 15 December 1983 - 1 BvR 209/83 et al. Federal Constitutional Court, Karlsruhe. Available in German at: http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm
[Last visited 20.11.2007]

Injunction by the Federal Constitutional Court, Karlsruhe, April 13th, 1983, 1 BvR 209.

*Iceland*

Supreme Court of Iceland, case 151/2003, Reykjavík, 2003, p. 4153-4181. Available in Icelandic at: http://www.haestirettur.is/domar?nr=2566
An unofficial translation in English is available at:
http://www.epic.org/privacy/genetic/iceland_decision.pdf
[Last visited 20.11.2007]

Supreme Court of Iceland, case 417/2001, Reykjavík, 2001, p. 3962-3971
Available in Icelandic at: http://www.haestirettur.is/domar?nr=2117
[Last visited 18.10.2007]

**Treaties/Statutes**

*Germany*

Basic law for the Federal Republic of Germany (de. Grundgesetz, GG) as of 23 May 1949 with later amendments. Available in English at:
http://www.iuscomp.org/gla/statutes/GG.htm#1
[Last visited 17.11.2007]

Federal Act governing Access to Information held by the Federal Government (de. Gesetz zur Regelung des Zugangs zu Informationen des Bundes) as of 5 september 2006. Available in English at:
http://www.bfdi.bund.de/cln_029/nn_672714/IFG/Gesetze/IFG/TextIFG__EN,templateId=raw,property=publicationFile.pdf/TextIFG_EN.pdf
[Last visited 24.11.2007]

Federal Data Protection Act (de. Bundesdatenschutzgesetz) as of 15 November 2006. Available in English at:
http://www.bfdi.bund.de/cln_029/nn_535764/EN/DataProtectionActs/DataProtectionActs__node.html__nnn=true
[Last visited 17.11.2007]

*Iceland*

Access to Information Act no. 50/1996 (is. Upplýsingalög). Available in English at:
http://eng.forsaetisraduneyti.is/acts-of-law/nr/15
[Last visited 24.11.2007]

Act on the Protection of Privacy as regards the Processing of Personal Data no. 77/2000 (is. Lög um persónuvernd og meðferð persónuupplýsinga). Available in English at:
http://eng.domsmalaraduneyti.is/laws-and-regulations/nr/1306
[Last visited 17.11.2007]

Bill on a Health Sector Database, submitted in Althingi, Iceland, in 1998, document no. 109. Available only in Icelandic at: http://www.althingi.is/altext/123/s/0109.html
[Last visited 17.11.2007]

Constitution of the Republic of Iceland no. 33/1944 (is. Stjórnarskrá lýðveldisins Íslands). Available in English at http://government.is/constitution
[Last visited 17.11.2007]

Health Sector Database Act no. 139/1998 (is. Lög um gagnagrunn á heilbrigðissviði). Available in English at: http://eng.heilbrigdisraduneyti.is/laws-and-regulations/nr/659
[Last visited 17.11.2007]

Regulation on the Health Sector Database no. 32/2000. Available in English at:
http://eng.heilbrigdisraduneyti.is/laws-and-regulations/nr/670
[Last visited 17.11.2007]

*International*

Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, C 364, 18.12.2000. Available at:
http://www.europarl.europa.eu/charter/pdf/text_en.pdf
[Last visited 17.11.2007]

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. Official Journal L 281, 23/11/1995, P. 0031-0050. Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=
CELEX:31995L0046:EN:HTML
[Last visited 17.11.2007]

The European Convention on Human Rights and Fundamental Freedoms. Available at:
http://www.echr.coe.int/ECHR/EN/Header/Basic+Texts/Basic+Texts/
The+European+Convention+on+Human+Rights+and+its+Protocols/
[Last visited 17.11.2007]

International Covenant on Civil and Political Rights.
URL: http://www.ohchr.org/english/law/ccpr.htm
[Last visited 17.11.2007]

Treaty Establishing a Constitution for Europe, Official Journal of the European Union, C 310, Volume 47, 16.12.2004. Available at: http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ:C:2004:310:SOM:EN:HTML
[Last visited 17.11.2007]

Universal Declaration of Human Rights, Office of the High Commissioner of Human Rights. URL: http://www.unhchr.ch/udhr/lang/eng.htm
[Last visited 21.11.2007]

**Secondary Literature**

*Annual Report 2002*, The Icelandic Data Protection Authority, 23.4.2003. Available only in Icelandic at: http://www.personuvernd.is/utgefid-efni/arsskyrslur/2002/ [Last visited 30.10.2007]

Article 29 Data Protection Working Party: *Working Document on Genetic Data*, Article 29 Data Protection Working Party, 17 March 2004. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_en.pdf [Last visited 18.10.2007]

Article 29 Data Protection Working Party: *Working Document on the Processing of Personal Data relating to Health in Electronic Health Records (EHR)*, Article 29 Data Protection Working Party, 15 February 2007. Available at: http://www.orpha.net/actor/EuropaNews/2007/doc/wkg-party-doc.pdf [Last visited 14.09.2007]

Bygrave, Lee A: *Data Protection Law – Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague/London/New York, 2002.

Bygrave, Lee A: *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, vol. 6, 1998, p. 247-284. Also available at: http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf

Caplan, Jeremy: *Kari Stefansson: The Time 100 Scientists and Thinkers*, Time, 2007. URL: http://www.time.com/time/specials/2007/time100/article/0,28804,1595326_1595329_1616840,00.html [Last visited 24.11.2007]

Church, Clive H. and David Phinnemore: *Understanding the European Constitution: An Introduction to the EU Constitutional Treaty*, Routledge, London and New York, 2006.

*Convention for the Protecion of Human Rights and Fundamental Freedoms,* Council of Europe. URL:
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=&DF=&CL=ENG
[Last visited 20.11.2007]

Drake, William and Rikke F. Jørgensen: "Introduction" in *Human Rights in the Global Information society,* ed. Rikke F. Jørgensen, Massachusetts Institute of Technology, USA, 2006, p. 1-49.

*EUROPA*, European Union. URL:
http://europa.eu/abc/european_countries/index_en.htm
[Last visited 21.11.2007]

*EUROPA,* European Union, Directorate General External Relations, last updated October 2007. URL:
http://ec.europa.eu/external_relations/eea/index.htm
[Last visited 21.11.2007]

*The EU Constitution: The Best Way Forward?,* Deirdre Curtin, Alfred Kellerman and Steven Blockmans (ed.), TMC Asser Press, The Hague, 2005.

*The European Constitution and National Constitutions: Ratification and Beyond,* Anneli Albi and Jacques Ziller (ed.), Kluwer Law International, The Netherlands, 2007.

*European Court of Human Rights*, Council of Europe URL:
http://www.echr.coe.int/echr/
[Last visited 20.11.2007]

Gertz, Renate: *An Analysis of the Icelandic Supreme Court Judgment on the Health Sector Database,* (2004) 1:2 *SCRIPT-ed* 241- A Journal of Law, Technology & Society. URL: http://www.law.ed.ac.uk/ahrc/script-ed/issue2/iceland.asp
[Last visited 13.11.2007]

Goldsmith, Lord: “A Charter of Rights, Freedoms and Principles” in *The Treaty of Nice and Beyond: Enlargement and Constitutional Reform*, Mads Andenas and John Usher (ed.), Hart Publishing, Oxford and Portland, 2003

Gómez-Arostegui, H. Tomás: *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, California Western International Law Journal, vol. 35, no. 2, 2005, p. 153-202. Also available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=669401

Gunlicks, Arthur B: *The States (Länder) and German Federalism*, Manchester University Press, Manchester/New York, 2003.

Hosein, Gus: “Privacy as Freedom” in *Human Rights in the Global Information Society*, Rikke F. Jørgensen (ed.), Massachusetts Institute of Technology, USA, 2006, p. 121-147.

Jacobs, Francis and Robin White: *The European Convention on Human Rights*, 4. ed., Oxford University Press, Oxford-New York, 2006.

Jacoby, Nicole E: *Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, bepress Legal Series, Working Paper 1515, 2006.
URL: http://law.bepress.com/expresso/eps/1515/
[Last visited 20.8.2007]

Kilkelly, Ursula: *The Right to Respect for Private Life and Family Life: A Guide to the Implementation of Article 8 of the European Convention on Human Rights*, Directorate General of Human Rights, Council of Europe, Strasbourg, 2001.

*The Official Gateway to Iceland*, The Ministry for Foreign Affairs
URL: http://www.iceland.is
[Last visited 24.11.2007]

*The Online Network of Freedom of Information Advocates.* URL:
www.freedominfo.org
[Last visited 24.11.2007]

Polo, Cristina Pineda and Monica den Boer: "The Charter of Fundamental Rights: Novel Method on the Way to the Nice Treaty" in *The Treaty of Nice: Actor Preferences, Bargaining and Institutional Choice,* Finn Laursen (ed.), Martinus Nijhoff Publishers, Leiden / Boston, 2006.

Rehm, Gebhard Marc, *Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law*, European Journal of Comparative Law, vol. 2, 2001, p. 209-286. Also available at:
http://ssrn.com/abstract=216348
[Last visited 8.10.2007]

Riedel, Eibe H: *New Bearings in German Data Protection – Census Act 1983 Partially Unconstitutional*, Human Rights Law Journal, vol. 5, No. 1, 1984, p. 67-75.

Riedel, Eibe H: Federal Constitutional Court, Karlsruhe: Judgement of the First Senate of 15 December 1983 – Census Act 1983 Partially Unconstitutional, Human Rights Law Journal, vol. 5, No. 1, 1984, p. 94-116.

Schwartz, Paul M: *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, American Journal of Comparative Law*, 1989, p. 675-701.

*Theory and Practice of the European Convention on Human Rights*, Peter van Dijk …[et al.]: 4. ed., Intersentia, Antwerpen-Oxford, 2006.

Warren, Samuel and Louis D. Brandeis: *The Right to Privacy*, 4 Harvard Law Review 193, 1890.

Westin, Alan: *Privacy and Freedom*, Atheneum, New York, 1967.

Wong, Rebecca: "Privacy: Charting its Development and Prospects" in: *Human Rights in the Digital Age*, Mathias Klang and Andrew Murray (ed.), The GlassHousePress, Cavendish Publishing Ltd, London, 2005, p. 147-161.