FIDIS

Future of Identity in the Information Society

Title:	"D13.3: Study on ID number policies"
Author:	WP13
Editors:	Hans Buitelaar (TILT, The Netherlands)
Reviewers:	Gloria González Fuster(VUB, Belgium) James Backhouse (LSE, UK)
Identifier:	D13.3
Type:	Deliverable
Version:	1.0
Date:	Friday, 14 September 2007
Status:	Final
Class:	Internal
File:	fidis-wp13-del13 3 number_policies_final

Summary

The objective of this deliverable is to present a view on the sensible use of the identification numbers, especially in the public domain. The question of whether proper use can be achieved by a single global identifier or multiple identifiers will be answered.

In this deliverable several FIDIS partners investigate different aspects of ID numbers, such as the history of the use of identification documents, the legal framework, the sociological theoretical aspects and the possible use of ID numbers in the technique of profiling. Thus the investigations presented in this report provide a sound basis for determining the risks and opportunities in using ID numbers, especially the area of e-government.

Country reports illustrate the choices made of using either a single global identifier or multiple identities. The report shows how the ID number can be put to good use while at the same time not unduly harming the privacy interests of the individual.

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	15.08.2007	- Initial release (Hans Buitelaar)
0.2	17.08.07	- Review by J. Backhouse
0.3	22.08.07	- Executive summary, introduction, conclusions checked on correct English (V. Carter)
0.4	23.08.07	- Summary revision (J. Backhouse)
0.5	27.08.07	- Review by G. González Fuster
0.6	28.08.07	- Footnotes and references standardisation (M. Knapen)
0.7	29.08.07	- Changes due to comments reviewers made by I. Oomen, X. Huysmans, M. Meints, M. Rost
1.0	30.08.07	- Definite release by Hans Buitelaar

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 Executive Summary	Hans Buitelaar
2 Introduction	Hans Buitelaar
3.1 History of ID documents	Marita Häuser
3.2 Legal Aspects	Xavier Huijsmans
3.3 ID Numbers from a social perspective	Martin Rost, Martin Meints, Isabelle Oomen
3.3.2 Functions, benefits and drawbacks of ID numbers	Martin Rost, Martin Meints
3.3.3 ID numbers: symbols of democracy	Isabelle Oomen
3.3.4 Summary of the sociological approaches	Martin Meints
3.6 Profiling practices	Mireille Hildebrandt
4.1 Country Report Belgium	Xavier Huijsmans
4.2 Country Report France	Fanny Coudert
4.3 Country Report Three Visegrad Countries	Adam Foldes, Robert Pinter
4.4 Country Report Germany, Austria, Switzerland	Sebastian Meissner
4.5 Country Report The Netherlands	Hans Buitelaar
5 Summary and conclusions	Hans Buitelaar
Annex Composition of ID Numbers in EU Countries	Hans Buitelaar, John Zeegers

Table of Contents

1 Executive Summary

Without any doubt, modern democratic states need to be able to identify their citizens and inhabitants. This is not an easy task in an increasingly polycentric and mobile society. Identification is needed to ensure the citizen's equality with respect to benefits and grants the state offers, but also because of their duties. In the first context it is important for fraud prevention in social insurance systems, in the second for the equality and equity of taxes.

To facilitate citizen identification, citizen registers and ID documents were introduced as early as the late medieval times. In the 20th century the need for rationalization of administration led to the introduction of ID numbers. Since the introduction of electronic data processing in the 1980s, the use of ID numbers seems to have increased.

ID numbers are introduced and used by organisations (a) to name objects, (b) to identify them (use as identifiers) and (c) to address them in the context of operations (business or governmental procedures) and communication. Besides individuals, objects can also be groups of individuals (e.g. project teams), organisations, organisational structures within organisations (e.g. departments) and functions carried out and services offered by organisations (e.g. a help desk and corresponding support). ID numbers are also used as indices for data sets and thus enable the linkability of objects and related data. As a result, data and transactions of members and clients of organisations become potentially transparent, once access to stored data has been made possible. Linked data may be further explored using profiling techniques such as data mining or Knowledge Discovery in Databases (KDD).

ID numbers have been discussed intensely within constitutional democratic states. The benefits of ID numbers for an efficient administration are largely accepted. This became even more understandable when concepts for e-government were discussed at the beginning in the late 1990s. ID numbers and their linkability also play an important role in the security of national states. Profiling is used extensively to fight crime and terrorism by e.g. mining travellers' data and money transactions.

On the other hand, there has also been much discussion concerning the impact of ID numbers and their linkability on the shift between opacity and transparency. As a result, there is a potential shift in the balance of power in favour of the state. All Visegrad countries investigated in Part II of this deliverable experienced totalitarian systems abusing linkability for surveillance purposes, political and religious oppression, discrimination of parts of the population or violation of international law including genocide. Also the right for informational self-determination and privacy have been taken into consideration.

Taking into account the above-mentioned factors, national political strategies and existing infrastructures four different basic concepts on how to deal with ID numbers can be determined from the studies as reported in the deliverable. They are:

1. Introduction of sector spanning ID numbers with a large area of use inside and outside the public sector mainly based on mutual transparency of use (example: The Netherlands)
2. Introduction of sector spanning ID numbers with regulations how they may be used (examples: Switzerland, Czech Republic and Slovakia)
3. Introduction of sector specific ID numbers and organisational enforcement of borders of sectors (examples: Hungary, France, Germany)
4. Introduction of sector specific ID numbers and organisational as well as technical enforcement of borders of sectors (example: Austria)

In more general terms, these four concepts may be characterised as illustrating a shift in balance of opacity and transparency towards more transparency. Opacity should be understood in this context as measures by which the individual is not easily recognisable e.g. by applying encrypting measures. Transparency naturally makes it easier to identify an individual. In this context different approaches are discussed.

One approach is to ask citizens to be more transparent by introducing cross context or sector spanning and unique ID numbers while, at the same time, attempts are also made to make the state and its actions more transparent. In the Netherlands, for example, they have introduced the National Trust Function to log the use of the national ID number. In Germany they have introduced the Freedom of Information Acts allowing citizens to access their own data files maintained by the state. Unfortunately, these attempts often do not achieve the objective of creating the desired mutual transparency.

In addition to limitations for citizens to access secret data, which can be understood and could be alleviated by trust based models, the use of profiling creates additional limitations for transparency. Certain types of profiles are not linked with the data they were derived from, so there are no personal data any more and they may be used to the disadvantage of the citizen in a non-transparent way. Owing to the complexity of the underlying profiling processes, regulatory attempts to increase transparency fall short. Transparency Enhancing Technologies (TETs) have only a limited effectiveness or are still non-existent.

Another approach is to introduce additional opacity functions and tools. This generally involves developing and implementing different methods to restrict and control the linkability facilitated by ID numbers.

The authors believe that an appropriate balance of transparency and opacity should be aimed for. This target can be best achieved by using multiple identifiers in combination with the appropriate organisational or technically enforced rules for linkability such as is the case in Austria.

2 Introduction

As becomes apparent in this deliverable much discussion takes place about the desirability of a single identification number in the context of eGovernment development. This is a matter of a fundamental nature. It goes without saying that personal identification forms an important part of the foundation of our society. It allows us to create a link between people, actions and responsibilities. In many ways it is one of the lubricants which allow society to function.[4] Whereas in the past, physical means of identification predominated, we are now on the eve of an era where digital equivalents of these forms of identification will take over.[5] Without these measures, fighting crime will be obstructed, ambitions in the field of e-government will be frustrated, companies and citizens will lack faith in e-commerce, to name but a few things that could go wrong. Careful attention to the design of the system of digital identification is essential. The question is to assess whether there is sufficient consideration of the advantages and disadvantages of the use of an identification number, without which, a digital identification system cannot function.[6]

Generally speaking it may be argued that it is exactly the will of giving the image of an actor seeking to introduce trustworthy measures at all levels that allow (governmental) organisations to develop innovative ICT systems. These innovations make it possible for commercial organisations to increasingly rely on sophisticated technologies with which to improve their customer services but also to increase their own profits. Governmental organisations can apply these innovations in new areas such as the measures to combat terrorism or improve the health care system. Once the client or citizen trusts an organisation to correctly use personal data, the necessity decreases for expensive measures like PETs etc..[7] This calls for careful attention to find an appropriate balance between the introduction of new technologies for which the personal identification number is an important element and, building up and securing the citizen's trust in the measures governments actually carry out to ensure their right to informational privacy.[8]

As the argument goes, an identification number is in itself a meaningless number. Who would object to a meaningless number? However, a number is of course never meaningless because it is always assigned to a person with a view to identifying them for a specific purpose. Governments introduce ID numbers to facilitate back-office functions and to exchange information about citizens to enable them to provide services to citizens. The danger, alluded to in many publications[9], is, that, because the ID number is so important, it also becomes more attractive to malicious individuals to get hold of this number in order to use it for criminal purposes. Identity theft and identity fraud assume ever larger proportions in the

[4] Prins & De de Vries 2003, p. 13.
[5] College Bescherming Pbescherming ersoonsgegevens 2002.
[6] Koops 2001 thinks the time is ripe for a reconsideration because once the information society is there it cannot be turned back.
[7] Working Party on Information Security and Privacy 2001.
[8] Lasky & Fletcher 1998.
[9] Grijpink 2006, p. 47.

EU[10] as in other parts of the world. In that way the increasing use of identity numbers by government can be said to backfire on the issuer, the government.[11] If this development continues, faith in eGovernment and e-commerce will be undermined. Instead of helping government to fight crime, government has a new crime issue at hand. It seems reasonable to assume that governments will take timely and well-considered measures to prevent this scenario from happening.

ID numbers are used throughout the public sector. These numbers originated in distinct areas of the public sector. Examples are taxation, public health, law-enforcement, local administrations and social services. In the light of attempts to streamline government operations by making systems interoperable and in fighting fraud and terrorism, different developments can be witnessed in various EU countries. The various solutions proposed, offer different benefits and pose different threats to both governments and citizens. The most eye-catching solution in this respect is the introduction of a single personal identification number to be used throughout the public sector. Undoubtedly, the advantage in reducing the administrative burden for both government and citizen makes the single identification a very attractive proposition. At the same time, the costs of security measures to safeguard it, may not be sufficient to retain the citizen's trust in a reliable government. The findings of the deliverable 7.8 on Ambient Law may be referred to in this context. In the scenario, where substantial user control is absent, the introduction of a unique identifier makes the consumer and citizen more transparent. Thereby, facilitating the linkage of a profile to the number ID and linking different profiles to each other via this number, could potentially result in undesirable surveillance opportunities.

This report aims to provide suggestions for recommendations for a well-balanced and privacy-friendly policy for the use of ID numbers in the public domain. The phenomenon of the ID number is therefore first discussed conceptually. The study begins by providing an overview of the historic developments. Next a conceptual framework is presented consisting of legal and socio-cultural approaches. Finally, there is a discussion concerning the most prominent and current use of ID-numbers in the technical context. A single global unique identifier seems to especially have many advantages. This is in the area of profiling and interoperability. However, from a privacy point of view, profiling harbours many risks and solutions for these potential harms are being sought. Deliverables 4.2 (interoperability) and 7.2 (profiling) provide valuable input for these sections. In Part II an empirical study is given of the background and present policy and usage of ID numbers in a sample of various EU countries[12]. These country reports illustrate how the conceptual aspects described in Part I are

[10] The EU has an Action Plan 2004-2007 to prevent fraud in non-cash means of payment. In this Action Plan it is observed that identity theft is a cross-sector problem affecting governments, businesses and citizens, and is growing rapidly in some sectors and countries. Comprehensive measures against identity theft are called for "as the verification of identities is extremely important for the integrity of society." Commission of the European Communities 2004. See also Prins & Van der Meulen 2006. In 2006 President Bush has set up an Identity Theft Task Force in the USA. Www.ftc.gov/opa/2006/09/idtheft.htm.

[11] In Sweden, which is generally seen as an example of a successful usage of a general personal number, as long ago as 1994 a state commissioner was appointed to introduce measures to limit the use of the national personal number. Personal Identification Number Enquiry 1994.

[12] An attempt is made to provide an overview that shows how the attitudes towards and the choices made with respect to the usage of ID numbers can be very different in the EU region. For this reason country reports have been included on Belgium, France, The Netherlands, Czechoslovakia, Slovak Republic, Hungary, Germany,

put into practice. The empirical and conceptual approaches make it possible to elicit lessons learned and provide benchmarks, by which to develop arguments for policy recommendations.

As befits the Fidis network of excellence, this deliverable has been realised through a community of researchers, working together from different perspectives on common objectives. It aims at contributing to a better understanding of the advantages and disadvantages of single versus multiple identifiers in the public domain. It is therefore part of the analysis of the implications of technologies for protecting and enabling the secure and trusted distribution of identity digital assets.

References

College Bescherming Persoonsgegevens 2002
College bescherming persoonsgegevens, *Electronische overheid en privacy. Bescherming van persoonsgegevens in de informatiestructuur van de overheid*, Den Haag, 2002.

Commission of the European Communities 2004
Commission of the European Communities, *A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment*, Brussels, 20.10.2004 COM (2004) 679 final.

Grijpink 2006
J.H.A.M. Grijpink, Identiteitsfraude en overheid, Justitiele verkenningen, *jg* 32 (2006), nr 7.

Koops 2001
B.J. Koops, Een nieuwe GBA, digitale kluisjes en identificatiedrang, *NJB* 32 (32) (2001), pp. 1555-1561.

Lasky & Fletcher 1998
K. Lasky & A. Fletcher, *The future of privacy volume 2: Public trust and the use of private information,* London: Demos 1998.

Personal Identification Number Enquiry 1994
Personal identification Numbers – Privacy and Efficiency. Personal Identification Number Enquiry. Sweden, 1994.

Prins & Van der Meulen 2006
J.E.J. Prins & N.S. van der Meulen, Identiteitsdiefstal: lessen uit het buitenland, *Justitiele Verkenningen* 32 (2006), nr 7.

Prins & De Vries 2003
C. Prins & M. de Vries, *ID or not to be? Naar een doordacht stelsel voor digitale identificatie*, Den Haag: Rathenau Instituut 2003, Working document 91, p. 13.

Working Party on Information Security and Privacy 2001
Working Party on Information Security and Privacy, *Report on the OECD forum session on privacy-enhancing technologies,* Parijs: OECD 2001.

Switzerland and Austria. In the annex a broader selection of countries is provided to give an indication of the various ways in which ID-numbers are composed.

3 PART ONE – PROBLEM DOMAINS

3.1 Your Passport, please! – An overview of the history of ID Documents

Marita Häuser, ICPP

3.1.1 Introduction

"Your passport, please!" – In most cases this request does not cause spontaneous joy and happiness.

Passports, passwords and the like are not instruments originating from the "digital era" where most actions in the digital world require an authentication. In former times there were many occasions where individuals needed to authenticate, e.g., to prove that they were the person they seemed or claimed to be. Attributes such as clothes, signs of social status or physical properties were used for that purpose. In addition friends or partners were able to act as witnesses. Already in medieval times passports and citizens' registers for purposes of passport verification were introduced. This chapter gives a non-exhaustive overview of the development of identifiers in European societies taking examples mainly from France and Germany.

3.1.2 Identity and Identification in Early European States

To be able to identify individuals in a reliable way always has been of importance, especially in the context of social groups (e.g. clans) and later in the context of States. This need typically covered all phases of human life, from birth to death. The context for identification always has been the determination of membership or non-membership in a group, a clan or State, and the regulation of access to resources, ownership or participation in this context.

In early societies such as the Greek Polis, identification was done by inspection. Societies were not very large, so every citizen knew every other citizen of his Polis in person. In fact in times of Solon (ca. 640 to 560 B.C.) a largely accepted thesis was that a democracy could not exceed 20,000 citizens, as this number would lead to a situation where people stopped knowing each other and thus society could not function effectively.

This situation changed dramatically already in the Roman Empire. From time to time Roman Emperors tried to count their citizens using a census, as reported for example in the Bible (e.g. by the evangelist Lukas in chapter 2.1). The census information was important to calculate taxes, the number of slaves and the number of possible soldiers. A census did not provide a means for identification of individual citizens.[13]

[13] By the time of the Emperor Augustus, 30BC to 14AD, Censuses were taken every 5 years. The Censor was an important public position in Rome. The census was also about taxation potential.

3.1.3 Identity and Identification in the Medieval Age

In the 13th century King Friedrich II, Holy Roman Emperor, introduced a modern, for that time, administration in Sicily (Italy). This approach included the first citizens' registers run by the State. This was the first attempt to create a written basis for the identification of individuals. But it did not become common practice.[14]

Instead another practice became common: the use of travel documents for individuals. Typically these documents were used for persons with a special status such as rich citizens and noblemen. These travel documents typically were documents for passing through an area: visa or letters of recommendation. The purpose of these documents was to reduce the risks of travelling. This was accomplished by a certificate of a reference person (typically a person of high status that was widely known) that the travelling person travelled for legitimate reasons, was trustworthy and worth being protected and supported on the journey by local authorities.

Taking in criminals was supported by using warrants of apprehension. They included a detailed description of the person searched for, the so called 'signalement', and were copied many times after printing of books was developed.[15]

An example for early registration of large numbers of persons is the registration of colonists in Portugal at the end of the 15th century. The reason for this registration was that certain groups were not allowed to move to the colonies. Overall this system proved to be not effective at all, as the authenticity of the registered names remained questionable.

After the reformation the Catholic Church needed to know – among others for tax reasons – how many members belonged to it. To facilitate this, the Council of Trent decided in 1563 that priests should write lists of persons who were baptised and married, and later also of those who were confirmed and buried. From the perspective of the Catholic Church this information was most important as it showed the real identity of a member of the church: Through baptism people became members of the church, a Christian marriage was important for a Christian life of couples and families, and a Christian burial also was very important. This way of showing the identity of the church member helped in guaranteeing that a person could be resurrected from death with a complete body, despite illness, wounding and death in his physical life.[16]

3.1.4 Identity and Identification in Modern Times

After the Holy Roman Emperor King Josef II (Heiliges Römisches Reich Deutscher Nation) gave the order in the 18th century that a copy of each church's lists should be taken for purposes of the State, local authorities gained wide access to citizens' data. This included their number, age, sex, place of birth and residence, and in some cases profession. This information mainly was used for tax calculation purposes, recruitment of soldiers and the calculation of money needed to support poor people.

[14] Groebner 2004.

[15] Groebner 2004.

[16] Brockhaus 1898.

In 1796 Johann Gottlob Fichte stated that citizens need to be detectable for public authorities at any time. For this purpose he suggested the introduction of a passport for every citizen, which precisely describes the passport holder. Pursuing the same target, Jeremy Bentham suggested in 1843 that every citizen should bear a unique name. This name should be noted in a citizens' register and also should be tattooed on the wrist of the corresponding citizen. This permanent link between a physical person and a name certified by public authorities would strengthen the law and result in the disappearance of many criminal activities, Bentham claimed. In addition the identification would support prosecution in case of criminal actions.[17]

The French Revolution led, among other things, to the introduction of the "Code Civil" as civil law on 20th of September 1792. Because of the resulting modern understanding of citizenship, citizens' registers were run by the State instead of the churches. Identification of citizens of the State was based on a paper-based ID document together with an appropriate entry in the citizens' register by public authorities.[18]

The reintroduction of ID documents that were terminated earlier in the French Revolution resulted in a dilemma that was quite typical for the 19th century. On one hand increasing liberalisation required free movement without passports standing in the way. On the other hand in times of real or perceptible crises, inner security (today often called homeland security) became a bigger issue and thus registration of citizens and foreigners together with issuing ID documents was undertaken regularly. But the target of effective administrative control in practice was seldom achieved due to putting off implementation of identifying measures. Noblemen typically did not need any ID documents, while normal citizens needed them as soon as they were leaving the county where they were living. Foreign travellers in addition had to keep strictly to a prescribed route and faced in addition numerous controls on their way. De facto migration started to be a serious issue already in the 19th century. Millions of people moved around without any passport, changing effectively the demographic, political and economic landscape of Europe.

But ID documents also became important in another context in the 19th century. Police forces throughout Europe had introduced registers of poor people and of people that were moving around such as beggars, crippled people, veterans from various wars, prostitutes, lepers and showmen. Security of the local population was a motivating factor for this registration, but different treatment of the local bereaved persons compared to moving poor people also was an issue. Based on the right of people at home the local poor population got better support (e.g., food and housing) compared to other groups. In any case to receive grants, people had to identify themselves using ID documents.[19]

When States in Europe changed from absolute monarchies to constitutional States in the 19th century, the relationship between State and its citizens changed. Passports (pass from the French term passer: going from one place to another, port from porter: to carry) turned to be

[17] Caplan 2001; Cf Fidis D 5.4, Anonymity in electronic government: a case-study analysis of governments' identity knowledge, chapter 2, Jeremy Bentham on the need for identification by governments.

[18] Groebner 2004.

[19] Probably for this reason many VIPs think that a request for identification comes close to an offence (Wesel 1997).

more than an ID document, they also confirmed that the holder was member of the issuing State and thus accepted as citizen and protected by it. Especially the issuing State allowed the travelling, including return and reintegration in the State of origin after return. Though the 19th century also is called the passport-less century – most States in middle and western Europe cancelled the obligation to carry a passport in the last third of this century –, a number of different regulations on ID documents and citizens' registration remained.[20]

An example for this is the "passport law for the Prussian monarchy (Pass-Edikt für die Preussische Monarchie)" from 1817 and the "law on the integration of newly arriving persons (Gesetz über die Aufnahme neu anziehender Personen)" from 1842. Both laws required the registration of travellers in hotels and the transfer of the registration data to the police by the hotel owners. In contrast to this the Federation of Northern German States (Norddeutscher Bund) since 1876 had a "law on free movement (Gesetz über die Freizügigkeit)", which remained generally in place in Germany until 1933.[21]

In the First World War (1914-1918) in Germany an ID card was introduced, as in times of war control of people moving around and their identification seemed to be very important. Originally it was planned to have fingerprints in this ID card, but this was not implemented as dactyloscopy (comparison of fingerprints) typically was used as a forensic method at that time, replacing the anthropometria (registration and comparison of physical properties of persons) developed by Alphonse Bertillion at the end of the 19th century. At that time the German State decided to use photos in ID cards in order not to convey the impression that the ID card holder might be a criminal.[22]

To verify identity information stated in ID documents various registers such as citizens' registers or registers of the status of persons are used.

In the local "law on citizens' registration (Gesetz über das Meldewesen)" issued in 1929 in the city of Hamburg in Germany, taken over by Prussia in 1933, the transfer of personal data to other public administrations was regulated. The use of personal data, originally stored for citizens' registration purposes, became common also for other purposes. In 1938 a centralised citizens' register issued by the Ministry of the Interior was introduced for the whole of Germany. In the context of the National Socialist ideology, control of citizens in every aspect of life and registration duties at hotels, meeting places and the like were expanded and enforced. In case of data transfer among different registers and authorities a feedback (so called Rückmeldung) to the central citizens' register was introduced. The underlying idea was to establish a central citizens' register as **the** source for various purposes of the State, municipalities, the police and even the National Socialist Party. In cases of any "remarkable data" such as the belonging to a certain ethnic group, genetic diseases and migration, the "Secret State Police" (Geheime Staatspolizei, Gestapo) was informed. In this context the transfer of data could result in serious harm for persons concerned.

In the 1930s in Germany a national ID card (so called Kennkarte) was established. Originally nobody needed to have or carry one, but in 1938 carrying the ID card at any time became mandatory for Jews. This ID card was made of grey paper, strengthened by using linen, and it

[20] Gosewinkel 2001.
[21] Meder & Süßmuth 2006.
[22] Donatsch 2000.

contained a photo and a fingerprint together with a big J (for Jew) stamped on it. Since 1939 carrying an ID card became mandatory for every citizen, but under the pressure of the "total war" since 1944 this was not enforced any more. The (ab)use of citizens' registers and ID documents in totalitarian States is an interesting story on its own – for sure the history of the German Democratic Republic (GDR) also belongs to that chapter.[23] But this is not in the scope of this contribution .[24]

After the Second World War already in 1945 a new national ID document, the so called "Personalausweis", was introduced as a grey booklet for every citizen aged 16 or older. In difference to the passport, the "Personalausweis" does not confirm the German citizenship and need not to be carried by its holder at any time. Since 1987 the "Personalausweis" is implemented as polycarbonate laminated ID card. This contains a Machine Readable Zone (MRZ) and since 2001 in addition a so-called "Identigramm" which is a holographic security element. Data contained in the MRZ are described in the German country report.

Today citizens use a large variety of ID documents, e.g., passports, national ID cards, e-health cards, social insurance cards, credit cards, driving licenses, membership cards of various organisations, customer loyalty cards etc. These ID cards are used as a certificate for the (partial) identity of its holder, confirmed by private enterprises or public institutions. They confirm certain attributes, properties or authorisations of their holders, such as the membership in an organisation, the right to drive cars in certain countries or to get access to a certain area. They are meant to be used in a specific context. Typically they contain personal data such as the name, first name, date of birth, address, signature and photo of the holder and (official) seals or stamps. Usually the content that is certified is limited; for example a national ID card is not used to confirm that someone is allowed to drive a car, or a driving license cannot be used to cross borders. In case one could analyse all ID documents of a person, a quite impressive overview of his or her partial identities would result. This could give an overview on properties, interests, authorisations, abilities and possibly also intentions.

Today citizens' registers in Germany store many personal data based on the federal law for citizens' registers (Melderechtsrahmengesetz). The registers are publicly accessible, so everyone has the right to access certain citizens' data for defined purposes. Generally available data are:

- Surname, name of birth, first name
- Doctoral degree, pseudonymous name if existent
- Date and place of birth, gender
- Status of employment
- Children in custody younger than 27
- Nationality
- Membership of churches

[23] See Meder & Süßmuth 2006.

[24] See the chapter on the use of ID-numbers in Hungary, TsjechCzech Republic and Czechoslovakiathe Slovak Repubic later on in this deliverable.

- Address, secondary address if existent, former addresses and dates when they were changed
- Family status (single, married etc.), date and place of marriage, name of spouse, children younger than 27
- Existence of a national ID card and passport, issuing authority and expiry dates
- Date and place of death
- Reasons for the revocation of the right to vote (if revoked)
- Tax data
- Reasons for not being issued a passport (if existent)

The "Melderechtsrahmengesetzt" also states who is allowed to access which data for which purposes. In special cases the access to these data can be blocked totally, e.g., in cases of danger to life, health or freedom.

In addition to the citizens' registers, Germany since 1876 has a citizens' register office (Standesamt). Based on the law on persons' status (Personenstandsgesetz), books on the persons' status are administered. These books contain data on birth, marriage and death and additional data of changes of person's status such as divorcement, changes in the membership of a church or change of gender. It is planned to substitute the traditional books by a central database by 2009.

Currently national ID documents and passports are changing their character, as smart chips, RFID chip, magnetic stripes or laser engraved zones (a so-called laser band) are increasingly introduced. They are used to store information about the holder of the ID document digitally. In fact digital storage, transfer and processing of identifying information become increasingly important. One example of this is credit cards which also can be used for payment purposes via the internet. In the USA where currently no national ID card exists, the credit card also is used for identification purposes, e.g., in hotels or when booking a flight. In fact in Anglo-American countries national ID documents never were really established except in times of war.

The corresponding illegal use of digital identities (or more precisely: digital identifiers) leads to identity fraud and identity theft. In case somebody is able to obtain and use relevant attributes, he is able to carry out (digital) transactions in the name of the original identity bearer. In this context reliable identification is an important instrument often referred to.[25]

To improve the reliability of identification of citizens, new attributes are increasingly used by states. One example for this is the use of biometrics, e.g., in the context of epassports introduced in various European member states since November 2005. Reliable identification is of interest for public authorities such as police forces, border control authorities and the military, and also for the private sector to secure financial transaction and credit card payment.

[25] Groebner 2004.

3.1.5 Summary

In this contribution the spotlight was directed at the history of reliable identification of persons, the establishment of citizens' registers and the use of personal data stored on ID documents and in the registers. In the context of citizens' registers, originally introduced as a means to verify data on ID documents, digital and central storage in databases and ID numbers for addressing and indexing purposes gain increasing importance.

References

BROCKHAUS 1898
Brockhaus, *Konversationslexikon*, Leipzig, 1898.

CAPLAN 2001
J. Caplan, 'This or that Particular Person', in: Caplan & Torpey, *Documenting individual identity*, Princeton, 2001.

DONATSCH 2000
A. Donatsch, 'Identifizierung von Tatverdächtigen', in: *unipublic, Veröff. der Uni Zürich*, Oktober 2000.

DÜLMEN 2001
R.V. Dülmen (Ed.), *Entdeckung des Ich*, Köln, 2001.

FAHRMEIER 2000
A. Fahrmeier, *Citizens and Aliens*, New York, 2000.

GOSEWINKEL 2001
D. Gosewinkel, *Einbürgern und Ausschließen*, Göttingen, 2001.

GROEBNER 2004
V. Groebner, *Der Schein der Person*, München, 2004.

MEDER & SÜßMUTH 2006
K. M. Meder & M. Süßmuth, *Kommentar „Melderecht des Bundes und der Länder“*, Stuttgart, 2006.

WESEL 1997
Wesel, *Geschichte des Rechts*, 1997.

3.2 Legal aspects of global vs. sector-specific identification numbers

Xavier Huysmans, K.U.Leuven, ICRI

After the historical sketch in the previous chapter, the legal aspects of the use of identifiers receive attention. In the setting of this deliverable, this description focuses especially on the usage of single ID numbers versus multiple ID numbers in the public domain. Point of departure is the European Data Protection Directive. Since in the public domain e-government development depends hugely on the use of ID numbers, this chapter starts by defining several concepts that play an important role in the tehnical area. It then elaborates from a legal perspective the most relevant principles in the Data Directive. The chapter rounds up by trying to find an answer to the question whether the usage of global identifiers within a sound legal framework can be acceptable from a legal perspective for the default data exchange between two or more government entities or not.

3.2.1 Introduction

An identifier is an attribute or a set of attributes of an entity which uniquely identifies an entity in a certain context.[26] For example, the attribute of wearing a hat is an identifier to distinguish both men in this figure from each other:

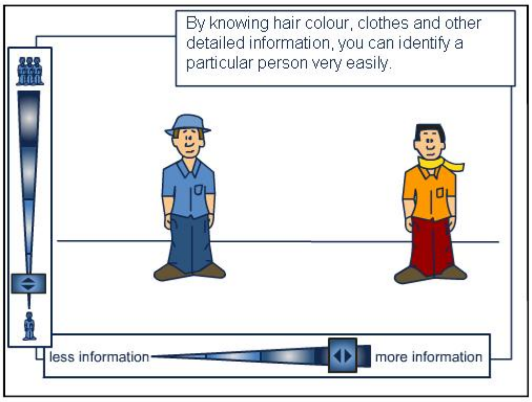
By knowing hair colour, clothes and other detailed information, you can identify a particular person very easily.
less information
more information

Figure 1. Identifiability © Prime Project, March 2006[27]

In an online environment, identifiers are usually numerically structured and are therefore called *identification numbers* (ID numbers). The fact that they are *uniquely* identifying someone or something in a particular context is an important property, because they can be used to link data from one context to another, in both admissible and inadmissible ways.

Unlinkability is often said to be a privacy protecting feature. It can be defined as the state in which two items of interest (typically sets of personal data) in an identity management system

[26] Based on Modinis IDM 2005, p. 11.
[27] http://blues.inf.tu-dresden.de/prime/EUT_Tutorial_V0/PRIME_nm.htm

are not more related after the observation by an attacker than they were related taking into account the a priori knowledge.[28]

Our starting point is the finding that Privacy Enhancing Technologies (PETs) that focus on *concealing the identity* (anonymity) or on the *usage of different sector or context- specific identifiers* (pseudonymity) only have a limited sales potential, namely where the non-respect of privacy causes obvious direct damages, for instance, with sensitive data. For instance, in Belgium, discussions continue about adding specific context-specific identifiers for health and judicial data. Also, for some years, specific regulation exists for reusing personal data for scientific, historical or statistical purposes. It requires anonymization, encoding or limited unencoded disclosure, following consent of the data subject (depending on the situation at stake).

Besides these measures, the question remains what should be the default position for all other personal data in eGovernment. Is the usage of *global identifiers* – when surrounded by a sound legal framework – enough, or should *technical unlinkability* also be a requirement of an eGovernment architecture?

In this contribution we try to answer a small part of this question, by describing what we can learn from the Data Protection Directive[29] and the European Convention on Human Rights on the topic of global identifiers in the public sector.We start by saying a few words on the reason why identifiers are necessary in eGovernment. It helps us to understand why eGovernment managers are clearly reluctant to restrain technically the opportunities they have to crosslink data sets about their clients.

3.2.2 Identifiers in the public sector

There are probably as many definitions of the term eGovernment as there are people working in that field. The Belgian definition is based on one from the World Bank.[30] The Belgian Federal government defines it as '*the continuous optimization of service delivery and governance by transforming internal and external relationships through technology, internet and new media'*.[31] This optimization of service delivery and governance relies on a number of important building blocks. One of them is the *integration of back-offices*.[32]

In Belgium, integration is sought via a 'Service Oriented Architecture' (SOA) that spans multiple administrative contexts. Identity management components such as authentication and authorization mechanisms are being integrated as basic service components of a SOA, and compiled with other components to so-called value-added services.[33] An important requirement to achieve back-office integration is to make sure that the stakeholders (i.e., the different government levels) agree on an *interoperability framework*. On the Belgian Federal

[28] Based on Pfitzmann & Hansen 2006, p. 8.

[29] Directive 95/46/EC.

[30] Due to the fact that the author is most familiar with the Belgian situation, Belgium is taken as the source for the considerations in this chapter.

[31] Based on Deprest & Robben 2003, p. 6.

[32] For more information, see Deprest & Robben 2003, De Bot 2005 p. 4-13, the federal portal http://www.belgium.be on the page `about eGovernment', Robben 2006. and Deprest & Strickx 2005

[33] Based on Robben 2006, slide 13

level, this framework consists of technical and functional interoperability measures and the usage of *common ID numbers* for all relevant entities.[34]

Against this background it is easy to understand why the usage of ID numbers is paramount for eGovernment:

- When government entities that do not share the same information infrastructure[35] want to offer efficient, effective services to all their clients (citizens, enterprises etc.), they need to *share data about these clients* between the relevant administrative contexts of the 'integrated back-office'. To make sure the data exchange concerns the correct clients, identifiers are needed.
- When the exchanged data is personal, confidential or protected, sharing it has to be carefully controlled, among other things, in order to comply with data protection regulation and with information security best practices.

  Identity management systems are often designed to do exactly that, for instance, identifying[36] and authenticating[37] internal and external users of the organization, and managing their authorizations[38] to perform actions on the information system.

  Typically, these services are part of a lifecycle[39] and thus strongly interconnected: authorization typically requires successful prior authentication and the latter typically requires a successful prior identification, which in its turn is normally based on a sound *registration.*[40]

  The registration process results in the assigning of a partial identity to the entity, and this typically includes identifiers that are valid at least in that context (context-specific) or sector (sector-specific). If the identifier needs to be used by the data owner itself (employee, citizen, enterprise…), it is then often used as username to uniquely identify the user in that context. During the registration process, the entity also receives the means to authenticate that identity in the future with one or more credentials (e.g., a password).
- Very often, in eGovernment, the goal is not only to identify, authenticate and authorize users in respect of their *own* information system, but also that of other entities that are part of the so-called 'circle of trust'.[41] In practice, in an integrated

[34] For more information about this, see Deprest & Robben 2003, p. 20 ff.

[35] E.g., because they are horizontally structured, in a federal state.

[36] Identification is the process of using claimed or observed attributes of an entity to establish a partial identity of that entity (definition based on Modinis IDM 2005, p. 9 and http://wordnet.princeton.edu/perl/webwn?s=identify).

[37] Entity authentication is a service that provides assurance of the claimed identity of an entity, as it corroborates the (claimed) partial identity of an entity and a set of its observed attributes (definition based on ITU-T 2005, p. 6 and Modinis IDM 2005, p. 7)..

[38] Authorization is the process of determining permissions to an entity by an authorization entity, to perform a defined action on a defined controlled or protected resource. Authorizations are granted or denied based on the result of data or entity authentication, and on the allowed activities, as defined within the system (Robben 2005, Nabeth & Hildebrandt 2004, Hodges 2006 and Slone 2004, p. 13 ff.)

[39] See Slone 2004, p. 24.

[40] In the technical jargon, *registration* is the process of actively verifying a specific set of attributes (e.g., the age), a characteristic or a mandate of an entity, with sufficient certainty, before putting at the disposal means by which the entity can be authenticated, or the characteristic or mandate can be verified. Based on Robben 2005, slide 5 and the definition from Modinis IDM 2005.

[41] A circle of trust is a group of service providers that share linked (partial) identities and have pertinent business agreements in place regarding how to do business and interact with identities. The definition is based on Rössler 2002, p. 29 and Hodges 2006, p. 7.

> back-office the available *identity data of the users is also shared* between the different members – in this case administrations – of this circle of trust.
>
> As a result of this shared data, *trust decisions*[42] can be made and *cross-level, integrated identity management and eGovernment services* can be offered to the users (e.g., single sign on).

The tension we're pointing at in this contribution has nothing to do with the usage of identifiers as such, but with the usage of permanent identifiers that remain valid across several contexts and sectors of action. We call them '**global identifiers**'. As we will see below, it is absolutely not self-evident to use common (global) identifiers to refer to the same entity in different contexts and information systems.

3.2.3 Context specific, sector-specific and global identifiers

A **context** is a sphere of activity, a geographic region, a communication platform, an application, a logical, or physical (security) domain.[43] Contexts are, for example, taxes, social security, health care, judicial, education, etc, and restrained to a geographic region, e.g. Belgium on the federal level.

In identity management we typically refer to its meaning as a *communicational context*. The latter is then qualified by roles and behavioral schemes participants in communication take over. The term is also often used in its meaning as a *security domain*.[44] This is an environment defined by security models and a security architecture, including a set of resources and set of system entities that are authorized to access the resources. The traits defining a given security domain typically evolve over time.[45] An example of a context is Belgian Federal Social Security. It is a *sphere of activity* (social security), *a communicational context* (e.g., two or more entities communicating via some form of platform (or interface) that is only available for social security purposes), and *a security domain* to which specific security policies apply.

When we refer to *context-specific identifiers*, we mean that the used (persistent[46] or transient[47]) identifiers are not common to the different contexts in which data is being exchanged. Alternatively, when we refer to *global identifiers*, we mean that the used identifiers are persistent and have global application (often but not necessarily on a national level), between two or more contexts *or sectors*.

The picture becomes more complicated when *a context spans multiple sectors*. A **sector** is a synonym for an administrative domain, i.e., an environment that is defined by a combination of:

- one or more administrative policies,
- Internet Domain Name registrations,

[42] An entity can be said to trust a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This assumption is shared by all those in an exchange. Trust may apply only for some specific actions (definition based on Based on ITU-T 2005, p. 51 and Zucker 1986, p. 54, Slone 2004, p. 6.)
[43] Definition by Stefan Brands on http://www.idcorner.org/?p=32
[44] A domain is a set of entities, their information objects and a common policy. Definition based on Kissel 2006, p. 27 (referring to SP800-27). We modified this definition, by replacing the word 'subject' by the more general term 'entity' and the words 'security policy' by the more general term 'policy'.
[45] Based on Hodges, Philpott & Maler 2005, p. 10.
[46] Based on Hodges, Philpott & Maler 2005, p. 8.
[47] Based on Hodges, Philpott & Maler 2005, p. 11.

- civil or public legal entities (for example, individuals, corporations, or other formally organized entities), and
- a collection of hosts, network devices and the interconnecting networks (and possibly other traits), and (often various) network services and applications running upon them.[48]

In the mentioned example of 'Belgian Federal Social Security', the Federal Unemployment Allocation Fund, the Federal Service for Pensions and the Federal Children's Allocation Fund are sectors of that context. In this example, the used identifier is common to all the sectors within this Social Security context. In other words: the identifier is not *sector-specific*.

As we will see in the Belgian country report, the problem in this case is not so much the non-usage of sector-specific identifiers, but the non-usage of *context-specific identifiers*: the used identifier – the Belgian National Registry number – is *not limited to the context* of Social Security either. It is a '*global identifier*'.

In addition to all this – and this is what makes the picture even more complicated – a sector of action (or administrative domain) is not necessarily limited to an action in exactly one context.

In the mentioned example of Belgian Federal Social Security, the Belgian Crossroads Bank for Social Security acts in the first place as a facilitator for the exchange of *social data within the Belgian Federal social security context* (this is enacted in the articles 3, 3bis, 4 and 6 of the Law of 15 January 1990). However, in view of a decision of the Privacy Commission of 28 September 2005, it is clear that the *Crossroads bank also has an identification function that exceeds the social security context.* [49] In other words, one part of a sector – the Crossroads Bank – plays a role in several contexts. For instance (1) it acts as a social data facilitator in the context of Belgian Federal Social Security and (2) it acts as an identification service provider with regard to a specific category of persons in Belgian (national) eGovernment.

To sum up, government entities that are a sector of even a part of a particular sector can act in multiple contexts. The entities that act in one or more contexts can also act in multiple sectors. Typically, in eGovernment, the (relevant) entities that act in these contexts and sectors will be assigned either a global, sector-specific or context-specific identifier. The usage of these numbers is largely influenced by data protection rules, which we will explain in the following sections.

3.2.4 Application field – ID numbers are 'personal data'

Generally speaking, data protection regulation provides for a series of rights for natural persons. They generally demand good data management practices on the part of the data controllers and include a series of obligations. Even though some exceptions and limitations for the public sector are foreseen, these rules in principle apply to both public and private sector data processing.[50]

[48] Based on Hodges, Philpott & Maler 2005, p.5.

[49] See Belgian Privacy Commission 2005.

[50] Based on Hildebrandt, Gutwirth & De Hert 2005 p. 15-20.

The data protection Directive only applies to the processing of personal data. According to the Directive, personal data is *any information relating to an identified or identifiable natural person (the data subject)* (article 2 of the Directive). Recital 26 of the Directive further explains what should be understood with 'identifiable'. For instance, it says that '*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'.*

In general terms, a natural person can thus be considered as 'identified' when, within a group of persons, if he or she is distinguished from all other members of the group. Yet, the natural person will be said to be 'identifiable' when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix '-able').

Article 2 of the Directive further states that *'a natural person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.* The extent to which certain identifiers are sufficient to achieve identification is something *dependent on the context* of the particular situation.[51]

Identification through the name is the most common occurrence in practice. Nevertheless, a name may itself not be sufficient, nor necessary in all cases to identify an individual:

- In order to ascertain an identity, the name of the person sometimes has to be *combined with other pieces of information* (date of birth, names of the parents, address or a photograph of the face) to prevent confusion between that person and possible namesakes.
- The name may also be the *starting point (the key) leading to other information* (e.g. about where the person lives or can be found). All these new pieces of information linked to the name may allow someone to zoom in on the flesh-and-blood individual, and therefore through the identifiers the original information is associated with a natural person who can be distinguished from other individuals.
- The term *'indirectly'* identified or identifiable persons, refers to the situation where the available identifiers do not allow anyone to single out a particular person.[52] This is where the Directive comes in with the phrase *'one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.* Some characteristics are so unique that someone can be identified with no effort (e.g., the present Prime Minister of Spain), but a combination of details on categorical level (age category, regional origin, etc) may also be conclusive in some circumstances, particularly if one has access to additional information of some sort.

[51] The commentary to the articles of the amended Commission proposal to the data protection Directive says that: *'a person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.)'.*

[52] Nevertheless, that person might still be 'identifiable' because the available information combined with other pieces of information (whether the latter is retained by the data controller or not) allow the individual to be distinguished from others. This is particularly relevant in data mining and profiling (see the deliverables of FIDIS WP7).

eGovernment information systems can typically be seen as 'FIDIS type 1 IDM systems', since the identity of its users, clients etc. is being assigned by the organization itself.[53] In such information systems, it is nor feasible nor desired to choose for identification via the name. To avoid confusion between two persons in the database or file, they typically assign unique ID numbers to all the persons registered.

In other words, the individual's personality is put together in order to attribute certain decisions to him or her. It is possible to categorize the person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. [54]

Important for our analysis, *is that ID numbers that refer to natural persons can definitely be qualified as personal data in the sense of the data protection Directive.* This is because – when we evaluate the reasonable means likely to be used by the data controller or by any other person – the purpose for which an ID number is assigned is an important factor.[55] This purpose is – obviously – to identify the natural person and as a result, ID numbers are personal data.

This has important implications. When we take into account the other criteria for the Directive to apply (not being set out here), we can conclude that the data protection rules normally also apply to ID numbers when they are used in the public sector. It means, among other things, that the processing of personal data – i.e., the ID number – is carried out in a *fair and lawful way* with respect to the data subjects:[56]

Data processing is only lawful if it takes place in accordance with the law. In a nutshell, this means that the data controller should take into account:

- the *legitimacy* of the data processing;
- *special categories of data*;
- the *data quality* (including the 'finality' principle);
- the data subject rights;
- *confidentiality and security* of the personal data;
- notification and transparency; and
- export of personal data to third countries outside the European Union.

[53] In FIDIS deliverable 2.3 and 3.1 we come to the conclusion that there are three main types of IDM systems, namely (1) The ones used for account management (FIDIS type 1), in which case we can speak of an *assigned identity*, (2) the ones used for profiling of user data (FIDIS type 2) and (3) the ones used for user-controlled context-dependent role and pseudonym management (FIDIS type 3). More information on the classification of IDM systems can be found in Nabeth 2005, Bauer, Meints & Hansen 2005 and Meints 2005.

[54] The Article 29 WP calls this evaluation a 'dynamic test'. The relevant factors to be taken into account, are, for example the cost of conducting identification, the intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures. This test is a dynamic one and should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed. Identification may not be possible today with all the means likely reasonably to be used today. Article 29 Data Protection Working Party 2007, p. 20-21.

[55] Article 29 Data Protection Working Party 2007, p. 15.

[56] Art. 4,§1,1° Data Protection Law 1992 and art. 6§1(a) Directive 95/46/EC.

In the next sections we briefly elaborate on the most relevant of these principles (underlined in the list) and on article 8,7° of the Directive (that refers to the usage of global identifiers).

3.2.5 Legitimacy principle

In a nutshell, this principle means that *data controller* should verify that the processing falls under one of the criteria for making data processing *legitimate*. The general rule is that processing of personal data is *not allowed*, *except* when it is based on one of the following legitimacy grounds:

- *The consent of the data subject*;
- *A legal obligation which the controller has to comply with;*
- *A task carried out for the public interest;*
- A contract to which the data subject is or will be party;
- Protection of the vital interests of the data subject; or
- The legitimate interests pursued by the controller.

In the public sector, the processing of the ID number that refers to natural persons typically will need to comply with one of the first 3 grounds. This is so because the legitimacy grounds on which governments act can at times overlap the legitimacy grounds of the processing of personal data.

3.2.6 Data quality and the reuse of personal data

The processing of personal data should be respecting the minimum data and data processing quality principles, such as the 'finality' and the 'proportionality' principle (article 6 of the Directive).

Briefly summarized, the term **finality** refers to the obligation to only collect personal data for specified, explicit and legitimate purposes. Personal data shall not be *further processed* it in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible if the appropriate safeguards are taken. The purpose of the processing should be defined the latest at the moment of the collection of the data.

The **proportionality** principle has to be understood in terms of:

- storage duration: The processed data may not be kept in a form permitting identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- necessity of the data: The processed data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.

- further processing of the data: The purposes of further processing should not be incompatible with the purposes initially defined the data were collected.
- accuracy: personal data should further be accurate and, where necessary, kept up to date.

Applied to ID numbers, it is clear that the data controller that decides to make use of a global, sector-specific or context-specific identifier should:

- *make sure that the chosen data (for example, a global ID number instead of a sector-specific one) is adequate, relevant and not excessive in relation to the purposes for which it is being collected and/or further processed;*
- make sure that the ID number is accurate and, where necessary, kept up to date and
- not kept in a form which permits identification of data subjects longer than is necessary for the purposes for which the data were collected or for which they are further processed.

These findings are important for our analysis when we evaluate the question raised above with regard to *technical unlinkability* as a requirement of an eGovernment architecture.

In addition, on the topic of finality and proportionality, it is important to note that when two or more *government entities integrate their back-offices*, there will typically be a *reuse of personal data* for another purpose than the one that was originally indicated. For example, when a particular set of data has been collected from a citizen for unemployment allowance purposes, the idea of eGovernment would be to make that data directly available to the tax authorities – of course within the borders of the law – instead of asking it again to the citizen.

As mentioned, the finality principle requires the further processing to be compliant with the original purposes.[57]

In Belgium, the legislator has clarified the criteria that should be taken into account at interpreting whether or not a planned data processing is *compliant* with the original purposes. The law says that account should be taken of *'all relevant factors, in particular the reasonable expectations of the data subject and the applicable legal and regulatory provisions'* (article 4 of the Belgian Data Protection Act).

Yet, with or without this additional clarification, it is important to note that data processing purposes can be adapted by changing the legal provisions. We take this finding with us when we evaluate which technical and organizational security measures are 'appropriate' for ID numbers in eGovernment (see below).

3.2.7 Specific provision on the usage of global ID numbers

Before we come to that analysis, it is appropriate to say a few words on the specific provision on the processing of global ID numbers in article 8.7° of the data protection Directive. It runs as follows:

[57] For instance, this means that it is absolutely unacceptable for a bank to process client payment data for *direct marketing purposes* (pricing for its own insurances). This further processing is here clearly incompatible with the original purposes.

> *'Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.'* (Article 8.7°)

At first sight, the article only seems to say that the EU Member States should decide if and how they protect 'identifiers of general application', i.e., global identifiers. Nevertheless, the location of the article in the Directive is also important here: it has been inserted in the chapter on 'sensitive data' (next to, for example, provisions on the processing of personal data revealing racial or ethnic origin).

Therefore, it is not unrealistic to conclude that the authors of the Directive believed that global identifiers are indeed a special category of data, which might need additional protection. Nevertheless, when we take into account what we explained in the previous sections, we can at least conclude that it is surprising that they have left the matter up to the member states, especially given the (not necessarily illegal) *linkage capacity* that arise from the usage of global identifiers.[58]

As a result, the following scenarios can be formulated:

- If the usage of global identifiers is forbidden in the Member State, the Data Protection Authority has the important task of verifying that context-specific numbers are indeed not being used outside their respective contexts.
- If the usage of some or all global identifiers is regulated, the Data Protection Authority mainly verifies whether the conditions under which that identifier can be processed are fulfilled.
- If the usage of global identifiers is allowed or at least not being regulated, the Data Protection Authority only verifies whether the number is being processed within the limits of the data protection regulation (finality, proportionality, protection level etc.), as explained above.[59]

3.2.8 Appropriate technical and organizational security measures

The fact whether the usage of global or other ID numbers is regulated or not by a Member State does not affect the application of the data protection rules. These rules serve as a minimum, from which the Member State cannot derogate.

As a result, in addition to the rules briefly recapitulated in the previous chapters, the data controller should take the appropriate organizational and technical security measures to protect the personal data against a number of things (e.g. destruction, loss, alteration etc), including *any unlawful form of data processing* (article 17 of the Directive).[60]

[58] See on the topic also, for example, Cullen International 1999, p. 58, where is explained that these numbers can be used as a key to connect files on a national level, and consequently build a very complete profile of the individual.

[59] See De Bot 2005, p. 56.

[60] 'Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'

To evaluate the ‘appropriateness’ of the measures, three factors play a role, namely (1) the state of the art, (2) the cost of their implementation and (3) the risks represented by the processing and the nature of the data to be protected (article 17 of the Directive). This requires some additional explanation:

- The risks resulting from the *nature of the data* for example result from the data itself, the nature of the purposes of the data processing, the legal relation between the data controller and the data subject etc.
- Risks represented by the *data processing* are, for example the location where the data are being processed, the fact that there are multiple data processors, the used technique etc.
- The fact that account should betaken with the *‘state of the art’* means that the data processing should take into account the technological evolution. The security measures should progress accordingly. Recital 46 of the Directive further explains that the security obligation requires that appropriate technical and organizational measures are in place, both at the time of the *design* of the processing system and at the time of the *processing itself*, particularly in order to maintain security and thereby to prevent any unauthorized processing.[61]

The whole idea is thus to ensure a level of security appropriate to the risks represented by the processing at stake.

Interesting in a public sector context is that it is not possible to make exceptions to these security rules: *exemptions and derogations are possible for the purpose of balance between fundamental rights as regard to legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority, but not with regard to the security of the processing* (recital 37 of the Directive).

3.2.9 Evaluation

Our basic finding and main point of departure is that identifiers are definitely needed in the public sector, especially to achieve the goals of eGovernment, for instance, *‘the integration of back-offices’*. Without data protection rules, it seems obvious to choose common, *global identifiers* between these back-offices, and not technically to be constrained by *context- and or sector-specific identifiers*. The question we have raised is whether the usage of global identifiers within a sound legal framework can be acceptable from a legal perspective for the default data exchange between two or more government entities or not. The alternative would be to choose *technical unlinkability* as a *requirement* of an eGovernment architecture, which would imply the usage of context- and/or sector-specific identifiers.

At the other side of the spectrum, we also analyzed the data protection rules. From this perspective, we conclude that:

- If the usage of global identifiers is forbidden in the Member State (e.g., because it is unconstitutional), technical unlinkability should be a requirement of the architecture design.

[61] Cuijpers 2006, p. 68 Title III, referring, among other to the Advice 9/2001 of the Article 29 Working Party on computer crime.

The Data Protection Authority has the important task of verifying that context-specific numbers are indeed not being used outside their respective contexts.

- If the usage of some or all global identifiers is regulated, the basic data protection rules still apply. The additional rules should take the data protection principles as a minimum. The Data Protection Authority here mainly verifies whether the conditions under which that identifier may be processed are fulfilled.
- If the usage of global identifiers is allowed or at least is not forbidden, the Data Protection Authority only verifies whether the number is being processed within the limits of the data protection regulation (finality, proportionality, protection level etc.), as explained above.[62]

We also conclude a number of additional, crucial issues when having a closer look at the data protection principles. From this analysis we indicate that:

- The data controller should make sure that the chosen data (for example, a global ID number instead of a sector-specific one) is adequate, relevant and *not excessive* in relation to the purposes for which it is being collected and/or further processed. In other words, a global identifier can be excessive in relation to the purposes for which the data is being collected. For instance, if no legitimate cross-context or cross-sector data exchange is present at the first processing the ID number, a context- or sector-specific identifier should suffice.
- The data controller should make sure that the ID number is *not kept in a form which permits identification* of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed.

  In practice, this means that when the purposes of processing the ID number have been realised, it should be anonymized. Encrypting or encoding the ID number will most probably not be sufficient if the reason why the ID number is being processed like that (encrypted …) is to be able to re-identify the person if needed. In that case, as explained, the ID number would still be *identifiable* data – and thus also *personal data*.
- *To evaluate the necessary, 'appropriate' technical and organizational security measures*, 3 factors play a role, for instance: (1) the state of the art, (2) the cost of their implementation and (3) the risks represented by the processing and the nature of the data to be protected. We believe that the state of the art means that security measures should follow the technological evolution.

  This means that if technologies to ensure unlinkability between contexts and sectors mature sufficiently (which is more and more the case today) they should be chosen if they are more conducive towards achieving the goals of the processing. It also means that it can be an unacceptable risk to not take unlinkability measures.

  Yet, this is also the tricky part of the answer to the above mentioned question on 'technical unlinkability': *it depends on the evaluation of the case at stake.*

[62] See De Bot 2005, p. 56.

- *Until now, in Belgium*, the decision was taken to use only one global identifier as the default position in eGovernment. The usage of this identifier is legally controlled and in specific contexts with highly sensitive data (eHealth and justice data), negotiations are going on to add in context-specific identifiers.

  All in all, *at first sight* we could argue that in Belgium the technical and organizational security measures seem 'appropriate' given the concrete risks vs. cost evaluation vs. measures taken to protect against these risks.

  Nevertheless, there seem also to be valid arguments against the usage of global identifiers *as the default position for every data exchange in eGovernment in Belgium.* For instance, we should also take into account the fact that:

  - All data processing is important, especially because the default position is that data processing is forbidden.
  - The technology to implement sector- / context-specific identifiers that is, for example derived from the existing global identifier is not expensive.
  - The data controller should at least make sure – by restraining the technological means used to process the data, in this case the ID number – **that he avoids any unlawful data processing.** As we will explain in the country report, this is currently a problem in Belgian eGovernment.
  - *One important risk that should be taken into account, is that data processing purposes* are more likely to be adaptable (and thus legitimate) in the public sector than in the private sector. When two or more *government entities integrate their back-offices*, there will typically be a *reuse of personal data* for another purpose than the one that was originally indicated.[63]

    There is a realistic risk that once the necessary infrastructure which includes global ID numbers is in place, data exchange based on that number will take place anyway, legitimately or illegitimately, based on ad hoc arguments or on different political choices. As a result, this seems to be a strong argument for context- and/or sector-specific identifiers, when we have to balance the cost of its implementation and the risks created by the nature of the data and the processing.

3.2.10 Conclusion

To conclude, based on the mentioned data protection principles, there seems to be no general obligation to add in sector- or context- specific identifiers on a large scale, as the default position for every data exchange in eGovernment:

However, there are a number of arguments against the usage of global identifiers in eGovernment, as the default position as well.The evaluation takes into account a number of factors, being (1) the state of the art, (2) the cost of the implementation and (3) the risks created by the nature of the processing and the data itself.

[63] The Belgian law even explicitly says that account – to evaluate whether a particular 'reuse' or further processing is incompatible with the original purposes, account should be taken of *'all relevant factors, in particular the reasonable expectations of the data subject and the applicable legal and regulatory provisions.'*

If we take Belgium as an example, the appropriate technical and organizational security measures here seem at first sight to be taken, because we can also take into account *the legal framework that makes data exchange based on the global identifier subject to a prior authorization of the privacy commission (see the country report).*

Nevertheless, it appears that there are also important risks created by the usage of global identifiers in Belgian eGovernment, among other things, because it is much more easy for the public sector to adapt the purposes and legitimacy grounds upon which a particular data processing is based. Therefore, it seems reasonable that the data controller should at least make sure – by restraining the technological means used to process the global ID number (in this case the 'Rijksregisternummer', see the country report), to avoid any unlawful data processing.

References

Law of 11 December 1998 on the transposition of the Data Protection Directive 1995, Belgian State Gazette 3 February 1999.

Explanatory memorandum of the Reform of the Data Protection Law, session 1997-1998, document number 1566/1, available on the website of the Chamber of Representatives, available on www.dekamer.be.

Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, Belgian State Gazette 18 March 1993, as modified by the law of 11 December 1998 implementing Directive 95/46/EC, Belgian State Gazette 3 February 1999, and the law of 26 February 2003, Belgian State Gazette 26 June 2003.

ARTICLE 29 DATA PROTECTION WORKING PARTY 2007

Opinion 4/2007 of 20th June 2007 of the Article 29 Data Protection Working Party on the concept of personal data, available at: http://ec.europa.eu/justice_home/fsj/privacy/ workinggroup/index_en.htm.

BAUER, MEINTS & HANSEN 2005

M. Bauer, M. Meints & M. Hansen (eds.), *D3.1, Structured Overview on Prototypes and Concepts of Identity Management Systems, Deliverable 3.1 of the EU Funded FIDIS project,* available at: http://www.fidis.net/fileadmin/fidis/deliverables /fidis-wp3-del3.1.overview_on_IMS.final.pdf, 15 September 2005, last visited: 20 August 2006.

BELGIAN PRIVACY COMMISSION 2005

Advice of the Belgian Privacy Commission with regard to the evocation of the files SCSZ /05/70, SCSZ /05/90, SCSZ /05/110 and SCSZ/05/113 on identification via the Crossroads bank for Social Security or via the RRN, number SA2/EV/2005/001, 28 September 2005, available at: www.privacycommission.be, last visited: 23 March 2006.

DE BOT 2005

D. De Bot, 'Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart.', *Vandenbroele*, Brugge, 2005, 469 p.

CUIJPERS 2006

C. Cuijpers, 'De Europese Privacyrichtlijn van 25 oktober 1995', Afl. 20, Januari 2006, in P. De Hert (ed.), *Privacy en Persoonsgegevens*, Brussel: Politeia, losbladig.

CULLEN INTERNATIONAL 1999

Cullen International, *a business guide to changes in European data protection legislation*, The Hague: Kluwer Law International 1999.

DEPREST & ROBBEN 2003

J. Deprest & F. Robben, *eGovernment: the approach of the Belgian federal administration*, available at: http://www.ksz.fgov.be/En/Como/2003%20-20EGovernment%20paper%20v%201.0.pdf, June 2003, last visited: 20 June 2006.

DEPREST & STRICKX 2005

J. Deprest & P. Strickx, *eGovernment initiatives*, available at: http://www.ibbt.be/egov/pres/9._Jan_Deprest_-2005.10.26-_eGov_update_ initiatieven.ppt, 26 October 2005, last visited: 20 September 2006.

DIRECTIVE 95/46/EC

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 on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995, 31-50.

HODGES 2006

J. Hodges (ed.), *Liberty Technical Glossary*, available at: http://www.projectliberty.org/specs/draft-liberty-glossary-v2.0-05.pdf, 9 June 2006, last visited: 15 June 2006.

HODGES, PHILPOTT & MALER 2005

J. Hodges, R. Philpott & E. Maler, *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*, available at: http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf, 15 March 2005, last visited: 22 December 2005.

HILDEBRANDT, GUTWIRTH & DE HERT 2005

M. Hildebrandt, S. Gutwirth & P. De Hert (eds.), *Fidis Deliverable 7.4, Implications of profiling practices on democracy and rule of law*, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.4.implication_ profiling_practices.pdf; 5 September 2005, last visited: 15 September 2006.

ITU-T 2005

X, *Security Compendium Part 2 - Approved ITU-T Security Definitions*, available at: http://www.itu.int/ITU-T/studygroups/com17/def005.doc, May 2005, last visited: 20 April 2006.

KISSEL 2006

R. Kissel (ed.), *NIST IR 7298. Glossary of Key Information Security Terms*, available at: http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key _Infor_Security_Terms.pdf, 25 April 2006.

MEINTS 2005

M. Meints, *D3.5: Workshop on ID-Documents, Deliverable 3.5 of the EU funded FIDIS project*, available at: http://www.fidis.net/fileadmin/fidis/ deliverables /fidis-wp3-del3.5.workshop_on_id_docs.pdf, September 2005, last visited: 19 September 2005.

MODINIS IDM 2005

X., *Modinis IDM Terminology Paper*, available at: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis. terminology.paper.v2.01.2005-11-23.pdf, 23 November 2005, last visited: 23 November 2005.

NABETH 2005

T. Nabeth (ed.) *D2.3 Set of use cases and scenarios, Deliverable 2.3 of the EU funded FIDIS project*, available at: http://www.fidis.net/fileadmin/fidis/ deliverables/fidis-wp2-del2.3.models.pdf, September 2005, last visited: 28 March 2006.

NABETH & HILDEBRANDT 2004

T. Nabeth & M. Hildebrandt (eds.), *Inventory of topics and clusters, Deliverable 2.1 of the EU funded FIDIS project*, available at: http://www.fidis.net/fidis-del/period-1-20042005/d21/, 28 October 2004, last visited: 25 January 2005.

PFITZMANN & HANSEN 2006

A. Pfitzmann & M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, available at: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology _v0.27.pdf, 20 February 2006, last visited: 20 February 2006.

ROBBEN 2006

F. Robben, *Gebruik van de elektronische identiteitskaart in de sociale sector: concrete toepassingen en toekomstige visie*, available at: http://www.ksz.fgov.be/documentation/fr/documentation/Presse/20060314a.ppt, 14 March 2006, last visited: 20 September 2006.

ROBBEN 2005

F. Robben: *1st Modinis Workshop on Identity Management in EGovernment*, available at: http://www.law.kuleuven.ac.be/icri/frobben/presentations/ 20050504.ppt, 4 May 2005, last visited: 30 March 2006.

RÖSSLER 2002

T. Rössler, *Identification and Authentication in Networks enabling Single Sign-On*, available at http://www.iaik.tu-graz.ac.at/teaching/11_diplomarbeiten/archive/roessler.pdf, October 2002, last visited: 15 October 2005.

SLONE 2004

S. Slone, *Identity Management. A white paper*, available at: http://www.opengroup.org/onlinepubs/7699959899/toc.pdf, March 2004, last visited: 11 November 2004.

ZUCKER 1986

L.G. Zucker, 'Production of trust: Institutional sources of economic structure, 1840-1920', In, B.M. Staw & L.L. Cummings (ed.), *Research of organizational behavior*, London (UK): JAI Press Inc. 1986, pp. 53-111.

3.3 ID numbers from a social perspective

3.3.1 Introduction

In this chapter it is shown, that ID numbers, their functions and impact on society can be understood in different ways by using different theories established in social science. An analysis is presented, based on social systems theories. This allows for a more general analysis of the introduction and functions of ID numbers and the resulting consequences of their use in societies. The Weberian bureaucracy theory allows the detailed analysis of the introduction and use of ID numbers in the context of the administration of states. Though some findings can be commonly made, using in both angles theoretical backgrounds, they have a different focus and in combination make a better coverage of relevant social aspects possible.

3.3.2 Functions, benefits and drawbacks of ID numbers

Introduction

ID numbers fulfil mainly three functions. They are used:

- For naming an object
- As (context specific) identifiers ("this but not that") and
- As an address for (context specific) operations or communications.

This contribution looks into these functions of ID numbers in society, using social systems theories as a theoretical background. In this context the relationship between ID numbers and organisations is important.[64]

The difference between names, identifiers and addresses

Names are used as symbols[65] to describe "objects"[66], attributes and relations. Names start to be relevant when appearing in communications. Communication is understood as a logical representation of the world using languages, but reaches farther than a pure naming and description of objects and persons. Language allows naming an artefact, for example a "tree" or an "elbow". But in addition a status of an object or a relationship between multiple objects can be described. Typically such a status does not have a body. Examples for this are "to fall in love" or relationships such as "she/he is mother/father of someone". Names get their

[64] Social systems theory already was introduced and described in the FIDIS Deliverable D5.2b in chapter 4.3 (Leenes 2006, p. 43).

[65] The term symbol originates from the Greek terms "sym" and "ballein" describing "something that is put together". Symbols are used as representations for objects, persons, ideas, concepts and other abstractions. The use of symbols enables objective descriptions and at the same time supports abstraction and construction.

[66] In this context we understand objects as a physical entity, i.e., something that is tangible and within the grasp of the senses. Note that individuals (human beings) are also objects according to this definition.

meaning in the eyes of an observer as they are set in a specific context. Observing in the meaning of cognition, or more specific: of re-cognition. Even in a given context names are not necessarily unique. One example for this is a tree that is for sure not unique in the context of a forest.

Names turn into identifiers when they are used in a communicational context to discriminate objects, which could also be persons. For example an apple can be discriminated from a pear, and through this discrimination the apple in front of an observer can be identified. In this context two requirements have to be met: At first the difference between the identified object and the reference object needs to be stable. Simply put: An apple must not turn into a pear. The second requirement addresses the participants in the communication. They have to remember the difference between different objects with respect to the relevant aspects or a relevant perspective of observation. Names and identifiers always must be used in the same way by participants of communications. Or simply put: An apple has to be named and identified always as an apple, not as a pear. In this case a specific identifier has a comparable meaning for all participants of communications.

Certain identifiers are always used in the context of a specific operation, for example as a target for the operation. If this identifier in addition to an object also identifies a specific operation, we can speak more precisely of an address. For specific operations specific addresses are used. They typically show a certain structure which is built up using an operation specific set of rules. As a result a license plate number or Cartesian coordinates are for example not usable as addresses instead of a URL in a web browser or an e-mail address. The set of rules for generating and using an address typically is set up by at least one organisation.

Described in a more general way addresses are always administered (generated, assigned and deleted or deactivated) by organisations. Organisations also take care to resolve potential address collisions to keep addresses unique in the particular scope of the operation. In the context of persons, the State with its executive monopoly ensures addressability for governmental, private-sector or interactional (citizen to citizen) operations. Addressability today covers persons, families, organisations and objects in the context of communication techniques. Addressability is not possible without organisations.

To sum up: a name is used to construct objects. An identifier names (and constructs) a specific object in a particular communicational context in difference to other objects. An address identifies an object in the context of a specific operation. Addresses do not only identify objects in the context of the operation, but also the operation itself in difference to other operations.

Names, identifiers, addresses and ID numbers

ID numbers can fulfil all three described functions. They can be used as names for a data set or a number of data sets in a database. They can be used as identifiers if they name a data set or dataset linked to one person uniquely for example in the context of an administrative procedure. ID numbers also can be used as addresses. As shown in the country reports, the rules applied to constitute ID numbers in many cases identify the operation (e.g. administration of income tax, social insurance etc.) in which these particular ID numbers are used.

We now want to take a look at the use of ID numbers to get a more precise understanding of their use. Social scientists distinguish three types of social systems:

- *Interactional systems* (types of communities in which members are not subject to particular rules, but nevertheless schemes apply; examples are spontaneous meetings as neighbours, spontaneous encounters)[67]
- *Organisational systems* (characteristics are membership and effective production of decisions; examples are public bodies, institutes and companies)[68]
- *Functional systems* (economy, law, politics and science as "self-conducted" communication systems)[69]

Social systems theories makes it possible to distinguish between organisations and society. So one can analyse the influence of organisations in and on society. The advantage of this perspective is that research results and findings can be used for any organisation, including public administrations. At the same time specific aspects such as the influence of bureaucracy in the public sector on the development and use of ID numbers or socio cultural aspects do not directly fit in social systems theories. For this reason these aspects are not covered in this chapter. They will be elaborated in the next chapter.

Typically for interactional systems the first names and sometimes the surnames are used to name participants in communication, to identify and to address them. An example is the opening phrase: "Hello Peter, how are you?" In Germany and many other middle European countries such as UK and France, surnames in the medieval age in many cases evolved from the role of a person in society, especially from their job. Examples are Schneider (tailor), Fischer (fisherman), Meier (dairy-farmer) or Müller (miller). The job description as surname expressed the expectation of the society on a particular person bearing this name. This type of surnames is not an example of the use of names as identifiers only but also of addresses (including the function of the person in a local organisational context).

In medieval times the hierarchy of the society was very stable, largely accepted by the people and changes in this hierarchy were relatively small and did not occur very often. People carried out the same jobs for generations. The structure of the medieval society was accepted as introduced by God and thus as logical. Together with an increasing functional differentiation starting at the end of the medieval age polycentric societies evolved, with many organisations "in it". The autonomy of an individual became increasingly important in such societies; democracy offered a way in which citizens could select governments of their choice together with the corresponding political programme.

[67] Kieserling 2000.
[68] Luhmann 2000; Baecker 1999.
[69] Luhmann 1997.

With increased complexity of society traditional schemes to address individuals and organisations proved to be insufficient. As a result additional identifiers and addresses were introduced – in many cases ID numbers were used for this purpose as they are unique in a much larger context compared to names. This is an important aspect in the context of machine supported operation and machine accessibility and addressability of individuals and organisations and related data (industrialisation of data processing).

ID numbers are typically used in organisational systems, especially to identify and discriminate members and clients of the organisation. In addition to the examples of public or official ID numbers listed in this deliverable, also IP addresses, customer or vendor numbers issued by many enterprises and phone numbers can be listed. Other more specific examples for ID numbers are functional identifiers which are used especially in governmental institutions in Switzerland, Austria and Germany. They are used to describe functions within the organisation independent from the person holding the function at present. They are passed along to a successor in case the original holder of the function moves to another function or changes the organisation. Functional identifiers are also used to address the present function holder in processes and workflows within the organisation. In some cases they are used as naming part in functional e-mail addresses.

Examples are the functional identifier of the authors of this article within ICPP: LD3.2 and LD10.2. LD stands for ICPP in the context of the public administration of the Federal State of Schleswig-Holstein in Germany (LD is **L**andes-**D**atenschutzbeauftragter), 3 or 10 stands for the departments the authors work in and .2 is the forthcoming number of the authors in the corresponding departments. In this case the naming part of the e-mail addressees of both authors also is derived from the functional identifier: {LD32|LD102}@datenschutzzentrum.de. In many cases this type of functional identifiers also maps to a job description independent of the person currently carrying the correspondent ID numbers.

Other examples for functional identifiers are certain phone numbers used for functions in organisations. Traditional examples are service or service desk numbers which in many cases use special prefixes (e.g. +800 or +180x etc.) and frequently are used by many people at the same time.

ID numbers aim at identifying a person or organisation uniquely in the context of operations run by an organisation. In many cases ID numbers are introduced and used by governmental institutions. They allow due to their uniqueness linking up database entries, transactions or partial operations across data sources or borders of institutions.

Potential benefits and drawbacks of ID numbers

Potential benefits mainly can be observed for organisations and their members. Relevant benefits are increased effectiveness in administration, processes and decision making and increased accessibility and quality of data. Clients of organisations also may have benefits for example convenience in case ID numbers are used to simplify communication e.g. by avoiding repeated input of the same basic data.

Potential drawbacks can be observed mainly for clients of organisations in case linkability through ID numbers is used to create information asymmetry in favour of organisations. Information asymmetry may lead to market failure (so called lemon markets).[70] In addition information asymmetry may be used by organisations to reduce the autonomy of the individuals in society and thus may result in a shift of the balance of power in favour of organisations.[71]

From the perspective of citizens it is difficult to decide whether benefits or drawbacks are predominant. The reason may be that citizen are as well members of the state (as responsible citizen in a modern western democracy) as clients (when they have obligations towards governmental institutions e.g. to pay their tax or when they benefit from a service). While loss of autonomy on one hand increases obligations of citizens in their role as clients of the organisation (in this case the state) it may at the same time raise the benefit of the organisation and thus indirectly the benefit of citizens in their role as members of the state.

References

AKERLOF 1970
G. A. Akerlof, ‘The Market for 'Lemons': Quality Uncertainty and the Market Mechanism’, *Quarterly Journal of Economics* 84 (3): 488–500, Aug. 1970. Download: http://links.jstor.org/sici?sici=0033-5533%28197008%2984%3A3%3C488%3ATMF%22QU%3E2.0.CO%3B2-6

BAECKER 1999
D. Baecker, *Organisation als System,* Suhrkamp, Frankfurt am Main, 1999.

HILDEBRANDT, GUTWIRTH & DE HERT 2005
M. Hildebrandt, S. Gutwirth & P. De Hert, *FIDIS Deliverable D7.4: Implications of profiling practices on democracy and rule of law*, Frankfurt a. M., September 2005.

KIESERLING 2000
A. Kieserling, *Kommunikation unter Anwesenden – Studien über Interaktionssysteme,* Frankfurt am Main, 2000.

LEENES 2006
R. Leenes, *FIDIS Deliverable D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, Frankfurt a.M., 2006.

LUHMANN 2000
N. Luhmann, *Organisation und Entscheidung,* 1st Edition, Westdeutscher Verlag, Opladen/Wiesbaden 2000.

LUHMANN 1997
N. Luhmann, *Die Gesellschaft der Gesellschaft,* 1st Edition, Suhrkamp, Frankfurt am Main, 1997.

[70] Akerlof 1970.

[71] See e.g. Hildebrandt, Gutwirth & De Hert 2005 analysing the potential impact of profiling practice for democracy and rule of law.

3.4 ID-numbers: Symbols of Bureaucracy

Isabelle Oomen, University of Tilburg, TILT

Over the past centuries, Western societies have become more and more rationalized and this process is still ongoing. The process of rationalization took place in various domains, for example in arts, science, technology, economy, and politics. Rationalization in one domain enabled or accelerated rationalization in other domains. Rationalization of art resulted not only in using perspective in drawing, but also the use of pointed arches to span larger spaces. Science was, in this period, established as an empirical-theoretical founded science which stressed the use of rational thinking and testing theories in the empirical world. Inventions like the steam-engine and smallpox vaccine were made possible by the rationalization of technology. The invention of the steam-engine enabled, amongst other factors, the rationalization of economy, i.e. the transition of a traditional to a capitalistic economy. Political rationalization resulted in the formalization of the state. Formalized states have the form of a political institution with a unique combination of properties: 1) a written constitution, 2) a judicial system based on this constitution, and 3) a corps of civil servants that is specially trained and restricted to regulations.[72] At the end of the 18th century, two revolutions took place, one economical (the Industrial Revolution) and one political (the French Revolution). Both revolutions were not only a result of rationalization, but also a catalyst to rationalization. Although the Industrial Revolution started in England and the French Revolution took place in France, they influenced all Western societies.[73]

Economic rationalization resulted in standardization which, on its turn, led to both the expansion and internationalization of production. A first phase of globalization was created when the consumer culture, which was developed through standardization, increasingly crossed the borders of states, nations, and their traditions. The political rationalization and the formalization of the state took the shape of nationalism. Nationalism is both a component of and a reaction to globalization and the 'process of modernization'. By the turn of the century, the nation was represented as a unique and essential unity, the living body of its citizens. The idea of the nation state was consciously constructed by the state through a wide range of cultural manifestations that contributed to a deliberate policy. Rietbergen noticed that:

> 'All over Europe, traditions were 'invented' to give citizens a feeling of centuries old solidarity. All over Europe, history was rewritten or written anew from the point of view of the state as the natural structure in which the nation and the community expressed itself politically. This new past was then glorified by governments as a unity factor by emphasizing the importance and results of a commonly fought battles, the role of great men – rarely women -, and the glorious feasts of the past, now presented as a 'national' past of the nation's shared heroism'.[74]

[72] Ultee, Arts & Flap 1996.
[73] Rietbergen 1998.
[74] Rietbergen 1998, p. 352.

The main goal of these nationalizing campaigns was to secure internal cohesion and peace by creating unity. Both internal cohesion and peace were seen as necessary preconditions to pursue well-founded foreign policies and to maintain a leading position in the increasingly expanding world market. A general feeling of community among people would support the ruler's claims to sovereignty and the pretensions to power of those who led 'the nation'. The ideology of the nation state was propagated by all means possible by governments in order to advance solidarity.[75]

In order to establish who is part of the nation state and who is not, the government needs to identify its citizens. The necessity of identification is twofold: 1) in order to carry out its most fundamental tasks (i.e. tax collection, provision of social services, control of movements, etcetera), the government needs to know who is obliged or entitled to what and thus needs to identify its citizens and 2) as a nation state is a state of and for particular 'peoples' defined as a mutually exclusive group of citizens, identifying a person and establish his or her nation state membership is to create a social group and hence solidarity.[76] For the monopolization of the rights of the states, the procedures and mechanisms for identifying persons are essential because the notion of national communities must be codified in documents or files rather than merely 'imagined'. This stimulated techniques that uniquely and unambiguously identified each and every person from life to death (i.e. last name, given names, date of birth, town or city of birth, full names and birth dates of parents, partners, and children, etc. were all written down in documents) transforming states into administrative organizations. Bureaucracies were constructed, designed to implement this regime of identification and to scrutinize persons and documents in order to verify identities.[77] Bureaucracies are, according to Weber, the ultimate example of rationalization, which he defined in terms of five elements: 1) efficiency, 2) predictability, 3) quantifiability or calculability, 4) control through substituting human judgement by nonhuman technology, and 5) the irrationality of rationality. Bureaucracies are controlling both the bureaucracy's clients and their employees. The government provides only certain services, and not others and one must apply for the services on a specific form by a specific date, and one will receive those services only in a certain way. In offices, each task is broken up into a number of components, and each office is responsible for a separate portion of the task. Employees in each office handle only their own part of the task, usually following the rules and regulation in a predetermined sequence. The structure of bureaucracies is in such a way as to guide people or even to force people to choose certain means to ends.[78]

For these administrative purposes, it was necessary to distinguish people by identifying them uniquely and unambiguously, so 'cards' and 'codes' were developed. Cards, i.e. passports and identity cards, are the mobile versions of the 'files' governments used to store knowledge about their citizens. Therefore, the document held by the individual as ID corresponds to an entire series of files.[79] This also holds for codes, ID-numbers and file numbers for example, but they have additional characteristics. Because codes are numbers, and hence made up of

[75] Rietbergen 1998.
[76] Ultee, Arts & Flap 1996; Rietbergen 1998; Torpey 2000.
[77] Torpey 2000.
[78] Collins 1994; Ritzer 1998; Turner, Beeghley & Powers 1998; Wallace & Wolff 1999.
[79] Torpey 2000.

digits, they have no meaning in themselves until that meaning is communicated. ID-numbers are symbols of identities in, at least, the bureaucratic culture. Shiraev and Levy defined culture as followed:

> 'Culture is defined as a set of attitudes, behaviours, and symbols shared by a large group of people and usually communicated from one generation to the next. Attitudes include beliefs (political, ideological, religious, moral, etc.). Behaviours include a wide variety of norms, roles, customs, traditions, habits, practices, and fashions. Symbols represent things or ideas, the meaning of which is bestowed on them by people. A symbol may have the form of a material object, a colour, a sound, a slogan, a building, or anything else. People attach specific meaning to specific symbols and pass them on to next generation, thus producing cultural symbols'.[80]

According to this definition, ID-numbers are symbols because they only have meaning which is bestowed on them by people, i.e. one has to know that a particular number is an ID-number. This relates to the second characteristic: ID-numbers themselves are not important, but the information attached to this number, i.e. the quantity and nature of the files the ID-number refers to. Three types of files can be attached to national ID-numbers for three different purposes. The first and foremost purpose of ID-numbers is that they are used to distinguish among individuals and to identify the individuals uniquely and unambiguously: 'who is this?' or 'is this the same person?' The information used to identify individuals can be name, address, date of birth, place of birth, and a photograph. These types of files are passports or identity cards, but can also be the registration files at local or national level. Often, these files also include additional information like the names of the parents, children, partner, or other relatives along with the marital status of the individual. The second purpose of the usage of ID-numbers by the government is that the government has to carry out its most fundamental task. The basic questions here are: 'what obligations has this individual to the state?' and 'to which services is this individual entitled to?' For the collection of taxes, the provisions of services, and the control of movements of the individual, the government holds files containing information about individuals. Personal information in these files are, for example, income, entitlement to state benefits, criminal record, etc., along with personal information that identifies the individual. The third type of files are the files that are held by third parties, like banks hospitals, and health insurance companies. They can also use the national ID-number to identify an individual, which is regarded to be more reliable than other forms of identification.

Although an ID-number should uniquely identify the individual, it also depersonalizes that individual, i.e. the individual is no longer referred to by personal characteristics like a name, address, or date of birth, but by a number. The use of ID-numbers, instead of personal identifiers, can cause alienation of that individual from the state whereas the state's intention was to embrace their citizens by giving them a national identity. On the other hand, the use of ID-numbers can enhance the knowledge the government has about its citizens. Attaching more files and more types of files to an ID-number, enhances the linkability of the separate files and hence the possible knowledge the government or a third party has about the individual.

[80] Shiraev & Levy 2004, p. 4.

Conclusion

We have seen how the economic and political rationalization of Western societies have led to the emergence of bureaucracies and the intention of nation states to embrace their citizens. For both the fundamental tasks the government has to carry out and the wish of the government to create a national unity, it was necessary to distinguish individuals by identifying them uniquely and unambiguously. Therefore, 'cards' and 'codes' were developed. ID-numbers symbolize the identity of individuals, as well as all other files attached to this number, enhancing the linkability of the files and hence the possible knowledge about individual. ID-numbers don't create a notion of unity among citizens, but they create a notion of privacy loss instead. This is what Weber called 'the irrationality of rationality'. So, ID-numbers are not only symbols in the bureaucracy, but also symbols of bureaucracy.

References

BERRY, ET AL. 2002
J.W. Berry, et al., *Cross-Cultural Psychology. Research and Applications (2nd edition),* Cambridge: Cambridge University Press 2002.

COLLINS 1994
R. Collins, *Four Sociological Traditions,* Oxford: Oxford University Press 1994.

RIETBERGEN 1998
P. Rietbergen, *Europe. A Cultural History,* London: Routledge 1998.

RITZER 1998
G. Ritzer, The Weberian Theory of Rationalization and the McDonaldization of Contemporary Society. In P. Kivisto (ed.) *Illuminating Social Life. Cassical and Contemporary Theory Revisited,* Thousand Oaks: Pine Forge Press 1998.

SHIRAEV & LEVY 2004
E.B. Shiraev & D.A. Levy, *Cross-Cultural Psychology. Critical Thinking and Contemporary Applications (2nd edition),* Boston: Pearson Education Inc 2004.

TORPEY 2000
J. Torpey, *The Invention of the Passport. Surveillance, Citizenship and the State,* Cambridge: Cambridge University Press 2000.

TURNER, BEEGHLEY & POWERS 1998
J.H. Turner, L. Beeghley & C.H. Powers, *The Emergence of Sociological Theory (4th edition),* Belmont, CA: Wadsworth Publishing Company 1998.

Ultee, Arts & Flap 1996
W. Ultee, W. Arts & H. Flap, *Sociologie: vragen, uitspraken en bevindingen,* Groningen: Wolters-Noordhoff 1996.

WALLACE & WOLFF 1999
R.A. Wallace & A. Wolff, *Contemporary Sociological Theory. Expanding the Classical Tradtition* (5th edition), Upper Saddle River, NJ: Prentice Hall 1999.

3.5 Summary of the sociological approaches

Martin Meints (ICPP)

Based upon two different theories, social systems theories and a theory on the role of bureaucracy in national states, the functions of ID numbers have been investigated.

Social systems theories take a general perspective on society, allowing the analysis of the function of ID numbers in private and public organisations. ID numbers are introduced and used by organisations (a) to name objects, (b) to identify them (use as identifiers) and (c) to address them in the context of operations (business or governmental procedures) and communication. In addition to individuals, objects in this context also can be groups of individuals (e.g. project teams), organisations themselves, organisational structures within organisations (e.g. departments) and functions carried out and services offered by organisations (e.g. a help desk and corresponding support). ID numbers aim at identifying objects uniquely in the context of operations run by an organisation. In many cases ID numbers are introduced and used by governmental institutions. Because of their uniqueness they allow linking up database entries, transactions or partial operations across data sources or borders of institutions. Linkability enabled by the use of ID numbers may lead to information asymmetry and thus reduce the autonomy of individuals resulting in a shift in power in favour of organisations. In the context of States in many cases it is difficult to decide whether citizens overall take benefit from this development or not. The reason is that citizens typically take over two roles with respect to the State. On one hand they are members and thus take benefit from a strong state able to protect them, on the other hand as clients of the state they suffer from reduced autonomy.

The second social analysis focuses on the role of ID numbers in national states. Bureaucracy can be understood as the result of rationalization of governmental procedures. A necessary prerequisite for this rationalization is unique identification of citizens. ID numbers, by themselves in most cases meaningless, are used as symbols for an individual. This use automatically implies that not the ID numbers themselves are relevant, but the information, organised in files, and linked to them is. Their main purpose is creating linkability among these files. From the perspective of the citizens ID-numbers don’t create a notion of unity as citizens of a nation, but they create a notion of alienation and privacy loss instead. So, ID-numbers are not only symbols in the bureaucracy, but also symbols of bureaucracy.

3.6 ID-Number Policies and Profiling Practices

Mireille Hildebrandt, Vrije Universiteit Brussel

In this section we will explore the relationship between ID-number policies and advanced profiling practices, as envisioned in scenarios of Ambient Intelligence. After summarising the key findings of FIDIS research on profiling in the context of AmI (3.6.1) we will discuss the legal-technological infrastructure that enables automatic and autonomic profiling (3.6.2). To this effect we will explore three scenarios of AmI, defined in a FIDIS workshop of January 26th 2007, with regard to the choice between a policy of single or multiple ID numbers to be used in the public and/or private sphere. We will conclude with comparison of unification (attainable by means of a single ID-number policy) and interoperability (attainable by means of a multiple ID-numbers policy) (3.6.3).

3.6.1 Key findings of FIDIS research on profiling (workpackage 7)

- Profiling is another term for pattern recognition. All living organisms cope with their environment thanks to permanent profiling of and adaptation to (and of) their environment.[81] Automatic profiling (based on clustering, association rules, etc.) produces a new type of exploratory knowledge, used for decision-making in the context of business, insurance, credit-scoring, health(care), anti-money laundering and criminal investigation. The correlations 'discovered' in the process of KDD (knowledge discovery in databases)[82] may allow service providers and government authorities to predict the habits and preferences of individual citizens, without them being aware of this. This facilitates targeted services, preventive medicine, crime prevention, but also allows manipulation and discrimination.[83]

- Data protection regimes focus on personal data, not on the results of KDD. In the case of anonymisation D95/46EC may not even be applicable, while anonymisation does not exclude the use of data mining techniques such as KDD.[84] In fact, group profiling mostly builds on inferences made on the basis of large amounts of anonymised data (entirely outside the scope of data protection), while the application of such profiles does impact individual persons and societal checks and balances. The legal status of such inferred group profiles is unclear.

- The potential impact of the application of group profiles regards both more and less than the traditional concerns about privacy and security; the focus should be on equality, fairness, liability next to privacy and security.

[81] Hildebrandt 2007.
[82] Custers 2004; Hildebrandt & Backhouse 2005.
[83] Zarsky 2002-2003; Hildebrandt & Gutwirth 2005.
[84] Schreurs & Hildebrandt 2005, pp. 36-59

- The implications of profiling for democracy and rule of law disclose a need to rethink the relation between law, technology and public goods like e.g. privacy, security, equality, fairness and the possibility to attribute liability in the case of harm caused.[85]

- Data protection is focused on data minimisation (prohibition of unlimited collection, prohibition of use for other purposes) and seems to run counter to the need for maximum data collection needed to detect which data are relevant. The paradigms of data minimisation and KDD seem incompatible, because KDD is used to find out which data are relevant all data are needed. Also, data protection focuses on data instead of knowledge, losing interest after data has been anonymised, while the application of group profiles to individual citizens may have more of an impact than the use of personal data. Transparency is needed, for which reason we have introduced the principle of minimisation of knowledge asymmetry.[86]

3.6.2 Enabling legal-technological framework for automatic profiling

Automatic profiling (KDD) requires access to as much data as possible, not because all data are deemed relevant but because KDD is used to establish which data are relevant. In the vision of AmI,[87] the promotion of the Internet of Things,[88] based on pro-active computing, autonomic computing[89] and multi-agent systems (MAS),[90] profiling is *the* enabling technology. It provides the only way to distinguish noise from information and without such discrimination the systems response would become inadequate, causing inefficiency, ineffectiveness, irritation and risk dangerous malfunction. This is the reason that in the vision of AmI the environment is the embodiment of sensor technologies, RFID systems, all interconnected via wireless M2M (MachineToMachine) communications and online databases. The ubiquitous, pervasive and real time monitoring of each and every move, change in temperature, sound or whatever should deliver the content for databases that are continuously updated and mined for significant patterns.

The identification of such patterns allows the identification of individual subjects on the basis of, for instance, behavioural biometric profiling (BBP), without necessarily identifying the individual's name or address. This allows continuous (re)identification of an individual as the same individual – also within different contexts if the pattern recognition is exchanged – while the whole process falls outside the scope of data protection.

In as far as this is a problem, e.g. because a person is not aware of being categorized and not aware of the way the profile influences the risks and opportunities he is offered, one may need a legal right of access to the profiles that are applied. As will be analysed in FIDIS deliverable 7.9 and in the 4th workplan, such a legal right faces two types of obstructions:

[85] Hildebrandt & Gutwirth 2005.
[86] Hildebrandt 2006; Jiang 2002.
[87] ISTAG 2001.
[88] ITU 2005.
[89] Tennenhouse 2000; Want, et al. 2003.
[90] Ronger, et al. 2005.

- the profiles and/or the database in which they are stored, may be protected by an intellectual right or fall within the scope of the trade secret;
- even if these profiles can be accessed, the amount of profiles that is continuously constructed, applied and reconstructed can only be assessed by means of M2M communication. This generates the problem of how a human person can learn to access and assess the knowledge available on her own device: how to imagine a HMI (Human-Machine Interface) that provides meaningful information for the individual citizen.

Solutions for these obstructions are beyond the scope of this deliverable, but they will definitely need a joint effort of computer engineers, legal experts and policymakers.

However, one could try to imagine a situation in which individual subjects are monitored, profiled and identified in an AmI environment to the extent needed to adapt the environment, without necessitating any kind of transcontextual identification. In workpackage 3 this type of privacy protection has been developed conceptually by describing the identity of a person in terms of roles and partial identities, which allow a person to disclose only those personal data relevant within the specific context of either home, work, entertainment, travel, taxation etc. This approach fits with the purpose limitation principle and the requirement for consent in the case a data controller wants to transfer personal data to another organisation. The point of departure is a type of identity management based on user control. The technique to limit data exchange to data concerning the relevant partial identity is the use of pseudonyms.

In the FIDIS workshop on Ambient Law (26th January 2007, deliverable 7.8) 3 scenario's have been identified concerning Ambient Intelligence:

scenario I is user-centric: the user is empowered in AmI, carrying a device with which to control the environment, for example, by determining which data can be exchanged between user and environment. This may be a ‘privacy-friendly’ and perhaps a commercial doom scenario. Key concepts are 'data minimisation', 'contextual integrity', 'partial identities' (pseudonyms).

scenario II is provider-centric: AmI is controlled by the providers of services (and goods, if there still are goods by then). The environment knows exactly who is where and will interact without consent, and perhaps without knowledge, of the user. Data flows freely between users and their devices, service providers, and perhaps third parties as well. This may be a ‘user-friendly’ and commercial Valhalla scenario. Key concepts are 'data optimisation', 'networked environment' and 'distributed intelligence' (the intelligence flows from the interconnectivity).

scenario III is a mix: in acknowledging that hiding data can make the environment less intelligent, while unlimited access to data can make individual citizens vulnerable to undesirable profiling, this scenario aims to achieve some kind of balance by minimising knowledge asymmetry.

These scenarios will be developed in the report on Ambient Law (D7.9), which is due at a later point in time. To assess the choices to be made in ID-number policies, however, it seems highly relevant to determine what impact the choice between single and multiple identifiers would mean for the feasibility of each scenario. Hereunder we will briefly indicate the impact of the use of either single or multiple identifiers within each scenario.

User control

In this scenario the user determines if and which data she will 'leak'.[91] This will severely limit the capacity of the networked environment to match existing group profiles with data of the user; and it will also restrict the construction and testing of profiles because the data from which profiles are inferred are not complete. Some would claim that his will limit or make impossible the intelligence of the environment. We should note that not 'leaking' your data has an impact on the construction of group profiles, which will in the end be less accurate the more people choose to 'hide' their data. Hiding your data may thus result in the inaccuracy of group profiles applied to others, causing them irritation or even harm. This is not an argument against hiding one's data as it may also provide grounds against profiling whatsoever.

In the end this scenario may boil down to the fact that profiles are not inferred by the environment but programmed on the basis of a persons deliberate input. This allows for the use of partial identities and pseudonyms, which, combined with unlinkability beyond the relevant context would protect privacy in the traditional sense of non-disclosure of information.

A unique identifier would severely impact this scenario, because it allows governments and/or server providers to link the pseudonyms via this one cross-contextual identifier, which would enable profilers to link pseudonyms and in the end to create rich profiles out of the profiles linked with the different pseudonyms of the same person.

To facilitate user control via pseudonyms and unlinkability government policy should aim for a multiplicity of identifiers (separating ID numbers for healthcare, taxation, administration of justice, credit-rating and marketing).

We note that this preference for multiple identifiers does not only concern the fact that it facilitates unlinkability of personal data between contexts, but foremost facilitates unlinkability of group profiles per context. Considering the sophistication of profiles in some contexts (e.g. predicting the occurrence of disease) the risks of linking profiles across different contexts is way beyond the risk of linking personal data.

[91] The legal rights and obligations to sustain such a scenario are to be found in the present European data protection framework (D46/95 EC). The technological instruments to enable the exercise of these rights, from the perspective of citizens are discussed in FIDIS deliverable 7.9, chapter 5, especially 5.3: Opacity enhancing functions and tools, being transaction-specific or contex-specific pseudonyms (preventing linkability); privacy preserving data mining (PPDM); selective and non-selective disabling of sensors or RFID tags. Section 5.4 discusses Transparency enhancing functions and tools, being automated privacy policies and history management. Additional supporting technologies mentioned are DRM and Trusted Computing.

The transparent consumer- citizen

If the control of information flows is with the providers we may presume that data as well as profiles will be sold or kept secret to the extent that this generates profits and/or competitive advantages. The environment will be in constant flux, combining real time monitoring with autonomic profiling and automatic adaptation. At the same time government agencies may generate and/or buy profiles to anticipate citizens preferences as well as their violation of legal rules.

However, in the case of AmI many of the collected data will not necessarily be linked to a person's name or address. To achieve an intelligent environment BBP may be one of the most important enabling technologies, allowing pattern recognition and the identification of a person as the same person without a need to identify the person by name or address.[92] This could mean that even in this full-fledged AmI scenario – absent any substantial user control – a person could enjoy the benefits of customised services without being identified in the traditional sense of a unique identifier like a name or address. This means that the introduction of a unique identifier in this context could still make consumers and citizens substantially more transparent, by facilitating linkage of profile to the number ID and linking different profiles to each other via this single number ID. Especially in the case that a unique identifier was to be implemented in both the public and the private sphere, this could easily create the Big Brother watching all of us.

Distributed transparency& contextual integrity[93]

Analysing the violation of 'privacy in public', Helen Nissenbaum has described the increase of public surveillance technologies that tend to make people transparent in their public behaviour. In her argument defending the need to protect 'privacy in public' Nissenbaum has introduced the concept of 'privacy as contextual integrity'.[94] Her main aim is to object to a universal definition of privacy that restricts privacy to:

- limiting surveillance of citizens and use of information about them by government agents
- restricting access to sensitive, personal or private information
- curtailing intrusion into places deemed private or personal

Instead of this a-contextual definition of privacy she advocates a more refined understanding, which takes into account:

- norms of the *appropriateness* of a specific information flow
- norms of flow or *distribution* of information

[92] Note that art. 2 of D46/95 EC defines identifiability in terms of 'physical, physiological, mental, economic, cultural or social identity'. It is as yet unclear what this would mean if a person can be identified as the same person over a period of time or at different locations without being able to link this identity to the civil registration (name, adress etc.).

[93] The present legal framework does not provide a transparency right for the group profiles that are inferred from other people's personal data, unless an automated decision is taken. Within FIDIS deliverable 7.7 and 7.9 arguments are provides to regulate the legal status of profiles that are used to categorise people and influence their risks and opportunities. The technological tools or infrastructure to create effective access to group profiles have not been developed as yet.

[94] Nissenbaum 2004.

Her basic point is that to determine what should be considered a violation of privacy depends on the context and the (a)symmetry of power relations involved. Such contextual determination implies flexibility and a keen eye for detail, but it does not mean that 'context is all' in the sense that general rules lose their meaning. Norms of appropriateness and norms of distribution need to be inscribed at the constitutional, the legislative, the administrative and the judicial level: this would acknowledge the fact that privacy is an underdetermined concept with an open texture, though not undetermined and not open to the extent that it can mean anything.

In the mixed scenario the intelligence of the environment is distributed (which is also the case in the second scenario), but

- the flow of information is not unlimited (not every exchange of data or profiles is *appropriate*), and
- the transparency of consumer-citizens is countered by transparency of profiles (the flow of information is reciprocal, generating a fair *distribution* of knowledge and information)

In the case of multiple ID-numbers this combination of limitation of data/profile exchange and reciprocal transparency is supported by the multiplicity of partial identities, like in the case of the first scenario. The difference with the first scenario is that different contexts may be interoperable, depending on the appropriateness of the exchange; the difference with the second scenario is that different contexts do not have random access to data or profiles generated. A difference with both the first and the second scenario is the reciprocal transparency.

In the case of a unique ID-number it would be rather easy, like in the first and second scenario, to cross-link between contexts. This could make the limitation of data/profile exchange more difficult. On other hand, it could be fairly easy to gain access to all the data and profiles linked to this one ID-number, and this could facilitate transparency for a citizen in as far as she has access.

3.6.3 Unification or interoperability: single or multiple ID-number policies?

The choice between a single or multiple ID-number identifier(s) can be understood as the choice between unification and interoperability. A single unique identifier has the capacity to link all data and profiles regarding one person, thus providing a unification of all partial identities into one comprehensive profile. This unification makes transparency of the consumer-citizen easy and may even make transparency easy for the consumer-citizen if she can claim and manage access to the data connected with her ID-number. In fact a single ID-number could facilitate David Brin's *Transparent Society*,[95] discarding old-fashioned ideas like privacy, trusting the benefits of absolute reciprocal transparency.

[95] Brin 1998.

Multiple ID-number policies allow to discriminate between different contexts, providing tailored ID-number policies depending on which type of privacy is appropriate per context. At the same time the reciprocity or distribution of the transparency can be tailored, depending on the need for checks and balances per context. This does not necessarily rule out interoperability between contexts (as would be the case in the first scenario), because ID-numbers may be linked, e.g. via clearing houses, to provide interoperability (faciliting the third scenario).

From the perspective of democracy and rule of law interoperability, contextual integrity and multiple identifiers seem preferable. They allow a fine-tuned combination of transparency and opacity tools to be built into the technological infrastructure of AmI,[96] avoiding a kind of unification that makes individual citizens transparent to an unprecedented extent, while also avoiding a type of user control that precludes interoperability initiated by someone other than the user alltogether.

References

Brin 1998

D. Brin, The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?, Reading, Massachusetts: Perseus Books 1998.

Custers 2004

B. Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Nijmegen: Wolf Legal Publishers 2004.

Gutwirth & De Hert 2005

S. Gutwirth & P. De Hert, *Privacy and Data Protection in a Democratic Constitutional State. Profiling: Implications for Democracy and Rule of Law, FIDIS deliverable 7.4*. Brussels, 2005, available at: www.fidis.net

Hildebrandt 2006

M. Hildebrandt, 'From Data to Knowledge: The challenges of a crucial technology.', *DuD - Datenschutz und Datensicherheit* 30 (2006).

Hildebrandt 2007

M. Hildebrandt, *Defining Profiling: A New Type of Knowledge. Profiling the European Citizen. A Cross-disciplinary Perspective*, 2007. under review with Springer.

Hildebrandt & Backhouse 2005

M. Hildebrandt & J. Backhouse, *Descriptive analysis and inventory of profiling practices*. Brussels, FIDIS deliverable 7.2, 2005, available at: www.fidis.net

Hildebrandt & Gutwirth 2005

[96] Gutwirth & De Hert 2005.

M. Hildebrandt & S. Gutwirth (Eds.), *Implications of profiling practices on democracy and rule of law*, Brussels: FIDIS Network of Excellence 2005.

ISTAG 2001

ISTAG, *Scenarios for Ambient Intelligence in 2010*, Information Society Technology Advisory Group 2001**:** available at: http://www.cordis.lu/ist/istag-reports.htm

ITU 2005

ITU, *The Internet of Things*. Geneva: International Telecommunications Union (ITU) 2005.

Jiang 2002

X. Jiang, *Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social. Privacy Workshop September 29, 2002, University of California, Berkeley*, Berkeley, available at: http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf

Nissenbaum 2004

H. Nissenbaum, 'Privacy as Contextual Integrity', *Washington Law Review* **79** (2004), pp. 101-140

Ronger, et al. 2005

P. H. H. Ronger, et al., *A Multi-Agent Approach to Interest Profiling of Users. Multi-Agent Systems and Applications IV. 4th International Central and Eastern European Conference on Multi-Agent Systems, CEEMAS 2005, Budapest, Hungary, September 15 – 17, 2005. Proceedings*. M. P¡echou¡cek, P. Petta and L. Zsolt Varga. Berlin Heidelberg, Springer. 3690: 326-335

Schreurs & Hildebrandt 2005

W. Schreurs & M. Hildebrandt, *Legal Issues. Report on the Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*. W. Schreurs, M. Hildebrandt, M. Gasson and K. Warwick. Brussels, FIDIS deliverable 7.3, 2005, available at www.fidis.net.

Tennenhouse 2000

D. Tennenhouse, 'Proactive Computing', *Communications of the ACM* 43 (5) (2000), pp. 43-50

Want, et al. 2003

R. Want, et al., 'Comparing autonomic and proactive computing', *IBM Systems Journal* 42 (1) (2003), pp. 129-136

Zarsky 2002-2003

T. Z. '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion.', *Yale Journal of Law & Technology* 5 (4) (2002-2003), pp. 17-47

4 PART TWO – COUNTRY REPORTS

4.1 General trends with regard to ID numbers: Belgium

Xavier Huysmans, KU Leuven, ICRI

4.1.1 Introduction

In this country report we describe general trends with regard to *personal* ID numbers, i.e., numbers used to refer to natural and/or legal persons, assigned to or being used in a *Belgian public sector* context.

The main ID numbers being used in Belgian eGovernment are: (1) the National Registry number, (2) the ID card number, (3) the Social Security Card number, (4) the INSZ number, (5) the Crossroads Bank for Social Security number, (6) the Fiscal number, (7) the eGovernment registration number and (8) the Enterprise number. We briefly explain the properties and usage modalities of each of these ID numbers.

4.1.2 The RRN-number

4.1.2.1 Context

Belgian municipalities maintain a number of registries, such as the civil status register, the birth register and the **population register**. The latter consists out of 3 sub-registers[97], namely:

- The (core) 'population register': contains data about Belgians, foreigners who have a permanent residence permit, gypsies, commercial travelers and homeless people who have a reference address;
- The *foreigners register*: contains data about foreigners with a temporary residence permit. It is also called the 'bis-register'.
- The *waiting register*: contains information about candidate refugees. It is also called the 'ter-register'.

Municipalities also issue ID cards to Belgians and foreigners that are authorized to reside in Belgium. The card serves as a proof of registration in the population register.[98]

Belgian municipalities are responsible for keeping their population registers accurate and up to date. The law also requires them to synchronize a number of basic identification data from their population registry, as well as their change history with the National Registry.[99] In

[97] Art. 1 Population Registers Act 1991.

[98] Art. 6 et seq Population Registers Act 1991 and art. 1 Identity Cards Royal Decree 25 March 2003. A number of people are entitled to demand such a proof to ID card holders of at least 12 years old (e.g., policeman, bailiff, notary public etc.). See article 1 Identity Cards Royal Decree 25 March 2003.

[99] Namely: name and first names; date and place of birth, sex, nationality, place of main residence, date and place of decease, profession, civil status, family constitution, the population or other register in which the persons are registered, administrative

practice, this synchronization is being done via the *National Registry number* of the people to which the data refer ('data owners').[100]

The **National Registry** is an information processing system responsible for the intake, storage and communication of information regarding the identification of natural persons (art. 1 Act 8 August 1983). As the data of the law indicates, it officially exists since 1983. Since then, it evolved from an internal tool to rationalize the population registry management of the municipalities, to a major building block of Belgian eGovernment.

One of the main principles of the Belgian federal interoperability framework used in eGovernment is that every relevant entity (i.e., an entity that has to be identified), shall have *one and only one identification number that remains stable over time*.[101]

To achieve this, the law of 25 March 2003 altered the purpose of the National Registry Act. Its article 1 now indicates that the National Registry puts *a file with basic identification data* at disposal of a restricted group of government administrations, institutes and persons. Its purpose is to:

- *facilitate the exchange* of information between administrations and to enable the automated updating of the public sector databases and
- *enable the automated updating* of the databases of the public sector in regard to general data of citizens (within the limits of the law).
- rationalizing the communal management of the population registries, and
- *simplify some administrative formalities* requested from the citizens.

From a data protection perspective, this means that this new article of the National Registry Act has created a *legitimacy ground to some entities* to process the *identifier of the National Registry Number to exchange data* about the people that are registered in it *within the whole Belgian public sector context*. We come back to this below.

4.1.2.2 Properties

A National Registry Number (RRN-number) is attributed to each entity at its first registration in the National Registry (art. 2 Act of 8 August 1983). It is a meaningful ID number that consists of 11 digits:

- the first 6 digits stand for the date of birth (2 digits for the year, 2 digits for the month and 2 digits for the day)
- the 3 following digits stand for the serial number of the registration (whereas even numbers are reserved for women)
- the last 2 digits stand for the verification number (art. 1 et seq Royal Decree 3 April 1984).

state of the persons registered in the waiting register, *the existence* of the identity- and signature certificate, legal cohabitation (see Art. 4 Act 8 August 1983, modalities are dealt with by Royal Decree of 3 April 1984).

[100] See art. 2 Population Registers Act July 1991 and art. 1, 11° Royal Decree Information Population Register of 16 July 1992.

[101] DEPREST AND ROBBEN 2003, p. 21.

A first important property of the number lays in its uniqueness: there is one and only one RRN number per registered natural person. The same number cannot be assigned to several entities. Given the mentioned legitimacy ground, its usage is not limited to one specific or contexts or sectors. It is a **global identifier**, as previously defined.

Other important, related properties of the RRN-number are:

- Its stability through time: it does not contain variable characteristics of the registered entity. It is not transferable and cannot be reattributed to another entity.
- Its stability through attributes: it does not contain references to other entities. The ID number does not change when the quality or characteristic of the registered entity changes.
- It is meaningful: one can derive the data of birth and the sex of the registered person from it.
- Its exhaustivity: every entity that has to be identified (for the National Registry) has an ID number
- It is not revocable.
- As explained earlier in this deliverable, it is personal data.

There has not been a large debate going on in Belgium with regard to the appropriateness of having only one global ID number in Belgium. The point of view of the Privacy Commission is that only with regard to specifically sensitive data, being health data and judicial data, a separate sector-specific identifier is needed. With regard to the meaningfulness of the ID number, a law proposal has been filed to change it to a non-meaningful number, but apparently the cost to switch all numbers is currently too high (DE BOT 2005, p. 128, wetsontwerp 25 Maart 2003, p. 6-7).

4.1.2.3 Usage

eGovernment should obviously be done in accordance *with data protection regulation* (purpose binding etc.).

On the topic of global identifiers, in Belgian Federal eGovernment a particular model was chosen to comply with the data protection rules, namely one that puts the decision on the legitimate usage of one particular global identifier in the hands of the Belgian Privacy Commission.[102] More specifically, data exchange based on the RRN number is subordinate to authorizations by an independent committee, which is part of the Privacy Commission. It is called the ‘Sectoral Committee of the Privacy Commission’.

Access to and *usage* of the RRN Number requires a prior authorization, except for the National Statistical Institute (NIS) – a separate law regulates statistical processing and except in the cases foreseen by law or royal decree (article 8 of the National Registry Act). In other words, other legal rules can derogate from the general obligation to ask a prior authorization of the Sectoral Committee of the National Registry.

[102] This model was transposed in Belgian law by Act of 25 March 2003

The authorization to *use* the RRN number can only be granted to a limited set of entities, namely:

- Belgian public authorities, for the information they need to know based on a law, regional decree or ordinance;
- Public and private institutions of Belgian law that perform tasks of public interest that have been committed by or by virtue of a law, regional decree or ordinance or have been recognized as such by the sectoral committee, for the information they need to fulfill these tasks of public interest;
- Natural persons or legal persons that act as subcontractor (1) on the demand , control and responsibility or (2) Belgian public authorities and/or public and private institutions of Belgian law that perform tasks of public interest.
- Notary Publics and bailiffs (individually), for the information they have the right to know based on a law, regional decree or ordinance.
- The chamber of Pharmacies, to communicate the main residence of a client that has been delivered a dangerous medicine
- The chamber of Lawyers, for the information they need to fulfill their tasks as associates of the Court.

The law explicitly states that *the Identification number of the National Registry* (i.e., the RRN number) ***shall not be used without authorization or for other purposes for which the authorization has been granted.***

The National Registry Act does not explicitly state what should be understood under the term *'using'* the RRN number. Based on the prior advice of the Belgian Privacy Commission on that topic[103] we can conclude that a distinction should be made between internal and external usage of the number.

The term *internal usage* refers to the usage of the ID number by a public authority, an institution or person for the internal management of the data it disposes of in the context of a specific task. It should, of course, be limited to the exertion of these tasks of legal or regulatory nature. Examples of the concrete usage are, for instance, to include the number in specific files, records or registers that have not necessarily been computerized.

Another type of usage would be to use the number for user management, to manage the actions that specific users are authorized to do. The term *external usage* refers to the usage of the number in specific situations in contacts with external entities, such as other government authorities, institutions or persons. This type of usage should be explicitly granted in the authorization decision. It is only possible if the other entity is also authorized to process the RRN number.

The term *network connections* means that the number is being used to exchange data about specific persons with other government authorities, institutions or persons. Article 8,§1,4 of the National Registry Act explicitly allows the usage of the number for network connections, on the condition that the authorization demand explicitly lists the connections that will result

[103] Commissie voor de bescherming van de persoonlijke levenssfeer, Verslag over de Werkzaamheden 1998, Brussel, eigen uitgave, 1999, 52, as cited in DE BOT 2005, p. 187.

from this usage. There appears to be consensus in the literature that the mere *reading* the number on a document is, as such, not considered as ‘usage’.[104]

The 7 protection measures of the RRN number provided required by the National Registry law can be summarized as follows:[105]

- There is an obligation to notify new and modified network connections (exception if there has been a prior decision of a sectoral committee)
- A dedicated information security and data protection consultant should be appointed. His/her identity should be communicated to the commission.
- Penal sanctions apply when the number is being used for other purposes than the ones that are authorized.
- The Privacy Commission requests a list of organs / employees that are entitled to use the RRN number as well as an information security plan.
- There is an obligation to provide a confidentiality contract with and to provide training of the people that are authorized to use the RRN number.
- Each person has the right to access and correct personal data held about him/herself, including the one based on the RRN number (article 10 of the National Registry Act).
- The authorizations are made public via the website of the Privacy Commission (article 12 of the National Registry Act).

In addition to that, in the vision paper by Mr. Deprest and Mr. Robben (see the bibliography), we also read that:

- Each electronic exchange of personal information shall be preventively checked for compliance with current access authorizations by the used *service integrator* (for example, the Crossroads Bank for Social Security)
- Each electronic exchange of personal information shall be logged, to ensure the subsequent traceability of any abuse.
- Each time information is used to take a decision, the information used shall (ideally) be notified to the person concerned together with the decision made.[106]

4.1.3 Usage of the RRN in the Belgian eID. How it should be?

A specific type of usage of the RRN number is its integration on and in the Belgian electronic identity card. For instance, the number has been printed on the card and included in the X.509 citizen certificates (*authentication and non repudiation certificate*)[107].

This means that with each exchange of a digital signature created with the Belgian eID, the signatory *propagates* the National Register number to external parties that have not necessarily received an authorization to use the number by the Privacy Commission.

[104] DE BOT 2005, p 189.

[105] DE BOT 2005, p. 195 ff.

[106] We did not find back this obligation in legislation so far, which means there it is **not yet a formal obligation** to do so.

[107] For more information on the Belgian eID see FIDIS deliverables 3.6 (technical) and 5.4 (legal). See also the article of Prof. Dumortier, ‘eID en de paradoks van het rijksregisternnummer’ (Dumortier 2005).

Of course, strictly speaking, one could argue that the mere fact that third parties *can see* the RRN-number, shall not be qualified as *'usage'* in the legal sense of the term – and does therefore not conflict with the mentioned obligation to request a prior authorization for a particular purpose.

Nevertheless, as explained in the general legal chapter of this deliverable, using a global identifier to interchange data between several contexts and/or sectors creates important linkage risks.

Even if we leave in the middle whether this linkage risk is affordable or not in the public sector, it is clear that the RRN number is not supposed to be used:

- outside the public sector (according the legal provisions mentioned above, only a limited number of government entities, their processors and subcontractors can use it), and
- without the legal controlling mechanism of authorizations by the Sectoral Committee of the RRN at the Privacy Commission.

When we take one step back and apply the theory we've mentioned in the legal contribution of this deliverable *to evaluate whether or not the appropriate technical and organizational security measures have been taken to protect the number against any unlawful processing* (article 17 of the Data Protection Directive and article 16§4 of the Belgian Data Protection Act) we are not sure whether it is indeed the case. Moreover, article 11 of the National Registry Act goes one step beyond, with regard to the processing of data of the National Registry (thus: including the RRN number).

It requests from everyone that intervenes in the data processing to take all the necessary precautions to guarantee the safety of the data and, among others, to prevent that they are being communicated to persons that *have not received an authorization to view it* (Dutch: 'inzage nemen')

The main reasons why we are not sure whether *in casu* the appropriate *technical security* measures have been taken can be summarized in terms of these two rules:

- The eID is designed and targeted *to be also used outside a strict eGovernment context*. For instance, on the website www.eid.belgium.be, one can for example read that the eID will be usable, among others, as a library card, to sign your purchases via the web, as an access key to the network of your company, as the access key to safe chatboxes, as the identity proof at the reservation of your hotel etc.
- However, to process a global ID number in a legitimate way, appropriate technical and organizational security measures are needed. These measures shall prevent any unlawful data processing of that number.
- Also, to process the RRN number in a legitimate way, the necessary precautions should have been taken to prevent it from being communicated to entities that have not received an authorization to view it.

In practice, we believe that the data controller should in this case have taken the measures needed to prevent processing of the number outside a governmental context (e.g., in eCommerce), since the usage outside this context is not allowed.

In addition, we believe that he should also have taken the appropriate measures to avoid the number from being processed by government entities (mentioned above, article 5 of the

National Registry Act) *that are not entitled to process the number, e.g. before they dispose of the necessary legal provision or authorization of the Sectoral Committee of the RRN at the Privacy Commission.*

As far as we know, none of these precautions have been taken in the design of the current version of the eID. Possible measures are, for example, to encrypt the number, and make decryption available to the authorized entities only.

The problem is known to the Belgian administration, and we are sure that they are taking the necessary steps to solve this issue.

4.1.4 Other ID numbers processed by municipalities

4.1.4.1 Context

As explained, the population register contains a number of data that is needed for the identification and localization of the inhabitants (art. 2 Act 19 July 1991).[108]

This list partially differs from the data contained in the National Registry. For instance, in addition to the basic identification data being synchronized with the National Registry, population registers for example also contain:

- passport details (including the passport number),
- the number of the Belgian ID card,
- the number and date of issuance of the Social Security Card and
- pseudonyms.

These 4 identifiers are, in principle, not being processed by the National Registry. Nevertheless, in practice, municipalities are allowed to delegate the processing of these (and other) additional data to the National Registry. Municipalities regularly do so when they do not dispose of a data center of their own, or one that is jointly operated with one or more other municipalities.

From a data protection perspective, in this case, the National Registry is not a *data controller*, but a *data processor* with regard to the mentioned additional data.[109] By consequence, the

[108] These data are enumerated in the Royal Decree of 16 July 1992, namely: name, first names *and* ***pseudonyms***, date and place of birth, sex *and the reference to the court decision that corrected the birth certificate act,* nationality, place of main residence, *its changes, its removal and/or its temporary residence*, date and place of decease, profession, civil status and *– where applicable – the declaration by the person of the existence of a marriage contract, or a contract of legal cohabitation*, family constitution, legal cohabitation , *the status of being a refugee*, *the status of being a displaced person (staatloze)*, *the status of temporarily having no or unspecified* nationality, *the descent (afstamming)*, *acts and decisions in regard ot the incapacity of a minor*, *funerary choice*, *type and category of driving license*, *passport details*, ***the number of the Belgian ID card*** , ***the number and date of issuance of the social security card*** ,*pension certificates*, *expression of ones will in regard to organ transplantation*, *military titles*, *expiration date of the card of a traveling salesman*, *categories of art. 95 Voting codex* (some professional categories, such as lawyers are more likely to be chosen as president of a voting district), *statement that a person is not a voter and until when.* The underlined data categories are in principle not included in the national Registry (but see below, the comments in regard to information types).

National Registry is only allowed to process the data (and a fortiori communicate it) on behalf of the municipalities themselves, *unless it is required to do otherwise by law*.[110]

In other words, one can only confirm that, *at the moment*, the law says that if the National Registry is requested to process additional data, it can only communicate it to the administration that communicated it in the first place.[111] It offers no guarantee for the future (laws can change) and it is not technically verifiable.

Pursuant to Council Regulation 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals, the *passport document number* should be included in the residence permit, produced as a ICAO compliant visa or travel document. The number should include special security features and be preceded by an identification letter.

With regard to the eID and the social security card, it is relevant to note that *both cards* contain a separate ID *card number* that is also being stored by the above mentioned population register. The card number of the eID consists of 12 numbers, the first and the last 3 separated by a dot. An example of a possible eID card number is '591.0831050.76'. The card number of the SIS card consists of a string of 10 numbers. An example of a possible SIS card number is '0352936373'.

Apart from the obligation to include the number in the eID card registry, no specific regulation is foreseen to protect these measures. As a result, only the general data protection rules apply. The last type of identifiers processed by the Population Registry are *pseudonyms*. We come back to them in the next section ('usage').

4.1.4.2 Usage

An interesting finding is that – contrary to the National Registry Number – no specific data protection guarantee has been foreseen with regard to these 4 identifiers. As mentioned earlier in the legal background contribution of this deliverable, this is not surprising, because the general Data Protection Directive leaves the decision whether or not to protect identifiers with general application to the member states. In other words, in Belgium *only the general data protection rules* apply to these identifiers (and ID numbers – a pseudonym is not necessarily a number).

As far as we know, these numbers are currently not being used by government entities to interconnect data ('network connections' as mentioned above). Therefore, the legal risks applying to them may at first sight be less important than those applying to the RRN number.

Yet, this situation could easily change. For example, in 2006 a popular private website for elderly people www.seniorennet.be granted access to its chatbox via the eID and the SIS card,

[109] This implies, for instance, that the National Registry is acting on behalf of the municipalities and is not part of their internal organization. The definition of article 2(e) Data Protection Directive runs as follows: *'processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'*

[110] Article 16 of the Data Protection Directive says: 'Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.'

[111] Article 3, §3 National Registry Act.

by just identifying the users via the content data of these cards (the basic identification data is not encrypted).[112]

When reading out the SIS / eID card, besides the RRN number, the SIS / eID card number is also being disclosed…

Strictly speaking, if a data controller would decide to use this *card* number, or easier, the *certificate* number of the eID[113], instead of the strictly regulated RRN number, linkability risks would be similar to the risks with the RRN mentioned above, without being illegal (*since the data controller could fulfill the data protection requirements, e.g., processing based on informed consent).*

As a result, the card holder has no other choice but to trust the data controller of the counterparty in the communication, and to hope that the data will not be used for other purposes, and will never be *'further processed in a way incompatible with the original purposes'.*

We believe this is not sufficient, especially in a governmental context, where – as we explained – purposes can much more easily be changed by adapting the law. In our view, the balancing exercise to know which security measures are appropriate or not, should:

- take the risks connected to the nature of the data processing in the public sector into account,
- prevent any unlawful processing of these numbers *outside the public sector context* and
- prevent any unlawful processing of these numbers before the necessary legal ground is available (either a legal provision or an authorization of the competent Sectoral Committee of the Privacy Commission).

For example, the Royal Decree of 8 January 2006[114] has made officially clear, that when an administration is authorized to receive access to the *name and surname of a citizen or group of citizens* (art. 3,1,1° National Registry Act, part of the official basic data that a municipality has to synchronize with the National Registry), it also receives access to the *person's surname, first names,* ***pseudonym****, (nobility) title, and the changes in surname, first names and nobility title* (art. 1,1,1° of the Royal Decree).

Both the Privacy Commission and the Raad van State (Supreme Administrative Court) to this Royal Decree disagreed with the enlargement of the definition. Nevertheless, their advice to not include some of the information types, such as the change of sex, or the pseudonym, or the disappearance of the person, has not been taken into account.

As a result, today, the processing of a *person's pseudonym* by the National Registry is not incompatible with the *original purposes*. It can *legitimately be processed at the same level as*

[112] See, with regard to the SIS card, http://www.ksz.fgov.be/nl/carteSIS/cartesis_2.htm and with regard to the eID, the contribution by Danny De Cock in FIDIS D3.6. As far as we know, Seniorennet does no longer support this kind of access control via identification only.

[113] See the contribution by Danny De Cock in FIDIS D3.6.

[114] Koninklijk Besluit van 8 Januari 2006 tot bepaling van de informatietypes verbonden met de informatiegegevens bedoeld in artikel 3, eerste lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.*, 25 Januari 2006, p. 3916 ff.

it processes the first name or the surname of that person[115] The pursued (new) finality is not incompatible with the original ones.This illustrates that there is a risk that legislation will change the granted purposes later on, and make what is illegal today, may be allowed tomorrow.

4.1.5 ID number for social security

4.1.5.1 Context

As explained earlier in this deliverable, one of the main principles of the Belgian federal interoperability framework used in eGovernment is that every relevant entity shall have *one and only one identification number that remains stable over time*.[116]

Even though the numbers managed by the Population Registry and the National Registry cover most of the entities that need to be identified in eGovernment, there are also a number of entities that are not. For instance, some categories of natural persons that are relevant for social security, fiscal and other purposes are not included in it (for example, people that are radiated *ex officio* of the population registers, or people that only work but do not reside in Belgium etc).

This is where the ID number for social security (INSZ number) comes in. Article 8 of the Crossroads Bank for Social Security Act of 15 January 1990 (as amended by law of 16 January 2003) says that for the processing of the data needed in application of this law – which means: for social security purposes – *it shall use the National Registry number or, when applicable the identification number of the Crossroads Bank itself.*

4.1.5.2 Properties

The INSZ number is the combination of both the Crossroads Bank number and the RRN number (article 1,4° Royal Decree 18 December 1996). The Crossroads Bank number is built in the same way as the RRN-number. It consists out of 11 digits:

- the first 6 digits stand for the date of birth (2 digits for the year, 2 digits for the month and 2 digits for the day)
- the 3 following digits stand for the serial number of the registration (whereas even numbers are reserved for women)
- the last 2 digits stand for the verification number (art. 1 et seq Royal Decree 8 February 1991).

4.1.5.3 Usage

The law explicitly states that the usage of the Crossroads Bank number is free. By consequence, the INSZ-number falls under two different usage regimes:

[115] One should not forget that – as indicated in the general legal contribution of this deliverable – the Belgian law explicitly says that, to evaluate a further processing of personal data, account should be taken of *all relevant factors, in particular […] the applicable legal and regulatory provisions* (article 4 of the Belgian Data Protection Act).

[116] DEPREST AND ROBBEN 2003, p. 21.

- first, the (restricted) usage rules that apply to the RRN-number explained earlier and
- second, the limited usage that applies to the Crossroads Bank for Social Security number. Since this number can be qualified as personal data, the general data protection law applies.

4.1.6 The Fiscal number

4.1.6.1 Properties

Article 314,§1 of the Belgian Income Tax Code (Wetboek van Inkomstenbelastingen) foresees that all taxable persons are assigned a fiscal ID number.The second part of the paragraph explains that for natural persons, this number corresponds to the RRN number. The third paragraph confirms that for legal persons that are not registered in the National Registry, a fiscal ID number is being assigned, according to the rules set by Royal Decree.

The fiscal ID number for legal persons is their VAT number, which consists of the country code BE plus a *string of 9 numbers* between 0 and 9. An example of a Belgian VAT can be BE123456789.

Other persons that are not registered in the National Registry receive a separate ID number, which is built according to the same rules as those applying to the Crossroads Bank for Social Security number (Royal Decree of 8 February 1991).

4.1.6.2 Usage

The fiscal ID number can, be used for identification purposes of a number of internal and external relations the Fiscal administration has with other entities.

Such external relations are, for example possible with the holders of the number, his/her successors, and identification government entities that have received a prior authorization based on article 8 of the National Registry Act (see above).

4.1.7 The Enterprise number

4.1.7.1 Properties[117]

The Crossroads Bank for Enterprises is a register that has the obligation to record, store, manage and put at disposal data related to the identification of enterprises (article 3,3° Crossroads Bank for Enterprises Act).

The purpose of the register is in the first place to simplify administrative formalities, to organize public services more efficiently and, to some extent, to commercialize the data of the registry (article 3, second part and article 19 of the Crossroads Bank for Enterprises Act). Important for our deliverable, is that at its first registration in the registry, each entity is assigned a unique ID number (article 5 Crossroads Bank for Enterprises Act). Enterprises[118]

[117] This section is based on the legal provisions and complemented with DE BOT 2005, p. 279 ff.

[118] An enterprise, in the sense of the law is a registered economical or social actor on the Belgian territory, namely: (1) a legal person established according to Belgian law, (2) a legal person established according to foreign or international law, with its

get a so-called 'Enterprise Number' (Ondernemingsnummer) and branches get a so- called 'Branch Number' (Vestigingsnummer).

The Enterprise number consists of a *string of 10 numbers* represented as follows: ZNNN.NNN.NNN. The 'Z' stands for 0 or 1 and each position 'N' stands for a number between 0 and 9. If Z is equal to zero, is should not be mentioned. The Enterprise Number of an enterprise that is subject to Belgian VAT, is its VAT number (without the country code) preceded by the index 0. Similarly, any enterprise that is registered in the National Legal Persons Registry gets the latter number, also preceded by the index 0 (Royal Decree of 24 June 2003).

The composition of the Branch Number is very similar. It is represented as ZNNN.NNN.NNN, with 'Z' being a number between 2 and 8 and the position 'N' being a number between 2 and 9 (Royal Decree of 24 June 2003).

Both numbers are not limited to a specific context or sector. It is a **global identifier**, as previously defined.

Other important, related properties of the Enterprise-number are:

- Its stability through time: it does not contain variable characteristics of the registered entity. Contrary to the Branch Number, the Enterprise Number is not transferable and cannot be reattributed to another entity, except when the enterprise is being divided.[119] If the Enterprise Number was assigned to other types of legal entities, the transfer is not possible. If it was assigned to a natural person, the transfer is not possible either. The number remains assigned to that natural person, even if the activities are suspended or stopped, when the registered activities change or if the person dies. The number cannot be taken up by the successor.[120]
- Its stability through attributes: it does not contain references to other entities. The ID number does not change when the quality or characteristic of the registered entity changes.
- Its stability through attributes: it does not contain references to other entities. The ID number does not change when the quality or characteristic of the registered entity changes.
- It is meaningful: if the number holder is subject to VAT, one can derive the VAT number from it. This is, however, public data.
- Its exhaustivity: every entity that has to be identified has an ID number
- It is in principle not revocable. However, if an Enterprise Number is being crossed out, it cannot be reassigned to a third party.[121]
- It is *in principle not personal data*, unless it refers to an identified or identifiable <u>*natural person*</u>. In that case, the higher mentioned data protection principles, including article 8,7° of the Data Protection Directive should be taken into account.

seat or with registration obligation in Belgium, (3) Merchants, Artisan, Employers, entities subject to VAT and self-employed person or (4) a Branch of this entity.

[119] Article 4 and article 6 of the Royal Decree of 24 June 2003.

[120] Article 4 and 5 of the Royal Decree of 24 June 2003.

[121] Article 7 and article 6 of the Royal Decree of 24 June 2003.

4.1.7.2 Usage[122]

In principle, the usage of the Enterprise and the Branch Number is free. This means that – contrary to the RRN number – enterprises can also use this number in their internal relations. The usage of the number is compulsory for all the contacts the enterprises have with administrative and judicial administrations, and for all the contacts these administrations have among each other.

Moreover, the number should also be mentioned on a number of fixed items, e.g., all acts, invoices, official announcements, orders letters and all other documents of commercial nature (e.g. by artisans, vendors etc.), on commercial buildings, etc.

The usage of the Enterprise and the Branch number should respect the rights and liberties of others. The Crossroads Bank of Enterprises Act therefore imposes a prior *notification* to the thereto competent Sectoral Committee of the Privacy Commission, for *all other data* exchange between government entities that is based on the Enterprise or the Branch number (article 18 of the Crossroads Bank of Enterprises Act).

In other words, the legislator felt that when these numbers are being used to link different data sources between 2 or more *government* entities, it was necessary to map the interconnections via a registry and to make them public. In this case, the task of the Sectoral Committee of the Crossroads Bank of Enterprises is (1) to register the interconnections in a registry and (2) to verify whether the legislation has been respected (e.g. exchange of this 'other' data only within the limits of the law). Contrary to the rules applicable to the RRN-number, the Crossroads Bank for Enterprises Act does not impose additional guarantees, such as the appointment of a information security consultant.

4.1.8 Conclusion

In this country report we've given an overview of the main ID numbers that are being used in a Belgian public sector context, especially in the context of eGovernment. At first sight it appears that a multitude of numbers are being used, such as the National Registry Number, the Social Security Number, the Tax number, the Enterprise number etc.

These numbers are, however, in most cases synchronized with each other. The statement taken from the vision paper by Deprest and Robben that every relevant entity shall have *one and only one identification number that remains stable over time, seems therefore to be totally the case in practice.*

As a result, this brings us back to the point we've explained in the general legal contribution of this deliverable, whether or not *technical unlinkability* should be a requirement in eGovernment. Our main finding is that because the situation that applies to the RRN number is similar to the risks that apply to other global ID numbers in eGovernment, at least the unique legal authorization mechanism that was explained above should be made applicable to all global ID numbers used in eGovernment.

[122] This section is based on the legal provisions and complemented with DE BOT 2005, p. 292 ff.

In addition, because this legal mechanism alone does not solve the data protection issues, we believe there is a strong case for *technical unlinkability* in eGovernment as an appropriate security measure to prevent unlawful processing of these numbers.

If the Belgian eID has to be useable outside the strictly eGovernment context, one should for example consider encrypting the identifiers and adding in a more user-centric architecture, where the user can decide for himself whether or not some of these attributes can or cannot be processed. If we take the long term risks sufficiently into account, we believe the necessary costs to implement this type of infrastructure with compulsory context- and/or sector-specific identifiers can be worth the cost of its implementation.

References

BELGIAN INCOME TAX CODE
Belgian Income Tax Code, available at www.staatsblad.be.

DE BOT 2005
D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart,* Brugge: Vandenbroele 2005.

DE COCK, WOLF & PRENEEL 2006
D. De Cock, C. Wolf & B. Preneel, 'The Belgian Electronic Identity Card', in M. Meints and M. Hansen (eds.), *FIDIS D3.6 Study on ID Documents, Deliverable 3.6 of the EU funded FIDIS project*, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf, December 2006, last visited: 16 January 2007, 94-98.

COUNCIL REGULATION 13 JUNE 2002
Council Regulation 1030/2002 of 13 June 2002: COUNCIL REGULATION (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals.

CROSSROADS BANK FOR ENTERPRISES ACT 2003
Law of 16 January 2003 on the creation of a Crossroads Bank for Enterprises, on the modernization of the trade register, on the creation of recognized companies' dockets and on diverse rules, Belgian State Gazette 5 February 2003, http://www.staatsblad.be.

DATA PROTECTION ACT 1992
Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, Belgian State Gazette 18 March 1993, as modified by the law of 11 December 1998 implementing Directive 95/46/EC, Belgian State Gazette 3 February 1999, and the law of 26 February 2003, Belgian State Gazette 26 June 2003.

DATA PROTECTION DIRECTIVE 1995
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 on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995, 31-50.

DEPREST & ROBBEN 2003

J. Deprest & F. Robben, *eGovernment: the approach of the Belgian federal administration*, available at: http://www.ksz.fgov.be/En/Como/2003%20-%20EGovernment%20paper%20v%201.0.pdf, June 2003, last visited: 20 June 2006.

DUMORTIER 2005

J. Dumortier, 'eID en de paradoks van het Rijksregisternummer', *Trends Business ICT*, March 2005.

IDENTITY CARDS ROYAL DECREE 25 MARCH 2003

Royal Decree of 25 March 2003 concerning the identity cards, Belgian State Gazette of 28 March 2003, http://www.staatsblad.be.

INFORMATION TYPES ROYAL DECREE 8 JANUARY 2006

Royal Decree of 8 January 2006 to the attribution of the information types connected with the information data meant in article 3, first paragraph of the National Registry Act of 8 August 1983, Belgian State Gazette, 25 January 2006, http://www.staatsblad.be

KOOPS, BUITELAAR & LIPS 2007

E.J. Koops, H. Buitelaar & M. Lips (eds.), *D5.4: Anonymity in electronic government: a case-study analysis of governments' identity knowledge, deliverable 5.4 of the EU funded FIDIS project*, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5.del5.4-anonymity-egov.pdf, May 2007, last visited: 13 June 2007.

NATIONAL REGISTRY LAW 1983

Law of 8 August 1983 on the organization of a Registry of natural persons, Belgian State Gazette 21 April 1984, http://www.staatsblad.be.

NATIONAL REGISTRY ROYAL DECREE 1984

Royal Decree of 3 April 1984 on the access by some public administrations to the National Registry of natural persons and on keeping and controlling the information, Belgian State Gazette 21 April 1984, http://www.staatsblad.be.

POPULATION REGISTERS ACT 1991

Law of 19 July 1991 on the population registers and the identity cards, adapting the National Registry Law, Belgian State Gazette 3 September 1991, http://www.staatsblad.be.

POPULATION REGISTERS ROYAL DECREE 1992

Royal Decree of 16 July 1992 on the population registers and the foreigners registers, Belgian State Gazette 15 August 1992, http://www.staatsblad.be.

REFORM OF THE NATIONAL REGISTRY ACT 2003

Law of 25 March 2003 on the modification of the Law of 8 August 1983 on the organization of a Registry of natural persons and the Law of 19 July 1991 on the population registers and the identity cards, adapting the National Registry Law, Belgian State Gazette 28 March 2003, http://www.staatsblad.be.

ROYAL DECREE COMPOSITION ID NUMBER IF NOT RRN 1991

Royal Decree of 8 February 1991 on the composition and the attribution modalities of the identification of natural persons that are not registered in the National Registry, Belgian State Gazette 19 February 1991, http://www.staatsblad.be.

ROYAL DECREE ENTERPRISE NUMBER ATTRIBUTION 2003

Royal Decree of 24 June 2003 on determining the attribution rules, the composition and the transfer modalities of the Enterprise Number and the Branch Number in the Crossroads Bank of Enterprises, Belgian State Gazette 30 June 2003, http://www.staatsblad.be.

ROYAL DECREE SIS CARD 1996

Royal Decree of 18 December 1996 on measures for the introduction of a social ID card for the benefit of all social insured persons, in application of the articles 38, 40, 41 and 49 of the law of 26 July 1996 on the modernization of t-Social Security and the safeguarding of the legal pension systems, Belgian State Gazette 7 February 1997, http://www.staatsblad.be.

4.2 ID number policy: Report on France

Fanny Coudert, Katholieke Universiteit Leuven, ICRI

The national directory of natural persons' identification (RNIPP, *répertoire national d'identification des personnes physiques*) was created in 1941 by the Ministry for Internal Affairs of Vichy Government with the purpose of organizing administrative files and establishing demographic statistics. It has been maintained after the war but its administration has been transferred to the INSEE, the National Institute for Statistics and Economic Studies (*Institut National de la Statistique et des études économiques*)[123].

Every individual born in the French territory or who becomes a beneficiary of the French Social Security is attributed a registration number (NIR - *numéro national d'inscription au répertoire des personnes physiques*). It thus appears more as a population register than a French citizens' directory.[124] The sole purpose of the Directory is to prevent mistakes about the identity of individuals. Its use for the purpose of individual tracking is explicitly forbidden, except under the circumstances foreseen by the Law which mainly refers to judicial proceedings (Art. 60-1, 77-1-1 and 93-3 of the Penal Procedure Code).[125] The RNIPP is currently and mainly used, apart from Social Security agencies, by Fiscal Agencies, the National Bank, and by the INSEE for the administration of the companies' directory (SIREN) and of the electoral file.

The NIR is a meaningful identifier and it is based on the gender and the year, month, province and city of birth of the individual (Art. 4). Therefore, although its structure makes it stable and reliable, the information it provides may lead to gradual use of data for purposes other than those for which they were collected (commonly known as 'function creep'). Actually, it has been immediately deviated from its original purpose in order to identify 'Jews' and 'non-

[123] Decree n°46-1432 of 14 June 1946 relative to INSEE, an update version is available at: www:legifrance.gouv.fr

[124] Lecerf 2005.

[125] Article 7 of Decree n°83-103 of 22 January 1982, relative to the national directory of natural persons' identification, an update version is available at: www:legifrance.gouv.fr

Jews' through the gender key which was more 'complete' in its origin.[126] This painful memory remains attached to the use of the NIR.[127]

After World War II, it has been largely used by the Public Administration as a reliable identifier and particularly by Social Security Agencies. However, in 1972, its computerization with the aim of obtaining a unique identifier for French citizens together with the launch of a large project for the centralisation of police databases (SAFARI), initiated a large public debate. The fear raised by the impact of this project on private life, individual freedom and public liberties led to the adoption of the Data protection Act in 1978. This Act restrains the use of the NIR and of data matching processing to a previous authorisation given either by the French Data Protection Authority, the CNIL (*Commission Nationale de l'Informatique et des Libertés*) (Art. 25.6°), by legal provisions, or by regulatory provisions taken after the (non-biding but public) opinion of the CNIL (Art. 27.1°) and under the control of the State Council (*Conseil d'Etat*) [128]. The infringement of these provisions is punishable with a maximum of five years of imprisonment and a fine of 300,000 euros (Art. 226-16-1 of the Penal Code).

The opinion of the CNIL as regards the use of the NIR as identifier will be further discussed as it is expressly endorsed by the French government in its e-administration policy.[129] Since 1984, the CNIL has claimed that the RNIPP was a civil register, created for preventing mistakes in the identity of individuals based on homonymy. [130] A "universalistic" concept of the NIR which would convert it into a national identifier, should be avoided. This means that the NIR cannot be used as unique identifier and should be completed with other information such as the address, when it is used. Moreover, the use of this number by Public Agencies for the linkage of databases is limited to a strict application of the finality principle[131]: if two public agencies are legally authorised to use the NIR and to transfer personal data to each other, thus they can use it as a key for their transfers of personal data. In any other case, the CNIL considers that the sole need of linking two databases is not sufficient reason for justifying the use of this number.[132] This interpretation has played a key role in preventing the use of the NIR by Public Agencies as a common identifier for the linkage of different public databases, compelling them to create their own identifier and maintaining its use, expanding it each time, within the health sector.

[126] The gender key which stands in first position has been used under the Vichy Regime to identify not only the gender but also whether a person was Jew, Muslim, foreigner, etc. see: http://fr.wikipedia.org/wiki/Code_INSEE, last consultation on 16 February 2007.

[127] CNIL 1999, p.61.

[128] The State Council is the highest administrative jurisdiction in France. It ensures the legal validity of administrative acts.

[129] PSAE 2004-2007, p. 15.

[130] CNIL, Délibération n° 83-058 du 29 novembre 1983, available at : http://www.cnil.fr/index.php?id=1380&delib[uid]=35&cHash=52a059c87b

[131] Under the finality principle, data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes. For more information about data protection principles, see FIDIS, D.11.1. "Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity", available on-line at: http://www.fidis.net/fidis-del/period-2-20052006/d111/doc/31/ (last access on 17 April 2007).

[132] CNIL 1999, p. 65

This doctrine has only been breached once by the legislator in 1998 when the Finance Act for 1999[133] authorised some Fiscal Agencies to use the NIR for fraud control. The provision allows these Agencies to use the NIR with the only purpose to avoid mistakes about identity and to verify the address of individuals in the framework of some of their competencies. This provision has been put to the Constitutional Council, which has validated it. The fact that Agencies' employees are bound to professional secrecy and that the CNIL has supervisory power over the processing, as well as the existence of a data protection legislation, were considered as sufficient safeguards. The Council also observed that the finality principle was clearly defined and that the use of the NIR would not lead to data processing non-related with the competencies of Social Security and Fiscal Agencies. [134]

The Finance Act, as well as the possible use of the NIR as identifier for the Medical Personal File and the implementation of electronic identity cards using biometrics, has relaunched the public debate, raising new fears related to the use of a unique national identifier. However, the French government in the Electronic Administration Strategic Plan 2004-2007 expressly opted for adopting sector based identifiers in electronic identity management systems, in accordance with the position of the CNIL.[135] In that sense, a connection should be established between the certificate number of the card and the sector based identifier used by the public authority. Introduction of the concept of a federate identity is also foreseen. This allows the user to get a unique identifier for accessing public services and prevents any link to be made between public databases. Following this statement, the CNIL suggested in its opinion on the Medical Personal File, that in order to benefit from the large use of the NIR in the health sector and of its stability and reliability, a specific identifier could be generated from the NIR according to certified procedures of anonymisation. [136]

References

BRAIBANT 1998

G. Braibant. Données personnelles et société de l'information, Rapport au Premier Ministre sur la transposition en droit français de la Directive no 95/46, La documentation française, 3 March 1998

CNIL 1998

CNIL, 19è Rapport, La documentation française, 1998

CNIL 1999

CNIL, 20ème Rapport, La documentation française, 1999

CNIL 2007

CNIL, Conclusions on the use of the NIR as health identifier [Conclusions sur l'utilisation du NIR comme identifiant de santé], 20 February 2007, available at: http://www.cnil.fr/index.php?id=2197&news[uid]=434&cHash=dd6d3df873

GMSIH 2002

[133] Art. 107 of the Act no 98-1266 of 30 December 1998, J.O. n° 303 of 31 December 1998, p.20050.

[134] Constitutional Council, DC n°98-403, Finance Act for 1999, 29 December 1998, Recueil p. 326 – J. O. of 31 Décember 1998, p. 20138.

[135] PSAE 2004-2007, p.16.

[136] CNIL 2007.

Groupement pour la modernisation du système hospitalier (GMSIH), Project Si 1.1 "Principes et Processus d'identification du patient" Synthèse de l'analyse réglementaire, 6 March 2002

LECERF 2005

J.-R. Lecerf. Intelligent Identity and Liberties [Identité intelligente et libertés], Information Report to the Senate n°435, 29 June 2005, available at : http://www.senat.fr/rap/r04-439/r04-439.html

PSAE 2004-2007

Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.15

TRUCHE, FAUGERE, FLICHY 2002

TRUCHE P., FAUGERE J.-P., FLICHY P., Administration électronique et protection des données personnelles : Livre blanc, La documentation française, 2002.

UJA 2000

Colloque de l'Union des jeunes avocats (UJA), L'anonymat dans la société de l'inform@tion : fichage et démocratie, où en sont nos libertés ? , Paris, 26 April 2000, http://www.delis.sgdg.org/menu/nir/uja2000.htm

4.3 Universal ID numbers in three Visegrad countries

Adam Foldes (Hungarian Civil Liberties Union)

Robert Pinter (BME – UNESCO Information Society Research Institute)

4.3.1 ID number in Hungary

4.3.1.1 Historical aspects

The Hungarian story of the universal ID number corresponds perfectly with the story of the deconstruction of the party-state. Throughout the communist regime a basic experience of the population was the defencelessness against the ubiquitous state. As the history of the surveillance state, the personal stories of the observed and their shadows, the everyday deals, the voluntary or forced collaboration with power, have yet not been written, thus suspicion remains even after 18 years of democratic change. More than a million people in a country of ten million were observed: in their workplace by colleagues who worked or collaborated with the secret agencies, in their home where caretaker of the public owned building noted the activities of the residents, in small communities where people reported on friends, relatives if they were blackmailed by the secret agencies, in churches where priests worked for the system. The entire society was interwoven by the paranoid system of power. The methods used by the secret agencies to reach cooperation varied on a wide scale. They had about 30,000 officers in service of the secret agencies in the Rákosi Era (1948-56) and about 20,000 in the Kádár period (1956-88)[137]. In addition, masses were blackmailed. If they did not report they would lose their jobs, would not get promotions, their children would be banned from current or further studies, their passport would be revoked, etc.. Most people did not even consider whether or not to collaborate with the totalitarian system or even supported it and helped the agencies voluntarily.

The Hungarian legislation could not solve the conflict between privacy and freedom of information which latter entails working on the dark side of the society in the comunist regime. Since the transition Parliament was unable to adopt legislation[138], which could provide access to the former secret agencies' archives, by which means the details of the everyday observation, the stories of the victims and perpetrators, not to mention of those who were both the same at the same time, could be written. Many files have disappeared since 1989 and numerous have reappeared since, causing scandals over and over again.[139] Every

[137] György Gyarmati, the head of the *Historical Archives of the State Security Agencies* has given these figures in an interview. See at: http://www.mkih.hu/content.php?pg=4_1&cikkid=15

[138] There were several attempts, but each of them has been challenged by the Constitutional Court due to their failure to reconcile the two competing fundamental rights. Only the Act III of 2003 was adopted which gives a limited access to the archives of the secret agencies of the former regime. However, the archives contrary to its name *Historical Archives of the State Security Agencies* does not even store the entire material of the agencies, as numerous files are still withheld by the current secret agencies, which have in service a considerable number of employees of the non-democratic agencies.

[139] The most famous case was of Péter Medgyessy who became the prime minister in 2002 and right after he has taken his office, his file as a former reconnaissance officer of the communist secret agency has been leaked.

citizen had records in different registries: with their employer, for education, for medical care, with the political party, and many of them even with the political police. Since 1954, every citizen was obliged to carry an ID card that had to be shown to the authorities on request.[140] The records could be linked with the help of the universal ID number which had been given to everybody at birth from the year 1974 on.[141]

The first step towards dismantling the "Big Brother" system was the abolishment of the universal ID number in 1991. The Constitutional Court (CC) had started its work 1st January 1990, within five months it issued in its very first decisions that a ministerial decree cannot oblige anybody to disclose their ID number as it is a limitation of privacy, which can be prescribed only by Act of the Parliament.[142] Not even a year had passed by the time before the Constitutional Court issued its ever since most cited privacy decision[143] on the universal ID number, in which they abolished the universal ID number. The CC prescribed that the state shall pursue a shared information policy[144] which means that the major registers must be split and each of them should introduce ID numbers on their own, independently from each other. The state registries were given deadlines to realise the separated systems and as long as they established them they were authorised by provisional legislation to use the old universal ID number but only to upkeep the elementary functions of the state. The interim period was to expire on the last day of 1995. In 1994 the CC has reaffirmed its previous decision on the ID numbers as they examined the Act on misdemeanours and a Governmental decree on social security numbers (both of them using the universal ID numbers) and abolished the decree which enabled the authorities to use the old universal ID numbers for social security administration purposes.[145] The CC banned even the partial revival of the old system.

In 1995 the Government has started a major economic stabilisation programme which was implemented in an Act of the Parliament[146]. In the frame of this Act the Government made an attempt to extend the interim period (see above) for the use of the universal ID number by 4 years. This was the second time that the CC abolished the universal ID number by concluding that the interim period shall not be extended any further as there was no guarantee that the legislative power will not seek even further extensions.[147]

[140] 1/1954. (I. 9.), Decree of the Council of Ministers on the introduction of the ID card.
[141] Law-decree 8. of 1974 on the public population register.
[142] 11/1990. (V. 1.) Constitutional Court decision.
[143] 15/1991. (IV.13.) Constitutional Court decision.
[144] There are four decisions of the CC where it stresses the requirement of shared information systems. All the decisions are quite short on the requirements of these systems, but it is clear from them, that separated, sector specific state registries must be set up. 15/1991. (IV.13.) Constitutional Court decision; 29/1994. (V.20.) Constitutional Court decision; 46/1995. (VI.30.) Constitutional Court decision; 44/2004 (XI.23.) Constitutional Court decision.
[145] 29/1994. (V.20.) Constitutional Court decision.
[146] Act XLVIII of 1995 on particular law amendments for the reason of economic stabilisation.
[147] 46/1995. (VI.30.) Constitutional Court decision.

In 1997 the Government presented a plan on *Central National Network for Updating and Forwarding Data*[148] and issued a decision on a network connecting the state registries. It would have been financed by the World Bank and 2.5 billion HUF was proposed in the 1998 National Budget for setting up the system. The Government argued for the system that the then introduced private pension system would not function without connecting the Central Statistics Bureau and the social security database, as the social security system had lost sight of 637 000 citizens and they were supposed to be earning their living in the black economy. Connecting these databases would have been only the first step, the cross-checking of personal data with the election register and the tax register was also foreseen. The Parliamentary Commissioner for Data Protection sharply criticised the plans of the system and recalled the CC's decisions which prohibited the establishment of such universal registries. This universal database has never been set up due to the resistance of the Data Protection Commissioner and the change of the Government. Regarding this question the latest decision of the CC was issued in 2004 on an Act regulating among other things the data handling of the tax authority. The CC has reminded the legislator of its early decisions and stressed that no tax ID number can be established which could function as a universal ID number.[149] Occasionally, public officials give statements in the media on their plans for universal databases, but none of them has reached so far as the plan on *Central National Network for Updating and Forwarding Data* in 1997.

4.3.1.2 Legal aspects

In 1991 the Constitutional Court (CC) laid down the cornerstones of the Hungarian ID number policy and even repetitious attempts of the legislature could not bring any change in this field. This decision of the CC founded the Hungarian personal data protection law.[150] The decision comprises several important arguments which add up to a coherent general prohibition of the universal ID number.

The CC found that the legislature (in the early eighties) had a concept of setting up an integrated personal data bank which would have consisted of the widest possible range of personal data of the citizens including health care data, financial data, administrative procedures records. Therefore it had become compulsory to use the ID number in the population registry and in the administrative and judicial registries.

1. They pronounced that it is absolutely unconstitutional to process data merely for the 'stock' without specified purposes, which is due to the lack of defined purposes indivisible to different applications and renders the data accessible to undefined users. The CC also maintained no guarantee can overhaul the lack of the purpose-bound requirements of data processing as the legal conditions of the data transfer and the

[148] Központi Adategyeztető és Továbbító Országos Rendszert (KATOR). See Annual Report of the Hungarian Data Protection and Freedom of Information Commissioner at: http://abiweb.obh.hu/adatved/indexek/besz/szoveg55-76.htm#4.5.

[149] 26/2004. (VII.7.) Constitutional Court decision.

[150] 15/1991. (IV.13.) Constitutional Court decision.

purpose-bound nature are not alternative but coupled guarantees of the informational self-determination (privacy).

2. The CC warned if there is no defined circle of data processors – as in the case of the universal ID number which can be used by anybody owing to its universality – it is natural for the data processors that they can access aggregated and interrelated data of the individuals. It renders the individual defenceless, makes their private life transparent and results in an asymmetric communicative situation where the individual will not know what is known about him by the data processor. It is a humiliating situation and excludes the free choice of the individual who does not know what kind of information his partner has on him. As the use of the universal ID number is wide-spread not only the administration gains power over the individual, but also the private bodies which have access to the ID number. At the same time the administration can extend its power through the control of the data originating from the private sector. As a result, if personal profiles are created, it violates the right to human dignity.

3. The CC declared that there is no constitutional right or interest which could require the restriction of the informational self-determination resulting from data processing without defined purposes. The efficiency of the administration especially can not be regarded as such an interest, as there is no proof that the grave restriction of the informational self-determination is the only possible way of the efficient work of the administration.

4. Consequently the CC pronounced the unconstitutionality of the universal ID number, required the legislature to adopt an Act on personal data protection, abolished the universal ID number, prohibited the use of the universal ID number in official documents, registries, administrative or court procedures, imposed a ban on requesting the ID number for any purposes be it the exercise of a right or performing a duty. They only allow the registries use it provisionally for internal purposes as long as new systems based on non-universal but specialised ID numbers would be set up.

The new systems were to be constructed with specialised ID numbers useable only within the administrative sub-system and, for an interim period, as an internal code between the separated sub-systems. Meanwhile the CC had rendered void[151] the appendices of a Governmental Decree[152] as it, not much later, reintroduced the use of the universal ID number without regard to the fact that the health care card has its own registry number and also comprises personal data of the holder. The CC announced that it was unconstitutional to use two parallel identification systems for the same purpose and nor is it allowed to use the old universal ID number for the health care cards, as the administration is authorised only to use it

[151] 29/1994. (V. 20.) Constitutional Court decision.

[152] 54/1992. (III.21.) Governmental Decree on social security health care card.

as an internal ID. The Data Protection Act entered into force 1st May 1993, since then it explicitly prohibits the universal ID number.[153]

In 1995 the CC abolished the universal ID the second time as the government adopted the economic stabilisation programme which upheld the once abolished ID number.[154] They reaffirmed the above principles and noted that the logic of the universal ID number is contrary to the principles of the personal data protection, such as the purpose-bound nature of the data processing and the shared information systems. Without the latter the route of the personal data becomes untraceable which precludes the individual of exercising his fundamental rights. In this case the automatic connection of databases through the universal ID number might end up in a personal profile on which basis the administration takes decision although the profile will not perfectly correspond with the reality, but will leave the individual at the mercy of the administrative power.

Finally, in 1996 the universal ID number has been divided into three specialised ID numbers.[155]The *Tax ID Number* is created by the tax authority, and it is shown on the Tax ID Card together with very basic personal identification data. Tax ID can be used only for the purposes regulated in different Acts by social security authorities, labour authorities, courts, law enforcement, national security bodies, private pension funds and health care institutions. The *Health Care ID Number* is created by the National Health Insurance Fund, contained on the Health Care Card together with very basic personal identification data. For purposes regulated by Acts the health care ID number can be used by health care providers, private pension funds and approximately the same sphere as authorised by law for the tax ID number. The third ID number is the old universal ID number which was renamed and its scope of use has been significantly limited. It can by used within the limits enacted by different Acts for the purposes of personal data and address register, registrars, embassy authorities, land-register, military register, election register, register of persons without suffrage, assessors register, criminal register, referendum, gun register, law enforcement, courts, national security and traffic authority. The different registers are allowed to contact each other in individual cases by connection codes (with some exceptions); the connection codes are temporary sequences and must be different from the three ID numbers. Personal data can be transferred only when the authority needs updated information for legal purposes, the transfer must be limited to those individuals whose data needs to be updated.

4.3.1.3 Political aspects

The abolishment of the universal ID number and its division into three specialised ID numbers seems to be irreversible. Any attempt to set up a new universal ID number would be considered by the public as an attack against the rule of law by giving up the data protection in Hungary. The key actors in this issue are the following.

[153] „The application of general and uniform personal identification codes which can be used without restriction shall be prohibited." Article 7 para (2) of the Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest.

[154] 46/1995. (VI.30.) Constitutional Court decision.

[155] Act XX of 1996 on the ways of identification and the use of ID codes substituting the ID number.

The current *President of the Republic*, László Sólyom has been the first President of the Constitutional Court between 1990 and 1998, in the period when the public debate on the personal ID number has taken place. Throughout his Constitutional Court presidency he tended towards the German type of data protection which was determined by the Volkszählungsurteil of the German Federal Constitutional Court.[156] The *Constitutional Court* time and again consistently cites the first decision on the abolishment of the universal ID number, their jurisprudence seems to be unchanged in the last fifteen years.

According to his common practice, developed since 1995, the *Parliamentary Commissioner on Data Protection* would also clearly oppose any change in this question and he would be backed by the civil society. Presumably it would also cause public unease, as the *population* considers ID numbers as generally prohibited and precariously use even its successor which has the same form as the old universal ID number.

The only window of opportunity to develop the current ID number practice is to leave the legal framework untouched and find solutions within the current system. The use of the connection codes can be further developed so as to enhance the work of the public administration and, at the same time, privacy concerns which are clarified by the Hungarian legal practice, must be also addressed. If individuals were enabled to follow the way of their personal data handled in any sector of the public administration (which they cannot at the moment), their right to informational self-determination would be highly enhanced. Thanks to IT technologies this improvement could, at the same time upgrade the quality of privacy and administration. As good governance is the antithesis of the surveillance state, privacy and user friendly ID number policy is contrary to the once dismantled universal ID number system.

4.3.2 ID number in the Czech Republic

4.3.2.1 Historical and legal aspects

Apparently there are some common aspects in the history of the ID number in the Visegrad group countries. The universal ID number persists from the communist time in the Czech Republic. In the 1980s of the twentieth century a massive data revision[157] took place in Czechoslovakia as the automation of the data processing in the registries was introduced. After the verification of the registers a brand new regulation was adopted.[158] It lasted for 18 years and the „rodné číslo“ (birth number) survived without sharing the fate of the Hungarian birth number which was split into three. The next regulation was adopted in 2000 and it is the

[156] BVerfGE 65,1.
[157] Regulation of the federal ministry of the interior No. 4/1980 Coll.
[158] Act No. 135/1982 Coll., on reports and registration of place of stay of citizens, implemented by the regulation adopted by the federal ministry of the interior No. 146/1982 Coll.

one still in force with amendments from 2004.[159] The administrator of the register of inhabitants is the Ministry of Interior.[160]

The ID number is widely used both in the various fields of public administration such as election register, land register, tax register, social security register and in the private sector. In 2004 the Office for Personal Data Protection has issued an interpretation on the use of the Act. No. 133/2000 Coll. after it was amended.[161] They pointed to several risks which might be solved by the amending Act. The Office has been entrusted by a new competence to impose sanctions for "other administrative torts" in case of unauthorised disposal or utilisation of a birth number. An administrative delict has been also introduced for legal person or any natural person - entrepreneur that repeatedly make unauthorized utilisation of birth numbers.

The amending Act regulates that the birth number 'may be used by the subjects listed in the said provision, i.e. ministries and other administrative authorities, bodies authorized with the exercise of state administration, courts when acting within their jurisdiction defined by law, and notaries in administering the Central Register of Testaments' and these authorities 'may act only for what the law authorizes them, they are obliged to enable bearer to do the choice of the identification data whenever the Act enables the selection to use as an identification data the birth number or other personal data'. According to the legislator the purpose-bound nature of the data processing and the thriftiness with the data are the principles, backed by sanctions, which might result in a privacy friendly system.

A Bill which seems to be the greatest challenge to the right to privacy with regard to the ID numbers has been mentioned by Vladimír Šmíd, Karel Schelle and Renata Veselá in their study.[162] 'The strategic documents of the government of the Czech Republic titled State Information Policy Way to Information Society dated 1999 and the State Information and Communication Policy e-Czechia 2006 dated 2004 envisage the advancement in the particular field up to an even higher level. The central idea thereof is the establishment of basic registers of public administration, which will extend usability of information systems, interconnecting subsystems and registers of public administration usable also for the needs of the general public, with the goal to achieve not only cost cuts but also acceleration of administrative processes, removal of duplicities and cuts in state machinery'. The Draft Bill on Data Sharing in Public Administration was proposed by Ministry of Informatics in 2005 and has not been adopted until the spring of 2007.

4.3.2.2 Political Aspects

In the Czech Republic there has not been much criticism on the use of the ID numbers. Sometimes the Head of the Office for Personal Data Protection warns the public not to

[159] It is regulated in the Act no.133/2000 Coll. on population register and birth numbers and the Act No. 53/2004 Coll. amending the previous.
[160] Smid, Schelle, Vesela.
[161] Position No. 4/2004 July 2004. See at: http://www.uoou.cz/index.php?l=en&m=left&mid=02:110&u1=&u2=&t=.
[162] Smid, Schelle, Vesela

disclose their birth number if it is not explicitly required by law.[163] The Office was established only in 2000 and it might take many years before the population becomes privacy conscious.

In 2000 there was a national census (registering all population, houses and flats and other data), that has raised privacy concerns and civic protests, especially in the internet community.[164] The administrative court later ruled that one question on the questionnaire form exceeded what the state is allowed to ask.

In 2006 the Finance Minister won a Big Brother 'award for its proposal to create a new tax identification number that would be partly composed of the numbers on peoples' national ID cards. An unsecured national ID number opens the door to identity theft[165]', as the data would be available in a database accessible by public' – stressed the jury of the award.[166]

4.3.3 ID number in the Slovak Republic

Until 1st January 1993 the history of the ID number for the Slovaks is the same for the Czechs as the two republics used to be the same country. In Slovakia there is a universal ID number that every citizen holds from birth (birth number). This number is used by all state registers in order to identify the person. During the communist regime, only the universal ID number existed, later a tax ID number has been introduced, but most institutions use the ID number.

The Slovak Data Protection Act[167] prescribes that '[i]n the processing of personal data, an identifier of general application stipulated by a special Act may be used for the purposes of identification of a natural person only provided that its use is necessary for achieving the given purpose of the processing. Processing of a different identifier revealing characteristics of the data subject, or releasing of an identifier of general application shall be prohibited.'

The purpose-bound nature of data processing is enacted here as in the Czech Republic and in Hungary with the difference that in Slovakia only legal guarantees can safeguard the personal data in the public registries, but the registries are not split and the universal ID number is useable in all of them. As we can see above in the Slovak Data Protection Act, the 29/1994. (V. 20.) decision of the Hungarian Constitutional Court and the above cited interpretation of the Czech Office for Personal Data Protection of the same tenor as the Czech Data Protection

[163] Lazarova 2003
[164] More details in Czech at www.blisty.cz , topic Sčítání obyvatel.
[165] See details at the Identity Theft Resource Center at: http://www.idtheftcenter.org/cresources.shtml
[166] Alda 2006.
[167] Art 8 of the Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll. See at: http://www.dataprotection.gov.sk/buxusnew/docs/act_428.pdf.

Act stipulates[168], there exists a general approach in the three countries which means that no authority can request further identification details if the ID number is provided and is sufficient to identify a person. Therefore any further personal data is unnecessary.

In Slovakia there has not been much criticism about the universal ID number issue.[169] The only concerns were about the protection of the ID numbers from unauthorised disclosure, but not from its existence.

References

ALDA 2006

Kristina Alda. Watching you. The Prague Post November 8th, 2006. See at: http://www.praguepost.com/articles/2006/11/08/watching-you.php ; See further details at: http://www.bigbrotherawards.cz/en/index.html.

LAZAROVA 2003

Daniela Lazarova. Personal data protection still a problem in the Czech Republic [13-02-2003]. See at: http://www.radio.cz/en/article/37530.

SMID, SCHELLE, VESELA

Vladimír Šmíd, Karel Schelle, Renata Veselá. The Never Ending Story or 15,000 years of attempts to register inhabitants. See at http://www.fi.muni.cz/~smid/neverendingstory.html

[168] Art. 5 para (1) d) 'The controller shall be obliged to […] collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfilment of the specified purpose;' See at: http://www.uoou.cz/index.php?l=en&m=left&mid=01:01:01&u1=&u2=&t=.

[169] This is the view of a lawyer working at NGO Nadacia Obcan a Demokracia (Citizen and Democracy Foundation) in Slovakia.

4.4 Country Report Germany, Austria, Switzerland

Sebastian Meissner, ICPP

4.4.1 Introduction

This country report deals with important state-issued ID numbers that currently exist in Germany, Austria and Switzerland and with the policies that are pursued in this context by the respective country. It is described in which sectors and for which purposes the different numbers are used, of which elements they consist and on what legal basis they are used. Furthermore, current and forthcoming changes concerning ID numbers and the corresponding policies are presented.

4.4.2 Germany

4.4.2.1 Overview

Today in Germany only sector specific ID numbers are used. One important reason for this is the Census Decision[170] (Volkszählungsurteil) of the German Federal Constitutional Court (Bundesverfassungsgericht). This decision was of utmost importance for the development of data protection law in Germany. In the Census Decision the Federal Constitutional Court ruled among others that the introduction of a universal personal identifier is forbidden by German constitutional law. The decision is based on the consideration that such a universal personal identifier would allow an easy combination of different data sets and thus a comprehensive registration and indexing as well as the creation of detailed personal profiles about citizens[171].

At present one can identify some forthcoming changes with the potential to soften or even abolish the rigid sector specific approach for ID numbers in Germany: The most important ones are the introduction of a unique and inalterable lifelong tax number in 2007 and plans for the introduction of a central citizens register.

4.4.2.2 Registration System and Tax ID Number

Today the registration of citizens in Germany is organised in a decentralised manner. In most of the German federal states (Bundesländer) numeric sort features are used to run the registers. These sort features differ from state to state. Furthermore, they are not unique i.e. identical sort features can be found in indexes of different states and therefore be allocated to different citizens.

[170] BVerfGE 65, 1

[171] BVerfGE 65, 1 (53)

In 2006 there was a reform of the federal organisation of the German state (Föderalismusreform). One result of this reform was that the legislative competence for the citizen registration law was moved to the federal legislative organs. Recently plans of the German Federal Government emerged to set up a central database containing the registration data of all citizens[172]. In this central database there could and probably will be stored a universal ID number. In this context first and foremost the forthcoming tax ID number comes into consideration to be stored in the new central database. The introduction of this number is going to happen in the second half of 2007.

The tax ID is a unique and inalterable identifier for natural persons. It is allocated to each taxpayer and used for unambiguous identification in taxation procedures[173]. The Federal Central Tax Office stores the tax ID number and some other data about the taxable person such as name, date and place of birth, gender and current address in a central database. The additional data are provided by the local registration authorities; in return the Central Tax Office transmits the allocated tax ID numbers to the registration authorities which store the numbers in the local registration databases.

The Tax ID Number is composed of eleven numeric characters (example: 12345654321) that must not be built or derived from other data about the taxable person (non-descriptive number)[174]. The last digit of the number is an error checking number.

Legal basis for the introduction of the Tax ID Number is Article 139a ff. of the German Tax Code (Abgabenordnung – AO)[175]. Article 139b AO contains provisions that shall prevent the use of the tax ID number as a universal personal identifier in commerce and administration: In particular public or private organisations may only organise their data by means of the tax ID number if this is necessary for regular data transmission between them and the tax authorities. Private organisations that infringe these regulations commit an administrative offence that may be punished by a fine up to 10.000 €[176].

4.4.2.3 Summary and Conclusions

As already mentioned in the introduction, in Germany sector specific ID numbers for citizens are used so far, but at the moment one can recognize important forthcoming changes: Starting in July 2007 universal and unalterable tax identification numbers will be allocated to all

citizens. These ID numbers will be already assigned to newborns, they will be lifelong valid and they will be stored in a central database. This database will contain other personal data such as name and address of the citizens as well. It will be kept up to date by data

transmissions from the local citizen's registration authorities. Furthermore, the German Federal Government plans to centralise the system of citizen's registration. This could be carried out e.g. by adding a central registration index containing data about all German

citizens to today's local registration databases.

[172] See http://www.heise.de/newsticker/meldung/83859

[173] Additionally, pursuant to Article 139c of the German Tax Code an economy identification number is allocated to every economically active individual as well as to every legal entity.

[174] Article 139a paragraph 1 sentence 2 of the German Tax Code

[175] Furthermore the Tax Identification Number Ordinance (Steueridentifikationsnummerverordnung) rules details concerning the allocation of the Tax ID Numbers. It became effective in December 2006.

[176] Article 383 AO

If one examines the above-mentioned developments as a whole, one can identify a distinct tendency towards a central storage of data about the citizens and – most probably – also towards the implementation of a universal personal identifier. In particular, the already determined linkage of the forthcoming tax identity number to resident registration data from local indexes leads to the conclusion that the tax ID most likely will be stored in a future central registration database and that it might be extended to a universal ID number for the whole public administration.

The current development in Germany seems to be quite problematic from a legal point of view if one considers the jurisdiction of the German Federal Constitutional Court that illegalises the implementation of a universal personal identifier.

4.4.3 Austria

4.4.3.1 Overview

Concerning identification numbers Austria follows another approach than Germany. In order to achieve a synergetic effect the register data of citizens was verified parallel to the census of 2001. The corrected data was then used for a central registration index (Zentrales Melderegister - ZMR) which was implemented in Austria. In this registration index personal data about the citizens such as name and date of birth are stored as well as a registration index number – the so-called ZMR number (Melderegisterzahl - ZMR-Zahl). The ZMR number is allocated to guarantee the unambiguousness of each citizen. Nonetheless, due to data protection reasons the Austrian legislation decided not to use this number for authentication in E-Government applications. Instead different sector specific personal identifiers based on the regulation in the E-Government Act 2004 are used.

4.4.3.2 Resident Registration Number

The central registration index was introduced in March 2002. At the same time the amended Austrian Resident Registration Act (Meldegesetz 1991 – MeldeG) became effective. The ZMR is operated in parallel to the local registration indexes. It is a joint information system that stores data about every Austrian citizen. A single record contains personal data such as name, gender, date and place of birth as well as residence data like postal code, city, street and house number.

In order to guarantee the unambiguousness of every citizen also a ZMR number is stored in every citizen's record. The ZMR number consists of twelve numeric components (example: 1234567654321) and must not contain any personal information about the concerned citizen[177].

Legal basis for the allocation of the ZMR number is Article 16 Paragraph 4 of the Austrian Resident Registration Act.

As already mentioned the purpose of the ZMR number is to guarantee the unambiguousness of every citizen. Hence, it is used as a source for identification and authentication of citizens

[177] Article 16 paragraph 4 MeldeG

in the e-government context. However, due to data protection reasons not the ZMR number itself but so-called sector specific personal identifiers (ssPIs) are used in e-government applications (concept "Bürgerkarte" – see details at 3.5).

4.4.3.3 Social Insurance Number

In Austria a universal social insurance number is allocated to every insured person. This number is stored on the chip of the new electronic patient card (e-card) that was introduced in 2005[178]. The social insurance numbers of all citizens are stored in a central database. They are used by the social security authorities (health, pension and accident insurance funds) and the (local) employment offices.

The universal social insurance number is a descriptive number that consists of ten numeric characters (example: 1234030869). It is allocated by the umbrella association of the Austrian social security authorities (Hauptverband der österreichischen Sozialversicherungsträger).

Legal basis for the allocation of the number is Article 31 Paragraph 4 of the Austrian General Social Insurance Act (Allgemeines Sozialversicherungsgesetz - ASVG). The social insurance number may be used for purposes of social insurance and labour market services[179].

4.4.3.4 Citizen Card ("Bürgerkarte")

The citizen card concept[180] offers to the citizens a technology independent solution for a privacy-friendly e-government. The so-called "Bürgerkarte" isn't a card in a physical sense but a bundle of functions that can be implemented on different carrier media such as smart cards (e.g. the e-card), cell phones or USB sticks. In order to guarantee a secure identification and authentication electronic signatures are used. The legal basis to implement the concept citizen card was provided by the E-Government Act 2004[181] (E-Government-Gesetz - EGovG).

Within the implementation of the concept not only the ZMR number, but also other ID numbers play an important role: The source PIN that is calculated from the ZMR number and different sector specific personal identifiers (ssPIs) that are derived from the source PIN by one-way-hashing them with sector numbers defined by law.

The aim of the deployment of different sector specific personal identifiers is to prevent the usage of one single ID number (e.g. the ZMR number or the social insurance number) as a universal personal identifier. ssPIs are deployed as well in the public as the private sector.

[178] See http://www.heise.de/newsticker/meldung/60058

[179] Article 460d ASVG

[180] Detailed information can be found in chapter 5.5 of the FIDIS Deliverable 3.6 "Study on ID Documents". See also http://www.datenschutzzentrum.de/sommerakademie/2005/somak05_kotschy.pdf

[181] An English version of the E-Government Act is available at http://www.cio.gv.at/eGovernment/law/E-Gov_Act_endg_engl_Fassung1.pdf

4.4.3.5 Summary and Conclusions

In Austria ID numbers are used that have the potential to be extended to a universal personal identifier (e. g. the ZMR number and the social insurance number).

With the E-Government Act 2004 and the concept "Bürgerkarte" the Austrian legislator decided using an approach that offers an unambiguous identification and authentication but uses different sector specific personal identifiers instead of one universal personal identifier. This solution bases upon the awareness of the legislator that the use of digital identities implies severe privacy risks such as possibilities to link digital data via one digital ID number.

4.4.4 Switzerland

4.4.4.1 Overview

In Switzerland the Old Age and Survivors Insurance Fund number (Alters- und Hinterlassenenversicherungsnummer – AHV number) is the most important public ID number. In 2006 the Swiss legislator enacted changes to the respective law (Bundesgesetz über die Alters- und Hinterlassenenversicherung – AHVG). The new regulations are the legal basis for the introduction of a new AHV number: Starting in July 2008 the new AHV numbers will be issued to the citizens. One aim of the new regulations is to reduce the extensive usage of the current AHV number.

4.4.4.2 Social Insurance Number

In Switzerland a universal social insurance number, the so-called AHV number, is used. The Old Age and Survivors Insurance Fund (AHV) is the mandatory social insurance pension fund in Switzerland. The unique AHV numbers are allocated to every insured person by the Central Equalisation Board (Zentrale Ausgleichsstelle). A new AHV number will replace the currently used number in 2008.

Today's AHV number is a descriptive number that consists of eleven digits (example: 66869334113). So far the use of this number wasn't limited by law. Over the years this resulted in an extensive use of the number by different authorities and organisations. In addition today's number proved to be insufficient to guarantee the unambiguousness of every allocated person in the future[182].

Hence, the Swiss legislation changed the Old Age and Survivors Insurance Act (AHVG) in June 2006 setting up the legal framework for a new AHV number. Starting in 2008 the Central Equalisation Board will allocate new numbers to all people that are registered in the central insurants index. The new number will be issued to all insured persons and to the respective employers.

The new AHV number is a non-speaking number that consists of thirteen digits (example: 7561234567895). Legal basis for the introduction of the number is the new Article 50 c-g AHVG.

[182] Cp. http://www.avs-ai.ch/Home-D/allgemeines/nnahv/neueahvnummer.pdf and http://www.avs-ai.ch/Home-D/allgemeines/nnahv/AHV_neueNummer_NZZ_3_7_06.pdf

The new legal provisions allow the use of the new AHV number for social insurance purposes as well at federal as at cantonal level[183]. However, in some areas of the social security system additional legal provisions for the usage of the number will have to be issued. Outside of the social security system the AHV number may only be used if this is explicitly allowed by federal or cantonal law[184]. Authorised users have to take technical and organisational measures to guarantee the lawful use of the right AHV number and to protect the number against improper use[185]. Users who neglect this obligation are fined with an amount up to 10.000 francs (approximately 6.170 €)[186]. Unauthorised people who systematically use the number are punished by imprisonment up to six months or fined with an amount up to 30.000 francs (approximately 18.500€)[187].

4.4.4.3 Summary and Conclusions

The AHV number is the most important public ID number in Switzerland. As the currently used numbers the forthcoming new AHV numbers will be used in many different administrative sectors. Hence, the AHV number can be characterised as a universal personal identifier.

To prevent an uncontrollable use of the number the new AHVG-provisions require the issuance of specific legal provisions ruling the usage of the number for every additional purpose. People who systematically use the number without being legitimated are punished with severe penalties. Moreover, authorised users are obliged to take technical and organisational measures that guarantee protection of the number against improper use.

4.4.5 Findings: Comparison of ID number policies

Analysing the findings it can be surmised, that the three countries discussed in this chapter, follow different approaches dealing with public ID numbers:

In Germany at the moment only sector specific ID numbers are used. However, analysing current developments one can observe a trend towards using the forthcoming Tax ID number as a universal personal identifier in different public sectors.

In Switzerland such a universal personal identifier has already been established: It is today’s extensively used AHV number that will be replaced by a new number in 2008. The new AHV number is set up to prevent the extending use of today’s AHV number via the issuance of specific laws ruling the usage and via sanctions in cases of improper use. The disadvantage of this solution is that the AHV number may be used as a universal personal identifier never the less. This enables as a matter of fact the linkage of transactions and thus creation of detailed profiles about the respective person.

The Austrian legislation in 2004 issued the E-Government Act that prescribes the use of sector specific personal identifiers instead of one universal identifier. The so-called “Bürgerkarte” concept aims at preventing the development of a universal identifier in the e-

[183] Article 50d AHVG

[184] Cp. Article 50e AHVG that rules some view exceptions from this principle as well.

[185] Article 50g parapraph 2 a. AHVG

[186] Article 88 AHVG

[187] Article 87 AHVG

government context and therefore works against the creation of detailed profiles about Austrian citizens.

4.5 Country Report The Netherlands

Hans Buitelaar, Universiteit van Tilburg, TILT

The discussion about the desirability of one identifying number has been a persistent phenomenon in the Netherlands.[188] This discussion has long been pervaded with the experience of World War II, when many citizens were easily traceable due to the perfect registration of citizens at the local level. As a result, deportation actions for the *Arbeitseinsatz* but also in the context of the Holocaust, have long haunted the Dutch.

The introduction of the single personal ID number started already with the distribution of the social security number some decades ago. But this was still an application with a strictly limited value, i.e., it only had validity in the social and fiscal sectors (= sofinumber).[189] Other personal numbers were the so-called A-number, that was used in the local civic administration and other sectoral numbers, such as the Education number.

In the early nineties of the past century, two lines of development gradually become apparent as important for the way government ensures identification of its citizens. As will be shown they eventually in conjunction determine the outcome of the discussion about the identification number in the Netherlands. These are the technological developments and a different approach to the services public government provide.

Initially, on the technological side, a stream of legislation can be witnessed, that fortifies the control central government gets over its citizens. Especially the opportunities introduced to make use by the law-enforcement services of telecommunication tracings and DNA evidence, become increasingly important. Then, after about 1996, on the public administration theory line, elements of the movement of New Public Management also took hold in The Netherlands. This can be described as the electronic government with an external orientation (economic aspects, service and democracy).[190] The Dutch government became convinced, that ICT would provide a valuable contribution to realising the plans for its e-government vision. It was the intention that, in the future, all dealings of government with its citizens would take place via the Internet. In this context, government thought it necessary to simplify its contacts by providing the citizens with a uniquely registered means of identification. A supra-sectoral

[188] Kuitenbrouwer 1991, p. 80. In 1968 already the A-number was introduced by a simple amendment of a secondary regulation, not in a formal law. As soon as the general public and in its slipstream Parliament finds out about plans of the government to introduce a personal identification number, it gives rise to much concern. But as will be argued later, government consistently tries to downplay the discussion. Policymakers attempt to introduce the personal number as a service to the citizen even though it is an unsympathetic measure..

[189] Kuitenbrouwer 1991, p. 87, however, argues that the sofi-number provided a very handy opportunity to linking up fragmented data to obtain a total picture. The Council of Europe warned in 1990 also that the personal number was not a neutral matter because of the linking possibilities. CDJC 1990, p. 27..

[190] www.e-overheid.nl

number became necessary. Even though the sofi-number was to an ever greater extent taking on the appearance of this single identifying number,[191] it was deemed necessary to introduce a real citizen service number, the BurgerServiceNummer (BSN). Additional reason for this introduction, were the faults, that increasingly became apparent in the system of the sofi-number.

Then, of course, there were the attacks on the Twin Towers of September 11th 2001 and the resulting terrorist threat. Contrary to what is usually assumed, it was not this shocking event, that created a climate in which the introduction of a single identification number was acceptable to the Dutch people and government. 'Nine eleven' only provided an extra impulse for the trend by which government increasingly started to control its citizens.[192]

First, in 2002, a broad discussion took place about the personal identification number.[193] Upshot of this discussion was the advice to introduce a single identifying number. In the climate sketched in the above paragraphs, the Dutch population no longer objected to this instrument. It was argued moreover, that the single number was necessary as a prerequisite in the development of the Dutch e-government plans. Because of the priority, that safety enabling measures after 'nine eleven' are given, the original plans in the Van Thijn recommendations, to create equal safeguards at national and sectoral level for the personal number, it soon appeared, here also were set aside in favour of technology push. Most revealing in this discussion was, that the so-called unique Healthcare number is, by a last-minute legislative move, replaced by the BSN number.[194] The two strands of technological development and e-government vision seem to lead inevitably to the single personal number.

There was also criticism. Some outspoken spokesmen accused the Dutch government of gullibility by believing in "the panacea of digital identification".[195] It seems almost, they argue, as if every technique, that helps with law-enforcement and safety, is permissible. One becomes more and more convinced, that linking up all infrastructural systems will be facilitated by the use of a personal identification number. At a later stage, it is relevant to mention here, that the Data Protection Commission and the First Chamber of Parliament criticised this point of view. If a mistake is made somewhere in the chain of systems using the BSN, the citizen does not know where to make his grievance known and it will take much pain to correct it.[196] In such a way, it is maintained, the longstanding tradition of using personal data solely in the context for which they are collected, is disrupted.[197] The principle

[191] In article 55 Sv (Code of Criminal Procedure) it is stated that the sofi-number may be asked for to identify a suspect person.
[192] Vedder, p. 49.
[193] Tafel 2002. The so-called Tafel van Thijn (Table of Van Thijn).
[194] Regels inzake het gebruik van het burgerservicenummer in de zorg (Wet gebruik burgerservicenummer in de zorg), Kamerstuknummer 30380, nr 2, Tweede Kamer, vergaderjaar 2005-2006.
[195] Prins 2003, p. 2-3.
[196] CBP 2007.
[197] This is one of the principles of the Dutch privacy law. Wet bescherming persoonsgegevens. The Dutch Data Protection Commission on several occasions strongly objects to the proposed law. The use of the number for any task, public or not, is very worrisome. Cf Mom 2007, p. 8-11.

of self-determination by the citizen in the process of updating and selection of data collected and used about his person, is also damaged.[198]

On September 12th 2006 the General Provisions Citizen Service Number Act[199] was passed by the Second Chamber. Points of departure for the BSN are:

- Only the BSN may be used in the contacts between government and citizen in case a personal identification number is necessary
- Every citizen who has multiple contacts with the government is issued a BSN.

The BSN is meant to assist the national government in realising its goal of an improved service to its subjects and to make the administration more efficient. It is meant to reduce the administrative burden the government imposes on citizens by supporting the principle of single request for information.[200] Purportedly it also would contribute to the protection of the privacy of its citizens and the fight against identity fraud.

The primary register for BSN is the Local Government Basic Registration (GBA).

The responsibility for the GBA lies with the local governments. Data such as name, address, gender, civil status, nationality and residence permit but also data about parents and offspring are retained. The agency Basic Administration Personal Data and Travel Documents maintains a central index, which is nationally available for reference by authorised organisations. For non-citizens a Register Non Residents (RNI)[201] will be developed. The Ministry of Foreign Affairs will hold responsibility for RNI.

As a matter of fact, the BSN is the same as the sofi-number. For the migration of the sofi-number to the BSN the government has chosen to transfer the sofinumber automatically to the BSN by renaming the sofinumber. Just like the sofinumber the BSN consists of nine digits and fits the so-called elevencheck.

To ensure the safe use by government organisations of the BSN, the following conditions are set out[202]:

- The number has no informational value
- An operational organisation takes care of the security and correct granting, storage and consulting of the number.
- There will be a numberregister.
- Local government authorities are responsible for the correct issuing of the number. To obtain a BSN one has to identify oneself with his/her passport.
- In backoffice applications where a personal number is used only the BSN may be used.

[198] Nader Voorlopig verslag van de Vaste Commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat, Eerste Kamer der Staten-Generaal, Vergaderjaar 2006-2007, nr 30312 E, p.2.

[199] WABBN.

[200] WABBN, Memorie van Toelichting, Tweede Kamer 30312, nr 3, # 1, p.2 Inleiding and # 7, pp. 16-20.

[201] Register Niet-Ingezetenen

[202] Factsheet BSN 2006.

- The functioning of the BSN must be transparant. For that reason the government intends to realise the National Trust Function. This is a set of measures that ensure that the BSN is used properly. In this context the government intends to set up a so-called map by which citizens obtain insight into the use of the BSN. A complaints bureau, a data protection officer and a framework for checking the admissibility of the use of the BSN are also foreseen.

Unfortunately the present situation is that the last mentioned conditions are not progressing at the same pace as the basic conditions for use. The Data Protection Commission argues that this is a matter of serious concern because the additional risks of a general personal number require more safeguards than provided by the Data Protection Law.[203]

In spite of the fact that the bill for the BSN had not as yet passed the First Chamber of Parliament[204], the number appears since January 1st 2006 on all Dutch official documents such as passports and studentcards. Government organisations use the BSN via a private secure network. It is expected that the area, in which the BSN may be used, will be broadened to all organisations, carrying out a public duty,[205] such as the Internal Revenue. Numbers used in sectors, such as the judicial chain, will probably use their own number. Citizens can use the BSN for applying for various local services such as building permits. It is still uncertain whether private organisations will be granted access even though especially the banking world has shown much interest.

References

CBP 2007

Brief van het College bescherming persoonsgegevens aan de Leden van de Eerste Kamer, number z2007-00082, January 11th 2007 concerning Reactie op memorie van antwoord Wabb (EK, 2006-2007, 30312, D).

CDJC 1990

European Committee on legal cooperation (CDCJ), The introduction and use of Personal Identification Numbers: The Data Protection Issues, Council of Europe, July 1990, Add. III to CDJC (90).

FACTSHEET BSN 2006

Burgerservicenummer Introductie, Factsheet. Den Haag, Programmabureau Burgerservicenummer, 2006. www.programmabsn.nl

[203] CBP 2007.

[204] In July 2007 the law did eventually pass the First Chamber with a small majority. There was still much uncertainty about the way the government intends to handle complaints of citizens whose ID-number is used incorrectly. The creation of a kind of helpdesk for a period as long as it takes to evaluate the law was promised by the government in an attempt to assuage these doubts.

[205] WABBN Eerste Kamer, A, art 1 sub d.2 en d Memorie van Toelichting 30312, nr 3, p. 11 + comments on art 1 Wabbn.

KUITENBROUWER 1991

F. Kuitenbrouwer. Het recht om met rust gelaten te worden. Over privacy. Amsterdam, Balans, 1991.

MOM 2007

P. Mom, Invoer Burger Service Nummer minacht privacy, Overheid Innovatief nr 1/2007.

PRINS 2003

J.E.J. Prins, Het Burger Service Nummer en de strijd tegen Identiteitsfraude, Computerrecht (1).

TAFEL 2002

Advies van de Tafel 'Persoonsnummerbeleid in het kader van identiteitsmanagement', juni 2002.

VEDDER

A. Vedder, Niets meer te verbergen en toch bang, 911 en de privacy van de doorsnee burger, Filosofie en praktijk, jrg 27 – nr 5, p. 49.

WABBN

Voorstel van Wet algemene bepalingen burgerservicenummer (Wabbn), Kamerstuk nummer 30312.

WABBN EERSTE KAMER

Voorstel van wet Wabbn, Eerste Kamer 30312.

5 Summary and conclusions

5.1 Summary

The history of the need to identify persons provides an interesting view of the trends in various social and nation-state developments in Europe. Means of identification have always been necessary to run large organisations, such as churches, but also the early forms of nation states. The need to validate the authenticity of persons arose from the primary need for states to protect themselves against criminals or to regulate the movement of colonists. Churches wanted for tax reasons to know the number and names of persons who were baptised and married and later also of those who were confirmed and buried. An additional advantage for the church was that the sacraments due to be registered were considered necessary for a person to be later resurrected from the dead. Later it became important for states to identify individuals for tax reasons but also to recruit soldiers and to calculate the amount of money needed for the poor. A further important reason was the need to identify persons travelling from one country to another. This is why a passport was introduced long ago. A passport facilitated the free movement of persons. In fact it was a document to enable people to pass through an area.

Need to validate the authenticity of persons arose from the primary need for states to protect themselves against criminals or to regulate the movement of colonists

These various developments in and purposes for identification are reflected in the present patchwork of ways in which citizen verification takes place. After all, citizens today use a large variety of ID documents such as passports, national ID-cards, e-health cards, social insurance cards, credit cards, driving licenses, customer loyalty cards, etc. From a global point of view it seems increasingly reasonable to want to harmonise these verification registers and the means the citizen uses for this purpose. The technical means to facilitate this such as smart chips and RFID are becoming ever more available. Correspondingly the illegal use of this manner of identification leads to an increasing opportunity for fraud. Central storage is often thought to be a solution.

The illegal use of this manner of identification leads to an increasing opportunity for fraud

Considering the needs of eGovernment as a starting point, the legal contribution to this deliverable discusses the roles so-called entities can have in a particular sector. Entities can be attributed a global, sector-specific or context specific identifier. In e-government an attempt is made to optimise service delivery by channelling internal and external relationships through technology. Interoperability and the usage of common ID numbers for all relevant entities then make the usage of ID numbers tantamount for e-government. Bearing this in mind the question is whether they are supported by a sound legal framework, whether the usage of global identifiers is enough to guarantee the rights of the individual as defined in the European Data Protection Directive [206] or should technical unlinkability also be a requirement of e-government architecture. The contribution makes clear that ID numbers are personal data and therefore the processing of these numbers should be carried out subject to the Data Directive. This means that attention should be given to the legitimacy of the processing, the data quality and aspects of confidentiality and security. It may be said to be unfortunate that the Directive leaves the standards for safeguards that Member states put in place, up to the Member states. With the present state of knowledge it might have been expected that due to the value the Directive puts on the sound protection of the ID number, that technical unlinkability would have been prescribed. After all, the Directive does point out that appropriate technical and organisational security measures must be taken. These should take account of the state of the art, the cost of their implementation and the risks represented by processing and the nature of the data. Unfortunately the present legal framework therefore soon becomes inadequate in preventing the technical linkability of potentially privacy harmful data about citizens on the basis of ID numbers. Once the necessary infrastructure is in place, including global ID numbers, data exchange will take place anyway either legitimately or illegitimately, based on an ad hoc argument or on political choices. Therefore, there is a strong argument for context or sector specific identifiers.

Interoperability and the usage of common ID numbers for all relevant entities make the usage of ID numbers tantamount for e-government.

Data exchange will take place anyway either legitimately or illegitimately, based on an ad hoc argument or on political choices

ID numbers arouse strong emotions which cannot be solely comprehended from a legalistic suspicion of being potentially harmful to the individual’s privacy. Therefore a sociological analysis of the function of ID numbers is introduced. In this deliverable the sociological approach is looked at from two angles: social systems theory and a theory on the role of bureaucracy in national states.

[206] Directive 95/46/EC.

The social systems theory views society from a general perspective, allowing the analysis of the function of ID numbers in private and public organisations. By thoroughly analysing the function of names, identifiers and addresses it can be ascertained that ID numbers fulfill all three functions of a name, an identifier or an address. First, they can be used as names for a data set or a number of data sets in a database. Secondly, they can be used as identifiers if they link a person uniquely in an administrative context. Thirdly, they can also be used as addresses. In the communicational organisational context, social systems theory learns that addresses are always administered (generated, assigned and deleted or deactivated) by organisations. Organisations also are also careful to resolve potential address collisions by keeping addresses unique in the particular scope of the operation. The state ensures addressability for governmental, private-sector or interactional (citizen to citizen) operations. Addressability today covers persons, families, organisations and objects in the context of communication techniques. Addressability is not possible without organisations. These organisations need the unique identifiability to run their operations smoothly and efficiently. This in turn may lead to information asymmetry because, as shown in the legal analysis, it reduces the autonomy of individuals by the usage of linkability measures. In other words, a shift of power may occur in favour of the organisation. In the context of states in many cases it is difficult to decide whether citizens overall benefit from this development or not, the reason being that citizens typically take on two roles with respect to the state. On the one hand they are members and thus benefit from a strong state that is able to protect them and, on the other hand they are clients of the state who suffer from reduced autonomy.

Organisations need the unique identifiability to run their operations smoothly and efficiently.

The second sociological angle is based on the Weberian theory of bureaucracy. Against the background of the rationalisation processes going on in all areas of society, the function of ID numbers is described as having the purpose of providing the members of a state with a feeling of unity and cohesion within the perspective of increased globalisation. Political rationalisation resulted in the formalisation of the state. One of the unique properties of a state is a trained corps of civil servants specially trained in and restricted to regulations. This corps of civil servants has as its main task, the identification of the members of the state to enable the state to carry out its primary tasks. According to Weber these bureaucracies are the ultimate example of the rationalisation process because they aim at efficiency, predictability, quantifiability, control by substituting human judgement by non-human technology and irrationality by rationality. To carry out its tasks the bureaucratic government accordingly issued identity cards and codes. These identification means provided access to a whole series of files and data sets. ID numbers therefore became the symbols of this bureaucratic culture. Seemingly meaningless numbers acquire meaning in this bureaucratic context because the developing nation-states desired to attach meaning to this symbol. Sociologically speaking it is argued, this was an unfortunate choice because, as Weber already pointed out, this was the irrationality of rationality. The intention of creating a notion of unity and solidarity was not attained because citizens felt that the ID number identification led to depersonalisation. It could be argued that the mismanaged effort to create unity in states by the introduction of the ID-number actually led to a sense of loss of privacy without contributing to the sense of unity.

Seemingly meaningless numbers acquire meaning in this bureaucratic context.

Taking the risks and opportunities of ID-numbers in the modern technological age, we investigate the contrast between requirements techniques such as profiling pose vis-à-vis the protection of the individual's privacy privileges. Profiling provides a new kind of knowledge used for decision-making based on Knowledge Discovery in Databases (KDD). KDD requires per definition as much information as possible about the individual, whereas traditional privacy rights focus on data minimisation. There is no easy solution for this conflict. Research is being done concerning this problem in another workpackage (D.7.9). By introducing the concepts of contextual integrity and reciprocal transparency in combination with multiple identifiers, it looks like that both the needs of KDD techniques as well as the concept of privacy can be achieved. This does need a fine-tuned combination of transparency and opacity tools to be built into the new technogical infrastructure of an Ambient Intelligence society.[207]

KDD requires per definition as much information as possible about the individual, whereas traditional privacy rights focus on data minimisation.

One approach is to ask citizens to be more transparent by introducing sector-wide and unique ID numbers, while at the same time attempts are made to make the state and its actions more transparent. Examples are, in the Netherlands, the introduction of the National Trust Function to log the use of the national ID number and, the introduction of Freedom of Information Acts in Germany, allowing citizens to access their own data files maintained by the state. Unfortunately, these attempts fall short in certain cases. In addition to limitations for citizens to access secret data, which is very understandable because these could be covered by trust based models, the use of profiling creates additional limitations for transparency. Certain types of profiles are not linked to the data they were derived from, they are no longer personal data and, may be used to the disadvantage of the citizen in a non-transparent way. Due to the complexity of the underlying profiling processes, regulatory attempts to increase transparency fall short and, Transparency Enhancing Technologies (TETs) to fill this gap are limited in effectiveness or do not even exist yet. Another problematic aspect of transparency is that from a social perspective people think, communicate and act in communicational terms. Data freely used in one context cannot necessarily be used in another. Keeping data in its appropriate context is also called the concept of contextual integrity. Informational self-determination can be understood as an important attempt to put contextual integrity in legal norms, though certainly from a social perspective an inappropriate one in certain cases. These aspects are further elaborated in the FIDIS deliverable D7.9.

Keeping data in its appropriate context is also called the concept of contextual integrity

[207] Gutwirth De Hert 2005.

Yet another approach is the introduction of additional functions and tools that make the individual less recognisable or opaque. In this context different methods have been developed and implemented to restrict and control linkability facilitated by ID numbers. This is elaborated on in the second part containing the country reports.

In light of the above-mentioned factors four different basic concepts on how to deal with ID numbers have been developed in national political strategies and existing infrastructures. They are:

1. Introduction of sector-wide ID numbers with a large area of use inside and outside the public sector mainly based on mutual transparency (example: The Netherlands)
2. Introduction of sector-wide ID numbers with regulations on how they may be used (examples: Switzerland, Czech Republic and Slovakia)
3. Introduction of sector specific ID numbers and organisational enforcement of borders of sectors (examples: Hungary, France, Germany)
4. Introduction of sector specific ID numbers and organisational as well as technical enforcement of borders of sectors (example: Austria)

References

GUTWIRTH DE HERT 2005

S. Gutwirth, P. de Hert. Privacy and Data Protection in a Democratic Constitutional State. Profiling: Implications for Democracy and Rule of Law. FIDIS Deliverable 7.4, M. Hildebrandt and S. Gutwirth. Brussels

5.2 Conclusions

The analysis of ID-numbers and policies as provided in this deliverable shows that ID-numbers are an essential tool for the realisation of e-government and modern business processes. Due to the increasing pervasiveness of Internet as a means of communication by governments and enterprises, there is a growing necessity for a secure identity management. The need to identify who communicates with whom is essential in an Internet environment because the Internet, by design, lacks these provisions. Because of these shortcomings various solutions have been developed. The identity number is a prominent one. As is shown, the developments in this area could affect the privacy interests of individuals. Individuals often need to disclose more personal data than strictly required.[208] Several steps are still being taken to tackle this problem.[209]

[208] Cf Fidis Deliverable 5.4.

[209] Cf among other things the work done by the PRIME consortium as set out in the PRIME white paper v2, 27 June 2007.

The sociological and the historical analyses indicate that only a carefully attuned policy will allow the present possibilities and opportunities of ID-numbers to be used successfully. From the socio-cultural point of view, experiences in using the identification tool as a method by which to create a feeling of unity in a nation-state, that only exists in the minds of the heads of state, have led to the opposite result. From the social systems point of view, there are potential benefits as well as drawbacks in the usage of an ID-number. In the public domain one of the drawbacks could be caused by the fact that citizens are members of a state as well as clients. The state benefits from the advantages of using ID-numbers and therefore these benefits also are beneficial to its members. Drawbacks might arise when these measures harm the clients of organisations when ID-number linkability is used to create information asymmetry in favour of organisations. Organisations may use this asymmetry to reduce the autonomy of the individuals. This, in turn, may result in a shift in the balance of power favouring organisations.

In this deliverable the potential information asymmetry,as achieved by technical means, is illustrated by describing profiling techniques envisioned in scenarios for Ambient Intelligence. Even though there are the large risks of abuse in these scenarios,the suggestions for making good use of the opportunities technology has to offer are promising. This privacy-friendly scenario can be achieved through a joint effort of computer engineers, legal experts and policymakers. Within the scope of the European Data Directive the opportunities for using profiling techniques can thus be put to good use. Individuals can then be monitored without necessitating any kind of transcontextual identification. This fits in with the purpose of the limitation principle of the Directive.

On the whole it is necessary to reconsider the concept of privacy because the broad definition of the right to be left alone is no longer feasible in the present digital era. Nevertheless without a doubt, the protection of personal data is a fundamental right in the European Union. In many Member States it is a constitutional right.[210] However, if appropriate attention is given to the rights of individuals such as is expressed in the legitimacy of the processing, the data quality and aspects of confidentiality and security, the principle of the protection of personal data or so-called informational privacy, this will enable a sound identity management. In the area of profiling this seems to call for limiting the use of personal data to the proper context. However, this could preclude the use of profiling to its full potential.

This deliverable has shown that it is instrumental to redefine the concept of privacy in terms of “privacy as contextual integrity”[211] while, at the same time, underpinning it with the appropriate technical means. In this light it seems preferable and feasible to adopt multiple ID-number policies. These allow us to discriminate between different contexts providing tailored ID-number policies, depending on which type of privacy is appropriate per context. The point of departure is a type of identity management based on user control. At the same

[210] The Charter of Fundamental Rights of the European Union enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7 thereof and the same is the case in at national level in some states. Cf ARTICLE 29 DATA PROTECTION WORKING PARTY 2007, p.7.

[211] A concept introduced by NISSENBAUM 2004, pp. 101-140.

time, the reciprocity or distribution of the transparency can be tailored, depending on the need for checks and balances per context. This does not necessarily rule out interoperability between contexts, because ID-numbers may be linked, e.g. via clearing houses, to provide interoperability. The information asymmetry that looms behind the horizon may thus be turned to good use.

In essence it may be concluded that multiple identifiers in conjunction with interoperability and contextual integrity are the most promising solution for a sound identity management policy in the near future. This does require a fine-tuned combination of transparency and opacity tools to be built into the technological infrastructure. In such a way the individual will not become unnecessarily transparent nor will interoperability be precluded by excessive user control. The advantages of e-government can thus be achieved reciprocally for government and citizen alike. Measures to prevent identity fraud must be part of this IDM policy while, at the same time, the corresponding security measures must be construed in such a way as to inspire the citizen with sufficient trust that the government treats his data safely. It seems that the Austrian citizen card concept is an example that deserves to be pursued further.

References

ARTICLE 29 DATA PROTECTION WORKING PARTY 2007

Opinion 4/2007 of 20th June 2007 of the Article 29 Data Protection Working Party on the concept of personal data, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

Nissenbaum 2004

H. Nissenbaum, ‘Privacy as Contextual Integrity’, *Washington Law Review* 79 (2004), pp. 101-140

ANNEX Composition of ID Numbers in EU countries

France: Numéro d'Inscription au Répertoire des Personnes physiques (NIR)

Character	Content	Example
1	Gender (1 for men, 2 for women)	2
2-3	Last two digits of year of birth	53
1	Gender (1 for men, 2 for women)	2
2-3	Last two digits of year of birth	53
4-5	Month of birth (01 to 12)	07
6-7	Region of birth	75
9-10	Order of birth in the region	073
11-13	Number of birth certificate	004
14-15	Error checking number	83

Belgium: Rijksregisternummer (State registernumber)

Character	Content	Example
1-6	Date of birth (without century)	880515
7-9	Birth number (even for women, uneven for men)	275
10-11	Error checking number	16

Hungary: Tax number or Health care ID Number

Digit	Content	Example

1-10	Number with ten digits	1234565432
11	Error checking number	1

Czech Republic / Slovakia: Rodné číslo (RČ)

Digit	Content	Example
1-2	Year of birth	84
3-4	Month of birth (for females advanced by 50)	05
5-6	Day of birth	01
7-10	Semi-unique identifier that fits the elevencheck.	1330

Germany: Steueridentifikationsnummer

Character	Content	Example
1-10	Number with ten digits	1234565432
11	Error checking number	1

Austria (1): Zentrale Melderegister-Zahl

Character	Content	Example
1-12	Number with twelve digits	123456765432

Austria (2): Social Insurance Number

Character	Content	Example
1-3	Number with three digits	123
4	Error checking number	4
5-6	Birthday of the insured person	03
7-8	Month of birth	08
9-10	Year of birth	69

Switzerland: Alters- und Hinterlassenenversicherung (new)

Character	Content	Example
1-3	Swiss country code	756
4-12	Random number	123456789
13	Error checking number	5

The Netherlands: BurgerServicenummer (BSN)

Character	Content	Example
9	The BSN is random number that fits the elevencheck	148527711

Sweden: Personnummer

Digit	Content	Example

1-6	Year (without century), month and day of birth	640823
-		
7-9	Serial (birth) number (even for men, uneven for women)	323
10	Error checking number	4

Denmark: Personnummer / CPR-nummer

Character	Content	Example
1-2	Day of birth	15
3-4	Month of birth	08
5-6	Year of birth, without century	53
7-10	4-digit number (algorithm)	1234
	Last digit is a even number for women and a uneven number for men	

United Kingdom: National Insurance Number (NINO)

Digit	Content	Example
1-2	The first and second letter cannot be *D*, *F*, *I*, *Q*, *U* and *V*. The second letter also cannot be *O*.	AB
3-8	Six digit number	123456
9	Optional suffix letter, roughly (but not directly) linked to their date of birth	C

Slovenia: Enotna Maticna Stevilka Obcana

Character	Content	Example

1-7	Day of birth (without millenium) Last digit is a even number for women and a uneven number for men	0101006

Spain: Número del Documento Nacional de Identidad del Ciudadano

Digit	Content	Example
1-8	Random number	12345678
9	Error checking letter	Z

Italy: Codice Fiscale

Character	Content	Example
1-3	Three alphabetical characters for the first name	RSS
4-6	Three alphabetical characters for the last name	BBR
7-8	Two numerical characters for the year of birth	69
9	An alphabetical character for the birth month	C
10-11	Two numerical characters for the day of birth and the sex	48
12-15	Four characters (one alphabetical, three numerical) for the region of birth	F839
16	Error checking character	A