THE USE AND RISKS OF ELECTRONIC IDENTITY CARDS: THE CASE OF GREECE

Student: Eleni I. Kapralou
ANR: 363107
Supervisor: Professor Paul de Hert
Second Reader: Mr. Arnold Roosendaal
Tilburg- June 2011.
TABLE OF CONTENTS

Introduction ........................................................................................................... 6

Methodology ........................................................................................................ 8

CHAPTER 1
A general review of modern identification methods

1. Defining basic notions .................................................................................... 11
   1.1. Identity and Identification ..................................................................... 11
   1.2. Authentication and authorisation ....................................................... 12
   1.3. Anonymity ............................................................................................ 12

2. Identification: a philosophical discourse ...................................................... 13

3. A brief historical review of official identification methods ......................... 15

4. The real identity card in Greece ................................................................... 17

CHAPTER 2
Use of new technologies for identification purposes

2.1. New technologies ....................................................................................... 19
   2.1.1. RFID Technologies and current applications ................................. 19
   2.1.2. Biometrics ......................................................................................... 21
   2.1.3. PKI and Electronic Signatures .......................................................... 22

2.2. New technologies and e-ID cards ............................................................. 23

CHAPTER 3
The potential benefits of e-ID cards

3.1 “Understanding e-Government” ................................................................. 26

3.2. Enhancement of democracy: e-participation and e-voting ...................... 28

3.3. The e-ID card as an e-government catalyst ............................................. 29
   3.3.1. The Austrian “Bürgerkarte” ............................................................... 30
   3.3.2. E-voting in Estonia .......................................................................... 32

3.4. E-government initiatives by the OECD .................................................... 33
3.5. E-government initiatives by the EU .................................................................34
3.5.1. The Digital Agenda ..................................................................................34
3.5.2. E-health and social security .....................................................................34
3.6. E-government initiatives by Greece ..............................................................35

CHAPTER 4
Potential risks of the use of e-ID cards

4.1. The surveillance society ...............................................................................36
4.1.1. Privacy and data protection .....................................................................36
4.1.2. ID cards as tools of surveillance and discrimination ..............................38
4.2. The e-ID card scheme in the UK ..................................................................44

CHAPTER 5
Comparing the passport with the e-ID card

5.1. Historical background ..................................................................................47
5.2. The e-passport in the European Union .........................................................48
5.2.1. Legal Context .........................................................................................48
5.2.2. Technical Characteristics .......................................................................49
5.2.3. Security and privacy risks .......................................................................50
5.3. Differences and similarities between the two documents .............................51

CHAPTER 6
The e-ID card in Greece

6.1. The Greek Constitution ..............................................................................54
6.2 Law no. 2472/97 for the implementation of Directive 95/46 EC ..................54
6.3. The Greek tax-card .....................................................................................55
6.4. The Opinion 4/2010 of the HDPA ...............................................................56
6.5. Suggestions in order to strike a balance between benefits and risks .........57

Conclusions .........................................................................................................61
# ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BAC</td>
<td>Basic Access Control</td>
</tr>
<tr>
<td>EAC</td>
<td>Extended Access Control</td>
</tr>
<tr>
<td>e-democracy</td>
<td>electronic democracy</td>
</tr>
<tr>
<td>e-government</td>
<td>electronic government</td>
</tr>
<tr>
<td>e-ID card</td>
<td>electronic identity card</td>
</tr>
<tr>
<td>e-participation</td>
<td>electronic participation</td>
</tr>
<tr>
<td>e-passport</td>
<td>electronic passport</td>
</tr>
<tr>
<td>e-signatures</td>
<td>electronic signatures</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>e-voting</td>
<td>electronic voting</td>
</tr>
<tr>
<td>FIDIS</td>
<td>the Future of Identity in the Information Society</td>
</tr>
<tr>
<td>FTE</td>
<td>Failure To Enroll</td>
</tr>
<tr>
<td>HDPA</td>
<td>Hellenic Data Protection Authority</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organisation</td>
</tr>
<tr>
<td>ICTs</td>
<td>Information &amp; Communication Technologies</td>
</tr>
<tr>
<td>ID card</td>
<td>Identification (or Identity) card</td>
</tr>
<tr>
<td>IFF</td>
<td>Identification Friend or Foe</td>
</tr>
<tr>
<td>NIR</td>
<td>National Identity Register</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation &amp; Development</td>
</tr>
<tr>
<td>PETs</td>
<td>Privacy Enhancing Technologies</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POS</td>
<td>Point Of Sale</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>s-PIN</td>
<td>source PIN</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>ss-PIN</td>
<td>sector-specific PIN</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UPC</td>
<td>Universal Product Code</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
<tr>
<td>VAT</td>
<td>Value Added Tax</td>
</tr>
<tr>
<td>VWP</td>
<td>Visa Waiver Program</td>
</tr>
</tbody>
</table>

To Greek people who are struggling for Democracy and the national sovereignty of their Land.
INTRODUCTION

“Your identity card please”, seems like a very common request; certainly, each one of us heard it at least once in our life, when a police-officer randomly in the street, during usual checking at an airport or anywhere else asked us to do so. The current debate now in Greece rambles around the electronic citizen card that will be first used to fight against tax evasion. Subsequently, it will replace paper-based identity cards and constitute mandatory identification documents for all Greek citizens. Although it is a difficult time for such a project, as the on-going economic crisis negatively influences developments, the Greek Government decided to have implemented the new e-governance scheme by the end of 2011.

As far as “electronic identity cards” are obligatory citizenship documents, they have the potential to monitor the total population of a state, leading to what Clarke calls “mass surveillance”, with detrimental effects on privacy and personal data protection. However, at the other end of the spectrum, we should not ignore the benefits that society can reap from such an implementation. E-ID cards are vital for “electronic government” procedures. Therefore, they can contribute to the reorganisation and rationalisation of public administration of a state.

Hence, the question I intend to answer hereby is what kind of balance would be desirable to strike so that Greek society suffers the least negative effects on privacy and personal data protection, and at the same time gains the most of its benefits. In other words, what kind of balance can safeguard human rights, but also grant access to high quality public services?

The first reason I chose this topic is that it constitutes the current debate in Greece. Only recently, on the 27th of April 2011, was the Bill for e-government deposited before the Greek Parliament for vote. Second, in Greece there were and still are opposing voices that the new scheme raises significant privacy and data protection concerns. And third, it is a pan-European issue.

1 I came up with this catchy introductory sentence and later on I found out that David Lyon in his book Identifying citizens, ID cards as surveillance, (Cambridge: Polity Press, 2009), 1, starts with a similar way his introduction. This fact gave me confidence in continuing writing my thesis.

2 Henceforth e-ID cards.


4 Henceforth e-government.


6 The Bill was eventually voted by the Greek Parliament on the 24th of May 2011, and unfortunately, Law no. 3979/2011 on e-governance will not constitute the object of my legal analysis. Of course, I hope that I will have the chance to write a second paper in which I will explicitly analyse the new law.
that will be plaguing us for at least the next ten years\textsuperscript{7} and will place another building block to the political integration of European citizens.

In the first chapter, I examine the background of e-ID cards. I start by defining some basic notions, such as identity and identification. Then, I discuss about the philosophical aspects of these notions and make a historical review with regards to the use of official identification methods in the course of the time. This time trip has as a starting point the \textit{polis} or city-state in ancient Greece, and destination identification methods in modern states. Finally, a special reference is made to the current legal regime in Greece regarding ID cards in general.

The core of the second chapter consists of a brief study on the technologies of which e-ID cards make use. I mainly focus on Radio Frequency Identification\textsuperscript{8}, biometrics, and Public Key Infrastructure\textsuperscript{9} and electronic signatures.\textsuperscript{10} My foremost aim is to explain the functioning of these technologies, briefly mention some of their current applications, and underline their special characteristics with regards to identification of citizens.

Thereafter, in the third chapter, I examine the potential benefits of the use of e-ID cards and I focus on e-government and public electronic services. First, I explain what e-government is. Second, I analyse the potential benefit from the enhancement of democracy, focusing on e-democracy, e-participation and e-voting. Third, I explain why e-ID cards are important for e-government, with a special focus on the Austrian “Bürgerkarte” and e-voting in Estonia. Finally, I analyse various e-government initiatives taken by the OECD, the EU, and the state of Greece.

Afterward, in the fourth chapter, I focus and comment on the risks derived by the use of e-ID cards, in the light of privacy and personal data protection. I start by referring to the basic meanings of privacy and explain how the right of personal data protection evolved. Then, I clarify how e-ID cards can be used as tools of surveillance and discrimination. And, finally, I give an explicit picture of the e-ID card scheme in the UK and indicate the reasons of its cancellation in 2010.\textsuperscript{11}

Additionally, in the fifth chapter, I describe the general background and functions of “electronic passports”\textsuperscript{12}. I analyse the EU policy regarding the biometric passport, and I refer to the legal context, the technical

\textsuperscript{7} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, “A Digital Agenda for Europe”, (Brussels, 19.05.2010).
\textsuperscript{8} Henceforth RFID.
\textsuperscript{9} Henceforth PKI.
\textsuperscript{10} Henceforth e-signatures.
\textsuperscript{11} http://www.guardian.co.uk/politics/2010/may/27/theresa-may-scrapping-id-cards.
\textsuperscript{12} Henceforth e-passports.
characteristics and the privacy related issues. Finally, I make a comparison between e-passports and e-ID cards, by highlighting their differences and similarities.

Last but not least, in the sixth chapter I look at the legal regime in Greece with regards to the implementation of the e-ID scheme. First, I present the relevant provisions of the Greek Constitution. Second, I analyse Law no. 2472/97 for the implementation of Directive 95/46 “on the protection of individuals with regard to the processing of personal data and on the free movement of such data”. Afterward, I comment on the new tax-card and I expose the Opinion 4/2010 of the Hellenic Data Protection Authority13 on this issue. Finally, I make some suggestions on how to strike the right balance between the potential benefits of e-ID cards and the potential risks for privacy and personal data.

Methodology

The fact that on the 27th of April 2011 the Bill for e-governance was deposited before the Greek Parliament for vote indicates that the topic of this study constitutes a current issue in Greece. On the one hand, this was a disadvantage. The e-ID card scheme was developing intensively during the last five months and running in parallel with my writing this study. This meant that I had to be very careful and keep up with the latest developments, and continuously make the respective amendments in my work. Although this was overly time-consuming, on the other hand, it was also challenging, because there was still enough room for fruitful dialogue. Hence, I do not discuss in this study Law no. 3979/2011 on e-governance that was voted on the 24th of May 2011, long before which I had already submitted the draft version of my thesis.

Moreover, in this study I refer to both the tax-card and the e-ID card. The first will be optional and subsequently incorporated in a national e-ID card, which will mandatorily replace the paper-based identity cards used nowadays in Greece. I consider both cards as part of the same e-governance scheme. In addition, given that the period of time between the use of the tax-card and its replacement from the e-ID card is too short, if I excluded the e-ID card from my analysis, my study would be insufficient.

Concerning the methodology of my study, I make a multidimensional analysis of the issue. I do not solely focus on the legal aspects of the problem, but I want to stress that the issue has also to be seen from a historical and sociological perspective. Obviously Law has the final say, but even this, is the

13 Henceforth HDPA.
fruit of the interaction between legislators and society. The reason for which I chose such an approach is that I consider that all problems possess multidimensional features. It is only by examining all these features that the most viable, easily enforced and cost-effective solutions can be adopted. Furthermore, I do not endorse a one-sided approach, but I examine the issue in its real and overall dimensions, pointing out both the potential risks and benefits of the implementation of such a large-scale identification scheme.

Therefore, I use a historical and sociological analysis which deals with methods of identification from ancient years until the 21st century. What I want to indicate is that the birth of the nation state was the reason that gave birth to the need for identification of citizens. Lyon in his book “Identifying Citizens: ID cards as surveillance” states that the reason that we have to be acquainted with “past identification practices” and to recall their “dignity-destroying possibilities is not to tar today’s initiatives with the same brush so much as to strive to ensure that such egregious errors are not repeated”.14

During my research I felt that there is a great amount of literature that focuses on the drawbacks and risks of new identification methods. Arguably there is a fair amount focused on the potential benefits, but the weight tilts towards privacy and data protection concerns. However, there is no rich Greek bibliography on the use and risks of e-ID cards. In his book “Legal Issues of Informatics” Papakonstantinou analyses mostly the Greek Law no. 2472/97 on personal data protection, without any special focus on identity cards. Nevertheless, it is an important work because it comprehensively analyses the provisions of the Greek legal regime. Finally, I found very interesting the various deliverables of the “Future of Identity in the Information Society”15 and the Working Documents of the Working Party 29.

Besides, I make use of certain technological terms. I admit that is difficult for a lawyer or common reader to immediately understand the technological processes that take place during modern identification. However, I tried to make it as clear as possible, avoiding sophisticated and purely technical terms. I only want to give the reader a helicopter view in order to get a clearer image on how these technologies work.

Furthermore, I found very important the advice of Professor de Hert to include in my thesis a comparison between the e-passport and the e-ID card. The reasons were manifold. First, there is a clear EU policy with regards to the e-passport, whereas there is not for the e-ID card. Most EU policies on identity cards concern themselves with the digitisation of public administration and the use of the Internet. Generally speaking, national e-ID schemes took

place without “supra-national European co-ordination, leading to divergent implementations with regards to privacy issues, but also other elements”.\textsuperscript{16} Second, the e-passport policy is old and certainly has a lot of results to show, whereas the e-id card, comparatively new, is not suitable for processing any outcomes.

With regards to Cases, I first examine the case of the Austrian “Citizen Card”, called “Bürgerkarte” that is vital for e-government procedures.\textsuperscript{17} The reason I chose this case is that the Austrian scheme is not based on a physical identity card, but on an identity concept, safeguarding privacy and personal data protection, and without the use of RFID and biometrics. Interestingly, the Data Protection Agency of the Community of Madrid awarded in 2005 the Austria’s public authorities for the idea of the “Buergerkarte”.\textsuperscript{18} Moreover, I examine the case of e-voting in Estonia that although its effect on the increase of participation is vague, it is “a central reference point in the discussion about e-voting in Europe”.\textsuperscript{19}

Additionally, I examine the case of the UK, where the new identity card was recently cancelled because it was deemed too costly and privacy unfriendly. After having made a brief historical review, I then refer to Laurie who managed to break the e-id card and steal the data it contained within some seconds. What is shown is that e-ID cards are vulnerable and not favored in some other states.

Finally, I focus on the case of Greece, by making a legal analysis. I first refer to the relevant provisions found in the Greek Constitution concerning privacy and personal data protection. Afterward, I provide an overview of the most important provisions of the Greek Law no. 2472/97 and then, I analyse the Opinion of the HDPA on the new tax-card that will gradually replace all the paper-based identity cards.


\textsuperscript{19} A background paper for the Workshop on “E-voting in Europe”, E-voting in Europe: why should we look at it, which arguments we should consider and what to expect in the future, 1, 17 March 2011.
CHAPTER 1
A GENERAL REVIEW OF MODERN IDENTIFICATION METHODS

In this chapter I examine the background of e-ID cards. I start by defining some basic notions, namely what identity and identification, authentication and authorisation, and anonymity stand for. The reader becomes acquainted with concepts with which I will deal in the next chapters of this study. Then, I discuss about the philosophical discourse concerning these notions. Moreover, a historical review is made with regards to the use of official identification methods, making a time trip that has as a starting point the polis or city-state in ancient Greece, and destination identification methods in modern states. Finally, a special reference is made to the current legal regime in Greece, regarding ID cards in general.

1. Defining basic notions

1.1. Identity and Identification

Etymologically the word “identity” has its roots in the Latin word \textit{idem} that means the same. This meaning also reflects the basic principle of Logic which holds that A=A and not A=non-A. According to Nabeth “identity is seen as a set of attributes characterising and representing the person”, whereas “identification is considered according to a set of processes relating to disclosure of information about the person and usage of this information”. Identity deals with data that are used to identify someone, such as the name or sex, whereas identification encompasses various means of identification, such as identity cards and passports. Thus, the two terms are interrelated, the first involving a substantial and the second a procedural aspect of the same issue.

Generally speaking, the word identity has a host of meanings in different scientific disciplines. Philosophers are concerned with autonomy and freedom. For sociologists, a person might have various identities. He can be a member of a family or an association of employees, to name but a few. Thus,

\footnotesize{20} Answering the question of what identity is I recall the distinction that Paul Ricoeur made in his book “Oneself of the other” between ipse identity and idem-identity; the first is constantly changing and developing, referring to the perception by the self of its existence, whereas the second is static and answers more the question of whom I am.

\footnotesize{21} Thierry Nabeth, “Identity of Identity”, in The future of identity in the information society (FIDIS): Challenges and Opportunities, eds. Kai Rannenberg, Denis Royer, André Deuker, 36 (Dordrecht [etc.]: Springer, 2009).}
in this sector, identity is closely related to membership. In the field of Psychology identity means the way a person perceives himself as well as how the person is perceived and represented. Finally, lawyers are engaged with concepts such as citizenship, civil responsibility, surveillance, security, administration, privacy and personal data protection.

1.2. Authentication and authorisation

The abovementioned terms are distinguished, although still correlated, from the terms “authentication” and “authorisation”. The first is the process of proving that something or someone is valid or genuine or true. An illuminating example is when someone wants to open a bank account. In this case, although he claims to be that specific person, he also has to prove the validity of his claims by showing an official document, such as an identity card. Authorisation, however, is the permission or power given to somebody to do something. For instance, a student has a set of attributes which grants him with a student card which in turn authorises him to borrow books from the university library.

1.3. Anonymity

Anonymity is the state of being unknown to others. It is not perceived towards one’s self, but only towards others; this means that an anonymous person always possesses an identity. The term comes along with considerable controversy. According to Froomkin anonymity has not only positive implications, but also various drawbacks. On the one hand, it strengthens privacy, because, when anonymity is retained, people’s private sphere is safeguarded. On the other hand, it augments the problem of rendering responsibility for illegal actions, and makes transactions more difficult. In modern societies preserving with any price anonymity seems suspicious because people normally refrain from trusting anonymous entities. Hence, even though anonymity offers a great range and degree of

25 Ibid., 68.
26 Hornby, Oxford Advanced Learner’s Dictionary, 41.
28 See also: Gary T. Marx, “Identity and Anonymity: some conceptual distinctions and issues for research”, in Documenting individual identity, the development of state practices in the modern world, eds. Jane Caplan and John Torpey, 319 (Princeton University Press, 2001): “mutual revelation is a sign of good faith that makes it easier to trust (not unlike the handshake, whose
freedoms, at the end, it might be the price of isolation that an agent pays in a society.

2. Identification: a philosophical discourse

Jenkins recognises a host of questions that relate to identity and identification, such as “How do we know who we are and how do others identify us?”29 He also argues that identification is crucial because it is the “basic cognitive mechanism that humans use to sort out themselves and their fellows”30. In this section, I will try to answer these questions and apply the above mentioned arguments to the specific case of identity cards and official identification methods.

Humans belong to the same genre of living beings, sharing the same generic physical characteristics. It is difficult to identify people in everyday transactions, as human memory is of limited capacities and identity fraud a frequent phenomenon. How would someone know who I am? The only way is that I tell them so. But then, how would one know that I am telling the truth?31

The issue of trustworthiness is partly solved by appointing a trusted third party.32 In official situations, it is the state in the form of public sector authorities that are competent to identify citizens. A common way in which they solve complex situations of identification, such as identification of persons with the same name or physical characteristics (e.g.: twins), is by appointing a unique number to each citizen.33 The use of numbers entails the advantage of infinite combinations that each time can produce a unique result. However, the drawback that could reasonably be mentioned is that it is likely that individuals are transformed into numbers and lose their individuality.34

An illustrative example of identification by numbers is clearly reflected on the rationale of identity cards, which are based on the uniqueness of different numerical combinations. In most countries each person within the first days of origin reportedly was to show that one was not carrying a weapon). It also makes possible reciprocity, perhaps the most significant of social processes” and see also Jane Caplan, “Protocols of identification”, in Documenting individual identity, the development of state practices in the modern world, eds. Jane Caplan and John Torpey, 51 (Princeton University Press, 2001): “...by granting that identity is at the same time that which distinguishes an individual from others and that which assimilates him to others”.

29 Richard Jenkins, Social Identity, (London etc.: Routledge, 2008), 16.
30 Ibid., 13.
33 This is not far from the common practice that imposes that each book when published bears a unique number of identification, called ISBN (International Standard Book Number).
its birth has to register to his municipality’s archives, and above a certain age to be issued an identity card. This is justified if we keep in mind that when born, every human being becomes a member of society and registration to the state’s archives is an official way of confirming this membership.

Citizenship, however, is not a carefree status. It implies that citizens have not only rights, but obligations as well. Knowing who you are seems like promising that you would be responsible for your actions and/or omissions that might harm others in a democratic society. Accountability is the exchange for the benefits and rights citizens enjoy, such as pension and education. For instance, in literature the need for identification of absent fathers with children supported by welfare is repeatedly emphasised. Consequently, being granted an ID card means that you gain official proof of your existence as a citizen and equal member of society, whatever duality this comes with.

To conclude, I agree with Wright and others that it should not mean that identification and its methods should be unchurched. Governments by definition have power and are by nature controllers. For, they find ways to identify, monitor, track and watch citizens. Anyhow, power exists in every expression of life and it is a matter of difference in strength. Even in the microcosm of a family, parents exercise power upon their children. Their strength lays on the difference of age, experience and money, all meaning greater independence. What we should care about, however, is not the power per se, but its potential usurpation that could lead to the violation of autonomy, freedom and other civil liberties. Abuse may also lead to the use of very intrusive ways of identification, especially now that high-tech technologies promise efficient identification methods, using the human body as an identifier.

But, when exactly did official identification start? And why do modern states need to identify their citizens? What was the role that the development of the nation-state played in the identification of citizens and foreigners? These questions I try to answer in the next chapter which is essential in order to acquire a deeper understanding of the issue I address hereby.

35 Article 24 of the United Nations International Covenant on Civil and Political Rights (1966) states: “Every child shall be registered immediately after birth and shall have a name”. See also: Hannah Arendt, The human condition, (Chicago: University of Chicago Press, 1958): “Without such registration the newborn may fail to gain recognition as a being with rights on the world and endowed with the power of creation which is the vital essence of human existence”, quoted in Documenting individual identity, the development of state practices in the modern world, eds. Jane Caplan and John Torpey, 6 (Princeton University Press, 2001).
3. A brief historical review of official identification methods

Going back to history, various modes of unofficial identification have always existed. A telling example is the name of the ancient Greek philosopher Aristotle, who is still known as Aristotle of Stagira, meaning Aristotle who originates from Stagira. In the previous example the geographical place of origin was used as an identifier for persons. Another illuminating example is the use of nicknames as informal methods of identification.

Such identification methods, although mostly oral, informal and primitive, were sufficient to cover the needs of small societies, which were organised on a face-to-face basis. In this elementary, from an administrative point of view, societal organisation, daily activities were organised in the microcosm of a family or later of a city. An illustrative example is the evolution of the ancient Greek polis; Plutarch describes in his work, how at the beginning Attica was divided by families. Then no cities existed and each family lived independently as a closed group. In the course of the centuries the numerous little groups grew together into fewer and larger associations, until finally they became united into one city. The polis was an association of families, phratries, and a tribe and was born when several tribes associated together. This example indicates the tendency of primitive societies to magnify and eventually end up to the large nation-states we are acquainted of. A similar contemporary example is the federal state of Germany or the European Union itself with the vision to become in the long term a large state with its own Constitution, but which will be consisting of several smaller regions.

According to Valentin Groebner, "...the centuries between 1400 and 1600 stand for what we describe as the origin of the modern state system. In the cities and territories of Italy and Central and Western Europe, the growth of

---

40 Diogenes Laertius Lives of eminent philosophers, trans. in English R.D Hicks, (M.A., Harvard University Press, 1972), 20. See also the Greek text: «Ἀριστοτέλης Σταγειρίτης».
43 Greek historian who lived between 46-127 A.C.
47 Ibid., 499.
50 Andreas G. Dimitropoulos, General Constitutional Theory, (Athens, Komotini: Sakkoulas, 2004), 154-156.
51 Groebner, Documenting Individual identity, 15.
administration...extended the reach of the authorities over individuals, both native subjects and foreign visitors.” Official ways of identification were then used. For instance, couriers were obliged to carry special insignia (badges) on their purse and clothing.\textsuperscript{52} Later on in the Middle Age a kind of passport was granted to merchants, diplomats and couriers.\textsuperscript{53} However, the identification of each single citizen appeared only after the French Revolution in 1789, when—although still within a constitutional monarchy landscape—the legislative body of France adopted a decree regulating citizens’ civil status.\textsuperscript{54}

The enlargement of territorial size did not come alone, though. The new states had borders, national unity, bureaucratic and administrative organisation and executive powers.\textsuperscript{55} Moreover, in the course of the last decades we are witnessing an increase in mobility because of the internationalisation of transactions and of the technological development that made movement and travel beyond the borders of national states easier. As a result, the desire of the states to identify not only their citizens, but also foreigners who cross their borders in an accurate way grew respectively.\textsuperscript{56} Governments have claimed a host of different reasons to introduce identification methods. British identity cards and National Registration, for instance, introduced to fight against bigamy,\textsuperscript{57} or for fair distribution of food,\textsuperscript{58} were mainly “an instrument of war”\textsuperscript{59} serving the purpose to identify and recruit soldiers\textsuperscript{60} during the First and Second War World.\textsuperscript{61}

According to Amitai Etzioni identity cards are “domestic passport like documents that citizens have to bear and that provide identity data about the bearer...such as name and age”.\textsuperscript{62} They are official documents, issued by the state, intermediate between the person and the result of identification and have probative value of the identity of the owner. Nonetheless, in recent years real identity cards and papers remind more of medieval times. We once talked about paper-based identity cards or the password of a safe. Now we refer to

\textsuperscript{52} Groebner, Documenting Individual identity, 18.
\textsuperscript{54} Noiriel, The identification of the citizen, 28: “the legislative authority will establish for all inhabitants, without distinction, the manner in which births, marriages, and deaths will be certified; and it will designate the public officials who will receive and maintain these files” (Tit. II, art. 7 of the Constitution of 3 September 1791) and ibid., 39-40: “in order for the new republican citizenship to become effective, totally uniform procedures of identification had to be put in place throughout the entire country.” See also: David Dunkerley, Changing Europe: Identities, nations and citizens (London, New York: Routledge, 2002), 25.
\textsuperscript{55} David Dunkerley et al., Changing Europe: Identities, nations and citizens (London, New York: Routledge, 2002), 27 and 129.
\textsuperscript{58} Ibid.
\textsuperscript{59} Ibid., 119.
\textsuperscript{60} Ibid., 108.
\textsuperscript{61} Ibid., 107-108: “it was a means of facilitating call-up for compulsory service.”
\textsuperscript{62} Amitai Etzioni, The limits of privacy, 103.
magnetic or electronic cards, electronic archives, biometrics and cyborgs\textsuperscript{63}, as our life became more computer-dependent.\textsuperscript{64} The digitisation of information and the expansion of computer systems changed the above described landscape. Everything now is processed electronically and personal data have not evaded such a radical change.

4. The real identity card in Greece

In Greece the first identity card was introduced in 1936. The fact that a statute was first adopted during the dictatorship of Ioannis Metaxas is not without reason, although his national identity cards scheme was not completed because of the outbreak of World War II. During the dictatorship they were intended to be used for the identification of dissidents, mostly communists.\textsuperscript{66} Before that period, only certain groups of citizens were obliged to bear identity cards, among which the army officers in 1911 in order to get reduced tickets for transportation\textsuperscript{67} and policemen in 1931.\textsuperscript{68}

Later on, Law no. 85/1945 provided that both migrants and foreigners, residents of Greece were obliged to carry identity cards.\textsuperscript{69} Besides, it introduced the mandatory indication on the card of religious beliefs. However,\textsuperscript{67} For instance, Neil Harbisson was allowed to include his eyeborg photo in his passport by the British authorities.
\textsuperscript{64} Lyon, Under my skin, 298.
\textsuperscript{65} Source of the picture: \url{http://www.libertoad.com/2010/04/27/your-papers-please/}.
\textsuperscript{66} It was a period of four years of constant watching, torture and censorship.
\textsuperscript{68} Royal Decree of 26.2.1911, see also: ibid.
\textsuperscript{69} Greek Government Gazette (FEK) 9/A/12.01.1945 “concerning the obligatory provision of identity cards”.
Law no. 2472/1997 for the implementation of Directive 95/46 changed the pre-existent settings. The collection, documentation and recording of data-in the case of identity cards-come under law 2472/1997 on “the protection of the individual from the processing of personal data”. Religious beliefs were no more written on the identity card because article 8 of Law no. 2472/1997 considers them to be sensitive personal data.

In 2008 a new social insurance number (AMKA) was introduced. Article 153 of law 3655/2008 reads that “AMKA is imposed as a mandatory number of identification for the working and insurance identification of every single citizen of the country. No one will be able to occupy either as employee or as self-employed, to get insurance or deposit insurance contributions, to issue or renew his insurance booklet, to be entitled to earn pensions and generally provisions of any kind, allowances and aid.”

Greek citizens are obliged to carry their identity card all the time with them and show it when a police officer or any other public authority asks them to do so. Besides, movement and travel is simplified. It is now permitted to travel within the Schengen Area without any passport, on condition that you are an owner of an identity card that contains also data in Latin letters.

In September 2010 the Minister of Interior Affairs, Decentralisation and Electronic Governance announced the provision of a new e-ID card, called tax-card which has to be implemented until the end of 2011. The tax-card will be at first optional and will constitute a tool against tax-evasion. Later, its function will be incorporated in an e-ID card which will be mandatory for all citizens and will replace the paper-based ID cards.\textsuperscript{70}

\textbf{Conclusion}

In this chapter, it was shown that the formation of modern states came together with the power to identify citizens, both indigenous and foreigners. In the course of the time, the state power augmented due to technological developments that led to more intense identification capacities. Once writing was the only way to communicate with each other.\textsuperscript{71} Nowadays, modern citizens come across with new identification methods, which become invisible and more intrusive.

After the above etymological, philosophical and historical outline, it is these new types of technologies used by modern states for the identification of citizens that I will contend with in the next chapter.

\textsuperscript{70} For more details see Chapter 6 hereby.
\textsuperscript{71} Noiriel, \textit{The identification of the citizen}, 39-40.
CHAPTER 2
USE OF NEW TECHNOLOGIES FOR IDENTIFICATION PURPOSES

RFID, biometrics, and PKI and e-signatures\(^\text{72}\) are technologies that will be discussed in this chapter as the most important technologies used for identification purposes. My main aims here are to explain how they function, and underline their special characteristics with regards to identification of citizens.

2.1. New technologies

2.1.1. RFID Technologies and current applications

RFID technologies are the evolution of the Identification Friend or Foe (IFF) transponder, used for aircraft identification during World War II.\(^\text{73}\) Frequency tags are electronic circuits in the size of a speck of dust or as small as a grain of sand.\(^\text{74}\) They are affixed to or embedded in objects for the purpose of identifying them via a radio link.\(^\text{75}\) There are two different types of frequency tags, namely the passive and active\(^\text{76}\) ones. The former do not emit any signals except from when they are passed through or close to a device called tag-reader. On the contrary, the latter make use of a battery which enables them to emit signals received by a reader. Frequency tags, whether passive or active, also contain an antenna\(^\text{77}\) which emits data in the form of radio waves.\(^\text{78}\) The reader, which is also equipped with an antenna and a demodulator, translates the waves into digital data, which are then suitable for being processed by a computer.\(^\text{79}\)


\(^\text{73}\) The James A. Baker III Institute for Public Policy, Rice University, “Innovation by policy: a study of the electronic passport”, 33.

\(^\text{74}\) [http://www.spychips.com/]. In February 2010, researchers from Sunchon National University in Suncheon, South Korea and Rice University in Houston managed to build —using nanotubes— a radio frequency identification tag that can be printed directly on the package of products. Thus, the current debate is about the miniaturization of RFID tags, as with the help of nanotechnology it will be feasible to design and manufacture in the future invisible tags that operate on the nano-scale.


\(^\text{76}\) Ibid.


\(^\text{79}\) Ibid., 3.
But how does identification take place? In effect, the tag delivers a unique code similar to a key that unlocks information stored in databases, maintained by trusted parties within the system. The data stored on the tag are checked and if matched with the data stored in the database, identification occurs. This process takes place in a wireless way as frequency tags can be read remotely, without getting into physical touch with the reader. The higher the frequency of the tag, the longer the distance from which the tag is possible to be read. That is why identity cards with frequency tags incorporated on them are usually called contactless identity cards.

---

81 van’t Hof, Outcome of the project “RFID and Identity Management” commissioned by STOA, 15.
82 Ibid., 15.
83 Commission of the European Communities, Recommendation of 12.05.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, 2.
84 Meints and Gasson, “High-Tech ID and emerging technologies”, 150.
However, RFID technologies should not be confused with the Universal Product Code (UPC) or in common parlance bar code technology. One major difference between the two types of technology lays on accuracy and efficiency. To be precise, different bar codes cannot be read simultaneously by optical bar code readers. In contrast, RFID readers can read data on more than one object simultaneously. Moreover, RFID technologies offer the alternative not only to read the data stored on them, but also to change, update or erase them.

Interestingly, the European Commission in its Recommendation of 12.05.2009 highlights the fact that RFID technologies gradually become more common as they are used in almost every part of citizens’ daily life. In particular, retailers use them as identification methods for products in the supply chain management. Besides, RFID is used for tracking luggage in long-distance air flights. Furthermore, in some regions of Greece, there is a payment system known as e-pass for the collection of public road tolls. Without e-pass, drivers most times have to wait in long queues, which is not at all convenient when they want to go to work or are in a hurry. Finally, another application of RFID is OV-chipkaart that is used in the Netherlands for granting access to public transport.

2.1.2. Biometrics

Biometrics enables the automated recognition of individuals based on their unique biological and/or behavioral characteristics, such as the eye iris and the fingerprint. Thus, recognition is based on something a person is. This is a direct way of identification. On the contrary, indirect identification occurs with regards to something one knows or remembers, such as a password or a Personal Identification Number. I consider biometrics to be much more intrusive than other ways of identification, because parts of one’s body are used as identifiers for the same person that possesses these body parts. In the case at hand, there is nothing to intermediate between the person and its

---

86 van’t Hof, *Outcome of the project “RFID and Identity Management”*, 15.
90 van’t Hof, *Outcome of the project “RFID and Identity Management”*, 35.
91 Etymologically the word has its roots in the Greek words “bios+ metrikos” which means “life+ measure” mentioned in The future of identity in the information society (FIDIS), Deliverable 3.2, *A study on PKI and Biometrics*, 62, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.2_study_on_PKI_and_biometrics.pdf. See also picture 4.
94 Ibid., 60.
95 Henceforth PIN.
identification. The same body is at the same time both the identifier and the identifiable entity. However, in the case of e-ID cards, identification takes place through something someone carries,\(^96\) and therefore the card is an indirect means of identification. Most times e-ID cards combine various factors of verification\(^97\) and enable identification through something someone knows, such as a PIN, or is, such as a biometric trait, or carries such as a token.\(^98\) Biometrics incorporated in e-ID cards still constitutes an indirect means of identification.

![Biometrics](image)

**P.4. - categories of biometrics\(^99\)**

The function of a biometric system is quite simple as a rationale. It is based on a measurement process,\(^100\) where certain unique physical characteristics\(^101\) of a person are collected \textit{a priori}.\(^102\) This is what is called the “enrollment stage”.\(^103\) The person that has to be identified has to scan the relevant body part that functions as a “sample” through a reader. Special software compares automatically the body part presented in front of the scanner with the stored information, or otherwise called “reference template”.\(^104\) Only if the submitted information- that of course is susceptible to changes- matches with the “reference template”- that is fixed and unchangeable- is the person identified to be the one that he claims to be.

### 2.1.3. PKI and E-Signatures

\(^{96}\) FIDIS, Deliverable 3.2, A study on PKI and Biometrics.

\(^{97}\) The term is borrowed by The future of identity in the information society (FIDIS), Deliverable 3.2, A study on PKI and Biometrics, 60, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.2.study_on_PKI_and_biometrics.pdf where it is stated that “there are three concepts to establish a link between a physical person and its digital identity: something the person knows...,something the person carries..., and something the person is.”

\(^{98}\) FIDIS, Deliverable 3.2, A study on PKI and Biometrics, 60.


\(^{100}\) Meints and Gasson, “High-Tech ID and emerging technologies”, 140.

\(^{101}\) These characteristics are also called biometric data, see: Working Party 29, Working Document on Biometrics, WP 80, 1 August 2003, 4.

\(^{102}\) Ibid., 4.

\(^{103}\) Meints and Gasson, “High-Tech ID and emerging technologies, 139.

\(^{104}\) Ibid., 139.
Encryption is based on the secrecy of the cryptographic keys that a specific cryptographic algorithm makes use of. There are two kinds of keys, the symmetric and asymmetric ones. We talk about a symmetric key when both communicating parties know exactly the same secret key which is used for both encryption and decryption. In the case of asymmetric keys, though, each party has a unique secret, private decryption key and a publicly known encryption key.

Public-key cryptography makes use of a pair of keys. The distribution of those keys is made through a trustworthy private certification authority, by means of digital signatures. A packet of information is encrypted with the public key and can be decrypted only if one knows the relative private key. Thus, the recipient of the information is certain that he is eligible to open the message because he possesses the relative private key. However, he is not sure whether the sender is the real author of the message.

For, e-signatures create a unique link between the signed data and the signatory. They ascertain the integrity and authenticity of data processed in or transmitted through a system. Technically, e-signatures are the counterparts of asymmetric keys. They ensure that the document signed is derived by the signatory that signs it, and its content is genuine and not altered.

In conclusion, the use of electronic signatures is harmonised among the EU member states with the Directive 1999/93/EC on a Community framework for e-signatures. The Directive imposes a technology neutral approach in order to facilitate the function of the Internal Market. However, it will not be part of my study.

2.2. New technologies and e-ID cards

The abovementioned technologies are not used solely in the private sector. Lately, the current debate rambles around the public sector more and more intensively. Illustrative examples are the e-passport and the e-ID card which tend to replace paper-based documents in more and more states. For

---

105 Kerckhoff’s principle, mentioned in Meints and Gasson, “High-Tech ID and emerging technologies”, 133-134.
107 Ibid., 134.
108 FIDIS, Deliverable 3.2, A study on PKI and Biometrics, 16.
110 FIDIS, Deliverable 3.2, A study on PKI and Biometrics, 16.
111 Ibid., 16.
112 Ibid., 16.
113 Meints and Gasson, “High-Tech ID and emerging technologies”, 137.
114 FIDIS, Deliverable 3.2, A study on PKI and Biometrics, 17.
115 Meints and Gasson, “High-Tech ID and emerging technologies”, 137.
instance, according to “FIDIS”, countries such as Belgium and Austria implement PKI in their national ID card schemes.\textsuperscript{116}

In particular, e-ID cards make use of RFID technology for communication purposes. The data stored in the card are scanned through the reader and compared with those stored in a database. The card and the reader, both equipped with an antenna, communicate with each other from a distance with the help of radio frequency waves. Moreover, biometric data is stored in the card and serves as a sample that once presented before the reader is compared -again with the help of radio waves- with the “reference template”. It is impossible that one “forgets” a part of his body, that is “tightly bound” to him.\textsuperscript{117} As human memory is of limited capacities, biometrics is a more accurate and effective method of identification than passwords or PINs that are easily forgotten.\textsuperscript{118} Finally, PKI and e-signatures are used in e-ID cards for authentication purposes.

From a legal standpoint, it is worth wondering whether the Directive 95/46/EC\textsuperscript{119} applies in the case of RFID and biometrics.\textsuperscript{120} First of all, article 2 (a) of the Directive states that “personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. Moreover, Recital 26 adds 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”. Finally, article 3 (1) of the Directive reads that the scope of the Directive contains “processing of personal data wholly or partly by automatic means, and ... processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system”.

Consequently, the Directive applies to the use of biometrics because the latter “by their nature” provide information about an individual and differentiate it from others.\textsuperscript{121} An exception, however, is mentioned under article 3 (2, second indent) of the Directive and includes the case where biometric data are used “by a natural person in the course of a purely personal or household activity”.\textsuperscript{122} Likewise, we cannot answer this question in the affirmative with

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{116} FIDIS, Deliverable 3.2, \textit{A study on PKI and Biometrics}, 18.
\item\textsuperscript{117} ibid., 61.
\item\textsuperscript{118} ibid., 61.
\item\textsuperscript{119} Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
\item\textsuperscript{121} Working Party 29, \textit{Working Document on biometrics}, WP 80, 1 August 2003, 5.
\item\textsuperscript{122} See also: Working Party 29, \textit{Working Document on biometrics}, WP 80, 5.
\end{itemize}
\end{footnotesize}
regards to RFID. It follows that only when the personal data collected by RFID relate to an identified or identifiable person does the Directive apply. Suffice it to say that e-ID cards, where personal data are stored and processed by RFID technology, and are linked to identifiable individuals, fall within the ambit of the Directive.

Conclusion

In this chapter, I focused on the possible technologies that can incarnate the use of e-ID cards. It was shown that e-ID cards that make use of RFID and biometrics fall under Directive 95/46. Moreover, it was indicated that they combine aspects that an individual is, has, and knows or remembers. There is great accumulation of personal data required by new technologies that make identification of citizens more intrusive. This, in combination with the functioning of e-ID cards from a distance, the creation of invisible databases and the use of a human body as an identifier have been described in literature as devastating from a privacy and data protection perspective. However, the potential benefits that spring from the use of the above mentioned technologies in modern identification methods should not be ignored and thus, are analysed at length in the next chapter.

CHAPTER 3
THE POTENTIAL BENEFITS OF E-ID CARDS

The European Commission in its “Digital Agenda for Europe” stresses the effectiveness of e-government, and points out that it can offer better and cost-effective services, enhancing transparency and openness in public administration. However, in 2009 only 38% of EU citizens used e-government services, compared with the 72% of businesses. Therefore, the EU has taken various initiatives in order to make e-government popular among EU citizens.

In the following chapter, I examine the potential benefits of the use of e-ID cards and I focus on e-government and electronic public services. First, I explain what e-government is and what malfunctions it could cure. Second, I analyse the potential benefit from the enhancement of democracy, focusing

---

123 Article 2 (a) of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
124 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, “A Digital Agenda for Europe”, (Brussels, 19.05.2010), 32.
125 Ibid., 32.
on e-democracy, e-participation and e-voting and analysing the case of the Austrian “Bürgerkarte” and e-voting in Estonia. Third, I explain why e-ID cards are e-government enablers. And finally, I describe various e-government initiatives taken by the OECD, the EU, and the state of Greece.

3.1 “Understanding e-Government”

Trying to understand what e-government stands for might prove an intricate task. A view shared by many scholars is that e-government incorporates government to government, government to business, and government to citizens relations. Nevertheless, there is no convergence with regards to a unique definition of e-government. I lean towards the definition given by Silcock, mainly because it is clear and comprehensive. According to Silcock, “E-Government is the use of technology to enhance the access to and delivery of government services to benefit citizens, business and employees.”

Silcock further suggests that “by applying the same principles and technologies that are fuelling the e-business revolution, public services can achieve a similar transformation.” Indeed, EU citizens have a multitude of properties with regards to their relations to the government, such as voters, tax payers, and consumers. However, Silcock’s claim seems to me partially true. Public services offered on a 24-hour per day basis on-line are one of the attractive principles that made e-commerce successful. On the contrary, as Rivest points out, the security mechanisms that are to be found within e-commerce transactions would not be effective to cover the security needs of e-voting. The receipt provided after an e-commerce transaction can be used for dispute resolution, whereas e-voters should not be identified in

128 The title is inspired by the title of the book: Vincent Homburg, Understanding e-government: information systems in public administration. (London and New York: Routledge, 2008). Moreover, in Kjaer, Anne Mette, Governance (Cambridge etc.: Polity, 2004), 3 the authors point out that the word “government” etymologically has its roots to the Greek verb “κυβερνώ” that means to “pilot or steer”. E-government means the delivery of services, but e-democracy is about representation and participation (Neil Collins and Patrick Butler, “When marketing models clash with democracy”, Journal of Public Affairs, Vol. 3, No. 1 (November 2002: 54)).
131 Ibid., S 180.
133 Ibid. 
134 Ibid.
respect with what they voted, as this would have detrimental effects on their privacy.\textsuperscript{138} Moreover, by applying the e-commerce paradigm\textsuperscript{139} on public administration would mean the “equation of customers and citizens”.\textsuperscript{140} As a result, citizens would be deprived from their power that originates from their being the state themselves,\textsuperscript{141} with negative effects on democracy.

Generally speaking, public sector is connected with long waits and cumbersome procedures.\textsuperscript{142} Moreover, the work that should be done by the employees is transferred upon the citizens. For instance, interaction between public authorities is missing and citizens bear the burden to communicate with each authority in order to receive a service.\textsuperscript{143} Surprisingly, despite the fast-moving environment of contemporary society,\textsuperscript{144} in which citizens live and interact, public administration seems to be incongruous.\textsuperscript{145} Furthermore, without a universal identifier as the e-ID card, it happens that citizens have to give multiple times to different public institutions the same information.\textsuperscript{146} Hence, public sector needs to be transformed as “the shift from the industrial to the information society implies new expectations for citizens.”\textsuperscript{147}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{red_tape_bureaucracy.jpg}
\caption{Red tape, bureaucracy.\textsuperscript{148}}
\end{figure}

\begin{itemize}
\item \textsuperscript{138} Rivest, “Electronic Voting Laboratory for Computer Science”.
\item \textsuperscript{139} Bernd Carsten Stahl, “The Ethical Problem of Framing e-Government in Terms of e-Commerce”, 80.
\item \textsuperscript{140} Ibid., 82.
\item \textsuperscript{141} Ibid., 83.
\item \textsuperscript{142} Silcock, \textit{What is e-government}, 1.
\item \textsuperscript{143} Ibid.
\item \textsuperscript{144} Ibid.
\item \textsuperscript{146} Beynon-Davies, “Personal Identification in the information age: the case of the national identity card in the UK”, 8, available at: \url{http://cs.cse.ac.uk/asp/aspecis/2005004.pdf}.
\item \textsuperscript{148} Source of the picture: \url{http://jimunro.blogspot.com/2010/09/cutting-red-tape-lengthwise.html}.
\end{itemize}
3.2. Enhancement of democracy: e-participation and e-voting

What is directly linked with e-government is the stimulation of democracy.149 “Democracy means rule by the people”.150 Nowadays, this ruling has the form of a “representational model of democracy”.151 Especially within the liberal political systems of today’s world dimensions of direct democracy, such as the referendum,152 are weakened.153 Because of the complexity and peculiarities of modern life, especially lack of time, citizens are represented in the Parliament, participating indirectly in a restricted type of democracy.154 Consequently, they are almost excluded from decision making.155

There are two main direct participatory activities a citizen can officially be engaged with, in a mixed type of democracy,156 as the one of Greece. On the one hand, the referendum is the process through which people of a country decide upon a critical national issue conducting elections.157 However, there is the claim that participation of citizens in the political life and democracy itself can be enhanced even more by promoting e-democracy.158 “Use of IT in democratic processes”159 consists of initiatives as on line political debates,160 referenda, petitions, and consultations,161 in order to formulate the future political agenda, before decisions are taken. For instance, the Greek Minister of Internal Affairs, Decentralisation and E-Governance carried out a public consultation in November 2010162 in order to give Greek citizens the opportunity to demonstrate their view with regards to the introduction of the e-ID card and the relevant legislative draft. Nevertheless, I am in favour of an official participation of citizens in the decision-making process, the outcome of

---

151 Ibid.
152 Dimitropoulos, General Constitutional Theory, 433.
153 For instance, in Greece the process of referendum sleeps since 1974, when the last one took place, although there have been significant national issues to decide upon.
154 Dimitropoulos, General Constitutional Theory, 435.
155 On the contrary, the ancient Athenian democracy was a genuine form of direct democracy, where people decided for themselves and there was no distinction between governors and governed. See: Dimitropoulos, General Constitutional Theory, 433-438.
156 Mixed type of democracy is a type of representative democracy that also combines some direct democracy aspects. See: Dimitropoulos, General Constitutional Theory, 434.
157 Article 44, paragraph 2 of the Greek Constitution.
160 Homburg, Understanding e-government, 30: “In direct democracy wired up citizens will be able to engage directly in a spectrum of activities, such as electronic debates”.
162 http://www.opengov.gr/ypes/?e=863.
which would be binding for the government. In this formal participation the e-ID card could play a significant role for authentication purposes.

On the other hand, voting in elections gives citizens the opportunity to demonstrate their liking or disliking about political parties and decisions.\textsuperscript{163} Elections constitute a direct way of ruling, as people choose from whom they want to be governed. However, there will always be some parts of population to refrain from their voting rights, such as citizens who did not transfer their voting rights to the municipality they live in, or are too old to go to the polling station, or have special needs, such as the blind and handicapped or disabled.\textsuperscript{164}

The main benefit of e-government lato sensu\textsuperscript{165} is that it offers flexible and “customised” ways of delivering public services and participating in democratic processes\textsuperscript{166} on a “virtual agora”.\textsuperscript{167} This is essential in the modern era and could have a direct impact on the decision-making process. Nevertheless, there is an opinion in literature that democracy is impoverished because of the use of ICTs, as citizens lose control over governance.\textsuperscript{168} Sunstein argues that instead of plurality of information, it is possible that there will be a few opinions expressed with which people will agree or disagree,\textsuperscript{169} leading to what Kelly and others call “echo chambers”.\textsuperscript{170} Of course, this would be a negative development, but in my opinion the number of Internet users is also decisive for the success or failure of e-democracy. E-democracy needs more than virtual platforms and voting polls; a general policy for the increase of ICT users in a country, and educational schemes so that people become acquainted with new technologies.

To conclude, in the process of decision-making and delivery of public services secure identification and authentication of citizens is crucial.\textsuperscript{171} In order to be sure that a public service reaches the rightful person, or that each voter votes only once, citizens have to prove that they are the ones they claim to be.\textsuperscript{172} The examination of the Austrian “Bürgerkarte” and e-voting in Estonia, under the next section, will help to understand how this happens in practice.

### 3.3 The e-ID card as an e-government catalyst


\textsuperscript{165} In this section I use the term lato sensu so that e-government contains both e-government in stricto sensu and e-democracy.

\textsuperscript{166} See: Bernd Carsten Stahl, “The Ethical Problem of Framing e-Government in Terms of e-Commerce”.

\textsuperscript{167} Ismael Pena Lopez, “The disempowering gyverati: e-aristocrats or the delusion of e-democracy”, 1.

\textsuperscript{168} See: Ibid., 10 and Bernd Carsten Stahl, “The Ethical Problem of Framing e-Government in Terms of e-Commerce”.


\textsuperscript{170} Kelly and others, Debate, Division, and Diversity: Political Discourse Networks, 1.

\textsuperscript{171} See: Rachel Silcock, What is government?

\textsuperscript{172} Beynon-Davies, Personal Identification in the information age: the case of the national identity card in the UK.
3.3.1. The Austrian “Bürgerkarte”

Austria is one of the first EU countries to implement a national e-ID card scheme.\(^{173}\) The Austrian “Bürgerkarte” is vital for rendering e-government services.\(^{174}\) However, this is not a physical card, but a “virtual concept” that can be established optionally in a host of different carrier devices.\(^{175}\) For instance, an ATM card,\(^ {176}\) except from functioning for the purposes for which it was initially issued, it offers the additional option for a citizen card functioning, at any time.\(^ {177}\) As the “Bürgerkarte” is technology-neutral, it can be issued by both private and public entities.\(^ {178}\) It is mainly used for verifying the identity of the user and authenticating the validity of his request, as well as encrypting and signing documents.\(^ {179}\)

I will now briefly explain how the Austrian “Citizen Card” system works. In Austria the Central Register of Residents is mandatory and stores information of all residents, both native and foreigners.\(^ {180}\) Every citizen is granted a unique source PIN\(^ {181}\) that is secret and controlled only by the citizen who owns it.\(^ {182}\) The s-PIN is derived from a 12-digit identification number,\(^ {183}\) which is stored in the Register. Moreover, a unique alphanumeric code corresponds to every public administration sector.\(^ {184}\) When the citizen wants to use his card, this code is combined with the s-PIN, and each time a different and random\(^ {185}\) sector-specific PIN\(^ {186}\) is produced, giving access to a public service.\(^ {187}\)

From a privacy and data protection perspective one could say that the 12-digit identification number enables the linking of personal data to a specific natural person. However, this is not true, because the individual is not


\(^{174}\) Ibid., 69.

\(^{175}\) Ibid., 71-72.


\(^{180}\) Ibid., 69.

\(^{181}\) Henceforth “s-PIN”.


\(^{186}\) Henceforth “ss-PIN”.

\(^{187}\) Ibid.
identified when accessing e-government services. Privacy is safeguarded because first, any storage of the s-PIN by either public or private entities is forbidden by law. Second, the s-PIN is under the absolute control of the citizen and used only to produce the ss-PINs. Third, ss-PINs enable authentication of citizens and are produced through an “irreversible cryptographic function”, so that their elements such as the s-PIN are impossible to be calculated by working back. Besides, it is not possible to calculate any other ss-PIN if one knows another ss-PIN. And finally, law permits the storage of ss-PINs only within the sector to which each of them corresponds. Moreover, it is remarkable that the Austrian card does not use RFID technologies or biometrics.

P.6.1.- The use of ss-PINs in the Austrian system of “Bürgerkarte”

---

191 Ibid.
192 Ibid.
196 Ibid., 79.
3.3.2. E-voting in Estonia

E-voting was introduced in Estonia in 2005, and has been used for both national and European Parliament elections. Maaten points out that one of the principles of e-voting- which is also relevant to my analysis- is the use of e-ID cards for citizens’ identification purposes. E-ID cards are equipped with a chip that contains electronic data, certificates and private keys protected with PIN-codes. Their function is similar to banking cards and provides citizens with a technological component which is essential to grant access to the e-government infrastructure of the country. According to Sibul, head of the National Electoral Committee of Estonia, the e-ID card used

---

200 The other two principles are: 1) within the period of time allowed for e-voting, voters have the possibility to cast again their vote and then the previous vote should be deleted and 2) according to the principle of the priority of traditional voting, if a voter goes to the polling station and casts a vote, his e-vote should be deleted. See: Epp Maaten Elections Department Chancellery of the Riigikogu (Parliament), 85, available at http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding GI.47-9.pdf.
by Estonians in their everyday transactions with the government is a key tool for e-voting.\footnote{203}

However, in principle e-voting gave birth to great controversy among political parties. This conflict ended with the landmark ruling of the Estonian Supreme Court\footnote{204} that considered that e-voting did not violate the principle of secrecy and thus, was legal.\footnote{205} According to the official website of the Estonian National Electoral Committee in the parliamentary elections in 2007 30,000 voters chose to use their e-ID card to cast their vote.\footnote{206} This was the 5% of the all participants. In the parliamentary elections in 2011 there were 140,846 citizens who chose to vote electronically.\footnote{207} This was the 24% of the total number of participants.\footnote{208} Thus, there was significant rise of electors who vote electronically within a short period of time.

Yet, during the Parliament’s Science and Technology Options Assessment board\footnote{209} hearing hold on the pros and cons of e-voting on 17 March 2011, it was a common feeling that it is not clear whether e-voting will definitely increase participation of the electorate.\footnote{210} It is true that reliable empirical data is missing, mainly because e-voting is a relatively new process. However, I agree with the opinion of Professor Grimm\footnote{211} who argued that “With e-voting you can vote where ever you are, whenever you want - we don't have evidence but this must increase participation”.\footnote{212}

### 3.4. E-government initiatives by the OECD

The OECD has suggested various ways in which governments can best exploit ICTs.\footnote{213} With its e-Government Project, launched in 2001, OECD aims to promote e-government policies by reporting best practices and developing frameworks for addressing various issues.\footnote{214} Subsequently, countries members of OECD adopted a new approach and tried to make their government more customer-oriented.\footnote{215} Reformation and re-invention of

---

public administration would mean that government had to take a more “entrepreneurial position in society”.  

3.5. E-government initiatives by the EU

3.5.1. The Digital Agenda

In a bid to make electronic applications more popular among EU citizens, the European Commission launched its “Europe 2020 Strategy” in March 2010. One of the seven flagships that were set out is the Digital Agenda. Its aim is “to deliver sustainable economic and social benefits from a digital single market based on fast internet and interoperable applications.” Among the problems that are underlined by the Commission is the lack of interoperability, of a single market and a rise in cybercrime, to name but a few. As a response to these problems, European governments should take action and make “user-centric, personalised, multi-platform e-government services a widespread reality by 2015”. These public services should be working across borders in order to facilitate the mobility of citizens. Moreover the Digital Agenda highlighted that e-ID technologies are essential for the security of transactions on the Internet, both in private and public sector.

3.5.2. E-health and social security

The European Commission in its Digital Agenda also stresses the interest in e-health technologies and launched in March 2011 the “e-health Action Plan 2012-2020”. The Plan provides that “the deployment of eHealth technologies in Europe can improve the quality of care, reduce medical costs and foster independent living, including remote places.” Taking also into account the fact that EU citizens increasingly travel within the borders of the Union, they should be able to have access to health services in every member state they travel to. Moreover, all citizens who temporarily visit another member state can apply for the provision of the European Health Insurance Card that can be used for treatment in case of emergency.

216 Kettl, The global public management revolution: a report on the transformation of governance. However, see the counter arguments that are mentioned under 3.1. hereby.
218 Ibid.
219 Ibid.
222 http://ec.europa.eu/information_society/activities/health/policy/index_en.htm for more information see:
3.6. E-government initiatives by Greece

The “Digital Greece2020”\(^ {225}\) website seeks to get feedback and insight for the formulation of a project that will implement the “EU Digital Agenda 2020”. The most current implementation of the Digital Agenda followed by the Greek government is the so-called “Digital Strategy” (2006-2013). Moreover, the Greek government also launched a website under the name “National Portal of Public Administration”.\(^ {226}\) A multitude of services are provided such as the provision of birth certificates, application of consumers’ complaints, and provision of certificate of marital status, and so on. However, physical presence of citizens in front of the Citizens Service Centers is required for the reception of the certificate.\(^ {227}\)

In 2010 the e-government transactions in Greece were only 29.5% of the total transactions, although there was an increase of 4% comparing with previous years.\(^ {228}\) An encouraging finding, however, is that in the same year 88, 8% of the Greek citizens had broadband connection.\(^ {229}\) Moreover, it is shown that e-democracy initiatives are lacking and there is a focus on the provision of electronic public services.

Conclusion

Concluding, in this chapter it was shown that e-ID card schemes are vital for e-government and e-democracy. E-ID cards are deemed a tool that will completely change the “anachronistic paper-based administrative law.”\(^ {230}\) Furthermore, citizens will be disengaged from the inefficient and time-consuming public administration, and transparency will be increased. Moreover, it follows that e-government in Greece needs improvement. E-ID cards can give flesh and bones to the Greek citizens’ full enjoyment of the potential benefits of e-government by the end of 2011. Interestingly, the case of the Austrian “Bürgerkarte” and e-voting in Estonia further indicated that e-ID schemes can be implemented in ways that are more effective and less intrusive for privacy and personal data protection.


\(^{227}\) Iglezakis, “The development of e-government & the issue of digital inclusion in Greece with particular regard to the constitutional right of e-participation”, 11.


CHAPTER 4

POTENTIAL RISKS OF THE USE OF E-ID CARDS

In this chapter I provide an overview and comment on arguments discussed in literature about the risks derived by the use of high-tech ID cards, in the light of privacy and personal data protection. First, I make a reference to the surveillance society. I start by referring to the basic meanings of privacy and point out the evolution of the right to personal data protection. Then, I explain how ID cards can be used as tools of surveillance and discrimination, by answering the following questions: what surveillance is and how identification can become identical to surveillance, why the latter can be harmful, and what risks e-ID cards and the technologies of which they make use entail. Finally, I give an explicit picture of the e-ID card scheme in the UK and indicate the reasons of its cancellation in 2010.  

4.1. The surveillance society

4.1.1. Privacy and data protection

---

Defining privacy is a difficult task and its meaning has changed in the course of the time. Louis and Brandeis in their article “The right to privacy” defined it as the “right to be let alone”. Bloustein considered privacy to be a protection of “individual’s independence, dignity and integrity”. Moreover, in the Preamble of the Australian Privacy Charter we read that “a free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy”. Furthermore, privacy means the right of people to establish relationships to others. Thus, privacy has no single meaning, but incorporates various notions, constituting “a cluster of” or “an umbrella term that refers to” many distinct yet related things. Interestingly, the European Court of Human Rights has interpreted broadly article 8 of the European Convention on Human Rights.

In the course of the time, technological breakthroughs created a new landscape, where privacy could no more protect against new challenges and risks. For instance, in the past privacy was related to intimacy and private sphere, as people wanted to shield their household activities; nowadays, we are witnessing a public character of privacy and personal data. As processing of personal information became more intense, a personal data protection regime was deemed necessary.

---

238 The Greek Constitution in article 5 emphasises the right of citizens to develop freely their personality and to participate in the social, economic and political life of the country, insofar as they do not infringe upon the rights of others or violate the Constitution and moral values.
240 See Paul de Hert and Serge Gutwirth, “Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action”, in Reinventing data protection?, eds. Serge Gutwirth, Yves Poulet Paul de Hert, Sjaak Nouwt & Cecile de Terwagne, 3-44 (Dordrecht: Springer Science, 2009), and European Convention of Human Rights, article 8: “Everyone has the right to respect for his private and family life, his home and his correspondence.” See also ECtHR case Peck v. the United Kingdom, Application no. 44647/98, Judgement of 28 January 2003, §§57-63.
242 See the Convention of the Council of Europe of 1981 (108) for the protection of individuals with regard to automatic processing of personal data, the OECD Guidelines 1980 governing the protection of privacy and transborder data flows of personal data and article 8 of the Charter of fundamental rights of the European Union (2001-2007).
4.1.2. ID cards as tools of surveillance and discrimination

Citizenship has always been a status that distinguishes between “us and them”. For instance, in ancient Greece slaves and women were excluded from the “political community”. Later, the emergence of the nation-state gave birth to the desire of governments to identify their citizens, excluding foreigners from benefits. Identification is considered to be the starting point of surveillance. Clarke argues that the computerisation of government administration was the root of what he calls the “dataveillance” era. Besides, Lyon argues that although ID cards are the tool of identification, what really matters is the intangible component of ID card system, the database. The latter is a searchable networked collection of data with vast surveillance power.

In the light of the above mentioned, the first questions that rise are what surveillance is and how identifying citizens might lead to surveillance. According to Lyon, surveillance is “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered”. Lyon explains that surveillance is perceived “as soon as we are made aware that massive population registries are required to make an ID card system function and that this involves networked, searchable databases”. This is in my opinion true in the case of e-ID cards because such schemes contain personal data of the population of...

---

244 Pink Floyd, http://www.youtube.com/watch?v=rs_Yayz5o-10.
245 Dunkerley et al., Changing Europe: Identities, nations and citizen, 10-11.
246 See also: C. Tilly, Coercion, Capital, and European States (Oxford: Blackwell, 1992), AD 990-1992 quoted in Dunkerley et al., 27.
247 Lyon, Identifying Citizens, 4.
248 Ibid., 50 and see: http://www.rogerclarke.com/DV/.
249 Lyon, Identifying Citizens, 7.
250 Ibid., 4.
251 Lyon, Surveillace Society: monitoring everyday life, 2.
252 Lyon, Identifying Citizens, 11-12.
an entire country ("massive") which are stored in "networked, searchable databases".\footnote{253}

The second question is why surveillance in modern world might be harmful for individuals. Solove argues that constant surveillance causes a variety of negative feelings such as discomfort and stress.\footnote{254} He explains that when citizens know that all their actions are monitored, they abstain from not only illegal activities, but also lawful ones that might be somewhat embarrassing or sensitive.\footnote{255} This change of behaviour springs from over-deterrence and proactive prevention of crimes, where the principle of Criminal Law \textit{in dubio pro reo} is violated, and everyone is guilty unless found innocent.\footnote{256} Thus, according to Solove, too much social control might hinder "freedom, creativity, and self-development,"\footnote{257} with adverse consequences on the functioning of democracy.

Moreover, independent decision-making might be violated.\footnote{258} Profiling is the automated production of new knowledge about individuals or group of persons.\footnote{259} Profiling can be used in various ways, positively by enabling the "effective distribution of information"\footnote{260} or negatively by depriving individuals of their right to decide about themselves.\footnote{261} In our case hereby, the Greek tax card although at first optional, might prove a useful tool for insurance companies and private organisations. Once citizens use it, all their transactions with both the public and private sector will be stored in the card, enabling consumer profiling based on daily habits and needs. Insurance companies, for instance, have great interest in collecting and processing personal data in order to conduct risk analysis.\footnote{262} Consequently, they might refuse to give "home insurance to persons living in burglary prone streets".\footnote{263} This example shows that profiling enabled by smart cards in general lead to the making of powerful decisions for citizens,\footnote{264} often without human controls.
intervention, and influencing their life, and excluding them from services or discriminating by price. Citizens should be let unfettered to decide for themselves and need no paternalistic companies to determine their life. Thus, profiling can end to a kind of social sorting which is produced because “electronic environment automates processes of selection, inclusion and exclusion”.

Besides, autonomy of users might be weakened because of what Zarsky calls the “autonomy trap”. Profilers classify their potential clients in specific groups “with well-defined characteristics”. These profiles will be up-dated in real time every time the subject makes a transaction enabling real-time monitoring. Consequently, users can be manipulated as according to Zarsky profiling is invisible to them who do not know that the others know. Manipulation can be reality for instance with targeted advertisements based on the profile group to which the person belongs to. Profiling gives valuable knowledge not only about what happened in the past, but what behaviour should we anticipate in the future. Again, e-ID cards enable this process leading potentially to refined discrimination and social sorting.

Finally, the last question to answer is what role e-ID cards play in the surveillance process. Historically, ID cards have been used for unfair and dehumanising practices. For instance, in South Africa, pass laws restricted the mobility and the life-chances of black Africans. It was a kind of racial distinction based on identity cards. Furthermore, Torpey observes that internal passports were also used in Stalinist Russia, regulating the movement of citizens. Additionally, Longman explains how ID cards were the means that led to genocide. During the Belgian colony in Rwanda the tribe of Tutsis was

---

266 Hildebrandt, “Who is profiling who? Invisible Visibility”, 244.
268 Lyon, Surveillance Society: monitoring everyday life, 47.
271 Ibid., 239-243.
274 Lyon, Surveillance Society: monitoring everyday life, 83.
275 See also Hildebrandt, “Who is profiling who? Invisible Visibility”, in Reinventing data protection?, 244.
276 Lyon, Identifying, 25.
privileged because of their physical similarities to Europeans. In the 1930s the colonial administration issued ID cards that everyone was obliged to carry at all times. As a result, later in the 1990s ID cards were used as a tool of discrimination against the Tutsis and determined “who would live and who would die”. Finally, in the 1930s Nazi Germany based the persecution of undesirable Jewish populations on registrations.

However, one of the main differences between surveillance in real-life and in cyber-world is that in the last case surveillance is less perceptible because it is invisible. An online example is profiling of users and consumers when engaged with online activities or transactions. Profiling enabled by smart cards is a process that takes place “under the surface”. Thus, even the protection offered by article 15 of Directive 95/46 against decisions taken solely on automated processing of personal data is ineffective, because people have no way to know whether they are profiled or not in order to seek protection.

One could say that surveillance when secret does not threaten any civil liberties. Solove however, argues that in this case surveillance is deceptive and when a person is uncertain of whether surveillance takes place or not, invisible surveillance “can be just as inhibitory as actual surveillance”. I agree with Solove at this point, but I would like to add that perhaps secret surveillance might be worse than visible one. In the latter case, individuals are aware of it and have a choice between either to afford it or prevent it by adopting specific measures. For instance, if I notice that someone peeps from my window into my house, I can draw the curtains or tell him to leave. However, in the latter case, individuals have no choice but to live with the curtains drawn for a whole life, sacrificing their freedom and waiving privacy.

New technologies, mainly RFID implemented in e-ID cards, facilitate surveillance, because RFID tags are connected with one or more databases

278 Lyon, Identifying, 29.
279 Ibid., 30.
280 Ibid.
284 Lyon, Identifying, 43.
286 Solove, Understanding Privacy, 109.
287 At this point Solove agrees with Benn that “covert observation...deliberately deceives a person about his world”, see: Daniel J. Solove, Understanding Privacy, (Cambridge, London: Harvard University Press, 2008), 109.
288 Solove, Understanding Privacy, 109.
that is/are “searchable on a large scale and remotely”\textsuperscript{289} and “talk with each other”,\textsuperscript{290} and enables e-ID cards to function automatically.\textsuperscript{291} Moreover, computerisation of records in combination with “universal coverage”\textsuperscript{292} within the population of a country leads to the “social sorting”\textsuperscript{293} of citizens, reserving different treatment for different groups.\textsuperscript{294} Besides, the chip used in e-ID cards has great storage capacity and this means that a significant amount of data is gathered.\textsuperscript{295} Thus, aggregated data are combined and matched within various administrative entities\textsuperscript{296} very quickly and easily, by automated means for the classification of individuals.\textsuperscript{297} According to Solove, such processing where information is detached from its context might lead to misrepresentations.\textsuperscript{298} For instance, data mining is a technique used by the U.S. government in order to combine data from various databases with each other and create new information about an individual.\textsuperscript{299} The same technique can also be used by public entities that collect and process personal data for administrative purposes,\textsuperscript{300} with the help of e-ID cards.

Additionally, it often happens that technologies are “re-purposed” and are later on used for different purposes than initially.\textsuperscript{301} This phenomenon is called “function creep” and is against article 6 (b) of the Directive that reads that personal data should be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”\textsuperscript{302} Another fear is that making the e-ID card mandatory might violate the right of the data subject to “unambiguously”\textsuperscript{303} give its consent for any processing of its personal data. In the past, when e-ID cards were not used, surveillance could take place only for the parts of population that voluntarily made use of new technologies. By making the use of e-ID cards mandatory the data subject has no choice and this right is violated.

\textsuperscript{289} Lyon, Identifying, 41 and 47.
\textsuperscript{290} Wright et al., “Privacy, trust and policy-making: Challenges and responses”, 71.
\textsuperscript{291} Lyon, Identifying, 45.
\textsuperscript{292} See William G. Staples, Everyday Surveillance: Vigilance and Visibility in Postmodern Life, (Lanham, MD: Rowan and Littlefield.
\textsuperscript{293} Lyon, Identifying, 39-62.
\textsuperscript{294} Ibid., 41.
\textsuperscript{295} Ibid., 56.
\textsuperscript{296} Lyon in his book Lyon, Identifying Citizens, 44, for instance, mentions that the Italian e-ID card helps the sharing of data among the Ministry of Interior, the Italian Central Agency for Data Exchange, private providers such as Banks and telecom operators, databases of all relevant public services, health systems, the Italian population registration centre and the taxation code department.
\textsuperscript{297} Lyon, Identifying, 41.
\textsuperscript{298} Solove, Understanding Privacy, 121.
\textsuperscript{299} Solove, Understanding Privacy, 191-197. Actually, data mining analyses “personal information for patterns of suspicious behaviour”.
\textsuperscript{300} Lyon, Surveillance Society: monitoring everyday life, 31.
\textsuperscript{301} Wright et al., “Privacy, trust and policy-making: Challenges and responses”, 71.
\textsuperscript{302} Article 6 (a) of Directive 95/46.
\textsuperscript{303} Article 7 (a) of Directive 95/46/EC.
Biometric data is also incorporated in e-ID cards, especially the fingerprint and the eye iris which are considered to be the most accurate of all.\textsuperscript{304} It is not a new way of identification\textsuperscript{305} and is continuously gaining land worldwide,\textsuperscript{306} especially after 9/11 events.\textsuperscript{307} It is deemed to offer unique and accurate identification.\textsuperscript{308} However, “the tolerance range within which all matches must be made”\textsuperscript{309} might cause inconvenience, which is “false positives and false negatives”.\textsuperscript{310} Lyon explains further that every biometric system incorporates a decision threshold according to which the decision of matching is taken within a “continuum from low to high security”.\textsuperscript{311} Thus, when there is great tolerance there will be more “false positives”\textsuperscript{312} and vice-versa when there is strict tolerance, there will be more “false negatives”.\textsuperscript{313} Consequently, in the case of “false negatives” citizens are unfairly excluded from authentication and subsequently authorisation.

Additionally, there are some groups of people that are classified as “hard to enroll”.\textsuperscript{314} This happens when the sample is not sufficiently distinctive.\textsuperscript{315} For instance, the hands of people who work at hard labour cannot be sufficiently captured.\textsuperscript{316} Or people, who do not have a body part because they are handicapped or blind, are automatically classified as “hard to enroll”.\textsuperscript{317} The further implication of such a failure to enroll\textsuperscript{318} might mean complete exclusion from e-government services and other citizenship benefits.\textsuperscript{319} An illustrative example of exclusion is the case of a Los Angeles teacher, who cannot find a job because he suffers from “atopic dermatitis”\textsuperscript{320} that makes it impossible for him to be identified by his fingerprint or hand geometry.

\textsuperscript{304} “Retinal scan is restricted because of the high costs”. Moreover, voiceprints are not accurate as voice might change because of a cold and faces change significantly during a day: Lyon, \textit{Surveillance Society: monitoring everyday life}, 84.\textsuperscript{305} For instance, the fingerprint always existed in police archives and was also depicted on the old Greek ID card document. We now use digital biometric photos that are stored in databases and can be checked from a distance. See also: Lyon, \textit{Identifying Citizens}, 111. Moreover in the past, the face was measured and manually designed, a method known in France as “Bertillonage” or anthropometry: see: Martine Kaluszynski, “Republican Identity: Bertillonage as Government Technique”, in \textit{Documenting individual identity, the development of state practices in the modern world}, eds. Jane Caplan and John Torpey, 123(Princeton University Press, 2001).\textsuperscript{306} See Irma van der Ploeg, \textit{The machine readable body}, (Maastricht: Shaker, 2005).\textsuperscript{307} See Vincent Mosco, \textit{The digital Sublime: Myth, Power and Cyberspace}, (Cambridge, MA: MIT Press, 2004) quoted in Lyon, \textit{Identifying Citizens}, 118-119.\textsuperscript{308} Lyon, \textit{Identifying Citizens}, 53. See also Chapter 2 hereby.\textsuperscript{309} Ibid., 115.\textsuperscript{310} Ibid., 116.\textsuperscript{311} Lyon, \textit{Identifying Citizens}, 116.\textsuperscript{312} Ibid.\textsuperscript{313} Ibid.\textsuperscript{314} Ibid., 122.\textsuperscript{315} http://www.iwar.org.uk/comsec/resources/biometrics-aviation-security/05-19-2004-hearing.htm accessed 23/04/2011.\textsuperscript{316} http://www.iwar.org.uk/comsec/resources/biometrics-aviation-security/05-19-2004-hearing.htm.\textsuperscript{317} Lyon, \textit{Identifying Citizens}, 122.\textsuperscript{318} Henceforth FTE.\textsuperscript{319} Lyon, \textit{Identifying Citizens}, 120-122 and van der Hof and Prins, “Personalisation and its influence on identities, behaviour and social values”, 121.\textsuperscript{320} Atopic dermatitis is a skin disease that makes skin blister and peel. See: Lyon, \textit{Surveillance Society: monitoring everyday life}, 84.
Moreover, discrimination is a salient drawback when it occurs. According to Nanavati et al, only “certain ethnic and democratic populations are more prone to high FTE rates than others...Users of Pacific Rim/ Asian descent may have faint fingerprint ridges- especially female users.” Thus, as Pugliese adds, “this failure to enroll is neither random nor arbitrary....making whiteness the yardstick for access” and discriminating against certain groups using almost hostile criteria. In addition to this, fingerprints and the eye iris contain medical information that can reveal the potential to develop in the future certain diseases. Thus, as “none of us has perfect genes”, a risk of discrimination and racism is omnipresent. For instance, a citizen might be denied a job position or health insurance because of his medical record.

4.2. The e-ID card scheme in the UK

Lyon, Surveillance Society: monitoring everyday life, 84.
As Agar observes, there have been various efforts to issue identity cards for the British “in order to combat perceived threats to social order,” and mainly for recruitment of soldiers for the army as it happened in 1939. However, they were never permanent and have been highly contested among the public. When World War II was over in 1945 disagreement with regards to ID cards augmented. Interestingly, in February 1952 British ID cards ended after the Willock v. Muckle decision. Both the Middlesex magistrates and the Court of Appeal rejected Willock’s claims, but granted him an “absolute discharge.”

Willock refused to show his ID card to a policeman, on the grounds that the ID card was a war tool and thus, the police request was beyond the purpose of law. However, in 2006 the Identity Cards Act was passed in order to fight against benefit fraud under the name “Entitlement Cards.” The Act also provided for the establishment of a central National Identity Register that would contain personal information such as names and gender, and facilitate their linking to other databases. According to Sullivan, the intention of the Act was to make in the long term ID cards obligatory documents, for verification purposes in both the public and private sector. Again, the core component of the scheme would not be the e-ID card itself, but the NIR database, where significant personal data of citizens would be stored. However, in December 2010 the British ID cards scheme was cancelled and all ID cards issued were destroyed as they were deemed privacy intrusive and expensive.

Privacy problems occurred when Laurie managed to clone the electronic circuit of the newly introduced ID cards in the UK. According to Laurie, the

---

327 Ibid., 106-111.
330 Lord Goddard pointed out that “To demand registration cards of all and sundry- from a lady leaving her car outside a shop longer than she should for instance- is wholly unreasonable... We have always prided ourselves on the good feeling between the police and public, but this tends to make people resent the acts of police, to obstruct instead of assist them.”, quoted in Agar, Modern Horrors: British Identity and Identity Cards, 106-111.
331 Agar, Modern Horrors: British Identity and Identity Cards, 110-111.
332 Lyon, Identifying Citizens, 35.
335 Henceforth NIR.
337 Sullivan, “The United Kingdom Identity Cards Act 2006-Civil or Criminal?”, 322.
338 Ibid., 323.
new ID cards use the same technology as e-passports, namely the International Civil Aviation Organization standard, called Basic Access Control. Besides, he disagrees with the argument of manufacturers that RFID cards are like common keys and that if you lose them, everyone can copy them. On the contrary, he argues that because RFID tags are embedded in ID cards they can be copied “simply by standing next to the person who has” them “in his pocket” and by scanning remotely with a special device the RFID tag.

Additionally, Fedtke compares the UK regime with the German one. He concludes that British see ID cards like a “threat posed by an authoritarian and centralized Germany”. He describes how in 1977, when new technologies were at their infancy and not widely used, German Police managed by intelligently selecting and combining knowledge to identify criminals. Fedtke remarkably explains that now with the extremely developed sophisticated technologies, “a central database with the potential of the envisaged NIR would far exceed the surveillance and law enforcement capacity”. Even not dangerous citizens will be zealously scrutinized and profiled by security authorities, and that might lead to over deterrence.

Conclusion

In this chapter I presented the risks involved with the use of e-ID cards. I showed that in the past official identification discriminated among citizens and turned against human beings and even human life. History has proven that identification schemes based on new technologies are not “immune from the temptations of control or privilege”. Consequently, it is important that people know that historical errors such as mass murder, mobility restriction or even genocide will not be repeated. New technologies have the potential capacity to discriminate and violate citizens’ privacy more intensively than

---

341 Henceforth ICAO.
345 According to Laurie such devices are easy to make using materials that are circulated in the market, see: Laurie, Practical attacks against RFID, 5.
346 Ibid., 5.
348 Ibid., 171.
349 Ibid., 169-172.
350 Ibid., 171.
351 Ibid., 171-172.
352 Lyon, Identifying Citizens, 27.
353 Ibid., 20.
practices in the past.\textsuperscript{354} I also indicated that the e-ID card is a tool that enables identification and authorisation, but the real risks are to be found “under the surface”,\textsuperscript{355} where the processes of profiling and discrimination take place with adverse consequences on privacy and personal data protection. Interestingly, the fact that the scheme was cancelled in the UK, in combination with the fact that e-ID cards are easy to clone, should provide food for second thoughts about how secure the identification scheme will be in Greece.

CHAPTER 5

COMPARING THE PASSPORT WITH THE ID-CARD

An identification document akin to e-ID cards is the e-passport. It is also issued by the state, but has different functions, and aims at controlling the movement of citizens beyond their national borders. In this chapter, my main intention is to compare the e-ID card with the e-passport. The examination of the e-passport, first implemented in EU in 2004, may have some more insights to offer than the e-ID card. National e-ID schemes took place without “supra-national European co-ordination, leading to divergent implementations with regards to privacy issues, but also other elements.”\textsuperscript{356} On the contrary, there is an EU policy for e-passports which will be discussed hereby. First, I start with the general background and functions of e-passports. Second, I analyse the EU policy regarding the biometric passport, and I refer to the legal context, the technical characteristics and the privacy related issues. Finally, I highlight the differences and similarities between the two official documents.

5.1. Historical background

Fahrmeir explains that identification documents appeared as “evidence to back up”\textsuperscript{357} citizens’ claims with regards to who they are. In Middle Age identity was created in Europe by large profession organisations such as

\textsuperscript{354} Lyon, Identifying Citizens, 61.

\textsuperscript{355} Ibid., 43.


guilds which provided with passes mainly artisans.\(^{358}\) The first passports were first issued in 1792 in France. They were obligatory for all travelers and mostly politically-driven as they were to fight against “the assembly of discontented persons at strategic locations” and in general against crime.\(^{359}\)

During the 19\(^{th}\) century- as Marrus\(^{360}\) observes- movement of citizens beyond the borders of their national state did not meet any serious impediments.\(^{361}\) The developing trade and exchange made suspiciousness fade.\(^{362}\) However, Lucassen is cautious with this statement because of some exceptions that restricted the movement of certain groups at that time.\(^{363}\) Such groups were “highly mobile occupational groups”\(^{364}\) such as factory workers in Germany or itinerant craftsmen. In 1914, when World War I broke out, and especially in Germany, passport restrictions were imposed for both the nationals and the foreigners\(^{365}\) in order to “keep the soldiery fresh with recruits”.\(^{366}\) However, even after the War, passports were not abolished, but continued to exist for border controlling and “marking out” nationals and non-nationals.\(^{367}\)

5.2. The e-passport in the EU

5.2.1. Legal Context

E-passports within the EU were introduced by the Council Regulation No. 2252/2004\(^{368}\) of 13 December 2004, on standards for security features and biometrics in passports and travel documents issued by Member States. This Regulation does not apply to e-ID cards.\(^{369}\) Two further decisions of the Commission established the technical specifications on the above mentioned

---


\(^{360}\) Canadian historian (1941-).


\(^{364}\) Ibid., 252.


\(^{367}\) Ibid., 269-270.


\(^{369}\) Ibid., 50.
standards. On the one hand, C 409 of 28 February 2005 has to do with the incorporation of facial image on a secure chip embedded on the passport. On the other hand, C 2909 of 28 June 2006 refers to the protection of biometrics against possible misuse and also provides for the incorporation of fingerprints on the passport. At this point, it is worth mentioning that these regulations, originate from the so-called “Visa Waiver Program” that permit 36 nationals from 36 countries, among which is Greece, to travel to the USA for tourism or business for maximum 90 days, without obtaining a visa. According to VWP all its members should have adopted e-passports “with biometric chips” by October 2006.

5.2.2. Technical Characteristics

E-passports use the same technology that is described in Chapter 2 for e-ID cards. They are a combination of RFID and biometrics with the paper-based passport, having as a core component a “contactless chip”. Vakalis calls e-passports “the digital extension of the classic paper passport”. The data are divided into three categories, named Data Groups. Except from the basic biographical data, such as the name and age, it was decided at an EU level that second generation e-passports would also contain a facial image and a fingerprint template. In effect, European citizens have no discretion to choose between the inclusion or not of biometrics, because these are compulsorily incorporated in all new passports.

From a European Commission standpoint the e-passport is considered to be difficult to forge or duplicate as the electronic circuit enhances security and reliability of identification. Nonetheless, Vakalis is vigilant with regards to such large scale biometric applications, because they will “bring the
contemporary citizen into” an unfamiliar regime the effects of which are hard
to predict due to the newness of this technology. This point of view is
correct because unpredictability increases the probability of privacy breaches
to occur.

The European Commission underlines the interoperability of passport
systems. Travelers should face no functional impediments when they travel
all over the world and their passport should be compatible with every
reader. Such interoperability can be achieved if all border- checking
authorities agreed upon a common standard, which would enable checking
systems worldwide to “talk to each other”. E-passports are in compliance
with the ICAO- Document 9303.

5.2.3. Security and privacy risks

Since June 2009 EU member states issue second generation biometric
passports that include the facial image and the fingerprint of the owner following the Extended Access Control Protocol. The latter is deemed safer
than the Basic Access Control Protocol that was implemented for the first
generation passports. The EU EAC standard is implemented in all the
members of the “Schengen Area”, in order to protect sensitive data such as
the fingerprint and other biometrics more effectively. Vakalis however,
warns that an ideal situation would be that all data whether biographic or
biometric should be included in the much safer EAC.

Furthermore, Vakalis explains that in order to avoid confusion when more
than one passports are presented close to a reader, there is a 32-bit
number. This number is random, but the first two digits comprise of “08” in
order to be distinguished from other signals. However, this might raise
privacy concerns as it is transmitted that the specific chip belongs to a

385 Vakalis, Privacy and Biometric Passports, 483.
387 Ibid.
388 Ibid.
389 Ibid.
390 Ibid.
391 See also: http://www.consilium.europa.eu/prado/en/glosarypopup.html and ICAO, Machine Readable Travel Documents:
http://www2.icao.int/en/mrtd/Pages/default.aspx and FIDIS, Study on ID Documents, 13.
392 Henceforth EAC.
393 Henceforth BAC.
394 Ibid and Vakalis, Privacy and Biometric Passports, 486.
395 Ibid., 486.
396 Ibid.
397 Ibid., 485.
398 Ibid.
passport and thus, the latter “can be targeted for unauthorized reading”.399 Monitoring in this case is feasible.400

Besides, the holders of the passport should be informed in advance about what data their passport would contain and for what purposes they will be used. For instance, if the passport will be also used for e-commerce, there is a higher risk of function creep.401 This is not a science fiction scenario as the ICAO standard already mentions the potential use of e-passports for e-commerce applications.402 In such a case, the risks of function creep are higher because there will be “data spillover” across various systems.403 Digital data are easier to share, increasing privacy risks.404 For instance, Juels and others mention the illustrative example of cookies that were at first used for boosting the computer memory.405 Now, they are used by private companies in order to track and trace back individuals, and their on line preferences.406

Finally, the same risks derived from the use of RFID and Biometrics analysed in chapter 4 also apply to e-passports.

5.3. Differences and similarities between the two documents

It is important to have in mind that initially internal passports led to the evolution of the passports.407 The two documents differed from each other with regards to their implementation scale.408 The internal passport was national, regulating movement “within the jurisdiction of the state”409, whereas the “external passport”410 is supranational and part of a common policy among EU member states.411 The identity card is a “‘mixed’ type”412 and is to be found somewhere in the middle of the other two.413 This means to me, that ID cards are used for different purposes than e-passports, but in respect of the implementation scale they resemble to internal passports.

399 Vakalis, Privacy and Biometric Passports, 486.
400 Ibid., 487.
402 Ibid., 12.
403 Ibid.
404 Ibid.
405 Ibid. 12-13.
406 Ibid., 12.
408 Ibid., 158-165.
409 Ibid., 158.
410 Ibid.
411 Ibid.
412 Ibid.
413 Ibid.
In the course of the time, sophisticated technology gave a thrust to new identification methods. Generally, it is accepted that e-passports were the “harbinger of a wave of next generation ID cards”. Current debates ramble around RFID and Biometrics for domestic use in the form of ID cards. More and more governments have recently introduced legislation and e-ID card schemes. According to Raddlewimmer e-passports are part of a general security infrastructure. Thus, e-id cards and e-passports belong at large to the same security policy. However, interoperability is an e-passport characteristic because e-passports obey to the ICAO standard (document 9303), whereas e-ID cards schemes do not provide for a common standard.

With regards to ID cards they grant their owners citizenship which also encompasses the EU citizenship. The latter does not replace national citizenship, but complements it. Every citizen of a member state is at the same time citizen of the Union. Thus, the former enjoys more rights and has more obligations. For instance, EU citizens have the right to vote and stand as candidates at European Elections. All in all, ID cards define the relation between the citizen and the state mostly for administrative purposes.

Moreover, EU residents and visitors can travel within the “Schengen Area” without systematic passport checking. The Schengen Agreement, now integrated in the EU Treaties, gives the citizens of the Union the right to move freely without any border checking within the frontiers of the Union and live and work in any member state. The aim is to create a European identity among European citizens and eventually achieve political integration. Nonetheless, a significant question rises at this point: why do EU citizens need identification documents if they are rarely checked and enjoy the right of free movement? And subsequently, why disproportionate and proactive identification measures should be adopted?

On the contrary, passports are mainly used for border controls and enable national states to retain control of their territorial sovereignty. E-passports

---

415 Ibid., 1.
419 Ibid.
420 Ibid.
422 Ibid.
423 Ibid.
424 Ibid.
425 Ibid.
426 The James A Baker III Institute for public police, Rice University, 10.
determine “who is in and who is out.” In similar vein e-ID cards determine who is eligible or not to claim benefits. In some cases, both documents might constitute a “presumption of their bearer’s guild” undermining the trust that should exist between citizens and the state.

Conclusion

Both the e-ID card and the e-passport use the same technologies that have raised privacy concerns analysed in Chapter 4. However, these documents, although sharing some common features, are distinct identification documents. They both are a sign of what Torpey calls “monopolisation of the legitimate means of movement by modern states”. Identification documents might turn citizens into prisoners of identification, as they are absolutely dependent on their nation with regards to their cross-border movement. Thus, on the one hand, e-ID cards can facilitate travelling within the “Schengen Area”, but on the other hand might place impediments in citizens’ right of unhindered movement.

CHAPTER 6
THE E-ID CARD IN GREECE

In this last chapter I examine the legal regime for the introduction of e-ID cards in Greece. First, I present the relevant provisions found in the Greek Constitution. Second, I analyse Law no. 2472/97 for the implementation of Directive 95/46 in the Greek legal system. Third, I briefly refer to the case of e-ID cards among police-officers. Afterward, I describe the tax-card and make comments on its functioning. Then, I expose the opinion of the HDPA on the new tax-card and finally, I make some suggestions on how to strike the right balance between the benefits of e-ID cards and the risks for privacy and personal data protection.

427 Torpey, Surveillance, Citizenship and the state, 158.
428 Ibid., 158.
429 Ibid., 166.
430 Ibid.
431 Ibid., 158.
432 Ibid., 166.
433 Ibid., 159-167.
434 Torpey, The invention of the passport, 159-167.
6.1. The Greek Constitution

Article 9 of the Greek Constitution reads that “Every person’s home is sanctuary. Personal and family life of the individual is inviolable. No house search shall be made except when as specified by law and always in the presence of representatives of the judicial power.” The second paragraph of the same article reads that “Violators of the preceding provision shall be punished for violating the sanctuary of the home and for abuse of power, and shall be liable to full damages of the sufferer, as specified by law. This article was first introduced in the Greek Constitution with the amendment in 1975.

Later, the amendment of 2001 provided with the protection of personal data and led to a new individual right. Article 9A reads that “Every person has the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is assured by an independent authority, which is established and operates as specified by law.”

6.2 Law no. 2472/97\textsuperscript{435} for the implementation of Directive 95/46 EC

First of all, Law no. 2472/97 is applicable to e-ID cards because according to article 3 §1 the law applies to “the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system”.

In order that the processing of personal data is lawful, they need to have certain characteristics according to article 4. They should be collected fairly and lawfully, for specific, explicit and legitimate purposes and fairly and lawfully processed in view of such purposes. Unfair use might be lawful, but beyond the pale.\textsuperscript{436} For instance, unfair use would be the creation of a new file from the database of a hospital in which patients would be classified according to the place of residence, and thus, their high or low income.\textsuperscript{437} Moreover, personal data need to be adequate, relevant and not excessive in relation to the purposes for which they are processed at any given time. Furthermore, they have to be accurate and, where necessary, kept up to date. Finally, they should be kept in a form which permits identification of data subjects for no longer than the period required, according to the Authority, for the purposes for which such data were collected or processed.

\textsuperscript{435} In this chapter when I write “the Law” I mean Law No. 2472/97.


\textsuperscript{437} See: ibid., 61.
Additionally, article 5 defines the conditions under which processing of personal data is lawful. In paragraph 1 it is stated that processing of personal data will be permitted only if the data subject has given his/her consent. Article 2 (k) defines that consent shall mean “any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognisant signifies his/her informed agreement to personal data relating to him being processed.” Furthermore, according to article 10 the data controller is responsible for the confidentiality of the processing of personal data, and taking adequate measures for the security of the data processed.

Articles 11-14 refer to the rights of the data subject. Precisely, article 11 is about the right of information; “the controller must, during the stage of collection of personal data, inform the data subject in an appropriate and express manner of at least the following data: a) his identity and the identity of his representative, if any, b) the purpose of data processing, c) the recipients or the categories of recipients of such data, d) the existence of a right to access”.

Furthermore, article 12 provides for the right to access. The data subject has the right to know whether data related to him are being processed or have been processed. For instance, a data subject can ask for information on all the personal data relating to him, as well as their source or the purposes of data processing.

Additionally, article 13 grants the data subject the right to object at any time against the processing of his personal data. For instance, the data subject can ask for deletion or correction of its personal data. Finally, article 14 provides for the right to provisional judicial protection of the data subject before the competent court, in the case of a decision taken by an administrative authority or public law entity or association or natural person, which is based solely on automated processing of data intended to evaluate his/her personality and especially his/her effectiveness at work, creditworthiness, reliability and general conduct.”

6.3. The Greek tax-card

According to article 1 of Law no. 3842/2010, Greek tax-payers have to submit to the tax-authorities at the end of the fiscal year, paper-based receipts for all their transactions. The authorities will then decide whether citizens are eligible to receive a tax-discount or not. The purpose of the tax-card is...
twofold. On the one hand, it will be more convenient for tax-payers to store the expenses of all their transactions in a single card, rather than collecting paper-based receipts. On the other hand, it will help tax-authorities to enforce Tax Law and strike down tax-evasion, as cross-checking of transactions will be more effective.

Precisely, the tax-card will be issued by private banks from which citizens can receive it free of charge. Each card will correspond to a 19-digit number. Citizens will have to register the card only to the General Secretary for Information Systems of the Ministry of Economic Affairs. In that way, according to the Ministry, there will be no possibility for third parties to identify the owner. After a transaction takes place the tax-card will be scanned through the Point Of Sales that is also used for credit cards. The bank will receive all the information, distinguish the tax-card transactions from the credit card ones, and then, send everyday to the system of the Ministry only the following data: the number of the card, the date of transaction, the total amount of money paid and the Tax Identification Number of the enterprise. The Ministry asserts that no consumer-profiling of the owner will take place as only the aforementioned data will be sent from the bank to the Ministry. After the fiscal year ends, the details of each transaction will be erased and only the final total amount of all the transactions will be retained for tax return purposes.

6.4. The Opinion 4/2010 of HDPA

The HDPA in its Opinion 4/2010 of 13.12.2010 thought differently than the Ministry, though. It considered that the tax-card has no basis on Law no. 3842/2010 against tax-evasion, because such processing, as described by the Ministry, is more intrusive than the collection of paper-based receipts. It is more intense as it concerns the involvement of third parties (private banks),

---

442 Opinion of 13-12-2010, 5.
443 Ibid., 3.
444 Ibid., 2.
446 Opinion of 13-12-2010, 4.
447 Henceforth POS.
448 Henceforth TIN.
449 Decision of the Ministry of Economic Affairs 1104/9-5-2011, article 2.5.
450 Ibid., 3.
451 Ibid., 4.
452 Opinion of 13-12-2010.
453 Ibid., 5.
the retention of data for long periods (during the whole fiscal year) and the function of a central database.\textsuperscript{454}

Moreover, the HDPA is not persuaded that there is no risk to track consumers’ preferences and it fears that consumer profiling will be possible. Banks lawfully process their clients’ data. Thus, they might be in the position to identify an individual by combining clients’ data with regards to the use of credit cards and data of the same clients in respect of their transactions with the tax-card.\textsuperscript{455} It should be reminded that all this data will be stored in the same central database of various financial institutions, and hence, identification will be possible.

Finally, the HDPA suggests that identification of citizens should occur only when it is necessary for the purposes for which they will be used.\textsuperscript{456} On the one hand, in order to determine the tax-discount, identification is necessary only at the end of the fiscal year.\textsuperscript{457} Moreover, for the same purpose the Authority proposes that the use of a smart card under the total control of citizens, which they will submit by themselves to the Ministry at the end of the year, would be an appropriate measure.\textsuperscript{458} On the other hand, in order to check that the Value Added Tax\textsuperscript{459} was paid, the real-time communication of data makes identification irrelevant.\textsuperscript{460} For this second purpose, the Authority recommends that there should be the infrastructure that would permit online communication of cash registers of enterprises with the system of the Ministry. This would be an alternative to cope with the issue of cross-checking, without any processing of personal data of tax-payers by private banks.\textsuperscript{461}

6.5. Suggestions in order to strike a balance between benefits and risks

Citizens who will use the citizen e-ID card should be explicitly informed about what data will be processed and for which purposes.\textsuperscript{462} This information would protect against function creep\textsuperscript{463} and data subjects could exercise effectively their right to object.\textsuperscript{464} For instance, Malogardi is against the
inclusion of biometrics in the e-ID cards.\textsuperscript{465} In my opinion, the collection of biometric data is against article 4 of Law 2472/1997. Processing of biometric data goes against the principle of proportionality as it is excessive in light of the purpose of granting access to e-government services, for which they are processed. For instance, the Austrian “Bürgerkarte” makes use neither of RFID nor of biometrics. Nevertheless, it effectively fulfills its administrative goals for the reduction of red tape. Thus, there are milder ways to achieve identification, without the need of biometrics. Furthermore, if these data are to be used for police investigation, it should be clearly stated beforehand.\textsuperscript{466} In essence, police can link different databases in order to conduct investigation for a serious crime committed, after the order of the Public Prosecutor. However, preventive searches should be prohibited, because this would mean that data are now processed for a different purpose than initially.\textsuperscript{467}

Especially in the case of the tax card citizens are not comprehensively informed about what data will be possessed by banks. A lot of questions remain unanswered. What kind of agreement will be signed between the banks and the state?\textsuperscript{468} Will there be an agreement for non-disclosure to third parties? Why the Ministry did not conform to the Opinion of the HDPA to implement the alternative solutions it suggested?

To partly answer these questions, in my opinion, private banks should have no role to play in the processing of personal data. An alternative solution would be to conform to the Opinion according to which the potential on-line transfer of transactions from the cash registry to the Ministry would make the involvement of banks unnecessary. Moreover, why should identification occur every day? I agree with the recommendation of the HDPA that identification is only necessary at the end of the fiscal year.\textsuperscript{469}

Additionally, the tax-card is an implementation that will include all the daily habits of citizens, from what they bought to where they have been and at what time. As far as this might lead to an abridgement of privacy, the tax-card has to be seen from the outset as one of the paraphernalia that have the potential to make “a digital one-on-one copy of the physical public space” that would be possible to be easily tracked and monitored.\textsuperscript{470} Private Banks, being the processors of personal data, will have at their hands a powerful tool for the profiling of the consuming habits of all Greek citizens. Thus, the e-ID card scheme should be expansively scrutinised from a privacy angle, before its implementation.

\textsuperscript{465} http://www.enet.gr/?i=news.el.article&id=215715.\textsuperscript{466} van’t Hof, \textit{Outcome of the project “RFID and Identity Management”}, 73.\textsuperscript{467} Gilliot et al., “Privacy and Identity”, 355.\textsuperscript{468} Decision of the Ministry of Economic Affairs 1104/9-5-2011 and Opinion of 13-12-2010, 7.\textsuperscript{469} Opinion of 13-12-2010, 8.\textsuperscript{470} van’t Hof, \textit{Outcome of the project “RFID and Identity Management”}, 63.
Another important issue that is also relevant to e-ID cards in general is to define who will be the controller of the processing. I agree with the HDPA Opinion\textsuperscript{471} that ideally data subjects should have total control of the data processed.\textsuperscript{472} In concise terms, private banks should not intermediate in this process; instead, at the end of the year, citizens could submit to the Ministry all their transactions stored in the card that should be totally controlled by them.\textsuperscript{473}

Furthermore, there should still be a choice and citizens should be given the right to choose whether they want to use the card or not. It is disproportional to demand a holistic application of new technologies that will regulate the relations between the state and the citizens.\textsuperscript{474} Thus, paper based ID cards which are supposed to be replaced by electronic ones should still be valid. Although paper-based ID-cards deprive citizens from convenience, users should have the chance to make conscious choices about the processing of their personal data.\textsuperscript{475}

Taking into account that RFID and biometrics are in their infancy\textsuperscript{476} and it is not proven that they constitute trustworthy technologies, the ideal situation would be that more research should be done in this field. We cannot make experiments with unreliable technologies that are easily attacked by hackers and thus, compromise privacy.\textsuperscript{477} For instance, we already saw that an RFID card can be scanned without the owner even noticing it.\textsuperscript{478} In the UK the ID cards scheme was cancelled recently as too costly and unreliable.\textsuperscript{479} It seems to me that this happened not only because British have a tradition of denying identity cards throughout their history as a nation,\textsuperscript{480} but also because the new ID card was proven to be practically vulnerable.\textsuperscript{481}

In addition, Privacy Enhancing Technologies\textsuperscript{482} can be developed through research and offer more reliable identification means.\textsuperscript{483} PETs can offer data minimalisation and less linkability with the data subject.\textsuperscript{484} However, e-

\textsuperscript{471} Opinion of 13-12-2010, 8.
\textsuperscript{472} Ibid.
\textsuperscript{473} Ibid.
\textsuperscript{474} Fedtke, “Identity Cards and Data Protection: Public security Interests and Individual Freedom in Times of Crisis”, 181.
\textsuperscript{475} Ibid.
\textsuperscript{476} van’t Hof, Outcome of the project “RFID and Identity Management”, 62.
\textsuperscript{477} Ibid., 64.
\textsuperscript{478} See Chapter 4.
\textsuperscript{479} Fedtke, “Identity Cards and Data Protection: Public security Interests and Individual Freedom in Times of Crisis”, 181.
\textsuperscript{480} Ibid.
\textsuperscript{482} Henceforth Pets.
\textsuperscript{483} Vakalis, Privacy and biometric passports, 479.
government applications require the disclosure of various personal data.\textsuperscript{485} For instance, tax payment systems work on identification of citizens.\textsuperscript{486} However, PETs cannot offer control for the processing of data that occurs invisibly and without the user being aware of it.\textsuperscript{487} Hence, it is essential that policy-makers and other stake-holders should engage with more privacy-friendly implementations. Precisely, the Greek government should take action in order to adopt privacy-friendly policies and “construct applications so that transaction records cannot be used as surveillance tools.”\textsuperscript{488}

As a final point, Fedtke offers a privacy-friendly solution that excludes central databases. He argues that such databases “alter the relationship between the state and the citizen”.\textsuperscript{489} On the contrary, he argues, different decentralised databases for local public authorities that will be accessible “where absolutely necessary will suffice for the achievement of an adequate level of security”. Only then risks for function creep\textsuperscript{490} would be limited. Fedtke admits that the tempered convenience is “the price to pay, for a less effective state if we want to maintain civil liberties and privacy”.\textsuperscript{491} In my opinion, we should not adopt extreme solutions. For instance, the “Bürgerkarte” of Austria would give insights on how to get the most from e-government by maintaining privacy in a citizen-centered environment.

Conclusion

In this chapter it was shown that the Greek government did not conform to all the recommendations of the HDPA regarding the tax-card scheme. Thus, the tax-card might still be considered a serious would-be infringer for privacy and personal data protection. Now, before it is too late and the e-ID card runs into a curse, more privacy-friendly solutions should be adopted. To this direction, technology can be a co-driver, but also examples of other countries, should be thoroughly and comparatively scrutinised.

\textsuperscript{485} Gilliot et al. “Privacy and Identity”, 351.
\textsuperscript{486} Ibid., 351.
\textsuperscript{487} Ibid.
\textsuperscript{489} Fedtke, “Identity Cards and Data Protection: Public security Interests and Individual Freedom in Times of Crisis”, 181.
\textsuperscript{490} Willcock vs’ Muckle, Lord Justice Goddard.
\textsuperscript{491} Fedtke, “Identity Cards and Data Protection: Public security Interests and Individual Freedom in Times of Crisis”, 181.
Conclusions

My aim hereby was not to undercut or militate against the efforts of the Greek government to reform public administration, diminish officialdom and fight contrary to tax-evasion. Instead, I orientated towards overriding the main prejudices of Greek society with regards to new technologies, and presenting the issue with an objective and multidisciplinary analysis, based on facts. The goal of my study was to find out what kind of balance would be desirable to strike in order that Greek society feels comfortable with the risks that e-ID cards entail from a privacy and personal data protection perspective, while at the same time it takes advantage of the benefits of e-government lato sensu.

In order to answer the above mentioned question, I made a historical, sociological and legal analysis. Moreover, a comparison between e-ID cards and the e-passport was deemed necessary. Besides, in the context of e-government, I examined the case of the Austrian “Bürgerkarte” and e-voting in Estonia. And finally, in view of potential risks, I analysed the case of the UK, explaining the main reasons of the cancellation of the ID cards scheme in 2011.

In this respect, I can say that the approach I adopted paid off and gave important insights insofar that first, an overall image of the issue is provided hereby, and second, I did not come across any other literature focused specifically on e-ID cards in Greece. The main reason is probably that the e-ID scheme is recently being implemented in Greece. Therefore, my study has the advantage to be one of the first to analyse the issue. However, my research came across obstacles many times. During the last five months that my research lasted the e-ID scheme was developing at a fast pace in Greece.

P.10.-The Greek tax-card
Thus, I had to be in touch with current developments, and every time make the appropriate changes to the main body of the study, the structure of which changed a lot of times during this time.

The findings of my research are manifold, some of which also unexpected. First, it was shown that the birth of the nation-state between 1400 and 1600, led to a subsequent growth of administration and bureaucracy.\(^{492}\) A landmark development of bureaucratic organisation of the nation-state was the decree adopted by the legislative body of France after the French Revolution, regulating citizens’ civil status.\(^{493}\) I consider this to be the hallmark of when identification of citizens was deemed necessary in order to make the administrative machinery work successfully. This was to be done with various identification methods. At first, paper and writing were the main means. The main concern of identification authorities was to achieve the greatest possible accuracy of identification. Thus, as it was shown, with the help of groundbreaking advances in the field of technology, mainly RFID, biometrics, PKI and e-signatures, identification methods changed. The digitisation of information made new methods invisible and more intrusive.

Moreover, it was discovered that not only the risks, but also the potential benefits of e-ID technologies are stressed by both the instruments of the EU and national member states. However, only 38% of EU citizens used e-government services in 2009,\(^{494}\) showing that the latter are not popular among EU citizens. Along the same lines, OECD promotes e-government policies and is in favour of a customer-oriented policy of its members.\(^{495}\) Besides, the European Commission’s “Digital Agenda” recommends that member states should make e-government services widely available to all their citizens by 2015.\(^{496}\) Thus, on the whole, e-government constitutes an issue of pan-European interest. For, my study might offer insights at a European level, and not only for the case of Greece.

In a bid to comply with the above mentioned policies, Greece launched its “Digital Strategy, 2006-2013” and “Digital Greece, 2020” schemes.\(^{497}\) Nonetheless, it appeared that not many services are rendered on-line, with e-democracy opportunities being devoid of formality and not widely used by Greek citizens. Additionally, the physical presence of the citizen is still deemed necessary for the full rendering of a service. Consequently, it appeared that e-government in Greece needs enhancement.

---

\(^{492}\) Groebner, Documenting Individual Identity, 15.

\(^{493}\) Noiriel, The identification of the citizen, 28 and 39-40.

\(^{494}\) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, “A Digital Agenda for Europe”, (Brussels, 19.05.2010), 32.

\(^{495}\) Kettl, The global public management revolution: a report on the transformation of governance.


Interestingly, the comparative analysis of the identification schemes in different EU member states produced the most fruitful results. Both the examination of the Austrian “Bürgerkarte” and the case of e-voting in Estonia indicated that e-ID cards are central components of any e-government scheme. Accordingly, e-ID cards could be used as an authentication apparatus that could give flesh and bones to the Greek citizens’ full enjoyment of potential benefits of e-government, and lead to the upgrading of the latter. The examination of the Austrian “Bürgerkarte” further pointed out that e-ID schemes can be implemented in ways that are more effective and less intrusive for privacy and personal data protection.

In particular, in the fourth chapter it was proven that e-ID cards entail various risks from a privacy and data protection point of view. It was shown that the use of e-ID cards bears the potential risk of surveillance of citizens, with the help of “networked, searchable databases”, leading to excessive social control. It was also observed that new surveillance tools although invisible, can be even more harmful than visible ones, as they might bring about excessive deterrence of not only unlawful, but also lawful activities. Furthermore, ID cards in general do not have an innocent past. A historical overview showed that they were used for unfair, discriminating and even dehumanising purposes. This makes it clear that people have to be reassured that historical errors will not be repeated.

In addition, it was specified that these negative effects proliferate because of the use of RFID and biometrics. E-ID cards making use of RFID were cloned in the UK, proving that such documents are vulnerable to attacks. Moreover, biometrics might unfairly exclude or include certain individuals because of “false positives and false negatives”. Discrimination is also apparent because of the FTE rates that are much higher only for certain races on Earth. This constitutes racial discrimination, based on the criteria of colour and race, and which are not far from discrimination uses of ID cards in the past.

From the previously mentioned it follows that RFID and biometrics are in their infancy and more research should be done in order to acquire more reliable and secure applications. For this reason, and in combination with the fact that the e-ID cards scheme was cancelled in the UK as privacy unfriendly should make other countries think twice of the security and effectiveness of their future corresponding schemes. Why such a rush for technologies that need more research to comply with satisfying levels of security? Why not endorse for instance alternative milder solutions as the one of Austria?

---

498 Lyon, Identifying Citizens, 11-12.
499 Solove, Understanding Privacy, 108.
501 Ibid., 116.
Moreover, the comparison between e-passports and e-ID cards shows that both documents raise privacy concerns. It further illustrates that, as opposed to the e-passport, there is no common specific EU policy for e-ID cards. As a result, there is a discrepancy among member states in this field. Thus, in my opinion EU member states should adopt a common e-ID card strategy that will also accelerate political integration among EU citizens. EU member states should compare between their various national identification plans, with a special focus on privacy-friendly implementations as the one of Austria. Only through constant and comparative dialogue can they reach a cost-effective solution. Finally, an important question remains unanswered; why do EU citizens need e-ID cards to travel within the “Schengen Area” if they are to travel without any impediments? Is it not a partial restriction of their movement?

Specifically for the tax-card, I discovered that its use has the potential risk of profiling citizens, with unpalatable consequences for their autonomy and independent decision-making. Moreover, as it follows from the research I conducted, the Ministry did not comply with the recommendations of the HDPA. Thus, the tax-card and the way it functions might lead to discrimination and exclusion, as all the daily consuming habits of Greek citizens will be stored in a single central database. Moreover, it will be relevant to thoroughly revise the agreement that will be signed between the banks and the Ministry for the processing of personal data. Explicit provisions about the obligation of the controller for non-disclosure to third parties and the security measures of the processing are in my opinion essential for the lawfulness of the processing.

Alternatively, it would be more privacy-friendly if private banks were totally excluded from the processing of personal data. The Opinion of the HDPA for on-line transfer transactions from the cash registry to the Ministry is an alternative way to effectively ensure that the VAT is paid. Additionally, identification is only necessary once per year, and the everyday processing of personal data is disproportionate given the purposes for which it is conducted.

Another important issue that is relevant to the tax-card and e-ID cards in general is to define who will be the controller of the processing. I agree with the Opinion that ideally data subjects should have total control of the data processed. At the end of the year, citizens could submit to the Ministry all

---

502 Article 10 of the Law.
503 Opinion of 13-12-2010, 8.
504 Ibid.
505 Opinion of 13-12-2010, 8.
their transactions stored in the card that should be totally controlled by them.\textsuperscript{506}

What is more, taking into account that RFID and biometrics are in their infancy there should be more research done in this field. The examination of the reasons why the e-ID scheme was cancelled in the UK\textsuperscript{507} further showed that new identification methods lack predictability and reliability.

Hence, it is essential that policy-makers and other stake-holders should engage with more privacy-friendly implementations. Precisely, the Greek government should take action in order to adopt privacy-friendly policies and “construct applications so that transaction records cannot be used as surveillance tools.”\textsuperscript{508} However, this would lack effectiveness if done only at a national scale. As mentioned above, comparative discussion about implementation schemes with both positive and negative effects, in different EU countries, should constitute a compass that is necessary to reach at least the right direction to the solution of the problem.

Consequently, in the future, the indicator of the compass should be showing towards three directions. First, the closest examination of the “Bürgerkarte” or other privacy-friendly schemes would provide not only Greece, but also other countries on a global scale, with more insights. Second, in due time, the e-voting system of Estonia should be closely scrutinised. It is true that e-voting in Estonia is relatively new, as it was first implemented in 2005. Empirical data should be collected and analysed in the course of the time in order to bring about fruitful results. And third, the examination of schemes that failed, as the one of the UK, would give insights on avoiding ineffective or unsuccessful implementations, and win time with more successful ones.

On a national scale, I hope that I will be given the opportunity to conduct an analysis of the recently voted Greek Law no. 3979/2011 on e-governance that is the legal context within which the whole identification scheme for e-government services will take place. This analysis should also include the results of the 1\textsuperscript{st} Digital Agenda Assembly that took place in Brussels on the 16\textsuperscript{th} and 17\textsuperscript{th} of June 2011, that unfortunately I could not include in this study.\textsuperscript{509}

All in all, in my opinion, it would not be wise neither to accept e-ID cards unconditionally nor to severely renounce them. However, despite all the above mentioned recommendations that might prove effective in practice, it
seems that the tug of war between the advocates and the opponents of the new scheme in Greece is set to continue and will become much stronger in the future, when the e-ID card will be introduced. Privacy-friendly solutions cannot be built overnight; they need research, and investment of time and money, that Greece might be devoid of right now. For the time being, perhaps Fedtke is right that tempered convenience is “the price to pay, for a less effective state if we want to maintain civil liberties and privacy”.510

Bibliography

Books


van't Hof, Christian. Outcome of the project “RFID and Identity Management” commissioned by STOA. Rathenau Institute, 2007.


Journals & Articles


On-line Journals & Sources


Websites

BBC, http://news.bbc.co.uk/2/hi/4659093.stm


Eleftherotypia, Greek Newspaper. http://www.enet.gr/?i=news_el.article&id=218573

Eleftherotypia, Greek Newspaper. http://www.enet.gr/?i=news_el.article&id=215715


OECD. http://www.oecd.org/department/0,3355,en_2649_34129_1_1_1_1,00.html.


Supreme Court, Republic of Estonia. [http://www.nc.ee/?id=381](http://www.nc.ee/?id=381).


Workshop on “E-voting in Europe”, E-voting in Europe: why should we look at it, which arguments we should consider and what to expect in the future, 1, 17 March 2011. [http://www.go-online.gr/ebusiness/specals/article.html?article_id=1517.](http://www.go-online.gr/ebusiness/specals/article.html?article_id=1517.)


### Case law


### Legal Instruments

United Nations International Covenant on Civil and Political Rights (1966)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Greek Government Gazette (FEK) 9/A/12.01.1945 “concerning the obligatory provision of identity cards”.

The Greek Constitution.

The European Convention of Human Rights.

The Convention of the Council of Europe of 1981 (108) for the protection of individuals with regard to automatic processing of personal data.

The OECD Guidelines 1980 governing the protection of privacy and transborder data flows of personal data.


Royal Decree of 26.2.1911.

Law No. 2472/97.

Decision of the Ministry of Economic Affairs 1104/9-5-2011.
