EJLT European Journal of Law and Technology

Identification numbers as pseudonyms in the EU public sector

Niels Vandezande [1]

Cite as : Vandezande, N., 'Identification numbers as pseudonyms in the EU public sector', European Journal of Law and Technology, Vol. 2, No.2, 2011.

Abstract

In recent years the use of pseudonyms as false identities over one's actual birth name has increased rapidly. The main driver behind this growth is the Internet, where virtually every user employs at least one pseudonym. Also public legal entities have resorted to issuing pseudonyms - mostly in the guise of identification numbers - to their subjects. Contrary to the historical use of pseudonyms as a means for concealing one's identity, such public sector issued pseudonyms are rather used for unique and trustworthy identification. The use of pseudonyms can, however, entail a number of risks, specifically concerning the protection of the privacy of the citizen regarding data exchange and data linking. In this article, the national identity schemes of selected EU Member States will be analysed to assess how pseudonyms are introduced as means for public sector identification and what the practical impact is of the purported privacy concerns.

1. Introduction

The use of false identifiers has become part of the daily routines of ordinary citizens. Particularly on the Internet, one will more often than not use a nickname or username than one's actual birth name. For many Internet users, the username has even grown into a complete surrogate identity for an ever-growing number of online applications and services. False names, employed to conceal one's true identity, are called pseudonyms. In past times, pseudonyms were mainly used by a limited number of people finding themselves in particular situations that warranted the use of a false name instead of their birth name. Well known examples include pen names used by authors or stage names used by actors; their motives for employing a false name ranging from trying to evade political repercussions to hiding their gender in an age dominated by the opposite gender. Nowadays, mainly under the influence of the rise of the Internet as the main medium for almost every type of communication, the use of pseudonyms has become commonplace for virtually all private actors.

Although pseudonyms were originally mostly self-assumed and conceived to conceal the true identity of the users deploying them, they can also be used for achieving the exact opposite result: by having a third party assigning a pseudonym that is single, unique and fixed to each user in a particular system, this pseudonym can be used for unique and

trustworthy identification of these users. For the purpose of achieving this goal, single in this context means that every user in that particular system can only be assigned one pseudonym. Such pseudonym also has to be unique in the sense that no pseudonym can be issued to more than one user at the same time. Furthermore, such pseudonyms need to remain fixed, as unregulated changes to the pseudonym would tamper with its identification qualities. Many legal entities - be it business entities, educational institutions or others - have already resorted to issuing pseudonyms to their employees, students or costumers for identification purposes.

It is precisely the broad scope of the concept of pseudonyms that allows for such deviation from its general perception as being a self-assumed false name towards an identification number issued by a third party, be it a private institution or a public sector body. Grijpink and Prins, for instance, define a pseudonym as 'a distinguishing mark with which a certain transaction or act can be traced back to a certain existing or fictitious person', with that distinguishing mark being possibly anything, including personal numbers or even biometric numbers. [2] Grijpink and Prins go as far as specifically identifying a pseudonym issued by a private or public authority as being an 'organised pseudonym'. [3]Pfitzmann and Hansen refer to this as a 'person pseudonym', being a 'substitute for the holder's name which is regarded as representation for the holder's civil identity', which also includes State-issued identification numbers. [4]

As mentioned earlier, the Internet has played an important role in making the use of pseudonyms as means for concealing one's true identity standard practice in many of our daily communication routines. However, the Internet at the same time also provides the tools needed to link certain pieces of data together, ultimately leading to the potential identification of the user behind the pseudonym. In the broad context of the concept of pseudonyms, one could, for instance, refer to the IP address assigned to any device upon connecting to the Internet as a pseudonym to identify a particular device. Also cookies can be used to track which websites are visited by a particular user. The Internet's intrinsic abilities for data linking have indeed made it a very ambiguous medium. While on the one hand enabling its users to conceal their true identities behind pseudonyms, the Internet has also become the centre of the business model of data linkability. In this business model, service providers are remunerated for their free services by aggregating and selling bits of user data that can be linked together to compile a more complete and accurate user profile. For instance, popular service providers such as Google and Facebook endure ongoing criticism on how they govern the personal data obtained from their users and on how such data is transmitted to third parties.

Also public legal entities have resorted to using pseudonyms for the purpose of unique and trustworthy user identification. As, amongst others, the idea of re-use of public sector information is gaining more ground in government practice, different government agencies will more and more have to rely on each other to receive certain information regarding their citizens. Particularly in Belgium, the principle of 'single data collection' (in Dutch: 'éénmalige gegevensinzameling') dictates that government agencies cannot ask the citizen to provide the same information twice. If, for instance, the citizen has provided his fiscal information to the national tax agency, other government entities wishing to consult that citizens' tax situation need to obtain this information from the tax agency and cannot ask the citizen to provide this information directly to them again. As separate government agencies may use different methods for governing their administration, it is understandable

that these government agencies could benefit from a common method for the unique identification of the user involved when exchanging data between them, certainly when operating at a cross-border level.

The use of pseudonyms - be it to conceal one's identity or for the purpose of unique identification - can, however, entail a number of risks. For one, in the private sector there is no check on the distribution of pseudonyms. This can lead to several users claiming the same pseudonym or one user employing several pseudonyms. As a general rule, pseudonyms can be used to hinder the identification of the user behind it in case of gross misconduct or criminal activities. Another major risk regarding the use of pseudonyms concerns privacy protection. [5] As explained, both in the public sector and on the Internet, pseudonyms are used in data exchange and data linking. As such practices can lead to uncovering several aspects of the private life of the user involved, one may want to look for means to prevent or at least control such data exchange and linking. Alternatively, one may look for means to render data exchange and data linking using the pseudonym of the user more transparent.

The central question emanating from this is whether the widespread practical use of pseudonyms - particularly in the public sector - will indeed give rise to considerable privacy concerns or whether governments in EU Member States have found a way to manage the risks involved in using such unique identification schemes. Therefore, this article intends to examine the different types of identification numbers used as pseudonyms in EU Member States. As part of that examination, an assessment will be made of how such identification numbers are applied in a selected number of EU Member States. Not only will this enable the determination of how widespread the use of identification numbers as pseudonyms in the EU public sector is, but it will also serve as a basis to assess whether the risks regarding such use have been managed or whether they remain.

2. Pseudonyms for identification

As already discussed, public legal entities worldwide have resorted - be it in recent years or for a longer period already - to the use of pseudonyms for the unique identification of their subjects. [6] Such pseudonyms are mostly found in the guise of identification numbers. These identification numbers can, however, be found in many different incarnations. We can discern two main types as most suitable for the unique identification of citizens in the public sector: national identification numbers of general application and sector-specific identification numbers. [7] Apart from issuing these two types of identification numbers as pseudonyms for unique public sector identification, EU Member States are more and more resorting to the use of biometric identification methods.

The first main type of identification numbers is the national identification number of general application, as referred to in article 8 (7) of Directive 95/46/EC. Each of these identification numbers is - as identification numbers are supposed to be - unique in the sense that they are issued to one person only. Furthermore they are the single - or at least the dominant - identification number issued, in this case mostly by the central or federal government. As can be deducted from their name, national identification numbers of general application are used for unique identification in all layers of the public sector. Therefore, they are not limited to use within one particular sector only and can be used, for instance, for fiscal identification, for assessing the applicability of social security benefits and other purposes.

In more extreme cases, these national identification numbers of general application can also be used in the private sector. In such cases, they could, for instance, be used for unique user identification by banks, libraries and many others. The wide usage of such identification numbers - being the whole public sector and potentially the private sector as well - can, however, give rise to concerns regarding the protection of the privacy of the citizen. If one single identification number can be used to link together all information regarding a single citizen held by public - and potentially also private - entities, one should beware the potential for abuse of such number.

Also the EU has hinted at the particular status of national identification numbers of general application by including them under article 8 (7) of Directive 95/46/EC. [8] One can conclude from the text of this article that the processing of identifiers of general application requires additional regulation and can not only be considered as processing personal data, but even as processing the special category of data as mentioned in recital 33 of Directive 95/46/EC. [9] As article 8 (7) does not provide any specifications on how identifiers of general application need to be regulated, this matter is left to the Member States, potentially leading to divergent policies amongst Member States.

As was already hinted at earlier, not all identification numbers can be grouped in the category of a single national identification number of general application. One can also discern identification numbers that are limited to use within one particular sector only. In this case, an identification number issued for tax purposes, for instance, could identify every subject for fiscal matters within the issuing State. In principle, tax identification numbers of this kind cannot be used to identify a subject for social security purposes. In such cases, the social security sector will most likely have issued its own sector-specific identification number for the unique identification of each citizen within the social security sector in the issuing State. As a result, each subject will be issued several separate identification numbers, each being intended exclusively for unique identification within their respective sectors.

The policy choice between issuing a national identification number of general application versus issuing different sector-specific identification numbers is, however, not always very clear-cut. For one, as will become clear from the policy analysis conducted further on, there are States that have issued a single national identification number of general application, yet that at the same time still have a few sector-specific identification numbers in use. Furthermore, the reasons for not issuing a single national identification number of general application may differ greatly. This decision may purely be based on preference, for instance due to a societal mistrust against such identification numbers, but may also be based on a constitutional incompatibility of such national identification numbers of general application. Even if the policy choice was made to issue only sector-specific identification numbers, there is still the special case regarding such sector-specific identification numbers of what can be referred to as 'functionality creep'. This concerns the situation where a sector-specific identification number is used for so many transactions beyond its original sector that it evolves into a de facto national identification number of general application. A prominent example of this is the American Social Security Number. Originally intended for use in the social security sector only, it is now de facto the main identification number for US citizens for all types of cross-sector identification purposes.

As a result, even though one can distinguish two main types of State-issued identification numbers, one can divide their application into three policy groups. First, there is the group of States that has made the clear decision to issue a de iure single national identification number of general application. Second, there is the group of States that have chosen to issue several sector-specific identification numbers, yet where the issue of functionality creep has resulted in one of these sector-specific numbers becoming the dominant identification number, thus essentially serving as a de facto national identification number of general application. Third, there are the States that have constitutionally banned the issuing of a single national identification number of general application and that therefore may also exercise more control on their sector-specific identification numbers to manage the issue of functionality creep. It is especially this last group that holds profound concerns regarding national identification numbers of general application.

Additionally, public sector bodies have started to turn to biometric data for identification purposes. Given its inherent uniqueness and permanent relation to the person from which the biometric data was derived, this would provide a higher level of security in user and access management of identity management systems and would thus provide for more reliable identification. The use of biometric data in identifiers for public sector identification could at the same time, however, also augment privacy concerns. For one, one can think of issues regarding the revocability and unlinkability of biometric data. After all, while a randomly generated identification number can easily be revoked, this is less evident when using biometric data for identification purposes. Although the use of biometric data for identification purposes in both the public and private sector has been in talks for many years, it has only resulted in smaller projects as the large-scale use of such systems is still under debate.

Regardless of the privacy-related concerns voiced in the use of biometric data for identification purposes, the EU has already expressed its opinion on the matter by explicitly including the use of biometric data in its passports and travel documents. As a result, all passports and travel documents need to include a highly secure storage medium - that secures the data and has sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data - that stores a picture of the holder of the document, in addition to which two fingerprints taken flat in interoperable formats will also be included. [10]

In using biometric data for identification purposes, the raw data collected from a person - relating to his facial features, his fingerprints, his eyes, etc. - will be processed into an identifying characteristic that will be used for biometric identification and verification. As an identifying characteristic is used rather than the person's actual identity, this use of processed biometric data could fall under the broad scope of a pseudonym used for identification purposes, as defined earlier. As a result, the use of biometric data for identification purposes can be considered as an evolution to the use of identification numbers for public sector unique and trustworthy citizen identification.

3. Pseudonyms in the EU public sector

In order to assess how the two main types of identification numbers and biometric data used as identifier are distributed across the Member States of the European Union, research will need to be conducted on the policy regarding the use of identification

numbers for a select number of EU Member States. The Member States selected for this research are Belgium, Austria, Germany, Portugal, Sweden, the United Kingdom, Spain and the Netherlands. This research will provide a high-level insight in the use of identification numbers as pseudonyms in the EU public sector. It will also highlight a number of issues to be taken into account for future developments regarding the use of identification numbers, such as privacy considerations.

3.1 Belgium

The Belgian government officially deployed the system of a national identification number of general application used as a pseudonym for the unique identification of its citizens throughout most of the public sector in 1983, putting Belgium in the first policy group, as defined earlier. As a result, Belgian citizens are registered in a national population register and are assigned a corresponding general identification number. [11] This number - called the 'National Registry Number' (in Dutch: 'Rijksregisternummer') - is composed of the citizen's date of birth, a serial number which also denotes the gender of the citizen and a checksum. [12] As the government feared that the widespread use of such a national identification number of general application could be harmful to the privacy of its citizens, it was decided that the use of this number would need to be restricted. [13] Thus, the Belgian national identification number of general application can only be used if prior authorization thereto has been obtained. [14] These authorizations are granted by a specialised committee founded under the wings of the Belgian national Data Protection Authority. [15]However, the relatively protective stance once adopted has gradually weakened, as more and more government agencies have adopted the national identification number of general application as the main identifier for consistent and unique public sector identification, not only for internal use but also for external data exchange with other government agencies. For example, in the social security sector the National Registry Number is also used as the social security number of most Belgian citizens. Currently, the national identification number of general application is also present in the certificates on the electronic identity card used for authentication and for producing qualified electronic signatures, as well as on the chip of that card. [16] Oddly, the otherwise strongly protected national identification number of general application is therefore propagated every time the citizen uses his electronic identity card. Currently, the Belgian electronic identity card stores no other biometric data than a digital photograph of the cardholder. [17]

Throughout the years, the Belgian national identification number of general application has endured its fair share of criticism. For instance, this number contains the date of birth of the citizen and refers to his or her gender. Both of these are personal data in the meaning of Directive 95/46/EC and therefore need to be processed in compliance with the principles set forth by that Directive and its national implementations. [18] Secondly, as mentioned earlier, a national identification number of general application is considered under article 8 (7) by Directive 95/46/EC as requiring additional national regulation.

3.2 Austria

Contrary to Belgium, Austria uses sector-specific identifiers. After creating a national population register using data collected in a 2001 census, each citizen has been assigned

a meaningless identification number. [19] Instead of using this identification number as an identifier of general application, a so-called SourcePIN is derived from that number in such a way that this SourcePIN cannot be traced back to the original identification number. [20] Subsequently, a sector-specific Personal Identification Number (PIN) is obtained by hashing the SourcePIN with a sector-specific code assigned to each sector by law. [21] These sector-specific numbers, commonly called ssPIN, can be used by the citizen for all transactions vis-à-vis the government as well as for private transactions, thus resulting in each citizen being assigned one identification number per sector defined by law, as well as one identification number per service provider in the private sector. [22] An ssPIN can only be generated by consent of the citizen and only the SourcePIN Register Authority can generate SourcePINs without needing the citizen's Bürgerkarte. [23] The Austrian government has also taken measures to prevent unauthorised data exchange. [24] Another noteworthy phenomenon in Austrian public sector identity management is the Bürgerkarte. This is not a physical electronic identity card, but a concept of which the main functions are authentication and producing qualified electronic signatures. [25] Being a non-physical concept, the Bürgerkarte is not bound to a particular physical card. Therefore, all kinds of smart cards can be used as Bürgerkarte, for example a bank card, a social security card or a student card. The Bürgerkarte is connected to the SourcePIN by an identity link created by the SourcePIN Register Authority. [26]

By issuing sector-specific identifiers and by protecting these identification numbers against unauthorised use or data exchange, the Austrian government aims to provide maximum protection to their citizen's personal data. There are, however, still a number of remarks to be made. First, reports show that the adoption rate of the non-obligatory Bürgerkarte is rather low. [27] Second, as certain other identification numbers are left unprotected, there is a chance of them serving as a de facto national identification number of general application. [28] While Austria generally opposes a single national identification number of general application, the appearance of functionality creep may result in Austria leaning towards the second policy group, as defined earlier, rather than the third policy group. Third, one may question the efficiency of sector-specific identification numbers in terms of data exchange and communication between different layers of government entities as some authors argue that the use of sector-specific identification numbers would lead to more complexity. [29]The Austrian national identification scheme therefore does not appear to render the return on investment one would anticipate from a scheme deploying such elaborate security for privacy protection purposes. One explanation for this is that the elaborate security scheme may lead to a perceived lack of transparency, which in turn may very well lead to citizens refraining from adopting such scheme.

3.3 Germany

Germany has based its public sector identity management system on the Austrian system. As national identification numbers were abused during the Second World War, Germany has banned the use of unique identification numbers of general application, putting it firmly in the third policy group. [30] Even though Germany will conduct a census in 2011 and will use this data to introduce a central population register, it has been made clear that the ban on national identification numbers of general application will not be lifted. [31] The new German electronic identity card therefore uses sector-specific identification numbers by enabling the generation of ad hoc pseudonyms for use in different sectors, a system

inspired by the Austrian ssPINs. [32] Furthermore, the chip embedded in the identity card will use RFID-technology and contains biometric data - albeit that the storage of the citizen's digital fingerprints is optional.[33] A digital photograph of the citizen, however, is included mandatorily, as are the height of the citizen, his eye colour and his signature. The new identity card is also equipped for authentication purposes and can optionally be activated for producing qualified electronic signatures, provided by recognised certification service providers. The deployment of the German electronic identity card started in November 2010.

Given the similarities between the German and Austrian national identity scheme, one may suspect the remarks on the Austrian system to also apply to Germany. It should be noted, however, that possession of the German electronic identity card is mandatory, automatically leading to a higher adoption rate than the Austrian Bürgerkarte will ever know. [34] Secondly, given the German constitutional ban on national identification numbers of general application, it is unlikely that a sector-specific identification number will be allowed to develop into a de facto national identification number of general application, keeping the risk of 'functionality creep' under control. As in Austria, the German federal government has spared no expense in the development of the underlying security system for the protection of the citizen's privacy. However, at the time of writing it is too early to assess the impact and perception of the new national identification scheme.

3.4 Portugal

The Portuguese policy on this topic shows a number of similarities to the policy adopted by Germany. For one, article 35 (5) of the Portuguese constitution prescribes a constitutional ban on the use of a single national identification number of general application. However, as the use of multiple identification numbers of general application is allowed, Portugal has been able to issue an identification number for the national population register, which has been included in both the old and the new identity card. The use of this number, however, is strictly regulated. [35] Also different sector-specific identification numbers are deployed, such as the social security number, the tax number and the number for the National Health Service. The use of these identifiers is generally unprotected, making them candidates for expanded usage and gradual development into de facto identification numbers of general application in both the public and the private sectors. [36] It should be noted that only the mere use of these identification numbers is not specifically protected. If these sector-specific identification numbers are to be used as a mean for data interconnections, the Portuguese data protection legislation requires prior authorization granted by the Portuguese Data Protection Authority to the controller of the data interconnections, unless such data interconnections were subscribed by law. [37]Currently, Portugal is in the process of deploying a new national identity card, which will include all the different sector-specific identification numbers currently in use. This electronic identity card will be equipped with certificates for authentication and for producing electronic signatures. [38] Biometric data visible on the physical card includes a photograph, the citizen's height and his signature. [39] Biometric data stored on the chip embedded in the card includes a digital photograph, the citizen's height and his digital fingerprints. [40]

Even though Portugal - just like Austria and Germany - uses sector-specific identification numbers, it does not have a similar system for protecting and obfuscating certain

identification numbers for the sake of privacy protection. Even though the Portuguese approach certainly has its positive aspects - like a high degree of transparency - there are also a number of caveats to be taken in account. For one, if all sector-specific identification numbers are united on one identity card, there is a risk that the number of that identity card will be used as a central point of connection between these numbers, thus becoming a de facto single national identification number of general application. The constitutional ban on a single national identification number of general application would put Portugal in the third policy group. However, the issuing of an identification number for the national population register, albeit protected, and the potential risk for functionality creep when the new identity card will be fully introduced, makes it difficult to make a final assessment on what policy group Portugal belongs to precisely.

3.5 Sweden

Sweden is an EU Member State that issues a single national identification number of general application to its citizens, thus belonging to the first policy group. Like its Belgian counterpart, the Swedish identifier is composed of the date of birth, a number referencing the citizen's gender and a control number. [41] Unlike the Belgian identifier, the Swedish national identification number of general application is not restricted to use within the public sector, but can be used for business-to-consumer identification as well. Even though certain statutes attempt to restrict the use of the national identification number of general application, this number remains the main identifier in both the public and the private sector. For instance, section 22 of the Data Protection Act [42] states that the personal identification number of general application may only be processed if the citizen concerned gives his consent or - in the absence of consent - if such processing is justified for the purpose of the processing, for secure identification or for any other noteworthy reason. The broad scope of this article allows for the personal identification number of general application to be processed in almost every situation in daily life. The fact that this liberal use of the national identification number of general application does not give rise to any serious privacy concerns is thanks to the Swedish constitutional principle of publicity (Offentlighetsprincipen), which is regarded as being an integral part of the freedom of the press and is thus part of the Swedish constitutional framework. [43] Recent research confirms that the majority of the Swedish population is satisfied with the liberal use of their national identification number of general application. [44] The Swedish government does not issue an official identity card. In recent years, however, the national police have started issuing a non-compulsory identity card, which contains a contact chip as well as an RFID chip, but no biometric data. [45] Theoretically, this card could be used for authentication purposes and for producing qualified electronic signatures, but these functions have not yet been activated. [46] The Swedish government does allow for privately issued identity cards. Such cards, issued by commercial entities like banks, do often include the necessary certificates - which may include the national identification number - for authentication and for producing qualified electronic signatures. [47] These privately issued identity cards are, however, not valid travel documents. Also the National Tax Agency issues an identity card, containing certificates for authentication and for producing qualified electronic signatures issued by private telecom operator Telia. Even though this particular identity card is issued by a government agency, it bears no validity as travel document.

Even though there are a great number of similarities between the Belgian and Swedish national identification numbers of general application, the Swedish identification number of general application does not seem to give rise to the same remarks regarding the protection of the privacy. Even though one may argue that the protective stance on the Belgian National Registry Number has been lowered to a certain extent, Belgium does not seem ready yet to allow for this number to be used in the private sector as well. The reason for this is a culturally imbedded difference in views on privacy protection between these two EU Member States.

3.6 United Kingdom

As is the case in most Anglo-Saxon States, the United Kingdom has historically adopted a negative stance towards national identification numbers of general application or national identity cards. The United Kingdom has already experimented with identity cards in the past, eventually cancelling such schemes. Also identification numbers of general application have never been successfully implemented and sector-specific identification numbers - such as the National Insurance Number and the National Health Service Number - remain in use to this day. In recent years, however, the discussion on a national identification scheme was reopened. Eventually, this discussion has lead to the much contested Identity Cards Act, which established a national population register, issued a national identification number of general application to all citizens registered in said register and created a national identity card. [48] This register would also record biometric data and such data would be present on the chip of the identity card. As the act remained somewhat vague in a number of its provisions, concerns amongst the British population regarding this national identity scheme have only risen. [49] Therefore, one of the first proposals submitted to Parliament by the new government in 2010 was a proposal to repeal the Identity Cards Act 2006, thus voiding existing identity cards and requiring the identity register to be destroyed. [50]

The enduring criticism on the national identification number of general application and its dismissal could lead one to conclude that the United Kingdom would belong to the third policy group, joining Germany as a staunch opponent of such general identification numbers. However, the United Kingdom shows that even this division into policy groups is not necessarily clear-cut as the sector-specific identification numbers currently in use in the United Kingdom show that they are highly prone to functionality creep. The presence of functionality creep in its sector-specific identification numbers would place the United Kingdom in the second policy group. The British national identity scheme serves as a good example of how important transparency of the scheme is to the citizen. Despite a number of government efforts to raise awareness on the national identity scheme, the lack of clarity of the legal framework on the British national population register and identity card has ultimately lead to its demise.

3.7 Spain

Spain deviates from the path set by Belgium and Sweden by not deploying the identifier of the national population register as the national identification number of general application. Instead, the Spanish citizens are uniquely identified for every sector by the number of their identity card, which puts Spain in the first policy group. [51] Possession of such an identity

card is mandatory for all citizens over the age of fourteen, naturally leading to a very high adoption rate of both the national identification number of general application and the identity card. [52] The national identification number of general application has been left without much additional protection, allowing for the number to be used for other purposes such as for tax purposes, on the driver's license and in other transaction in both the public and private sector. [53] Currently, Spain is introducing an electronic identity card with a contact chip, which contains both the national identification number of general application and biometric data, such as digital fingerprints. [54] Certificates enable the card to be used for authentication purposes and for producing qualified electronic signatures. [55] The electronic identity card includes advanced security mechanisms, notably the requirement of entering a PIN before gaining access to the data on the chip. [56]

Even though it may seem that the Spanish national identity scheme has a close connection to the Swedish system because of the more liberal use of the national identification number of general application for identification in both the public and the private sector, there is a notable difference between these two systems. The Spanish national identification number of general application is a so-called 'meaningless identification number', meaning that this number is randomly generated and therefore holds no personal data such as the date of birth. It therefore leads to less privacy concerns than identification numbers that are composed of personal data, such as the Swedish and Belgian national identification number of general application. Regardless of the fact that no additional protection has been granted to the Spanish identification number of general application, each processing of this number needs to comply with the national implementation of Directive 95/46/EC.

3.8 The Netherlands

The Dutch national identification number of general application has only very recently been introduced, making it one of the younger identity schemes discussed here. The current Citizen Service Number, a 'meaningless identification number', replaces the so-called 'Sofi number', which was initially only meant for use in the sectors of taxation and social security. As the use of the original identifier gradually grew, the Citizen Service Number was adopted as a replacement identifier to be used for identification and authentication in the whole public sector, thus placing The Netherlands in the first policy group. [57] This identification number of general application can also be used in the private sector if a legal basis for such use would be found. [58] The national identification number of general application is present on the new identity card. [59] Interesting is that whilst the possession of a valid identity document is mandatory since 2005, the citizen can choose between a number of valid documents. This includes passports, identity cards and driver's licenses. [60] Even though this identity card contains biometric data and a RFID chip, there are no certificates present for authentication purposes or for producing qualified electronic signatures. [61] Instead, the DigiD platform has been set up for e-Government purposes, with PKIoverheid, controlled by the Dutch government, serving as root certificate for privately issued certificates. [62]

Like many States employing sector-specific identifiers, the Netherlands noticed a gradual expansion of the purposes for which the 'Sofi number' was used. Instead of ignoring or repressing this practice, the Dutch government chose to replace this sector-specific

identifier by a de facto et de iure identification number of general application. Even though this identification number was meant for use in the public sector only, it can be used in the private sector as well if a legal basis for such use would be present.

4. Conclusion

As can be deduced from this overview of certain aspects of the national identity scheme of a select number of EU Member States, the use of identification numbers as pseudonyms has been well adopted by EU Member State governments for the purpose of identifying their citizens in the public sector. Even though pseudonyms originated as a means for concealing one's true identity, they can indeed also be used to provide for unique and trustworthy identification. Because of this, governments have resorted to issuing pseudonyms - mostly in the guise of identification numbers - to their citizens. As explained, the identification numbers issued by States can be divided into two main categories. First, there are the single national identification numbers of general application. As this brief survey pointed out, such identification numbers can be found in Belgium, Sweden, Spain and The Netherlands. Second, there are the sector-specific identifiers, found predominantly in Austria, Germany, Portugal and the United Kingdom. However, it was found that States issuing a single national identification number of general application could still maintain separate sector-specific identification numbers, such as the Belgian VAT-number. Also within the category of States that prefer sector-specific identification numbers over a single national identification number of general application, one needs to distinguish between the States that have seen functionality creep - such as the United Kingdom - and States that strongly protect their sector-specific identification numbers, like Germany.

As a result, a further distinction was made into policy groups. A first policy group concerns the States clearly issuing a single national identification number of general application, such as Belgium, Sweden, Spain and The Netherlands. A second policy group concerns States that only issue sector-specific identification numbers, yet that have seen functionality creep, such as the United Kingdom. A third policy group are the States that strongly oppose a single national identification number of general application, such as Germany.

There are, however, still many differences to be found between the policies of Member States belonging to the same policy group. For example, Germany has created a secure system for generating sector-specific pseudonyms while obfuscating the citizen's true identity. Portugal on the other hand lists all its fixed sector-specific pseudonyms on a single identity card, providing a firm link between these identification numbers. Also, despite a constitutional ban, Portugal has been able to issue an identification number for the national population register, even though the use of this identification number is strictly regulated. Spain has a more liberal approach to the use of its identification number of general application, enabling use within the private sector. The Spanish national identification number of general application, however, is not composed of personal data like the citizen's date of birth, unlike the Belgian and Swedish national identification number of general application. And even with its privacy-sensitive composition, Sweden still has an even more liberal approach towards the use of its national identification number of general application.

Most of the Member States analysed here also issue national identity cards. These are commonly electronic identity cards with certificates enabled for authentication purposes and for producing qualified electronic signatures, as in Belgium, Portugal and Spain. Austria has opted for a radically different concept, enabling citizens to choose which existing smart card they would want to use for authentication purposes or for producing qualified electronic signatures. The Swedish and Dutch governments have decided not to monopolise the concept of the electronic identity card in the public sector by allowing private entities to issue their own certificates. Security measures for protecting the data stored on the electronic identity cards and their certificates can differ greatly between different Member States as well. For instance, in Belgium the otherwise protected national identification number of general application is automatically propagated every time the citizen uses his electronic identity card. Furthermore, the data contained on the chip of the Belgian electronic identity card can be read freely, while the Spanish electronic identity card requires the entry of a PIN for such action.

Most Member States discussed here have also started to use biometric data in their national identification schemes. All national identity cards issued contain at least a digital picture of the citizen, with a growing number of Member States also storing a digital impression of the citizen's fingerprints on the chip of their identity card. In order to comply with EU regulations, all passports and travel documents are required to contain a facial image and fingerprints as biometric data. As national identity cards of EU Member States can be used as travel documents within the EU, these identity cards will have to comply with said EU regulations.

The findings of this overview can be summarised as follows:

	Belgium	**Austria**	**Germany**	**Portugal**	**Sweden**	**UK**	**Spain**	**NL**
Single national ID-nr.	Yes	No	No, banned	Not officially	Yes	No	Yes	Yes
meaningful	Yes				Yes		No	No
Sector-specific ID-nr.	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Functionality creep	No	Possibly	No	Possibly		Yes	No	No
Electronic ID-card	Yes	Yes, conceptual	Yes	Yes, in progress	Yes, not activated	No	Yes	No
Mandatory	Yes	No	Yes	Yes	No		Yes	
Biometrics other than picture	No	No	Optional	Yes	No		Yes	

The many differences between the ways in which the EU Member States discussed here implement identification numbers as pseudonyms for the unique identification of their subjects, demonstrate that also the three policy groups defined here are not able to clearly categorise the policy decisions of the Member States. Several nuances in a policy may lead to the categorisation of a Member State into several categories. For instance, as the United Kingdom has clearly shown its preference for sector-specific identification numbers over a single national identification number of general application, one could argue that it

follows the German stance on such identification number - minus a ban upheld by its Supreme Court - thus placing the United Kingdom in policy group three. However, its clear case of functionality creep in its sector-specific identification numbers would place the United Kingdom more firmly in policy group two.

The difficulties in properly categorising the different policies maintained by the Member States analysed here makes it hard to draw general conclusions regarding the precise impact that these policies have on the protection of the privacy of the citizen. As found in this overview, the way in which a State will implement a national identification scheme, is to a certain degree determined by historical and cultural imperatives. States that have a steady history of opposing a national identification number of general application - such as the United Kingdom and Germany - will not find the societal support to successfully create such identification number in the foreseeable future. On the other hand, States that - such as Sweden - have a longstanding tradition regarding the open and liberal use of their national identification number of general application, will not let relatively recent data protection legislation interfere with practices they perceive as part of their open and transparent society. When introducing a new national identity scheme, also the perceived costs of the scheme, considerations regarding public sector efficiency and possible limitations on the interoperability of sector-specific identifiers can all attribute to the choices made by a State.

Even though there are many differences between the national identity schemes of the EU Member States discussed here, a few general remarks can be deducted from the previous overview.

First, one should beware the impact of functionality creep. While the introduction of a single national identification number of general application or different sector-specific identification numbers are both clear policy decisions of which the scope can be fully defined, functionality creep associated with sector-specific identification numbers can also occur on a de facto basis, thus lacking a clear legal framework demarcating its scope. While functionality creep could in theory occur with any sector-specific identification number, the overview here shows that it has only occurred - or is likely to only occur - in States that have not issued a single national identification number of general application. The exception here is Germany, which is known for the strong protection of its public sector identification numbers.

Second, one should note the so-called 'meaningful identification numbers' that are composed of personal data such as the citizen's date of birth. As identifiers of general application could already be considered as sensitive personal data according to Directive 95/46/EC, such identifiers should be processed with care and in compliance with national privacy regulations. Spain, for instance, demonstrates how a meaningless identification number can be used for secure and unique citizen identification throughout the public sector with also options for use in the private sector.

Last, there is the problem of intergovernmental data exchange. As identifiers can be used as a mean to exchange data on the citizen between different governmental entities, these identifiers can become the centre of a web of information shared between these entities. The citizen will often not know of these data exchanges and therefore holds no clear overview of which government entity has access to what information. The lack of transparency of these data exchanges will therefore need to be addressed. For this, one

could envision a central portal where the citizen - after proper authentication - will be enabled to track the interconnections of his personal data made using his identification numbers. As such central portal does not seem to be available at the national level of all EU Member States and certainly not at a pan-European level, research will have to be conducted on describing the legal and practical framework needed for implementing such transparency-enhancing measure.

---

[1] Niels Vandezande (LLM) is currently working as a Researcher at the Interdisciplinary Centre for Law and ICT, at the Katholieke Universiteit Leuven, Belgium.

[2] A. GRIJPINK, C. PRINS, 'New rules for anonymous electronic transactions? An exploration of the private law implications of digital anonymity.' In C. NICOLL, J.E.J. PRINS, M.J.M. VAN DELLEN (eds.), Digital anonymity and the law - tensions and dimensions, The Hague, T.M.C. Asser Press, 2003, 251-252.

[3] A. GRIJPINK, C. PRINS, 'New rules for anonymous electronic transactions? An exploration of the private law implications of digital anonymity.' In C. NICOLL, J.E.J. PRINS, M.J.M. VAN DELLEN (eds.), Digital anonymity and the law - tensions and dimensions, The Hague, T.M.C. Asser Press, 2003, 251-252.

[4] A. PFITZMANN, M. HANSEN, 'A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management', http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, August 2010, 26.

[5] Privacy aspects of identification numbers are discussed in: X. HUYSMANS, 'Legal aspects of global vs. sector-specific identification Numbers' in H. BUITELAAR, 'FIDIS - D13.3: Study on ID number policies', 2007, http://www.fidis.net, 20-35.

[6] An analysis of the presence of identification numbers in the identity policies of EU Member States has been performed under the IDABC project: IDABC, 'eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability', 2009, http://ec.europa.eu/idabc, 228p. 6 See also: H. BUITELAAR, 'FIDIS - D13.3: Study on ID number policies', 2007, http://www.fidis.net, 105p.

[7] See also: H. BUITELAAR, 'FIDIS - D13.3: Study on ID number policies', 2007, http://www.fidis.net, 105p.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, Official Journal (OJ) L 281, 23 November 1995, 31-50.

[9] Note that identifiers that are not generally used - such as sector-specific identifiers of which the use is limited to that particular sector only - are not addressed by this provision, DE BOT, Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart, Brugge, Vandenbroele, 2005, 56.

[10] Article 1 Council Regulation (EC) Nr. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member

States, OJ L 385 of 29 December 2004, last amended by Regulation (EC) Nr. 444/2009 of the European Parliament and the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 142 of 6 June 2009.

[11] Article 2 of the Act of 8 August 1983 on the National Register of the natural person, Belgian State Gazette (BSG) 21 April 1984.

[12] Article 1 of the Royal Decree of 3 April 1984 on the composition of the identification number of the persons inscribed in the National Register of the natural person, BSG 21 April 1984.

[13] Preparatory Works Chamber of Representatives 1982-1983, 513, nr. 6, 2. Preparatory Works Senate 1981-1982, 296, nr. 1, 8.

[14] Article 8 of the Act of 8 August 1983.

[15] Act of 25 March 2003 to amend the Act of 8 August 1983 on the National Register of the natural person and the Act of 19 July 1991 on the population registers and the identity cards and amending the Act of 8 August 1983 on the National Register of the natural person, BSG 28 March 2003.

[16] Article 6, §2 Act of 19 July 1991 on the population registers, identity cards, foreigner's cards and residence permits and amending the Act of 8 August 1983 on the National Register of the natural persons, BSG 3 September 1991.

[17] Article 6, §2 Act of 19 July 1991.

[18] H. BUITELAAR, 'FIDIS - D13.3: Study on ID number policies', 14 September 2007, http://www.fidis.net, 25.

[19] § 16 (1) & (4) Registration Act 1991, Bundesgesetzblatt (BGBl.) nr. 9/1992, amended by BGBl. I nr. 135/2009.

[20] FEDERAL CHANCELLERY AUSTRIA, 'Administration on the Net: The ABC guide of eGovernment in Austria', July 2008, http://www.digitales.oesterreich.gv.at, 91-92.

[21] The sector-specific codes can be found in the EGovernment - Scope Ordinance, BGBl. II nr 289/2004.

[22] FEDERAL CHANCELLERY AUSTRIA, 'Administration on the Net: The ABC guide of eGovernment in Austria', July 2008, http://www.digitales.oesterreich.gv.at, 92-95.

[23] § 10 (1) and (2) Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E-Government Act), BGBl. nr. 10/2004.

[24] § 13 E-Government Act, BGBl. nr. 10/2004.

[25] § 4 (1) E-Government Act, BGBl. nr. 10/2004.

[26] § 4 (2) & (3) and § 7 (1) E-Government Act, BGBl. nr. 10/2004.

[27] IDABC, 'eID Interoperability for PEGS: Update of Country Profiles Study - Austrian Country Profile', http://ec.europa.eu/idabc, 6.

[28] The national Data Protection Authority has already advised against using this identification number beyond its original scope. DATENSCHUTZRAT, 'Stellungnahme Zur

Untersuchung von Alternativen zur Sozialversicherungsnummer in der Bildungsdokumentation', 25 February 2010, http://www.bka.gv.at.

[29] J. DUMORTIER, F. ROBBEN, 'User and Access management in Belgian E-Government' in N. POHLMANN, H. REIMER AND W. SCHNEIDER (ed.), Securing Electronic Business Processes. Highlights of the Information Security Solutions Europe 2009 Conference, Wiesbaden, Vieweg + Teubner Verlag, 2009, 97-107. Also in Belgium the national Data Protection Authority has advised against the use of sector-specific identifiers: PRIVACY COMMISSION, 'Opinion 14/2008 of 2 April 2008', http://www.privacycommission.be, paragraphs 58-65.

[30] Upheld by the German Supreme Court: Volkszählungsurteil, BVerfGE. 65, 1 et seq.

[31] Census 2011 Act of 8 July 2009, BGBl. I S.1781. '... keine 'Nummer für alle Zwecke' geben wird, denn das wäre datenschutzrechtlich kaum vertretbar', BUNDESMINISTERIUM DES INNERN, 'IT-Projekte im Überblick: Bundesmelderegister', 2007, http://www.deutschlandonline.de, 2.

[32] BUNDESAMT FUR SICHERHEIT IN DER INFORMATIONSTECHNIK, 'Common Criteria Profile: Electronic identity card', 2009, http://www.bsi.bund.de, 8.

[33] § 5 Identity Cards Act of 18 June 2009, BGBl 1 2009, 1346.

[34] § 1 Identity Cards Act.

[35] IDABC, 'eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability', 2009, http://ec.europa.eu/idabc, 52.

[36] IDABC, 'eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability', 2009, http://ec.europa.eu/idabc, 57.

[37] Article 9 (1) Act nr. 67/98 of 26 October 1998 on the protection of personal data, Diário Da República - I Série A nr. 247, 5538. This provision is also included under article 16 (2) of the Act nr. 7/2007 of 5 February 2007 on the creation, regulation and emission of the identity card, Diário da República 1, nr. 25, 942.

[38] Article 8 (2) Act nr. 7/2007.

[39] Article 7 (1) Act nr. 7/2007.

[40] Article 8 (1) Act nr. 7/2007.

[41] Section 18 of the Population Registration Act, Svensk Författningssamling (SFS) 1991:481; NATIONAL TAX BOARD, 'Population Registration in Sweden', 2007, http://www.skatteverket.se, 11.

[42] Personal Data Act, SFS 1998:204.

[43] Article 2, chapter 2 of the Freedom of the Press Act, SFS 1949:105.

[44] X, 'Skyddet för den personliga integriteten del II - kartläggning och analys', Statens Offentliga Utredningar (SOU) 2007:22, annex 6 to annex 4, 1.

[45] National Identity Cards Decree, 1 September 2009, SFS 2005:661. 45 IDABC, 'eID Interoperability for PEGS: Sweden Country Profile', 2009, http://ec.europa.eu/idabc, 13. 46 IDABC, 'eID Interoperability for PEGS: Sweden Country Profile', 2009, http://ec.europa.eu/idabc, 16-19. IDABC, 'eID Interoperability for PEGS: Analysis and

Assessment of similarities and differences - Impact on eID interoperability', 2009, http://ec.europa.eu/idabc, 53.

[46] IDABC, 'eID Interoperability for PEGS: Sweden Country Profile', 2009, http://ec.europa.eu/idabc, 13.

[47] IDABC, 'eID Interoperability for PEGS: Sweden Country Profile', 2009, http://ec.europa.eu/idabc, 16-19. IDABC, 'eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability', 2009, http://ec.europa.eu/idabc, 53.

[48] Identity Cards Act 2006 (c. 15).

[49] HOME OFFICE IDENTITY AND PASSPORT SERVICE, 'National Identity Service Tracking Research Wave 8: June 2009', 2009, http://www.ips.gov.uk, 6 et seq.

[50] Identity Documents Act 2010 (c. 40).

[51] The same number is used for tax purposes: Royal Decree 338/1990 of 9 March 1990 regulating the composition and the use of the Fiscal Identification Number, Boletín Oficial del Estado (BOE) nr. 63 of 14 March 1990, 7256-7259. A. HEICHLINGER, P. GALLEGO, 'A new e-ID card and online authentication in Spain', IDIS 2010, DOI 10.1007/s12394-010-0041-3, 2-3.

[52] Article 9 Organic Law 1/1992 of 21 February 1992 on the protection of the civil security, BOE nr. 46 of 22 February 1992, 6209-6214.

[53] Article 4 Royal Decree 196/1976 of 6 February 1976 on the regulations regarding the national identity document, BOE nr. 38 of 13 February 1976, 3014-3016. Organic Law 15/1999 of 13 December 1999 on the protection of personal data, BOE nr. 298 of 14 December 1999, 43088-43099. A. HEICHLINGER, P. GALLEGO, 'A new e-ID card and online authentication in Spain', IDIS 2010, DOI 10.1007/s12394-010-0041-3, 3.

[54] Article 11 of Law 59/2003 of 19 December 2003 on the electronic signature, BOE nr. 304 of 20 December 2003, 45329- 45343. Article 11 Royal Decree 1553/2003 of 23 December 2003 on the issuing of a national identity document and its certificates for electronic signatures, BOE nr. 307 of 24 December 2005, 42090-42093.

[55] Article 1 of Royal Decree 1553/2003 of 23 December 2003 on the issuing of a national identity document and its certificates for electronic signatures, BOE nr. 307 of 24 December 2005, 42090-42093.

[56] http://www.dnielectronico.es/Preguntas_Frecuentes/segur/index.html.

[57] Kamerstukken II 2005/06, 30 312, nr. 7, p. 5-6.

[58] For example: Act of 10 April 2008 on the use of the Citizen Service Number in the healthcare, Staatsblad (Stb.) 1998, 164.

[59] Article 3 (4) Act of 26 September 1991 concerning the issuance of travel documents (Passport Act), Stb. 1991, 498, last amended by Act of 11 June 2009 amending the Passport Act, Stb. 2009, 252.

[60] Article 1 and 2 Act of 9 December 1993 on the identity documents, Stb. 1993, 660, amended by the Act of 24 June 2004 amending the Act on the identity documents, Stb. 2004, 300.

[61] Article 3 (3) Passport Act.

[62] Regulation of the Secretary of State for Economic Affairs nr. WJZ/03/02263 of 6 May 2003 on the conditions regarding the electronic signatures, Staatscourant. 8 May 2003, 88.