ID-FIX

IDentification and Federal Inter-administration eXchange

EINDRAPPORT

Draft 3 12042010

Onderzoekers:
Niels Vandezande [ICRI]
Danny De Cock [COSIC]

SAMENVATTING

Dit project werd uitgevoerd in het kader van de vijfde oproep tot voorstellen voor de actie ter ondersteuning van de strategische prioriteiten van de Federale Overheid (AP5-F-043), gecoördineerd door het Federaal Wetenschapsbeleid. **ID-FIX** – Identification and Federal Inter-administrative eXchange (project AP/00/038) handelt in de eerste plaats over het gebruik van unieke identificatoren, zoals het Belgisch Rijksregisternummer. In dit project wordt onderzocht hoe het gebruik van unieke identificatoren zich verhoudt tot de bescherming van de persoonlijke levenssfeer, alsook wat de impact is van het in een Staat gehanteerde systeem van unieke identificatoren op de transparantie, efficiëntie en gebruiksvriendelijkheid van de overheidsdiensten.

Unieke identificatoren – onder de vorm van personeelsnummers, rekeningsnummers en dergelijke – zijn niet meer weg te denken uit de huidige samenleving. Deze identificatienummers zijn "uniek" in de zin dat zij slechts één enkele persoon op unieke wijze zullen identificeren. Binnen de Belgische overheid bestaat al een aantal jaren de tendens om het identificatienummer van het Rijksregister als unieke identificator voor de burger in de publieke sector te gebruiken. Het veralgemeend gebruik van het Rijksregisternummer als enige unieke identificator in alle overheidstoepassingen is echter een steeds weerkerend onderwerp van discussie en vormt al vele jaren een rem op de realisatie van verdere overheidsmodernisering. Dit project wil daarom op objectieve wijze de voor- en nadelen van dit onderdeel van het Belgisch beleid bestuderen op zowel juridisch als technisch vlak.

Daarnaast is er nog de problematiek van de **gegevenskoppelingen** die tot stand kunnen komen door het gebruik van het Rijksregisternummer. Dit identificatienummer kan immers door de verschillende overheidsdiensten gebruikt worden om onderling informatie over de betrokken burger uit te wisselen. Aangezien er bij zulke gegevensuitwisseling ook persoonsgegevens betrokken zullen zijn, zal men rekening moeten houden met de geldende regels op het gebied van de bescherming van de persoonlijke levenssfeer met betrekking tot de verwerking van persoonsgegevens. Deze regelgeving vereist bijvoorbeeld dat een dergelijke verwerking voldoende transparant is. In het geval van gegevenskoppelingen tussen de overheidsdiensten door gebruik te maken van het Rijksregisternummer, kan men spreken van voldoende transparantie indien de burger op gestructureerde wijze op de hoogte gebracht wordt van de precieze gegevenskoppelingen. Hij zal met andere woorden het volledige gegevensspoor willen traceren van oorsprong tot eindpunt. We kunnen vaststellen dat er onder de huidige stand van zaken geen sprake is van een voldoende transparantie op het gebied van gegevenskoppelingen door het gebruik van het Rijksregisternummer. Het betreft hier bijgevolg een belangrijke materie die verder onderzocht moet worden.

In het eerste deel van het project wordt het **veralgemeend gebruik van het Rijksregisternummer in de Belgische overheidscontext** onderzocht. Dit onderzoek vangt aan met een kort overzicht van een aantal historische evoluties met betrekking tot identificatie en het gebruik van unieke identificatoren. Er zal geconcludeerd worden dat men twee belangrijke modellen kan aanduiden: het gebruik van een enkele unieke identificator – zoals in België en Zweden – en het gebruik van meerdere sectorgebonden identificatoren – zoals in Duitsland, Oostenrijk en Portugal. Na het bespreken van een aantal van de belangrijkste bouwstenen van het Belgisch beleid

met betrekking tot e-Government volgt een rechtsvergelijkend onderzoek waar het Belgisch beleid vergeleken wordt met dat van een aantal andere Europese lidstaten. Uit dit onderzoek zal blijken dat het huidige beleid van landen die een systeem van sectorgebonden identificatoren hanteren niet noodzakelijk leidt tot een meer transparante en efficiënte overheid. We concluderen daarom dat het huidige Belgisch beleid met betrekking tot het gebruik van een enkele unieke identificator binnen de gehele overheidssector wel verdedigd kan worden vanuit het standpunt van de transparantie, efficiëntie en privacybescherming. We merken hier echter wel bij op dat er toch een aantal punten zijn waar het huidige Belgisch beleid wel voor verbetering vatbaar is. Zo wordt er aangehaald dat de aanwezigheid van het Rijksregisternummer in het authentiseringscertificaat op de e-ID op gespannen voet staat met de gereguleerde status van dit identificatienummer. Om een dergelijke tegenstrijdigheid in het Belgisch beleid te verhelpen, stellen we een uitbreiding van het *Online Certificate Status Protocol* voor. Dit onderwerp zal onder het derde deel van het project nader onderzocht worden.

Daarnaast kan men zich nog de vraag stellen of het gebruik van een dergelijk nationaal identificatienummer **vrij of gereguleerd** moet zijn. Het Belgisch Rijksregisternummer is bijvoorbeeld sterk gereguleerd en kan slechts bij voorafgaande machtiging toegestaan worden. Het Zweeds equivalent van dit nummer is echter relatief vrij te gebruiken in zowel de publieke als de private sector. In dit project wordt daarom onderzocht onder welke omstandigheden men een geliberaliseerd gebruik van een dergelijk nationaal identificatienummer kan verdedigen. Voor België kan men in de eerste plaats denken aan een verruiming van de transparantie met betrekking tot het gebruik van het Rijksregisternummer, alsook van de gegevenskoppelingen die men kan maken door het gebruik van dit identificatienummer.

In het tweede deel van het project wordt gezocht naar een manier om het veralgemeend gebruik van het Rijksregisternummer te compenseren, door de transparantie van dit gebruik en de controlemogelijkheden voor de burger te vergroten. We denken hier aan het **Kadaster van Verbindingen**. Dit Kadaster zou een portaal vormen dat de burger – na authenticatie door middel van zijn e-ID – in staat stelt om te bekijken welke koppelingen van de persoonsgegevens die op hem betrekking hebben, worden gemaakt door gebruik te maken van het Rijksregisternummer. Hoewel de aanzet tot het Kadaster van Verbindingen al gevonden kan worden in de Wet op het Rijksregister, is men nog niet overgegaan tot de werkelijke realisatie van zulk project. In dit luik van het onderzoek willen we daarom komen tot een praktijkgerichte conceptstudie. We onderzoeken daarom in een eerste stap wat men onder het concept ‘Kadaster van Verbindingen’ dient te verstaan. Er wordt onder meer stilgestaan bij het nut van het Kadaster op zich en bij de inhoud van de logs waarvan het Kadaster aan de burger een gestructureerd overzicht zal bieden. In een tweede stap wordt gekeken naar een aantal juridische, praktische en technische problemen die men zal ondervinden bij de realisatie van het Kadaster van Verbindingen. Zo onderzoeken we de betrokken actoren, het benodigde wettelijk kader en het niveau waarop het Kadaster georganiseerd moet worden. De bevindingen van dit onderzoek worden samengebracht in een aantal praktische aanbevelingen bij de realisatie van het Kadaster van Verbindingen.

Het Kadaster van Verbindingen zal voornamelijk aanzien moeten worden als een **transparantieverhogende maatregel** die moet leiden tot effectieve transparantie met betrekking tot enerzijds het gebruik van het Rijksregisternummer en anderzijds van de gegevenskoppelingen die gemaakt worden door het gebruik van een dergelijk identificatienummer. Er zal daarom aangetoond worden dat het Kadaster een interessante maatregel kan zijn voor de verbetering van het huidige beleid. Daarnaast zal blijken dat het zelfs een noodzakelijk voorwaarde zal zijn indien men naar de toekomst toe zou willen evolueren naar een meer geliberaliseerd gebruik van het Rijksregisternummer.

Het derde deel van het project bestaat uit een technisch onderzoek naar de eerder aangehaalde uitbreiding van het ***Online Certificate Status Protocol***. Er wordt onderzocht hoe zulke uitbreiding uitgevoerd kan worden zodat bestaande toepassingen zonder – of met hoogstens minimale – aanpassingen kunnen blijven werken. Ook moet het mogelijk zijn om te bepalen of twee verschillende authentiseringscertificaten waarvan men vermoedt dat ze bij eenzelfde burger horen ook werkelijk bij elkaar horen. Dit kan gerealiseerd worden door ervoor te zorgen dat de OCSP-server naast de gewone taken controleert of de aanvrager gemachtigd is om het Rijksregisternummer te gebruiken. Indien dit het geval is, zal de OCSP-server naast het klassieke antwoord ook bijkomende informatie, namelijk het Rijksregisternummer, doorgeven. Om te voldoen aan het tweede criterium, kan de OCSP-aanvraag uitgebreid worden met een referentie aan het authentiseringscertificaat waarvan vermoed wordt dat het hoort bij dezelfde burger die hoort bij het te controleren authentiseringscertificaat.

Onder het vierde deel worden de bevindingen uit het gevoerde onderzoek samengebracht in een **eindconclusie**. Hier blijkt dat er in het huidige Belgisch beleid enigszins een gebrek aan consequentie bestaat. Hoewel het huidige gereguleerd gebruik van het Rijksregisternummer verdedigd kan worden vanuit het standpunt van de privacybescherming, blijkt dit beleid te conflicteren met een aantal andere aspecten van het Belgisch beleid – zoals de in dit onderzoek besproken aanwezigheid van het Rijksregisternummer in het authentiseringscertificaat op de e-ID. Indien men het gereguleerd gebruik van het Rijksregisternummer wil behouden, lijkt het ons daarom aanbevelingswaardig om zulke conflictpunten aan te pakken. Anderzijds blijkt uit dit onderzoek dat de grootste bedreiging voor de privacybescherming niet voortkomt uit het veralgemeend gebruik van het Rijksregisternummer binnen de overheidscontext op zich, maar uit de gegevenskoppelingen die gemaakt worden door het gebruik van het Rijksregisternummer. We pleiten daarom voor de realisatie van het Kadaster van Verbindingen als portaal dat de burger op gestructureerde wijze inzage kan bieden in deze gegevenskoppelingen. Door middel van zulke transparantieverhogende maatregel, zou men zelfs binnen de private sector kunnen denken aan het vrij gebruik van het Rijksregisternummer, mits expliciete en ondubbelzinnige toestemming van de betrokkene.

RESUME

Cette étude fait partie du cinquième appel à propositions pour l'action en soutien aux priorités stratégiques de l'autorité fédérale (AP5-F-043), coordonné par la Politique Scientifique Fédérale. **ID-FIX** – Identification and Federal Inter-administrative eXchange (projet AP/00/038) porte principalement sur l'utilisation des identificateurs uniques, comme le numéro d'identification du Registre National belge. Dans ce projet, nous examinerons comment l'utilisation d'identificateurs uniques est liée à la protection de la vie privée, ainsi que l'impact d'un système d'identificateurs uniques utilisés par l'Etat sur la transparence, l'efficacité et la convivialité des services publics.

Il n'est pas possible aujourd'hui d'imaginer la société sans **identificateurs uniques** – que ce soient des numéros personnels, des numéros de compte ou autres. Ces numéros d'identification sont «uniques» en ce qu'ils identifieront une seule personne. Il est possible d'observer dans le secteur public belge, depuis nombreuses d'années, une tendance à utiliser le Numéro du Registre National comme identificateur unique des administrés. L'utilisation généralisée du Numéro National comme seul identificateur dans toutes les applications du gouvernement est un sujet de discussion récurrent et fait obstacle à un approfondissement de la modernisation de l'État. Ce projet veut donc analyser objectivement les avantages et les inconvénients de cet élément de la politique belge d'un point de vue juridique et technique.

Ce projet traite également des de **connexions au réseau** découlant de l'utilisation du Numéro National. Cet identificateur peut en effet être utilisé par les différentes autorités pour l'échange d'information relatives à un citoyen donné. Cet échange impliquant nécessairement un échange de données personnelles, il faudra tenir compte des règles applicables à la protection de la vie privée à l'égard du traitement des données personnelles. Ces règles exigent par exemple que ce traitement soit exécuté avec suffisamment de transparence. Dans le cas des connexions au réseau découlant de l'utilisation du Numéro National par les administrations, le niveau de transparence sera suffisant si le citoyen est informé d'une manière exacte et structurée des connexions au réseau réalisées. Le citoyen doit donc être en mesure de retracer toutes les connexions au réseau. Force est de constater qu'en l'état actuel des choses, le niveau de transparence n'est pas suffisant en la matière Il s'agit donc d'une question importante qui doit être examinée de manière approfondie.

La première partie du projet examine **l'utilisation généralisée du Numéro National dans le secteur public belge**. Cette étude commence avec un sommaire de certaines évolutions historiques concernant l'identification et l'utilisation des identificateurs uniques. Deux modèles principaux peuvent être distingués: l'utilisation d'un identificateur unique – comme en Belgique et en Suède – et l'utilisation d'identificateurs sectoriels – comme en Allemagne, en Autriche et au Portugal. Après avoir discuté les piliers de la politique belge en matière d'e-Gouvernement, cette politique sera comparée avec celle menée dans d'autres pays européens. Cette étude comparative permettra de montrer que l'option pour un système d'identificateurs sectoriels ne résulte pas nécessairement en un gouvernement plus transparent ou plus efficace. Nous constatons donc que la politique belge concernant l'utilisation d'un identificateur unique dans tout le secteur public peut être défendue du point de vue de la transparence, l'efficacité et la protection de la vie privée. Nous notons toutefois qu'il y a un nombre de points où la politique belge ac-

tuelle pourrait être améliorée. C’est le cas par exemple de la présence du Numéro National dans le certificat d’autorisation sur l'e-ID alors que ce numéro bénéficie d’un statut protégé. Afin de surmonter cette contradiction nous proposons une extension de l’*Online Certificate Status Protocol*. Ce sujet sera examiné dans la troisième partie du projet.

La question se pose également de savoir si l'utilisation d’un tel identificateur national devrait être **libre ou réglementée**. Le Numéro National belge est fortement réglementé et ne peut être utilisé qu’après obtention d’une autorisation préalable. Contrairement à la Belgique, la Suède s’est dotée d’un numéro national qui peut être utilisé de manière relativement libre tant par le secteur public que par le secteur privé. Ce projet va donc examiner les circonstances dans lesquelles l'utilisation libre d’un tel identificateur national peut être défendue. Il est proposé pour la Belgique d’augmenter la transparence de l'utilisation du Numéro National, et les connexions au réseau découlant de l'utilisation de ce nombre d’identification.

Dans la deuxième partie du projet, nous cherchons comment l'utilisation généralisée du Numéro National peut être compensée en augmentant la transparence d’utilisation et les possibilités de contrôle pour les citoyens. Dans cette perspective, il est proposé de créer un **Cadastre des Connexions**. Ce Cadastre constituerait un portail permettant au citoyen – après authentification en utilisant son e-ID – de retracer les connexions au réseau découlant de l'utilisation de ce nombre d’identification. Bien que le principe du Cadastre des Connexions au réseau puisse être trouvé dans la loi sur le Registre National, ce projet n’a pas été mené en pratique.. Cette partie du rapport sera consacrée à une étude de concept pratique. Nous étudions dans une première étape ce que recouvre le concept « Cadastre des Connexions ». Seront explorés par exemple les avantages que présentent la mise en place d’un tel Cadastre, ainsi que le contenu des journaux que le Cadastre offre au citoyen lors d’un accès structuré. Dans la deuxième partie plusieurs problèmes juridiques, pratiques et techniques susceptible d’apparaître lors de la réalisation du Cadastre des Connexions sont analysés. Cela inclut par exemple les acteurs concernés, le cadre juridique requis et le niveau d’organisation du Cadastre. Les résultats de cette recherche seront présentés sous la forme de recommandations pratiques en vue de la réalisation dudit Cadastre.

Le Registre des Connexions doit principalement être vu comme **une mesure de transparence**, menant à une transparence réelle en ce qui concerne l'utilisation du Numéro National et les connexions au réseau découlant de l’utilisation de ce numéro d’identification. Il sera donc démontré que le Registre des Connexions peut contribuer à améliorer la politique actuelle et qu’il est même une condition nécessaire si l’on veut évoluer dans l'avenir vers une utilisation plus libre du Numéro National.

La troisième partie du projet comprend une étude technique sur l'extension de l’***Online Certificate Status Protocol***. On examine comment une telle extension peut être mise en œuvre afin que les applications existantes puissent continuer à travailler sans aucun ou avec des ajustements minimaux. Il devrait également être possible de déterminer si deux certificats d’autorisation différents, dont on soupçonne qu’ils appartiennent au même citoyen, peuvent être regroupés. Ceci peut être réalisé pour permette au serveur OCSP, en plus de ses tâches régulières, de vérifier que l’auteur de la requête est autorisé à utiliser le Numéro National. Dans ce cas, le serveur OCSP ajoutera l’information complémentaire, le Numéro National, à la réponse classique. Pour répondre à la deuxième demande la référence au certificat d’autorisation soupçonné d’appartenir à un même citoyen pourra être ajoutée à la requête OCSP.

La quatrième partie présente **les résultats de la recherche**. Certaines incohérences de la politique belge actuelle sont tout d'abord mises en lumière. Bien que l'utilisation réglementée actuelle du Numéro National puisse être défendue du point de vue de la protection de la vie privée, cette politique semble entrer en conflit avec d'autres aspects de la politique belge – comme par exemple la présence du Numéro National dans le certificat d'autorisation à l'e-ID examiné dans cette étude. Si le statut protégé du Numéro National est maintenu en l'état, il semble opportun de régler ces contradictions. En outre, cette étude montre que la plus grande menace à la vie privée n'est pas en soi posée par l'utilisation généralisée du Numéro National par le secteur public, mais par les croisements de données personnelles réalisées grâce à l'utilisation du Numéro National. Nous plaidons donc pour la mise en œuvre d'un Cadastre des Connexions comme un portail qui offrirait aux citoyens accès structuré aux croisements de données. En utilisant une telle mesure pour augmenter la transparence, il serait possible de libéraliser l'utilisation du Numéro National, même dans le secteur privé, à la condition que le citoyen ait donné au préalable son consentement de manière explicite et univoque.

SUMMARY

This research project was conducted in the framework of the fifth call for proposals in the action in support of the Federal Authority's strategic priorities (AP5-F-043), coordinated by the Federal Science Policy. **ID-FIX** – Identification and Federal Inter-administrative eXchange (project AP/00/038) is focused on the use of unique identifiers, such as the Belgian National Number. In this project, we will look at the influence of the use of such identifiers on the protection of the privacy, as well as at the impact of the system of unique identifiers employed in a State on the transparency, efficiency and usability of government services.

Unique identifiers – be it in the shape of staff numbers, account numbers or others – are omnipresent in our current society. These identification numbers are "unique" in the sense that they will only identify one single person. For a number of years, the Belgian government has been using the identification number of the Belgian National Register as a unique identifier in the public sector. This generalized use of the National Number as the single unique identifier used by all government agencies is, however, highly disputed and this discussion has for many years stalled the implementation of projects for the modernization of the government. Therefore, this project aims to objectively analyze the benefits and drawbacks of this part of the Belgian policy from both a legal and technical point of view.

Apart from the problem of the generalized use of the National Number, there is also the problem of the **data interconnections** that can be made by using such an identification number. Different government agencies can use this identification number to exchange information on the citizen. As such a data exchange will most likely involve the exchange of personal data one will have to abide by the rules set forth in the field of the protection of the privacy concerning the processing of personal data. These rules demand, amongst others, that the processing of personal data has to be sufficiently transparent. When considering data interconnections between government agencies that are made by using the National Number, one can deem such a processing to be sufficiently transparent when the citizen will be notified in a structured manner of the precise data interconnections that involve his personal data. In other words, he will want to trace the entire trail of data interconnections from start to finish. We can conclude that under the current state of affairs there is no sufficient transparency in the field of data interconnections that are made by using the National Number. This can therefore be considered to be an important matter worthy of further investigation.

In the first part of the project we analyze the **generalized use of the National Number in the Belgian public sector**. The research commences with a short overview of a number of historical evolutions concerning identification and the use of unique identifiers. We identify two main categories here: the use of a single unique identifier – as used in Belgium and Sweden – and the use of several sector-specific unique identifiers – as used in Austria, Germany and Portugal. After analyzing a number of the most important pillars of the Belgian policy regarding e-Government, we conduct a comparative research in order to compare these pillars to the policy of a number of other European member states. From this research, we conclude that the current policy of States using sector-specific unique identifiers will not necessarily lead to a more transparent or more efficient government. We therefore conclude that the current Belgian policy concerning the use of a single unique identifier for use throughout the whole public sector

can be defended from a transparency, efficiency and privacy point of view. However, we do stress that there are a number of issues present in the current Belgian policy that could use some improvement. We note, for example, that the presence of the National Number on the authentication certificate on the e-ID is at odds with the regulated status of this particular identification number. To solve such a contradiction in the current Belgian policy, we propose an extension to the Online Certificate Status Protocol. The research on how to achieve such extension to this protocol will be conducted under the third part of this project.

One also needs to consider whether the use of such a national identification number needs to be **liberalized or regulated**. The use of the Belgian National Number, for example, is highly regulated and this identification number can only be used after acquiring the proper authorization. The Swedish equivalent of this identification number, by contrast, can relatively freely be used in both the public and the private sector. In this project, we therefore investigate the circumstances under which a more liberalized use of a national identification number can be defended. In the case of Belgium, one can consider enhancing the transparency of the use of the National Number, as well as of the data interconnections that are made by using this identification number.

In the second part of the project we search for a way to compensate the generalized use of the National Number by adding transparency to this use and by enlarging the possibilities for citizen control. We focus our research on the **Register of Connections**. This Register will become a portal where the citizen – after identifying himself by using his e-ID – will be able to see which interconnections of his personal data have been made by using the National Number. Even though the notion of the Register of Connections is already present in the current version of the Act on the National Register, it has never been implemented. In this part of the project, we therefore aim to provide a conceptual framework for the practical implementation of this Register of Connections. In a first step, we look at what we can gather from the concept of the 'Register of Connections'. We analyze whether there is a use for this kind of Register and we look at the contents of the logs of which the Register will provide the citizen with a structured overview. In the second phase, we analyze a number of the legal, practical and technical problems that will be encountered when implementing the Register of Connections. We look at the actors involved in the Register, the necessary legal framework and the level at which we need to visualize this Register. The findings of this research are brought together in a number of practical recommendations for the implementation of the Register of Connections.

The Register of Connections will mainly have to be considered as a **privacy-enhancing measure** which should lead to more and effective transparency concerning the use of the National Number on the one hand, and the data interconnections that are made by using this identification number on the other hand. It is therefore the aim of this research to demonstrate that the Register of Connections can be an interesting measure for improving the transparency of the current policy in this field. Apart from this, it is also demonstrated that this register will be a necessary measure in order to evolve to a system that allows for a more liberalized use of the National Number.

In the third part of the project, technical research is conducted on the extension to the **Online Certificate Status Protocol** mentioned earlier. We analyze how such extension can be attained by at the same time ensuring that all existing applications will remain functional requiring no or minimal adaptations. It will also have to be possible to determine whether two different authentication certificates that are suspected to belong to the same citizen do indeed belong together. We attempt to meet these conditions by enabling the OCSP-server to check – next to his regular tasks – whether the applicant is authorized to use the National Number. If this is the case, then the OCSP-server will provide additional information – in this case: the National Number – together with the regular response. To meet the second condition, we try to broaden the OCSP-request with a reference to the authentication certificate that is believed to be connected to the same citizen as the one connected to the authentication certificate of which the validity status is requested to the OCSP-server.

In the final part of the project all conclusions from the previous research are brought together for a number of **concluding observations**. Here, it will become apparent that there is a lack of consistency present in the Belgian policy. Even though research points out that the current regulated use of the National Number can be defended from a privacy point of view, this policy seems to conflict with a number of other aspects of the Belgian policy – like the aforementioned presence of the National Number on the authentication certificate on the e-ID. If the government wishes to maintain the regulated use of the National Number, it seems recommendable to find a solution for such inconsistencies. On the other hand, research also points out that the biggest threat to the protection of the privacy is not the generalized use of the National Number – as is often believed – but the interconnections of personal data that are made by government agencies by using the National Number. We therefore advocate the implementation of a Register of Connections as a portal that can provide the citizen with insight in these data interconnections. By employing a transparency augmenting measure like this, one might start to think about allowing even the private sector to evolve towards the free use of the National Number, under the condition of express and unambiguous consent of the party concerned.

INHOUD

Federaal Wetenschapsbeleid
Actie ter ondersteuning van de strategische prioriteiten van de Federale Overheid
AP/00/038

DEEL I: HET VERALGEMEEND GEBRUIK VAN HET RIJKSREGISTERNUMMER BINNEN DE OVERHEIDSSECTOR

1. INLEIDING

1.1. DOEL VAN HET ONDERZOEK

DE ENKELE UNIEKE IDENTIFICATOR - Unieke identificatoren zijn niet meer uit de dagelijkse praktijk weg te denken. Elke burger kan door verschillende administraties herkend worden door middel van personeelsnummers, studentennummers of rekeningnummers. Het gegeven dat zulke identificator ‘uniek’ moet zijn, wil in deze context zeggen dat elke persoon op unieke wijze geïdentificeerd moet kunnen worden en dat men dus zeker kan zijn over de identiteit van de betrokken persoon. In België wordt hiertoe binnen overheidstoepassingen quasi uitsluitend het Rijksregisternummer gebruikt. Het gebruik van enkel het Rijksregisternummer voor verschillende overheidstoepassingen is het perfecte voorbeeld van wat we het gebruik van een enkele unieke identificator noemen. De identificator is uniek in de zin dat er slechts één enkele persoon geïdentificeerd kan worden aan de hand van het nummer. Daarnaast is het Rijksregisternummer het enige nummer dat men binnen de overheidscontext als identificator gebruikt. Het gaat daarom om een enkele unieke identificator.

SECTORGEBONDEN IDENTIFICATOREN - Als alternatief op het gebruik van een enkele unieke identificator, kan men ook verschillende unieke identificatoren gebruiken. Die kunnen dan bijvoorbeeld sectorgebonden - of zelfs regiogebonden - zijn. Hoewel er uiteraard nog andere variaties op dit thema onderscheiden kunnen worden, is het duidelijk dat de meeste landen een keuze hebben gemaakt tussen de enkele unieke identificator en sectorgebonden identificatoren.

OPZET VAN HET ONDERZOEK - In dit onderzoek zullen we eerst kort een overzicht geven van een aantal historische evoluties met betrekking tot identificatie en het gebruik van unieke identificatoren. Gelet op de technische aard van het onderwerp volgt daarna een glossarium van een aantal voor deze problematiek relevante begrippen (1.3). In een volgend deel van het onderzoek zal het huidige Belgisch beleid op het gebied van unieke identificatoren onder de loep genomen worden (2.1). De bevindingen van dat onderzoek zullen gebruikt worden in de daarop volgende rechtsvergelijkende studie (2.2). In deze studie zullen we voor een aantal Europese landen zoeken naar de bouwstenen van hun eigen beleid op het vlak van e-Government en zullen we trachten deze bouwstenen te vergelijken met die uit het Belgisch beleid. In een volgende fase (3) zal een meer technisch gericht onderzoek gevoerd worden naar wat er op technologisch vlak nog mogelijk is voor het Belgisch beleid. Het is ons doel om in dit deel van het onderzoek een aantal praktische aanbevelingen te formuleren waarmee het huidige beleid verder op punt gesteld kan worden.

AANZET TOT DEEL II - Tot slot zullen deze laatste bevindingen, alsook die van het voorgaande onderzoek, verwerkt worden in een conclusie voor dit onderzoek. Deze conclusie zal dienen als aanzet voor het tweede deel van het ID-FIX project, namelijk het Kadaster van Verbindingen.

1.2. HISTORISCH OVERZICHT

IDENTIFICATOREN HISTORISCH BEKEKEN - Het debat over het gebruik van unieke identificatoren is uiteraard geen puur Belgisch probleem. De geschiedenis van de notie 'identificatie' wijst uit dat quasi elk land vroeger of later geconfronteerd wordt met deze vraag. Het spreekt voor zich dat niet alle landen die vraag op dezelfde manier beantwoorden: wat goed werkt voor het ene land kan onwerkbaar blijken voor het andere land. We worden daarom in deze materie geconfronteerd met een gamma aan verschillende oplossingen die algemeen genomen ingedeeld kunnen worden onder twee categorieën. De landen uit de eerste categorie hanteren een enkele unieke identificator, zoals België, de landen uit de tweede categorie hanteren meerdere sectorgebonden unieke identificatoren, zoals Oostenrijk. Ook op Europees vlak zal blijken dat het onmogelijk is om die vraag eenduidig te beantwoorden. De Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens blijft maar zeer vaag over deze materie.[1] De hoofdreden hiervoor is uiteraard het gegeven dat de Europese lidstaten er in deze materie zeer uiteenlopende standpunten op na houden. Die standpunten zijn op hun beurt dan weer het gevolg van een historische ontwikkeling die we hier voor een aantal landen kort willen onderzoeken.[2] [3]

NOOD AAN IDENTIFICATIE - Een historisch onderzoek naar deze materie kan ook nuttig zijn omdat de nood aan identificatie alleszins geen nieuw gegeven is. De mens wil immers van nature uit weten met wie hij te maken heeft (identificatie) en of die persoon ook werkelijk is wie hij of zij beweert te zijn (authenticatie). In de oudste vormen van gemeenschappen was dat eenvoudig: de groep was zo klein dat iedereen elkaar kende.[4] We zien dat hier de intrinsieke waarde van identificatie al aanwezig is: men kende elkaar en wist dus met wie men te maken had. Toen de gemeenschappen - en later de stadstaten - groeiden, werd dat systeem van sociale controle echter onhoudbaar. Het is op dit punt dat overheden besloten om zelf informatie over hun onderdanen te verzamelen.[5]

DE VOLKSTELLING - Een historisch veelvuldig gebruikte manier om informatie over de bevolking te verzamelen, is de *census* of volkstelling, die we in West-Europa kunnen zien de volkstelling sterk opkomen vanaf de zeventiende en achttiende eeuw.[6] Ondanks het feit dat volkstellingen al voorkwamen in enkele van de vroegste beschavingen, werden de gegevens die hieruit gewonnen werden aanvankelijk niet voor identificatie gebruikt. De eerste volkstellingen kwamen er voornamelijk uit fiscale overwegingen of om de potentiële troepenmacht vast te stellen.[7]

[1] Artikel 8.7 richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb. L*. 23 november 1995, afl. 281, 31-50.
[2] Voor een overzicht van deze en meer landen: MODINIS/IDM, "National IDM Profiles", *www.cosic.esat.ku leuven.be/modinis-idm*; EUSER, "Country Briefs", *www.euser-eu.org*.
[3] Voor een meer compleet overzicht over de totstandkoming van de privacy-wetgeving in Europa in het bijzonder, zie: M.W. HEYDRICH, "A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract", 25 *Brook. J. Int'l L*., 1999, 417-422.
[4] FIDIS, "D13.3: Study on ID number policies", 14 september 2007, *www.fidis.net,* 13.
[5] *epic.org/privacy/census.*
[6] *www.ons.gov.uk/census.*
[7] De Romeinse censor is hier het bekendste voorbeeld van, zie: W. SMITH, *Dictionary of Greek and Roman Antiquities,* Boston, Little Brown and Company, 1870, 261-262; *www.ancientlibrary.com/smith-dgra.Ook* veel later vinden we nog

Volkstellingen ter identificatie zien we pas vanaf de 15de en 16de eeuw opkomen, voornamelijk onder invloed van de Kerk.[8] Vanaf de Middeleeuwen zien we ook sporadisch identiteitsdocumenten - zij het voornamelijk reispaspoorten - verschijnen.[9] Vanaf de Franse Revolutie zien we ook de opkomst van de eigenlijke identiteitskaart. Opmerkelijk is dat deze aanvankelijk vooral in tijden van onrust ingevoerd werd.[10]

1.2.1. DUITSLAND

EEN BELADEN GESCHIEDENIS - Van de West-Europese landen waren in de 19de eeuw vooral de volkstellingen van het Duitse Rijk - en ook al eerder onder Jozef II in het Heilig Roomse Rijk - bekend.[11] De resultaten van diezelfde volkstellingen werden echter in de jaren '30 door het Naziregime gebruikt om volledige controle over de bevolking - en bepaalde bevolkingsgroepen in het bijzonder - uit te oefenen. Zo beweren bepaalde historici dat men de volkstellingen misbruikte als middel om Joden op te sporen in de zogenaamde Kristalnacht van 9 op 10 november 1938.[12] Als gevolg hiervan werd het recht op privacy opgenomen in de naoorlogse grondwet. Ook het hoogste gerechtshof waakt erover dat nieuwe vormen van gegevensinzameling slechts onder zeer strikte voorwaarden mogelijk zijn.[13] Duitsland kent daarnaast ook een strenge privacywetgeving.[14]

VERBOD OP HET GEBRUIK VAN EEN ENKELE UNIEKE IDENTIFICATOR - Dankzij deze verregaande bescherming van de persoonlijke levenssfeer kent Duitsland geen nationaal persoonsnummer. Men gebruikt daarom een hele waaier aan unieke identificatoren voor de verschillende overheidstoepassingen. Sinds 2005 probeert de overheid een elektronische identiteitskaart te introduceren, met de beveiliging ervan als belangrijkste criterium.[15] Recent is de wet ter implementatie van de Duitse e-ID aangenomen, welke na een reeks proefprojecten pas in werking zal treden op 1 november 2010.[16]

1.2.2. ANGELSAKSISCHE LANDEN

voorbeelden van censussen voor fiscale redenen, zie ondermeer het *Domesday Book* uit 1086. Op vraag van William I werden hier enkel de grondbezitters opgenomen, *www.nationalarchives.gov.uk/documentsonline/domesday.asp.*

[8] FIDIS, "D13.3: Study on ID number policies", 14 september 2007, *www.fidis.net,* 14.

[9] FIDIS, "D13.3: Study on ID number policies", 14 september 2007, *www.fidis.net,* 15.

[10] Zo kwamen de eerste Franse identiteitskaarten er voornamelijk om bepaalde individu's te registreren. Ook tijdens oorlogen waren identiteitskaarten zeer populair, zie ondermeer Duitsland en het Verenigd Koninkrijk in beide wereldoorlogen.

[11] Onder Jozef II werden de registers van de Kerk geleidelijk aan door de Staat overgenomen. Ook onder de Franse Revolutie vinden we het idee van Staatsgecontroleerde bevolkingsregisters terug.

[12] L.C. KRAMER, "Private Eyes Are Watching You: Consumer Online Privacy Protection – Lessons from Home and Abroad", 37 *Tex. Int'l L.J.*, 2002, 397.

[13] Zie het zogenaamde Volkszählungsurteil, *BVerfGE* 65, 1 e.v.

[14] Bundesdatenschutzgesetz (BDSG), *BGBl.I* 1990 S.2954, laatste amendering 14 augustus 2009, *BGBl. I* S. 2814.

[15] Meer details zijn te vinden in de zogenaamde eCard-Strategie van de Duitse Bondsregering die aangenomen werd in 2005, *www.einblick.dgb.de/hintergrund/2008/13/chipkartenstrategie.pdf.*

[16] Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weitere Vorschriften van 18 juni 2009, *BGBl. I* nr. 33/2009, 1359.

VERENIGDE STATEN VAN AMERIKA - Net als Duitsland kennen de Angelsaksische landen een stevige geschiedenis van volkstellingen. In de Verenigde Staten van Amerika is de census zelfs grondwettelijk geregeld.[17] Toch zullen we zien dat deze landen geen goede ervaringen hebben met identiteitsbewijzen en dat pogingen om zulk document in te voeren steeds verkeerd zijn afgelopen.

SOCIAL SECURITY NUMBER - De Verenigde Staten kennen in principe geen enkele unieke identificator. Men heeft sinds 1936 echter wel een identificatienummer van de sociale zekerheid (het *Social Security Number)*, wat doorheen de jaren een veel ruimere rol is gaan vervullen.[18] Vandaag kan dit nummer voor talloze toepassingen gebruikt worden en wordt het zelfs gebruikt als bewijs van identiteit.[19] Men zou daarom kunnen stellen dat het *de facto* de rol van een nationaal identificatienummer op zich genomen heeft.[20] Het nummer van de sociale zekerheid is in principe niet de enige unieke identificator die men gebruikt in de Verenigde Staten, maar het is wel veruit de belangrijkste.[21]

IERLAND - Een gelijkaardig verhaal vinden we terug in Ierland. Het persoonlijk nummer voor openbare diensten (*Personal Public Service Number)* is net als het Amerikaanse nummer van de sociale zekerheid van oorsprong een identificator voor de sociale zekerheid. Dit nummer wordt intussen *de facto* gebruikt als enige unieke identificator voor de publieke administratie, maar kan niet beschouwd worden als een nationaal identificatienummer.[22] In die zin kan het dus ook niet beschouwd worden als de enige unieke identificator in Ierland, hoewel het in de praktijk wel zo gebruikt lijkt te worden.

VERENIGD KONINKRIJK - Ook het Verenigd Koninkrijk kent een gelijkaardig verhaal met het nummer van de sociale zekerheid (*National Insurance Number)* dat haar oorspronkelijk doel overstegen heeft en intussen in het dagelijkse leven vaak als een enige unieke identificator gebruikt wordt.[23] Net als in Ierland is dit oneigenlijk gebruik in principe niet toegelaten door de overheid zelf.[24] Recent heeft het Verenigd Koninkrijk nieuwe wetgeving aangenomen om een identiteitskaart in te voeren.[25] Die kaart zal gepaard gaan met het oprichten van een personenregister (het *National Identity Register)*, wat veel uitgebreider zal worden dan het Belgisch Rijksregister.[26]

[17] Artikel 1, sectie 2, derde lid Constitution of the United States of America, 17 september 1787, *www.law.cornell.edu/constitution.* Belangrijk is dat de census in de Verenigde Staten niet bedoeld is om de bevolking te identificeren, maar om de zetelverdeling in het Congres te bepalen.

[18] Zo verwijzen bepaalde wetten naar het gebruik van het SSN, 42 *U.S.C.* § 405(c)(2). Het is echter wel duidelijk dat het SSN aanvankelijk niet bedoeld was als algemeen identificatiemiddel: dit werd zelfs letterlijk vermeld op de kaart zelf, *www.nytimes.com/1998/07/26/weekinreview/the-nation-not-for-identification-purposes-just-kidding.html*.

[19] *www.americanchronicle.com/articles/view/3911.*

[20] Men wenst dit gebruik echter tegen te gaan. De Social Security zelf raadt de burgers af om het SSN buiten wettelijk bepaalde gevallen te gebruiken. Voor meer informatie, zie de *Frequently Asked Questions* op *ssa-custhelp.ssa.gov*.

[21] Naast het SSN is er nog het rijbewijs. Intussen is er ook de zogenaamde *REAL ID Act* uit 2005. Deze wet wil het rijbewijs of een identiteitskaart de enige officiële identiteitsbewijzen maken. Op dit moment is het echter nog niet zeker of deze wet ooit geïmplementeerd zal worden.

[22] De Ierse overheid kijkt streng toe op het gebruik van het PPS-nummer en benadrukt expliciet dat het PPS nummer geen unieke nationale identificator is. Zie ook: www.welfare.ie.

[23] Daarnaast is er ook nog het nummer van de *National Health Service* dat gebruikt kan worden als identificator. Het *National Insurance Number* wordt echter meer frequent gebruikt.

[24] www.hmrc.gov.uk/nic/ynino.htm.

[25] Identity Cards Act, 2006, *c.* 15 (Eng.).

[26] Zie Shedule 1 bij de Identity Cards Act, 2006, *c.* 15 (Eng.).

1.2.3. SCANDINAVISCHE LANDEN

ENKELE UNIEKE IDENTIFICATOR - In tegenstelling tot de Angelsaksische landen, hebben de Noord-Europese landen al langere tijd ervaring met het gebruik van enkele unieke identificatoren. Voornamelijk Zweden en Finland staan bekend als de praktijkvoorbeelden bij uitstek met betrekking tot het gebruik van een enkele unieke identificator.

ZWEDEN - Waar bepaalde landen pas nu bezig zijn met het invoeren van een systeem voor een enkele identificator of sectorgebonden unieke identificatoren, bestaat het Zweedse nationaal identificatienummer (het *personnummer*) al sinds 1947. Hoewel dit nummer in principe uitgereikt wordt door de Zweedse belastingsautoriteit, wordt het niet alleen in een fiscale context gebruikt. Net als het Belgisch Rijksregisternummer kan dit identificatienummer voor quasi alle overheidstoepassingen worden gebruikt. Wat zeer opmerkelijk is aan het Zweedse systeem, is dat alles openbaar is. De Zweden hebben een groot vertrouwen in de overheid en zien er geen graten in dat hun persoonlijke informatie relatief vrij toegankelijk is. Die openbaarheid van persoonlijke informatie geldt niet enkel tussen burger en overheid, maar tot op zekere hoogte ook tussen burgers en medeburgers.[27] Dit wil echter niet zeggen dat Zweden geen bescherming van gegevens met betrekking tot de persoonlijke levenssfeer kent. Die bescherming wordt geregeld door de wet van 29 april 1998, die de Zweedse implementatie is van Richtlijn 95/46/EG.[28]

FINLAND - In Finland vinden we hetzelfde verhaal: Ook hier is er een uniek nationaal persoonsnummer, beheerd door het centrale bevolkingsregister (het *Population Register Center*) dat in elke overheidstoepassing gebruikt wordt. Daarnaast is er ook een systeem met informatie met betrekking tot het kadaster. Net als in Zweden is bescherming van informatie met betrekking tot de persoonlijke levenssfeer niet de grootste zorg van de Finnen. Als lidstaat van de EU heeft echter ook Finland nieuwe maatregelen moeten nemen met betrekking tot de privacy.[29]

DENEMARKEN - Ook Denemarken kent een centraal register (*Det Centrale Personregister*) dat door quasi alle overheden gebruikt wordt.[30] Elke persoon opgenomen in dat centrale register krijgt een uniek identificatienummer. Opmerkelijk is dat Denemarken geen elektronische identiteitskaart uitgeeft. De Deense overheid heeft besloten zich in deze materie te beperken tot het leveren van digitale handtekeningen voor authenticatie. Als Europese lidstaat heeft Denemarken op 31 mei 2000 een wet betreffende de verwerking van persoonsgegevens aangenomen ter implementatie van Richtlijn 95/46/EG.[31]

NOORWEGEN - Noorwegen vult het lijstje van Scandinavische landen mooi aan, aangezien we ook hier een uniek nationaal identificatienummer vinden (het *fødselsnummer*) waar ook een centraal register bij hoort (*Det Sentrale Folkeregister*). Hoewel Noorwegen geen lidstaat van de Europese Unie is, heeft het als lidstaat van de Europese Vrijhandelsassociatie ook wetgeving aangenomen om Richtlijn 95/46/EG in Noors recht om te zetten.[32]

[27] Zie bijvoorbeeld een website waar men vrijuit het *personnummer* en de belastingsgegevens van burgers kan opzoeken, *www.ratsit.se.*
[28] Personal Data Act, 29 april 1998, *SFS* 1998:204.
[29] Personal Data Act, 22 april 1999 (523/1999), *www.finlex.fi.*
[30] *www.cpr.dk/cpr/site.aspx?p=34.*
[31] The Act on Processing of Personal Data, 31 mei 2000, *Lovtidende* 2 juni 2000, Act No. 429.
[32] Act No. 31 relating to the processing of personal data (Personal Data Act) van 14 april 2000, *I* 2000 hefte 8.

EEN TYPISCH SCANDINAVISCH GEGEVEN - De grote gelijkenissen tussen deze landen zullen uiteraard niemand verbazen. Door de eeuwenlange unies en fusies tussen deze landen, kennen zij in grote lijnen dezelfde historische ontwikkelingen. De huidige registers zijn een overblijfsel van de vroegere kerkgeoriënteerde maatschappij.[33] Zo gaan de Zweedse kerkregisters terug tot de vroegere zeventiende eeuw.[34] Naast die nauwe samenhang tussen Kerk en bevolkingsregisters kunnen we ook een zeer groot vertrouwen in de overheid terugvinden in de Scandinavische landen. Bescherming van de privacy komt voor deze landen daarom niet op dezelfde manier naar voren als in andere landen. Tot slot stellen we vast dat de burgers van die landen - dankzij de ontwikkelingen van de twintigste eeuw - nu door middel van een enkele unieke identificator geïdentificeerd worden voor quasi alle overheidstoepassingen.

1.2.4. OOSTENRIJK

OOSTENRIJKSE EVOLUTIE - De eerder aangehaalde Duitse volkstellingen uit de 19de eeuw waren het product van wat Jozef II, keizer van het Heilig Roomse Rijk, zijn burgers in de late 18de eeuw oplegde. Oostenrijk kent wat dit betreft bijgevolg een gelijkaardige geschiedenis als Duitsland. Hoewel Oostenrijk geen ruime ervaring met het onderwerp van unieke identificatoren lijkt te hebben, heeft de Oostenrijkse overheid intussen haar imago op voortreffelijke wijze opgepoetst met haar programma voor e-Government. Al in de jaren 1990 was de overheid dit programma aan het ontwikkelen, wat zich toen voornamelijk toonde in het in 1997 gelanceerde overheidsportaal *www.help.gv.at*. Sinds 2001 is Oostenrijk actief bezig met het uitrollen van een groots opgezette strategie onder leiding van de Bondskanselier.[35] In 2004 volgde met de wet met betrekking tot e-Government de juridische basis voor het uitrollen van toepassingen voor e-Government in Oostenrijk.[36]

BÜRGERKARTE - Intussen beweren bepaalde studies dat het digitale platform van de Oostenrijkse overheid tot één van de beste van Europa behoort.[37] Een onderdeel van deze digitalisering van overheidstoepassingen is de '*Bürgerkarte*'.[38] Dit is niet zomaar een elektronische identiteitskaart uitgegeven door de Oostenrijkse overheid, maar wat men kan omschrijven als een identiteitslink, of "*een elektronische attestatie welke een link slaat tussen persoonlijke identificatienummers en elektronische handtekeningen als een aparte ondertekende datastructuur*".[39] Dit wil zeggen dat het Oostenrijkse begrip '*Bürgerkarte*' niet zozeer slaat op de fysieke smartcard die men in handen krijgt, zoals bijvoorbeeld de Belgische e-ID, maar op het authenticatieproces dat er door kan plaatsvinden, oftewel de eigenlijke functie zelf.[40] Het voordeel van dit systeem is dat

[33] NATIONAL TAX BOARD, "Population Registration in Sweden", 2007, *www.skatteverket.se*, 3.
[34] Een zeer compleet overzicht van de geschiedenis van de Zweedse bevolkingsregisters kan gevonden worden op: *www.skatteverket.se.*
[35] Op de volgende website kunnen enkele documenten in verband met de *E-Strategie* worden teruggevonden: *www.bka.gv.at.*
[36] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl. I* Nr. 10/2004.
[37] Zo blijkt uit onderzoeken als dat van IDABC (*ec.europa.eu/idabc*) en eUSER (*www.euser-eu.org*).
[38] *www.buergerkarte.at.* Op deze website kan men alle informatie over dit concept vinden. Zo is er een lijst met voor het concept '*Bürgerkarte*' geschikte smartcards, een overzicht van de procedure tot registratie en het activeren. Ook de benodigde software kan hier verkregen worden.
[39] Zie onder '*History, Scope and Goals*' bij het profiel over Oostenrijk op www.*cosic.esat.kuleuven.be/modinis-idm.*
[40] Men beschouwt de '*Bürgerkarte*' daarom als een ontastbaar concept of functie, in tegenstelling tot de Belgische e-ID waar men wel degelijk enkel de fysieke kaart bedoelt.

er niet één enkele fysieke kaart is, maar dat er een heel gamma kaarten bestaat die gebruikt kunnen worden als '*Bürgerkarte'*.[41]

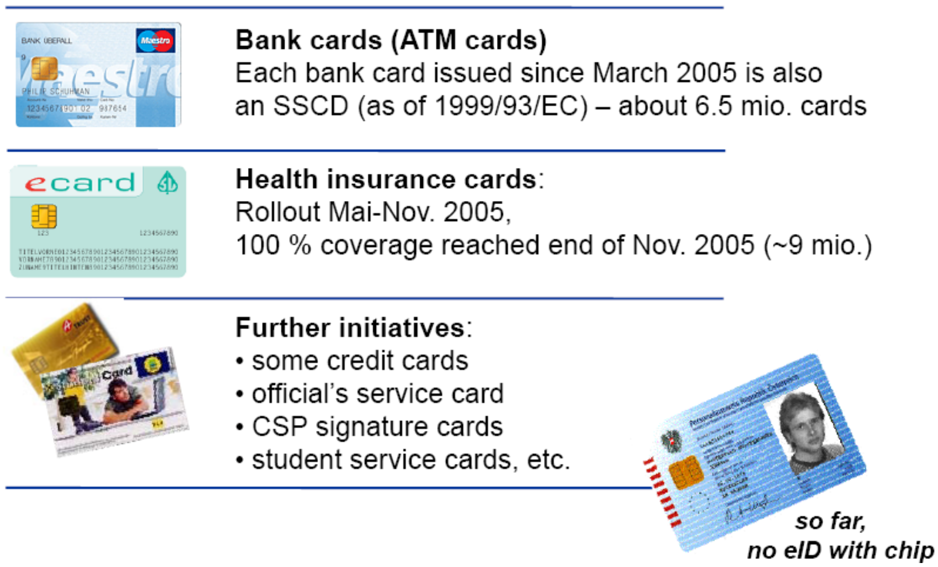

Fig. 1: 'Major initiatives - Citizen Cards' © Herbert Leitold 2009[42]

TECHNOLOGIENEUTRAAL CONCEPT - Bovenstaand schema geeft een overzicht van de bestaande chipkaarten die geschikt zijn om als '*Bürgerkarte'* te dienen. Het maakt duidelijk dat de '*Bürgerkarte'* dus geen fysieke kaart op zich is, maar een ontastbaar concept dat geïmplementeerd kan worden op de chips van bestaande kaarten.

SECTORGEBONDEN IDENTIFICATOREN - Belangrijk hier is het gegeven dat Oostenrijk in tegenstelling tot Scandinavische landen niet een enkele unieke identificator hanteert, maar sectorgebonden identificatoren. In de praktijk wil dit zeggen dat iedere burger één uniek nummer krijgt, namelijk dat van het pas recent opgerichte personenregister.[43] Dat nummer wordt versleuteld in een zogenaamde *SourcePIN*.[44] Die *SourcePIN* is dus voor iedereen uniek, maar zal ter bescherming van de persoonlijke levenssfeer van de burger veilig opgeslagen worden op de *Bürgerkarte*. Voor elk verschillend overheidsdomein kan er dan een sectorgebonden PIN afgeleid worden van de originele *SourcePIN*.[45] Essentieel in deze stap is dat de afgeleide PIN nooit teruggekoppeld kan worden naar de originele *SourcePIN*. Door middel van een elektronische handtekening wordt er een link gelegd tussen de *SourcePIN* en de afgeleide PIN. Daarnaast kent Oostenrijk als lidstaat van de Europese Unie sinds 2000 ook een wet ter implementatie van Richtlijn 95/46/EG.[46]

[41] Sinds 2005 kan men bijvoorbeeld ook gewone bankkaarten - en gedurende een bepaalde periode zelfs SIMkaarten uit mobiele telefoons - gebruiken hiervoor. Voor een overzicht van geschikte kaarten, zie: *www.buergerkarte.at/en/aktivieren/anbieter.html.*
[42] H. LEITOLD, "The Austrian Citizen Card, a European Best Practice - Innovation Forum 2009", 25 maart 2009, *online.tu-graz.ac.at,* 6.
[43] Het *Zentrales Melderegister* is in haar hedendaagse vorm pas acties sinds 2002, *zmr.bmi.gv.at.*
[44] Een meer technisch overzicht kan gevonden worden onder het hoofdstuk '*Technology*' van het profiel over Oostenrijk: *www.cosic.esat.kuleuven.be/modinis-idm.*
[45] Zie ook het rapport van HEC, "Digital Austria - Wat kan Nederland leren van de Oostenrijkse strategie voor eGovernment?", 2007, *www.hec.nl,* 22-23.
[46] Datenschutzgesetz 2000 (DSG 2000), *BGBl. I* Nr. 165/1999.

NOOD AAN VERDER ONDERZOEK - Concluderend kunnen we stellen dat net die snelle en minutieus geplande aanpak van het platform voor e-Government, het technologieneutrale concept van de *Bürgerkarte* en het gebruik van sectorgebonden unieke identificatoren in plaats van een enkele unieke identificator, van Oostenrijk een land maken dat we in dit onderzoek zeker niet links kunnen laten liggen. Bij het rechtsvergelijkend onderzoek dat later aan bod komt, zal Oostenrijk daarom dienen als voorbeeld van een land waar het gebruik van sectorgebonden unieke identificatoren al enige tijd in de praktijk omgezet is.

1.2.5. PORTUGAL

SECTORGEBONDEN IDENTIFICATOREN EN INTEGRATIE - Het Portugese verhaal is er één van integratie. Tot voor 2005 kende men een aparte identiteitskaart, een belastingskaart, een kaart voor de sociale zekerheid en een stemkaart. Al die toepassingen worden nu geïntegreerd in één enkele identiteitskaart, de *Cartão de Cidadão*.[47] Belangrijk is dat die verschillende nummers allen op die kaart aanwezig zullen zijn en dat er met andere woorden geen enkele unieke identificator voor al deze toepassingen ingesteld zal worden. De identificatoren zijn hier dus contextgebonden. Na een aantal pilootprojecten is men nu bezig om deze kaart algemeen in te voeren. Tegen 2012 zal die algemene invoer compleet zijn. De reacties op hoe deze kaart het in de praktijk doet, zullen dus nog moeten worden afgewacht.

CIDADES - Een bijkomende bijzonderheid aan het Portugese systeem is dat het project ook een zeer regionale focus lijkt te hebben.[48] Het risico van die lokalisering van diensten is uiteraard dat deze te ver uit elkaar kunnen groeien.[49]

PORTUGESE PRIVACYBESCHERMING - Wat de wettelijke bescherming van de persoonlijke levenssfeer betreft kent Portugal uiteraard ook een nationale implementatie van de Europese Richtlijn.[50]

1.2.6. UNIEKE IDENTIFICATOREN IN DE EUROPESE UNIE

RICHTLIJN 95/46/EG EN UNIEKE IDENTIFICATOREN - Het is echter niet alleen op het gebied van het gebruik van unieke identificatoren dat de Europese lidstaten onderling sterk verschillen. Ook met betrekking tot de bescherming van de persoonlijke levenssfeer was er aanvankelijk zeer veel verscheidenheid. Met Richtlijn 95/46/EG wou Europa enige harmonisatie brengen in dat verdeelde landschap betreffende de bescherming van de persoonlijke levenssfeer. Het voor deze materie relevante artikel in de Europese wetgeving, is artikel 8 (7) van Richtlijn 95/46/EG. Dit artikel bepaalt dat de lidstaten van de Europese Unie de voorwaarden dienen vast te stellen "*waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene*

[47] *"…will also be a practical document that combines and replaces the existing taxpayer card, National Health Service user's card, Social Security card and voter's card"*, *http://www.cartaodocidadao.pt/index.php?option=com_content&task=view&id=18&Itemid=28&lang=en*.

[48] Getuige het *Cidades Digitais* project: *http://www.cidadesdigitais.pt.*

[49] Zie '*Analysis: Successes, failures and lessons learned*' op: *https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/PortugueseProfile.*

[50] Lei da protecçao de dados pessoais van 26 oktober 1998, nr. 67/98, *DDR* I-A nr. 247, 5536-5546.

aard voor verwerkingsdoeleinden mag worden gebruikt."[51] Een eerste bedenking die we ons bij dit artikel kunnen maken, is dat de Richtlijn expliciet verwijst naar een nationaal identificatienummer of een andere identificator van algemene aard. De EU lijkt hier dus alleen de identificatiemiddelen van algemene aard te viseren.[52] Daarnaast kunnen we ons afvragen wat die voorwaarden dienen te zijn. Volgens de Artikel 29 Werkgroep gaat het hier om een bepaling uit artikel 8 die bijgevolg slaat op de verwerking van bijzondere categorieën van gegevens. Overweging 33 bij de Richtlijn omschrijft deze gegevens als "*gegevens die wegens hun aard op de fundamentele vrijheden of op de persoonlijke levenssfeer inbreuk kunnen maken*". Volgens de Werkgroep lijkt het daarom aannemelijk dat de wetgever unieke identificatoren ook als dusdanig ziet en daarom bijkomende bescherming wou bieden tegen het ongeoorloofd verwerken van die identificator.[53] De wat verwarrende formulering van dit artikel is het gevolg van een politieke keuze. De ratio achter artikel 8 (7) is immers dat men een hoge graad van bescherming wou bieden en dat men onder geen beding een lagere graad van bescherming zou mogen bereiken in lidstaten die al relevante wetgeving kenden.[54] Harmonisatie was politiek gezien geen realistische optie voor deze materie. Had men partij willen kiezen voor één bepaalde optie, dan was deze Richtlijn er waarschijnlijk nooit gekomen of zou de implementatie ervan door de lidstaten sterk te wensen overlaten.

1.2.7. DE VERWERKING VAN PERSOONSGEGEVENS

RICHTLIJN 95/46/EG OVER PRIVACYBESCHERMING - De Europese lidstaten hebben in het afgelopen decennium nieuwe wetgeving op het gebied van de bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens aangenomen ter omzetting in nationaal recht van Richtlijn 95/46/EG. Dit instrument is vooral bekend van de bepalingen betreffende de verwerking van persoonsgegevens. Gelet op de beperkte omvang van dit project en de ervaring van het doelpubliek ter zake, zal er op dit punt niet tot in detail ingegaan worden op de precieze bepalingen en bijzonderheden van de huidige Europese en Belgische regelgeving. We zullen ons daarom beperken tot een kort overzicht van een aantal belangrijke principes.[55]

TOEPASSINGSGEBIED - Allereerst moeten we kijken naar de benodigde definities. Het begrip 'persoonsgegevens' wordt gedefinieerd in artikel 2 (a) van de Richtlijn en in artikel 1 van de Belgische privacywet.[56] Belangrijk is dat men dit begrip zo ruim mogelijk gemaakt heeft. Ook de defi-

---

[51] Artikel 8.7 richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb. L*. 23 november 1995, afl. 281, 31-50.

[52] DEPARTMENT OF JUSTICE, EQUALITY AND LAW REFORM, "Consultation Paper on Transposition into Irish Law", november 1997, *www.privacyinternational.org,* 29.

[53] ARTIKEL 29 WERKGROEP, "Opinion 4/2007 on the concept of personal data, WP136", 20 juni 2007, *ec.europa.eu/justice_home*, 15.

[54] Zo blijkt uit de opinie van het Economisch en Sociaal Comité: CES0569/1991 van 24 april 1991, punt 1.5.

[55] Voor een meer diepgaand onderzoek naar deze materie kunnen we verwijzen naar volgende werken en studies: D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 32-52; J. DUMORTIER, *ICT-Recht*, Leuven, Acco, 2009, 98-116; R. HES et al., *At Face Value - On Biometrical Identification and Privacy*, Den Haag, Registratiekamer, 1999, 35-42; ARTIKEL 29 WERKGROEP, "Opinion 4/2007 on the concept of personal data, WP136", 20 juni 2007, ec.europa.eu/justice_home.

[56] Met 'Richtlijn' wordt verwezen naar richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb. L*. 23 november 1995, afl. 281, 31-50. Met 'Privacywet' doelen we op Wet tot bescherming van de

nitie van het begrip 'verwerking' wordt zo ruim mogelijk omschreven, met als belangrijkste *caveat* dat de verwerking in principe geautomatiseerd moet zijn. Artikel 3 van beide wetgevende instrumenten geeft de belangrijkste uitzonderingen in de wet aan: de verwerking voor persoonlijk of huishoudelijk gebruik is vrijgesteld van het toepassingsgebied van de wet. Ook de verwerking voor journalistieke, literaire of artistieke doeleinden wordt vrijgesteld, alsook verwerking door de overheid in het kader van een aantal opgesomde werkzaamheden.

BASISPRINCIPES - Vervolgens komen we tot een vijftal basisprincipes voor een rechtmatige verwerking van persoonsgegevens. Zo dient de verwerking allereerst te voldoen aan het finaliteitbeginsel.[57] De verwerking moet ook toelaatbaar zijn. Dit wil zeggen dat men in principe de toestemming van de betrokkene nodig heeft of dat er voldaan moet zijn aan de limitatief opgesomde criteria uit artikel 5 van de privacywet. Een derde principe bepaalt speciale categorieën van persoonsgegevens, die slechts onder zeer strikte voorwaarden verwerkt mogen worden. Het gaat hier om gevoelige gegevens (artikel 6 privacywet), medische gegevens (artikel 7 privacywet) en gerechtelijke gegevens (artikel 8 privacywet). Verder bepaalt de wet als vierde principe dat de verwerking strikt vertrouwelijk dient te gebeuren en dat de toegang tot de gegevens beveiligd dient te worden.[58] Het vijfde basisprincipe is dat er steeds een aangifte van de verwerking dient te gebeuren bij de Commissie voor de bescherming van de persoonlijke levenssfeer.[59] Op deze verplichting tot aangifte bestaan echter vrij ruime uitzonderingen.[60] Naast deze basisprincipes voorziet de wet nog in een aantal rechten voor de betrokken persoon. Allereerst is er een recht op informatie.[61] Daarnaast moeten de gegevens meegedeeld worden aan de betrokkene en heeft hij het recht om deze te laten corrigeren indien zij onjuist zijn.[62] Ook kan de betrokkene zich verzetten tegen de opname van zijn gegevens in een bestand. Tot slot voorziet de wet in ruime mogelijkheden tot handhaving van deze principes.[63]

UITZONDERINGEN - Algemeen kunnen we vaststellen dat de wetgeving betreffende de verwerking van persoonsgegevens enerzijds een aantal vrij strikte bepalingen en anderzijds vrij ruime uitzonderingen bevat. Het zal in deze materie daarom niet altijd even eenvoudig zijn om duidelijk aan te duiden wat toelaatbaar is krachtens de wetgeving en wat niet. Voor België liggen er veel verantwoordelijkheden ter zake bij de Commissie voor de bescherming van de persoonlijke levenssfeer. Het zal daarom belangrijk zijn de adviezen en aanbevelingen van deze Commissie indachtig te houden.

---

persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992, *B.S.* 18 maart 1993.

[57] Elke verwerking moet een doel hebben, mag niet verder gaan dan wat strikt nodig is om het doel te bereiken en de verwerkte gegevens mogen ook niet langer dan nodig bewaard worden. Art. 6 Richtlijn, art. 4 Privacywet. Dit wordt ook wel het proportionaliteitsprincipe genoemd.

[58] Art. 16 Privacywet.

[59] Art. 17 Privacywet.

[60] Art. 17 §1 en art. 20 Privacywet geven een aantal voorbeelden. Meer uitzonderingen zijn te vinden in het K.B. bij deze wet: Hoofdstuk VII van het Koninklijk Besluit ter uitvoering van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 13 februari 2001, *B.S.* 13 maart 2001.

[61] Art. 9 Privacywet. Ook hier zijn er uitzonderingen: statistische verwerking of wetenschappelijk onderzoek (art. 9 §2); journalistieke, artistieke of literaire doeleinden (art. 3 §3b); Staatsveiligheid en politietaken (art. 3 §§4 en 5)

[62] Art. 10 en 12 Privacywet.

[63] Deze worden dieper bestudeerd bij J. DUMORTIER, *ICT-Recht,* Leuven, Acco, 2009, 113-116.

1.2.8. EUROPESE INTEROPERABILITEIT

EUROPESE TOENADERING - Een laatste aandachtspunt dat hier niet vergeten mag worden, is het probleem van de interoperabiliteit.[64] Zoals uit het voorgaande onderzoek al blijkt, groeien de Europese lidstaten steeds meer naar elkaar toe. De grote diversiteit tussen die lidstaten kan er natuurlijk toe leiden dat zulke toenadering zeer moeilijk of zelfs quasi onmogelijk wordt. Er is daarom nood aan meer pan-Europese regelgeving of minstens een algemeen aanvaard referentiekader. Het is echter geen sinecure om deze materie op Europees vlak te regelen. We zagen al dat de Europese privacyrichtlijn op bepaalde punten - zoals het gebruik van unieke identificatoren - redelijk wat ruimte moest openlaten voor de persoonlijke wensen van de lidstaten. Europa stoot in deze materie dus op de grens van haar bevoegdheden.[65]

FEDERATIE OP BASIS VAN VERTROUWENSKRINGEN - In deze materie moet men zoeken naar een systeem voor gegevensuitwisseling dat overweg kan met alle verschillende systemen van identiteitsbeheer doorheen Europa.[66] Men kan hier dan voornamelijk denken aan de zogenaamde federatie waarbij Staten onderling afspraken maken met het oog op uitwisseling van identiteits- en andere gegevens, met in het bijzonder oog op authenticatie over verschillende domeinen heen.[67] Juridisch gezien zullen hier uiteraard de nodige overeenkomsten met betrekking tot betrouwbaarheid en privacybescherming nodig zijn. Zoals aangetoond wordt in onder meer het STORK project, kunnen we ook niet zonder meer de nationale identificatienummers op Europees vlak toepassen.[68]

NOOD AAN CONSENSUS - Het spreekt voor zich dat pan-Europese samenwerking op dit vlak zeker geen sinecure zal zijn. Het lijkt daarom meer wenselijk om eerst op supranationaal vlak een consensus voor concepten als ‘elektronische identiteiten’ tot stand te brengen.[69] Omdat Europa deze materie vooral aan de lidstaten lijkt te willen overlaten zal de uiteindelijke samenwerking wellicht door middel van onderlinge afspraken tussen de lidstaten bereikt moeten worden en zonder voorafgaande consensus tussen de lidstaten zal zulk akkoord uiteraard niet bereikt kunnen worden.

[64] Gezien de omvang van dit project kunnen we dit probleem niet *in extenso* bespreken. We verwijzen daarom naar andere projecten. Zie onder meer interoperabiliteit bij het FIDIS-project (*www.fidis.net*) en IDABC (*ec.europa.eu/idabc/en/chapter/5883*). Vooral de studie naar interoperabiliteit tussen e-ID kaarten is interessant voor dit onderwerp: IDABC, “eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability”, 2007, *ec.europa.eu/idabc*.

[65] Dit blijkt onder meer ook uit de opinie van de Artikel 29 Werkgroep over het Informatiesysteem Interne Markt (IIM): ARTIKEL 29 WERKGROEP, “Opinion 7/2007 data protection issues related to the internal market information system, WP140”, 20 september 2007, *ec.europa.eu/justice_home*.

[66] Meer uitgebreid besproken bij: MODINIS, “D.3.9: Identity Management Issue Interim Report II1”, www.*cosic.esat.kuleuven.be/modinis-idm*, 11-13. Zie ook p. 10-13 van die studie voor een overzicht van juridische vragen en p. 14-17 voor meer technische aangelegenheden.

[67] Pan-Europese interoperabiliteit is ook het doel van het Europese STORK project, *www.eid-stork.eu*.

[68] STORK, “D2.3. Quality Authenticator Scheme”, 2009, *www.eid-stork.eu*, 36. Zie ook IDABC, “eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability”, 2007, *ec.europa.eu/idabc*, 6.

[69] IDABC, “eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability”, 2007, *ec.europa.eu/idabc*, 209. Zo kan men bepaalde verantwoordelijkheden en bevoegdheden toewijzen aan de Europese Commissie. Dit gebeurde onder meer al bij het Informatiesysteem Interne Markt. Zie ook: ARTIKEL 29 WERKGROEP, “Opinion 7/2007 data protection issues related to the internal market information system, WP140”, 20 september 2007, *ec.europa.eu/justice_home*.

1.2.9. CONCLUSIE

TWEE MODELLEN - Uit dit beknopt overzicht van de historiek van deze materie en de ontwikkelingen die een aantal Europese landen doormaken, kunnen we inderdaad niet anders dan concluderen dat er een waaier aan oplossingen mogelijk is. *Grosso modo* kunnen we die oplossingen samenbrengen onder de groepen 'meerdere unieke identificatoren' en 'één enkele unieke identificator'. We zien ook dat sommige landen met betrekking tot deze materie een lange evolutie doorgemaakt hebben. Daarom is het mogelijk dat het voor hen niet wenselijk of haalbaar zal zijn om zonder meer een compleet ander systeem in te voeren. We kunnen ons echter wel afvragen of voor die landen een hybride systeem nog tot de mogelijkheden kan behoren. Men zou dan bijvoorbeeld de functionaliteit van de bestaande dienstverlening met betrekking tot het gebruik van een enkele unieke identificator kunnen behouden en de functionaliteit van nieuwe dienstverleningen kunnen baseren op meerdere sectorgebonden unieke identificatoren. Zulk voorstel vereist uiteraard een onderzoek naar de technische haalbaarheid ervan.

HET BELGISCH BELEID - Daarom kan het interessant zijn om eerst het Belgisch beleid betreffende het gebruik van het Rijksregisternummer als enkele unieke identificator onder de loep te nemen en om meer bepaald te zoeken naar wat de exacte doelstellingen en grondslagen van dat beleid zijn. Vervolgens kunnen we deze bevindingen gebruiken om naar equivalente doelstellingen te zoeken in het beleid van een aantal andere Europese landen.

1.3. TERMINOLOGIE

VERKLARENDE WOORDENLIJST - Omdat het hier een zeer technisch onderwerp betreft, lijkt het ons wijselijk om eerst een korte woordenlijst op te nemen in dit onderzoek. Het is immers van kapitaal belang om over een algemeen referentiekader te beschikken. Wat volgt is dus een verklarende woordenlijst met voor deze materie relevante termen. [70] Deze lijst is niet exhaustief en kan onderhavig zijn aan evolutie.[71] Als aanvulling op deze woordenlijst kunnen we nog verwijzen naar de studie uitgevoerd door het Institute for Prospective Technological Studies (IPTS) betreffende de barrières in de Europese sector voor digitale identiteiten.[72] In deze studie worden een aantal van de voor dit onderzoek relevante kernbegrippen uitgelegd, waarbij er ook beroep gedaan wordt op case-studies.

- **attribuut**: Fysieke of abstracte informatie die toebehoort aan een entiteit.
- **authenticatie:** Een proces waarbij wordt nagegaan of de identiteit die een entiteit beweert te hebben wel degelijk aan hem toebehoort. Men kan dit controleren op basis van onder meer kennis (bijvoorbeeld door een paswoord), bezit (bijvoorbeeld door een certificaat op de e-ID), biometrische kenmerken of een combinatie van voorgaande

[70] Deze lijst put ondermeer uit J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; wat schatplichtig is aan de Commissie voor de bescherming van de persoonlijke levenssfeer in haar aanbeveling SE/2008/028 van 24 september 2008, *www.privacycommission.be.*

[71] Meer complete glossaria: IDEM, "Deliverable 1.3 Conceptual Framework Annex I. Glossary of terms (v1.07)", 2007, *projects.ibbt.be/idem* en MODINIS/IDM, "Common Terminological Framework for Interoperable Electronic Identity Management, Consultation paper v2.01", 2005, *www.cosic.esat.kuleuven.be/modinis-idm.* Beide documenten werden extensief geconsulteerd voor het tot stand brengen van het hier opgenomen glossarium.

[72] IPTS, "Overcoming Barriers in the EU Digital Identity Sector", 2008, *ipts.jrc.ec.europa.eu*, 59 p.

middelen. Een persoon wordt geauthentiseerd door deze persoon bijvoorbeeld een vraag te stellen waar alleen hij een antwoord op kent. Hieruit kan worden afgeleid dat de entiteit werkelijk is wie hij beweert te zijn en doet dit met een bepaalde of afgesproken graad van zekerheid. Het invoeren van de geheime code in een bankautomaat is een ander voorbeeld van een onderdeel van een authenticatieprotocol. Het is belangrijk om authenticatie en identificatie duidelijk te onderscheiden van elkaar.

- **autorisatie**: Een proces of daad waarmee de toelating voor een entiteit om een bepaalde verwerking te verrichten of een bepaalde dienst te gebruiken vastgesteld wordt door middel van relevante informatie betreffende toegangscontrole. Authenticatie is meestal een voorafgaande voorwaarde om tot autorisatie te komen.
- **certificaat**: Een elektronisch document waarin een geaccrediteerde certificatieautoriteit de waarheid van bepaalde beweerde feiten verzekert. In identiteitsbeheer wordt deze term vaak gebruikt als referentie aan een digitaal certificaat met publieke sleutel, zoals de X.509 digitale certificaten die we op onze e-ID terugvinden.
- **digitale handtekening**: Data toegevoegd aan een data-eenheid of een cryptografische transformatie van een data-eenheid, die de ontvanger de mogelijkheid biedt om de bron en de integriteit van die data-eenheid vast te stellen en die de data-eenheid beschermt tegen vervalsing door de ontvanger. Belangrijk: een digitale handtekening is niet gelijk aan een elektronische handtekening. De digitale handtekening kan begrepen worden als het technische middel om een geavanceerde elektronische handtekening te plaatsen.
- **digitale identiteit**: Een identiteit in digitale vorm. Elke entiteit kan meerdere digitale identiteiten hebben, die al dan niet uniek zullen zijn.
- **elektronische handtekening:** Data die elektronisch toegevoegd wordt aan - of logisch geassocieerd wordt met - andere elektronische data en die dient als methode van authenticatie. Wanneer een elektronische handtekening (1) op unieke wijze aan de ondertekenaar verbonden is, (2) die ondertekenaar kan identificeren, (3) aangemaakt is met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en (4) op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden is, dat elke latere wijziging van de gegevens kan worden opgespoord, dan kunnen we spreken van een **geavanceerde elektronische handtekening**.[73] Wanneer zulke geavanceerde elektronische handtekening gebaseerd is op een gekwalificeerd certificaat en door een veilig middel aangemaakt is, kunnen we spreken van een **gekwalificeerde elektronische handtekening**. Deze laatste vorm is juridisch gezien gelijkwaardig aan een klassieke handgeschreven handtekening.[74]
- **gefedereerde identiteit:** Een certificaat van een andere entiteit die de identiteit uit de ene context kan linken met een identiteit uit een andere context.
- **identificatie:** Het proces waarbij beweerde of waargenomen attributen van een entiteit gebruikt worden om daaruit af te leiden wie de betrokken entiteit is. Identificatie verschaft met andere woorden een antwoord op de vraag naar wie deze entiteit is. Identifi-

[73] Art. 2.2 Richtlijn 1999/93/EG van 13 december 1999 betreffende een betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *Pb*. L 013 van 19 januari 2000, 12 e.v. Zie voor België: Art. 2, 2° Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, *B.S*. 29 september 2001, 33070 e.v.

[74] Art. 5 Richtlijn 1999/93/EG van 13 december 1999 betreffende een betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *Pb*. L 013 van 19 januari 2000, 12 e.v. Voor België: Art. 4, §4 Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, *B.S*. 29 september 2001, 33070 e.v.

catie verschilt met authenticatie in de zin dat authenticatie nagaat of de entiteit werkelijk is wie hij beweert te zijn.

- **identificator:** Een attribuut of een groep attributen van een entiteit welke die bepaalde entiteit binnen een bepaalde context of sector op unieke wijze kunnen identificeren.
- **identiteit:** Een identiteit is de verzameling van alle attributen die aan een bepaalde entiteit toebehoren. Dit impliceert dat een entiteit één en slechts één identiteit heeft. Het feit dat eventueel in bepaalde situaties een pseudoniem gebruikt kan worden, doet daar geen afbreuk aan.
- **identiteitsbeheer (*identity management*):** Het beheren van identiteiten van entiteiten.
- **kenmerk:** Een attribuut van een entiteit, anders dan de attributen die de identiteit van de entiteit bepalen, zoals een hoedanigheid, een functie in een bepaalde organisatie, een beroepskwalificatie, enz. Een entiteit kan verschillende kenmerken hebben.
- **logging:** Het opslaan van de link tussen de handeling en de identiteit van de entiteit. Dit creëert als het ware een archief met bewijs van bepaalde gebeurtenissen, ondernomen of gepoogde handelingen, enz.
- **mandaat:** Een herroepbaar recht verstrekt door een geïdentificeerde entiteit aan een andere geïdentificeerde entiteit om in zijn naam en voor zijn rekening welbepaalde (al dan niet juridische) handelingen te stellen. Een entiteit kan aan één of meerdere entiteiten één of meerdere mandaten verstrekken.
- **onherroepbaarheid (*non-repudiation*):** De mogelijkheid om te voorkomen dat een handelende entiteit op een later moment ontkent dat hij die bepaalde handeling heeft verricht. De verrichte handeling zal onherroepelijk gekoppeld kunnen worden aan de handelende entiteit.
- **persoonlijk identificatienummer (*Personal Identification Number* of PIN):** Methode van authenticatie waarbij gebruikelijk een geheim nummer van vier of meer cijfers ingevoerd dient te worden. Deze term kan ook gebruik worden in de context van persoonsnummers.
- **persoonsgegevens:** Informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Zie artikel 2, a) Richtlijn 95/46/EG.
- **publieke sleutel infrastructuur (*Public Key Infrastructure* of PKI):** Het systeem waarbij certificatieautoriteiten bepaalde handelingen betreffende het beheer van certificaten, en sleutels verrichten voor een groep gebruikers in een applicatie van asymmetrische cryptografie.
- **registratie:** Het proces waarbij de identiteit van een entiteit, een kenmerk van een entiteit of een mandaat met voldoende zekerheid wordt vastgesteld vooraleer middelen ter beschikking worden gesteld aan de hand waarvan de identiteit, een kenmerk of een mandaat kunnen worden geauthentiseerd of geverifieerd.
- **rol (*role*):** Omschrijft de organisatorische functies en plichten van een entiteit zonder een link te leggen tussen de autorisaties en de entiteit zelf.
- **unieke identiteit**: Een identiteit waarbij ten minste een deel van de attributen identificatoren zijn.
- **gebruikersidentificatie:** Een identificator die gebruikt wordt om een entiteit te identificeren in een digitaal informatiesysteem.
- **verificatie:** Het proces waarbij wordt nagegaan of een kenmerk of mandaat die een entiteit beweert te hebben om gebruik te kunnen maken van een elektronische dienst, effectief een kenmerk of een mandaat van deze entiteit is. Men kan dit doen op basis van dezelfde soort middelen als die gebruikt worden voor de authenticatie van de identiteit

of na authenticatie van de identiteit van een entiteit, door de raadpleging van een gegevensbank (authentieke bron) waarin kenmerken of mandaten betreffende een geïdentificeerde entiteit worden opgeslagen

- **vertrouwen (*Trust*):** De relatie tussen twee of meer entiteiten waarbij de ene entiteit er van uit mag gaan dat de andere entiteit zich op een op voorhand afgesproken manier zal gedragen.
- **verwerking van persoonsgegevens:** Elke bewerking of elke geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés. Zie artikel 2, b) Richtlijn 95/46/EG.

2. UNIEKE IDENTIFICATOREN IN BELGIË EN EUROPA

2.1. HET BELGISCH BELEID BETREFFENDE HET RIJKSREGISTERNUMMER

BOUWSTENEN VAN HET BELGISCH BELEID - In dit deel van het onderzoek zullen we het Belgisch beleid onder de loep nemen. We zullen in de eerste plaats zoeken naar de bouwstenen van dat beleid. Een belangrijk uitgangspunt hier is dat de overheid informatie over haar onderdanen wil inzamelen. Het is de bedoeling dat de overheid dit slechts eenmalig doet, om vervolgens die gegevens doorheen de verschillende overheidstoepassingen te kunnen gebruiken wanneer dat vereist wordt.[75] Toch dringen er zich ook bij zulke eenmalige gegevensinzameling vragen op naar wie die gegevens mag inzamelen, welke gegevens dit mogen zijn, hoe men ze dient op te slaan en hoe die gegevens geactualiseerd moeten worden. De burger zal immers willen weten wie er toegang tot zijn gegevens heeft en voor welke doeleinden die gegevens gebruikt en hergebruikt zullen worden. Men zal dus steeds voldoende aandacht moeten besteden aan privacybescherming. Ook zal de burger er uiteraard iets voor in ruil willen. Hij zal concrete, op de gebruiker afgestemde diensten van de overheid verlangen. Verder zal hij ook verlangen dat de overheid de ingezamelde gegevens zo goed mogelijk benut, namelijk door bepaalde diensten op basis van die ingezamelde informatie automatisch te verstrekken, door proactief op te treden, en dergelijke.[76] In het kader van e-Government zal hij een geïntegreerde dienstverlening verwachten.

GEDECENTRALISEERDE GEGEVENSOPSLAG - Vanuit het perspectief van de overheid zelf, zou men er natuurlijk aan kunnen denken om al die gegevens te centraliseren. Wanneer alles in één grote databank zit, dient men volgens zulke redenering immers enkel te bepalen welke overheidsinstanties toegang tot de ingezamelde gegevens mogen krijgen. Het is intussen wel duidelijk dat men zich ernstige vragen kan stellen in verband met de bescherming van de persoonlijke levenssfeer bij zulke praktijk van verregaande centralisatie. Vanuit het perspectief van de bescherming van de privacy, zou men daarom kunnen opteren voor een meer gedecentraliseerd model, namelijk op basis van een gefedereerd systeem.[77] Zulke federatie is gebaseerd op vertrouwenskringen, wat wil zeggen dat er afspraken met betrekking tot het gebruikers- en toegangsbeheer gemaakt

[75] De nood aan een eenmalig karakter van zulke gegevensinzameling wordt verder bestudeerd in: F. ROBBEN, J. DEPREST, "E-government: The Approach of the Belgian Federal Administration, 2003, *www.ksz-bcss.fgov.be*, 6.
[76] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr. 2, 52-60; *law.kuleuven.be/icri/frobben*, 2.
[77] Zie ondermeer ook aanbeveling SE/2008/028 van de Commissie voor de bescherming van de persoonlijke levenssfeer van 24 september 2008, *www.privacycommission.be.*

moeten worden tussen de verschillende betrokken instanties.[78] Dit kan verregaande centralisatie tegen gaan en kan voldoende waarborgen bieden voor de bescherming van de persoonlijke levenssfeer.[79] Wanneer zulk systeem toch centrale aggregatiepunten bevat, dienen er voldoende technische en organisatorische maatregelen ter bescherming van de privacy getroffen te worden.[80] Het opzetten en implementeren van een gefedereerd systeem zal echter enkel mogelijk zijn indien de betrokken overheden nauwgezet samenwerken. Voldoende transparantie, zowel van de overheid naar de burger toe als tussen de verschillende overheden, zal hier dus een belangrijk uitgangspunt zijn.

AANZET TOT RECHTSVERGELIJKEND ONDERZOEK - Daarom is het Belgisch beleid gefundeerd op een aantal bouwstenen die de leidraad vormen voor de precieze implementatie van dit beleid. We zullen nu die bouwstenen dieper onderzoeken. Aangezien zij bepalend zijn voor hoe het Belgisch systeem in de praktijk werkt, zullen het ook diezelfde bouwstenen zijn die we als referentie zullen gebruiken voor het rechtsvergelijkend onderzoek.

2.1.1. ENKELE UNIEKE IDENTIFICATOR

HET RIJKSREGISTERNUMMER - Een eerste pijler van het Belgisch beleid is het gebruik van een enkele unieke identificator.[81] Elke persoon ingeschreven in België krijgt een uniek nummer toegewezen.[82] Voor natuurlijke personen is dit in de regel het Rijksregisternummer.[83] Deze praktijk leidt er natuurlijk toe dat zowel burger als overheid maar één enkele unieke identificator moeten hanteren om onmiddellijk en overal toegang te krijgen tot alle gegevens die de overheid over die bepaalde burger bezit. Op het eerste zicht lijkt deze natuurlijk een meer efficiënte werkwijze dan de praktijk van sectorgebonden nummers die sommige andere landen er op na houden. [84] Vanuit het standpunt van de privacybescherming zou men echter wel bezwaren kunnen uiten tegen deze praktijk. Men zou bijvoorbeeld kunnen argumenteren dat het gebruik van een enkele unieke identificator het risico op onrechtmatige gegevensverwerking te zeer verhoogd. De Commissie voor de bescherming van de persoonlijke levenssfeer zelf geeft echter de voorkeur aan de enkele unieke identificator.[85]

---

[78] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", Computerrecht, 2009, nr 2, 52-60; *law.kuleuven.be/icri/frobben*, 3-4.

[79] F. ROBBEN, "eGovernment, eHealth en bescherming van de privacy", 18 april 2008, *law.kuleuven.be/icri/frobben,* slide 13.

[80] Ook in de verwijzingsrepertoria van de Kruispuntbank van de Sociale Zekerheid zijn er toch nog enige centrale aggregatiepunten, dit ondanks het feit dat deze dienstenintegrator een gedecentraliseerde gegevensopslag nastreeft.

[81] Voor dit onderzoek volgen we de bouwstenen zoals vermeld door Frank Robben en Jos Dumortier in J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60.

[82] F. ROBBEN, "1st Modinis Workshop on Identity Management in EGovernment", 4 mei 2005, *law.kuleuven.be/icri/frobben*, slide 9.

[83] Voor personen zonder Rijksregisternummer is er nog het identificatienummer voor de Kruispuntbank van de sociale zekerheid, zie art. 8, §1, 2° Wet houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid van 15 januari 1990, *B.S*. 22 februari 1990.

[84] Het begrip 'efficiëntie' zal voor het doel van dit onderzoek geïnterpreteerd worden als 'gebruiksvriendelijkheid'. Een systeem zal immers pas degelijk kunnen worden genoemd als zowel overheidspersoneel als burgers er werkelijk gebruik van willen en kunnen maken.

[85] In het kader van het project betreffende *eHealth* was de Commissie van mening dat "*een correcte identificatie van primordiaal belang is enerzijds en er thans, in de huidige stand van zaken, geen afdoende argumenten voorhanden zijn die daartegen opwegen anderzijds*." De invoer van een sectoraal nummer werd ook beschouwd als een

GEREGULEERD GEBRUIK - De vraag is dan of het Rijksregisternummer ook echt een ongebreidelde toegang tot persoonlijke informatie verschaft. Hoewel het gebruik van het Rijksregister net door de algemene verspreiding van het Rijksregisternummer vrij kan lijken, is het in principe toch sterk gereguleerd. Artikel 5 van de Wet op het Rijksregister bepaalt de voorwaarden waaraan voldaan dient te zijn vooraleer de toegang tot het register kan worden verleend. Artikel 8 bepaalt vervolgens de voorwaarden om het Rijksregisternummer te mogen gebruiken.[86] Toegang tot het register en gebruik van het Rijksregisternummer vereist met andere woorden een voorafgaande machtiging. Dit is uiteraard een interessant gegeven voor de privacybescherming. Zolang er immers voldaan wordt aan de bepalingen uit Richtlijn 95/46/EG - en de omzetting daarvan naar Belgisch recht - kan men hier immers weinig tegen in brengen.

OPBOUW VAN HET RIJKSREGISTERNUMMER - Het Rijksregisternummer zelf bestaat op haar beurt uit elf cijfers.[87] Het is echter geen onpersoonlijk nummer, wat problemen zou kunnen opleveren bij het uitputten van het volgnummer, bij correctie van de geboortedatum of bij geslachtsverandering.[88] Belangrijker is dat de in het Rijksregisternummer vervatte geboortedatum en geslacht van de persoon persoonsgegevens in de zin van de Privacywet zijn.[89] De bepalingen van de Privacywet moeten daarom zeker indachtig gehouden worden bij de verwerking van die gegevens.[90] Dit sluit aan bij de Europese overwegingen die geleid hebben tot het opnemen van de tekst van artikel 8 (7) in Richtlijn 95/46/EG.

BEDENKINGEN BIJ HET GEBRUIK VAN HET RIJKSREGISTERNUMMER - De bedenkingen die we ons met betrekking tot de privacybescherming kunnen maken over het Rijksregisternummer zijn dus tweeledig. Zo geeft de samenstelling van het nummer op zichzelf toegang tot persoonsgegevens, namelijk de geboortedatum en het geslacht. Daarnaast is het nummer *an sich* verbonden met het register met allerhande persoonsgegevens van het individu. We dienen daarom oplettend te zijn bij zowel het gebruik van het nummers als bij het beheren van de eigenlijke toegang tot het

---

organisatorische belasting die inefficiënte identificatie met zich mee zou kunnen brengen. Het effect van eventuele bijkomende privacybescherming die een sectorgebonden identificator zou bieden, werd afgedaan als minimaal. Zie het advies 14/2008 van de Commissie voor de bescherming van de persoonlijke levenssfeer van 2 april 2008, *www.privacycommission.be,* randnummers 58-63. Intussen gebruikt men binnen het eHealth platform het identificatienummer van de sociale zekerheid.

[86] Het gebruik van het identificatienummer van de Kruispuntbank van de sociale zekerheid is echter wel vrij: Art. 8, §2 Wet houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid van 15 januari 1990, *B.S*. 22 februari 1990.

[87] Dit is bepaald in artikel 1 K.B. betreffende de samenstelling van het identificatienummer van de personen die ingeschreven zijn in het Rijksregister van de natuurlijke personen van 3 april 1984, *B.S.* 21 april 1984. De eerst zes vormen de geboortedatum van de persoon. De volgende drie cijfers zijn een volgnummer, waarbij een even nummer een persoon van het vrouwelijk geslacht aanduidt en een oneven nummer een persoon van het mannelijk geslacht. De laatste twee cijfers vormen een controlecijfer berekend krachtens artikel 4 van het K.B.

[88] We verwijzen hier naar een bedenking die men in Nederland maakte bij de discussie over de invoer van een persoonsnummer. Zie: Advies van de Tafel 'Personeelsbeleid in het kader van identiteitsmanagement', juni 2002, *www.ejure.nl,* 136. België heeft al maatregelen genomen om de hier aangehaalde problemen aan te pakken.

[89] Hoewel geboortedatum en geslacht alleen wellicht niet voldoende zijn voor een volledige identificatie, kunnen ze wel helpen bij een identificatie en maken de persoon dus indirect identificeerbaar. 'Indirect' slaat hier op gegevens die op zichzelf geen volledige identificatie tot stand kunnen brengen, maar die daar in combinatie met andere attributen van het individu wel toe in staat zijn. FIDIS, "D13.3: Study on ID number policies", 14 september 2007, *www.fidis.net,* 25. Zie ook: art. 2 (a) Richtlijn 95/46/EG en artikel 1, §1 van de Belgische privacywet.

[90] Er is al debat gevoerd over de mogelijke invoer van een onpersoonlijk nummer. D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 128.

Rijksregister zelf. De vereiste van de voorafgaande machtiging door het sectoraal comité van het Rijksregister kan daarom een zeer interessante optie genoemd worden.

2.1.2. E-ID

TECHNISCHE ASPECTEN VAN DE E-ID - Een tweede pijler is de e-ID, de elektronische identiteitskaart. Deze smartcard kan gebruikt worden voor identificatie, authenticatie en het voor plaatsen van gekwalificeerde elektronische handtekeningen.[91] De informatie die op de chip van de kaart zelf geplaatst wordt, is echter erg beperkt. Het gaat hier voornamelijk om een herhaling van de informatie die ook visueel op de kaart aanwezig is. Wat betreft informatie die enkel elektronisch leesbaar is, gaat het in de eerste plaats om de hoofdverblijfplaats.[92] Daarnaast vinden we op de chip ook nog twee certificaten, het ene voor authenticatie, het andere voor het plaatsen van elektronische handtekeningen in de zin van Richtlijn 1999/93/EG. Deze certificaten corresponderen met twee RSA sleutelparen.[93] Tot slot is er nog een derde sleutelpaar voor de kaart zelf, dat enkel gebruikt wordt om de kaart te authentiseren ten overstaan van het Rijksregister, bijvoorbeeld wanneer de adresgegevens van de kaarthouder geactualiseerd moeten worden.[94] De certificaten worden uitgegeven door een erkende certificatieautoriteit volgens de X.509v3 standaard.[95] De sleutelparen worden gebruikt binnen een publieke sleutel infrastructuur en voor een bijkomende graad van zekerheid bij de authenticatie of de elektronische handtekening kan er ook vereist worden dat de kaarthouder zijn persoonlijk identificatienummer invoert vooraleer toegang te krijgen tot bepaalde faciliteiten.[96] We dienen hier wel op te merken dat er maar één enkele PIN wordt gebruikt voor beide functies, hoewel technisch gezien zonder problemen een tweede PIN kan worden opgenomen. Het gebruik van één PIN voor beide certificaten kan voor de burger onduidelijkheid scheppen over welk certificaat er nu precies gebruikt.[97] Indien elk certificaat over een eigen PIN zou beschikken, kan er geen twijfel bestaan over welk certificaat er door het presenteren van de PIN geactiveerd wordt. Dit zou allicht ook de gebruiksvriendelijkheid ten goede komen.

DE E-ID EN HET RIJKSREGISTERNUMMER - Dan is er ook nog het Rijksregisternummer. Waar het vroeger optioneel was om dit nummer te laten vermelden op de identiteitskaart, is het nu een *conditio sine qua non* geworden. Tijdens het ontwerpen van de wetgeving op de e-ID heeft dit voor een aantal controverses gezorgd.[98] Daarnaast vinden we het Rijksregisternummer ook terug in de twee certificaten op de chip. Bij iedere authenticatie of bij iedere elektronische handtekening met behulp van de e-ID, wordt dus - al dan niet gewenst - het Rijksregisternummer bekend gemaakt aan betrokken derden.[99] Daar de overheid op dit moment het gebruik van de e-ID buiten

---

[91] Meer details over de Belgische e-ID: www.ibz.rrn.fgov.be.
[92] IDEM, "Deliverable 1.2 Conceptual Framework (v1.0)", 31 oktober 2006. *onuitg.,* 124.
[93] RSA is een asymmetrisch encryptiealgoritme vooral gebruikt bij e-commerce en e-Government.
[94] IDEM, "Deliverable 1.2 Conceptual Framework (v1.0)", 31 oktober 2006. *onuitg.,* 125.
[95] Er zijn drie niveau's van certificatieautoriteiten: De commerciële Root CA (GlobalSign), de Belgische Root CA en de Citizen CA. Voor meer informatie: B. VAN ALSENOY, D. DE COCK, "Due Processing of Personal Data in eGovernment", *Datenschutz und Datensicherheit*, 3/2008, 178 e.v.
[96] De 'MijnDossier' applicatie vereist de zowel controle van het authenticatiecertificaat als de invoer van de PIN.
[97] B. VAN ALSENOY, D. DE COCK, "Due Processing of Personal Data in eGovernment", *Datenschutz und Datensicherheit*, 3/2008, 180.
[98] Zie: D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 340.
[99] J. DUMORTIER, "eID en de paradoks van het rijksregisternummer", *Trends Business ICT*, maart 2005.

de overheidscontext wil stimuleren, zal ook daar steeds vaker en vaker het Rijksregisternummer doorgegeven worden aan entiteiten die niet gemachtigd zijn om dit nummer te verwerken.[100] Men kan zich dan natuurlijk afvragen of dit nummer wel zo veralgemeend aanwezig dient te zijn.

HET 'GEBRUIK' VAN HET RIJKSREGISTERNUMMER - Ondanks de bescherming die artikel 8 van de Wet op het Rijksregister dankzij het gebruik van een voorafgaande machtiging biedt, zien we dat het nu wel erg gemakkelijk wordt om kennis te nemen van het Rijksregisternummer van een persoon. We dienen echter wel te onthouden dat artikel 8 spreekt over het 'gebruik' van het Rijksregisternummer. Men zou kunnen argumenteren dat de loutere kennisname van het Rijksregisternummer van een persoon niet voldoende is om van 'gebruik' in de zin van artikel 8 van de wet op het Rijksregister te spreken.[101] Ongeacht het al dan niet gelden van voorgaande redenering blijven echter wel de bepalingen met betrekking tot de verwerking van persoonsgegevens nog steeds van kracht.

2.1.3. GEVALIDEERDE AUTHENTIEKE BRONNEN

AUTHENTIEKE BRONNEN - De derde bouwsteen die we hier bespreken is die van de gevalideerde authentieke bronnen. Men kan er van uit gaan dat bepaalde gegevens zoals kenmerken of mandaten niet voldoende gestaafd kunnen worden door middel van loutere verklaringen van een gebruiker, of zelfs niet door middel van de e-ID. Zulke informatie vereist een bron die op afdoende wijze de validiteit en actualiteit ervan kan staven.[102] In een degelijk systeem voor gebruikers- en toegangsbeheer, zal men bijgevolg moeten kunnen terugkoppelen naar wat we kunnen omschrijven als gevalideerde authentieke bronnen. Deze bronnen dienen voldoende garantie te bieden dat de informatie waarover zij beschikken correct is en kunnen aldus ook bijdragen tot het bestrijden van fraude. Om zulk systeem op een werkbare manier te organiseren, dient men daarom te weten waar men welke informatie kan halen. Men dient bijgevolg te beschikken over een logisch georganiseerde inventaris van gevalideerde authentieke bronnen, waar men snel de benodigde informatie in terug kan vinden. Door bepaalde informatie bij authentieke bronnen te laten, zorgt dit systeem er ook voor dat men deze niet centraal hoeft te bewaren, wat uiteraard ook de eenmalige gegevensinzameling ten goede kan komen.[103]

2.1.4. DIENSTENINTEGRATOREN[104]

[100] B. VAN ALSENOY, D. DE COCK, "Due Processing of Personal Data in eGovernment", *Datenschutz und Datensicherheit*, 3/2008, 181.
[101] D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 189; FIDIS, "D13.3: Study on ID number policies", 14 september 2007, *www.fidis.net,* 58-59.
[102] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; *www.law.kuleuven.be/icri/frobben,* 5. Zie ook de definitie van authentieke bronnen op: *www.fedict.belgium.be.*
[103] IDEM, "D2.1b: List of Privacy Requirements and Recommendations", *onuitg.*, 11.
[104] Zie de Kruispuntbank van de Sociale Zekerheid (KSZ), *www.ksz-bcss.fgov.be* en het eHealth platform, *www.ehealth.fgov.be*. De Kruispuntbank voor Ondernemingen (KBO) is - ondanks haar naam - eerder te beschouwen als een authentieke bron, *mineco.fgov.be/kbo.htm.* Op internationaal vlak spreekt men van *clearing houses*, X. HUYSMANS, "Privacy-friendly Identity Management for eGovernment", 2006, *www.w3.org*, 3.

BELGISCHE KRUISPUNTBANKEN - De Belgische overheid heeft begrepen dat een verregaande integratie van diensten en informatie nodig is, maar dat dit ook niet gemakkelijk te bereiken is. Daarom doet men beroep op een derde partij om deze diensten te integreren. Deze derde partij zorgt er voor dat de communicatie tussen de verschillende overheidsdiensten vlot kan verlopen en dat de wetgeving in verband met de bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens gerespecteerd wordt.[105] Een belangrijke *caveat* hier is dat het Belgisch model enkel de diensten zelf op elkaar wil afstemmen. Een gecentraliseerde opslag van gegevens - met andere woorden gegevensintegratie - wordt niet nagestreefd en dient vermeden te worden.[106] Zulke dienstenintegrator wordt gecontroleerd door de Commissie voor de bescherming van de persoonlijke levenssfeer en wordt beheerd door vertegenwoordigers van de betrokken overheidsdiensten in die bepaalde sector.[107] Ten einde de dienstenintegratie vlot te doen verlopen, kan men gebruik maken van een verwijzingsrepertorium.[108] Zulk repertorium kan drieledig zijn.[109] Het personenrepertorium houdt bij wie welke dossiers bezit en in welke hoedanigheid en voor welke periodes. Een gegevensbeschikbaarheidstabel kan ons zeggen welke persoonsgegevens beschikbaar zijn bij welke actoren in de verschillende soorten dossiers. Een toegangsmachtigingstabel zegt ten slotte welke actoren welke persoonsgegevens van welke dossiers en voor welke periodes krijgen.[110]

2.1.5. SECTORALE COMITÉS

OPGERICHT BINNEN DE CBPL - De vijfde en laatste bouwsteen die we hier wensen te bespreken, is die van de sectorale comités voor de bescherming van de persoonlijke levenssfeer. Zoals de naam al doet vermoeden is elk comité verbonden aan de in de betrokken sector bevoegde dienstenintegrator.[111] Ze maken trouwens deel uit van de Commissie voor de bescherming van de persoonlijke levenssfeer.[112] Binnen hun sector staan de comités in voor onder meer het toezicht op de naleving van de wetgeving met betrekking tot de privacybescherming en de verwerking van persoonsgegevens, door voor hun sector de machtigingen tot uitwisseling van persoonsgegevens te verlenen. Een voorbeeld is het sectoraal comité van het Rijksregister waar naar verwezen wordt in artikelen 15 en 16 van de wet op het Rijksregister.[113]

[105] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; *www.law.kuleuven.be/icri/frobben,* 6.

[106] F. ROBBEN, "eGovernment, eHealth en bescherming van de privacy", 18 april 2008, *www.law.kuleuven.be/icri/frobben,* slide 8.

[107] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; www.law.kuleuven.be/icri/frobben, 6-7.

[108] Ook de Commissie voor de Bescherming van de Persoonlijke Levenssfeer raadt het gebruik van verwijzingsrepertoria aan: CBPL, aanbeveling 03/2009 van 1 juli 2009, *www.privacycommission.be,* 5.

[109] F. ROBBEN, "eGovernment, eHealth en bescherming van de privacy", 18 april 2008, *www.law.kuleuven.be/icri/frobben,* slide 9. Zie ook COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling 03/2009 van 1 juli 2009, *www.privacycommission.be,* 7.

[110] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; www.law.kuleuven.be/icri/frobben, 7-8.

[111] Het belangrijkste voorbeeld is hier het sectoraal comité van de Sociale Zekerheid en van de Gezondheid verbonden aan de KSZ. We herhalen dat de KBO meer een authentieke bron is in plaats van een werkelijke dienstenintegrator.

[112] Hun samenstelling is geregeld volgens artikel 3 Koninklijk besluit van 17 december 2003 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer, *B.S.* 30 december 2003, 62034.

[113] Art. 15 en 16 Wet tot regeling van een Rijksregister van de natuurlijke personen van 8 augustus 1983, *B.S*. 21 april 1984.

MACHTIGINGEN - Het zijn deze sectorale comités die beschouwd kunnen worden als één van de voornaamste waarborgen voor de bescherming van de persoonlijke levenssfeer tegen de verwerking van persoonsgegevens. Door het verlenen van machtigingen tot toegang of tot gebruik van bepaalde persoonsgegevens, zijn het immers zij die er voor dienen te zorgen dat de persoonsgegevens van de burgers - inclusief hun Rijksregisternummer - niet onnodig worden verspreid.

2.1.6. CONCLUSIE

RIJKSREGISTERNUMMER EN E-ID ALS BELANGRIJKSTE BOUWSTENEN … - Met dit overzicht kennen we de belangrijkste bouwstenen van het Belgisch beleid met betrekking tot e-Government. Zoals eerder aangehaald kan het gebruik van een enkele unieke identificator zoals het Rijksregisternummer zeker verdedigd worden vanuit de optiek van de gebruiksvriendelijkheid. We zullen echter moeten onderzoeken of het gebruik van sectorgebonden unieke identificatoren ook effectief tot een verlies aan gebruiksvriendelijkheid kan leiden. Ook de nood aan transparantie en privacybescherming zullen in deze pijler worden onderzocht. Wat betreft de e-ID was België bij de eerste Europese landen om zulk project succesvol op poten te zetten. Het kan daarom interessant zijn om te kijken hoe het zit met landen die pas later hun systeem hebben ingevoerd. Ook zullen we kijken welke unieke identificatoren verbonden zijn met de identiteitskaarten van andere landen. Voor de landen met een enkele unieke identificator, zoals Zweden, dienen we na te gaan of zulk nummer op actieve wijze verspreid wordt en of het gebruik van dat nummer geregeld is of niet. We zullen onderzoeken of het Belgisch gebruik van voorafgaande machtigingen kan volstaan vanuit het standpunt van de privacybescherming.

… MAAR MET AANDACHT VOOR DE ANDERE PIJLERS - Hoewel die eerste twee pijlers steeds de meeste aandacht krijgen, dienen we ook te onderzoeken wat andere landen denken over gevalideerde authentieke bronnen en de eenmalige gegevensinzameling. Ook het gebruik van dienstenintegratoren dient vergeleken te worden met andere landen. Zoals eerder aangegeven, kan het lijken alsof er een zeer dunne lijn loopt tussen de integratie van diensten en de integratie van gegevens. Hoewel België duidelijk enkel een geïntegreerde dienstverlening nastreeft en gegevensintegratie wil vermijden, is het mogelijk dat andere landen daar meer open voor staan. Ook de sectorale comités worden opgenomen in dit onderzoek. We dienen te kijken hoe andere landen een voldoende beveiliging van de gebruikte gegevens garanderen.

2.2. RECHTSVERGELIJKEND ONDERZOEK MET ANDERE EUROPESE LANDEN

NUT VAN EEN RECHTSVERGELIJKEND ONDERZOEK - Uit het voorgaande onderzoek zijn er al een aantal interessante punten naar voren gekomen. Het Belgisch beleid beschikt zeker en vast over een aantal sterke troeven, maar er zijn ook bepaalde punten die naar de toekomst toe nog verder zouden kunnen evolueren. In dit deel van het onderzoek willen we daarom voor een select aantal Europese landen onderzoek voeren naar wat de bouwstenen zijn van het beleid dat die landen er op na houden. Het spreekt echter voor zich dat niet elk land haar bouwstenen met betrekking tot e-Government op identieke wijze zal indelen als België. Toch zullen we voor dit rechtsvergelijkend onderzoek de Belgische bouwstenen als leidraad gebruiken bij het bespreken van het beleid van andere landen. Er zal daarom getracht worden om voor elk land een equivalent te vinden voor de vijf Belgische bouwstenen die we hier besproken hebben. Daarbij wordt er ook aandacht besteed aan de drie belangrijkste doelstellingen waarvoor gegevenskoppeling nodig zou zijn, namelijk de eenmalige gegevensinzameling, de geïntegreerde dienstverlening en de fraudebestrijding. Het doel is om deze rechtsvergelijkende studie zo pragmatisch mogelijk te houden. Dit onderzoek zal daarom de basis vormen voor de evaluatie van en de aanbevelingen voor het Belgisch beleid.

WELKE LANDEN TE ONDERZOEKEN? - Het spreekt voor zich dat het binnen het kader van deze studie onmogelijk is om alle Europese lidstaten op te nemen in dit rechtsvergelijkend onderzoek. Er zal daarom een selectie van te onderzoeken landen gemaakt moeten worden, met als belangrijkste criterium de mate waarin het beleid met betrekking tot unieke identificatoren en identiteitskaarten van dat land interessante punten kan aanbieden voor het Belgisch beleid. Om deze reden werd er besloten om Oostenrijk, Duitsland, Zweden, het Verenigd Koninkrijk en Portugal op te nemen in dit rechtsvergelijkend onderzoek. Er werd gekozen voor Oostenrijk wegens de reputatie die dit land geniet met betrekking tot het gebruik van sectorgebonden identificatoren. Aangezien het Oostenrijkse beleid intussen al een aantal jaren in de praktijk omgezet is, zal het geen probleem zijn om dit beleid te evalueren. Duitsland werd gekozen wegens de grondwettelijke problemen in verband met het gebruik van unieke identificatoren en omdat het interessant is om te kijken in hoeverre het beleid gesteund zal worden op het Oostenrijks model. Zweden behoort tot de selectie wegens het gebruik van een enkele unieke identificator en om een beeld te vormen van de Noord-Europese situatie. We kozen voor het Verenigd Koninkrijk omdat dit land – net als Duitsland – nog bezig is met het uitwerken van een eigen beleid en om op deze manier ook de problematiek vanuit een Angelsaksische invalshoek te kunnen onderzoeken. Tot slot kozen we voor Portugal omdat dit land op unieke wijze verschillende unieke identificatoren weet te balanceren en om zo ook de Zuid-Europese situatie te kunnen bekijken. Hoewel de Belgische wetgever traditioneel kijkt naar het beleid van onze Noorder- en Zuiderburen – Nederland en Frankrijk – werd besloten om deze landen niet in de selectie op te nemen. Het beleid van deze landen met betrekking tot deze materie staat op dit moment immers nog niet op punt. Daarnaast lijkt het erop dat het beleid van deze landen grote gelijkenissen zal vertonen met beleidspunten van de overige landen in deze rechtsvergelijkende studie. Een bijkomend onderzoek naar het beleid van Nederland en Frankrijk lijkt daarom op dit punt geen meerwaarde te bieden.

PUBLIEKE SECTOR VERSUS PRIVATE SECTOR - Een laatste beperking op de omvang van dit rechtsvergelijkend onderzoek houdt in dat het onderzoek zich enkel zal richten op het huidige beleid van de in deze rechtsvergelijking besproken landen. Dit wil zeggen dat er enkel melding gemaakt zal worden van de systemen voor identiteits- en toegangsbeheer zoals zij op dit moment door de overheden van de betrokken landen toegepast worden. Private initiatieven – zoals het recent gelanceerde Microsoft Forefront Identity Manager 2010 – zullen daarom niet besproken worden in deze studie. Deze toepassingen kunnen uiteraard een rol spelen in de verdere ontwikkeling in het beleid van een Staat, maar worden op dit moment niet als dusdanig toegepast in de hier besproken landen.

2.2.1. OOSTENRIJK

OOSTENRIJKS PLATFORM - Oostenrijk staat met betrekking tot deze materie vooral bekend door het gebruik van sectorgebonden identificatoren. Daarnaast zagen we ook dat Oostenrijk ondermeer door het unieke concept van de *Bürgerkarte* ook op andere vlakken een meer diepgaand onderzoek waard is. Het belangrijkste kenmerk van het Oostenrijkse platform is dat het zeer open is. De bedoeling is om een centraal portaal aan te bieden, waar men op eenvoudige wijze nieuwe toepassingen in kan voegen.[114]

SECTORGEBONDEN IDENTIFICATOREN - De voor dit onderzoek belangrijkste eigenschap van het Oostenrijkse systeem, is het gebruik van **sectorgebonden identificatoren**. Oostenrijk beschikt sinds kort over een centraal bevolkingsregister (het *Zentrales Melderegister* of ZMR), dat vergelijkbaar is met ons Rijksregister.[115] De toegang tot het register lijkt op het eerste zicht sterk op het Belgisch systeem van voorafgaande machtiging.[116] De eigenlijke toegang wordt echter verleend via het beveiligde centrale overheidsportaal.[117] Daar Oostenrijk geen onmiddellijke basis had voor de opbouw van zulk register, werden de resultaten van de volkstelling van 2001 hiertoe aangewend.[118] Het identificatienummer van het register wordt strikt geheim gehouden en er wordt daarom een *SourcePIN* berekend die opgeslagen wordt op de *Bürgerkarte*.[119] Van deze *SourcePIN* berekent men vervolgens sectorgebonden PINs.[120] Met dit systeem hoopt de Oostenrijkse overheid de identiteit van de burger volledig te kunnen afschermen tegen inbreuken op de privacy en fraude. Men kan immers hoogstens iemands sectorgebonden PIN zien, die niet voldoende mag zijn om de *SourcePIN* van die persoon te achterhalen. Dit is een sterk contrast met België, waar het Rijksregisternummer zeer open op de kaart aanwezig is en vervolgens ook gebruikt wordt in beide certificaten op de kaart.

GEBRUIKSVRIENDELIJKHEID - Het werkelijke succes van zulk systeem zal voor een groot deel afhangen van de gebruiksvriendelijkheid ervan. Zeker in een land waar het niet verplicht is om een identiteitsbewijs te bezitten, zal het succes van het platform volledig afhangen van de graad van gebruik door de burgers. Nu het systeem al een aantal jaren praktijkervaring achter de rug heeft, zal het geen probleem zijn om het initiële succes van dit beleid te evalueren. In een studie van de Verenigde Naties naar de aangeboden functionaliteiten van e-Government en het gebruik ervan door de burger landt Oostenrijk buiten de top tien van de op het vlak van e-Government meest geavanceerde landen.[121] Daarnaast blijkt uit recente cijfers dat er slechts een klein percentage van de potentiële *Bürgerkarten* ook effectief als dusdanig geactiveerd werd.[122] De Oostenrijkse burger lijkt dus niet onder de indruk te zijn van het project. Niet alleen slaat het geplande systeem niet aan, er blijken ook ondernemingen te zijn die proberen de sect-

[114] Dit is wat men hier als '*building blocks*' aanduidt: OOSTENRIJKSE FEDERALE KANSELARIJ, "Administration on the Net: The ABC guide of eGovernment in Austria", juli 2008, *www.digitales.oesterreich.gv.at*, 63.

[115] De in het ZMR opgenomen data zijn nagenoeg identiek aan wat er in het Rijksregister te vinden is, *zmr.bmi.gv.at*.

[116] Bepaalde personen of instanties vereisen immers een machtiging, artikel 16a Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 - MeldeG), *BGBl.* 9/1992, laatste wijziging in *BGBl.* I 45/2006.

[117] Het register maakt op deze manier deel uit van het geïntegreerde overheidsplatform, *zmr.bmi.gv.at*.

[118] "*Das Zentrale Melderegister (ZMR) wurde im zeitlichen Zusammenhang mit der Volkszählung -Stichtag 15.5.2001- geschaffen. Seit 1.3.2002 ist das neue Meldegesetz in Kraft und genau zu diesem Zeitpunkt erfolgte der Echtbetrieb des zentralen Melderegisters*", *zmr.bmi.gv.at.*

[119] Over hoe die berekening in zijn werk gaat: OOSTENRIJKSE FEDERALE KANSELARIJ, "Administration on the Net: The ABC guide of eGovernment in Austria", juli 2008, *www.digitales.oesterreich.gv.at*, 91-92.

[120] FIDIS, "D13.3: Study on ID number policies", 14 september 2007, *www.fidis.net,* 85-86.

[121] UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, *E-Government Survey 2008: From E-Government to Connected Governance (ST/ESA/PAD/SER.E/112),* New York, United Nations Publication, 2008, 20+58.

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

orgebonden PIN te omzeilen door *de facto* enkele unieke identificatoren te hanteren.[123] Zo gebruikt Oostenrijk bijvoorbeeld nog een identificatienummer voor de sociale zekerheid, wat aanwezig is op de *e-Card* – de Oostenrijkse tegenhanger van de Belgische SIS-kaart. Dit nummer wordt niet beschermd – in tegenstelling tot het ZMR-nummer – en kan dus in principe relatief vrij gebruikt worden. De *e-card* en het bijbehorende identificatienummer worden uitgereikt aan iedere Oostenrijkse burger die aangesloten is bij de Oostenrijkse sociale zekerheid. Aangezien Oostenrijk zulke aansluiting verplicht, wil dit zeggen dat de *e-card* in theorie quasi de gehele Oostenrijkse bevolking bestrijkt. Het identificatienummer van de sociale zekerheid heeft daarom het juiste potentieel om als *de facto* enige unieke identificator gebruikt te worden, wat in de praktijk ook lijkt voor te komen.[124] Hoewel de *e-card* in principe slechts bedoeld was voor gebruik binnen de sector van de sociale zekerheid, is deze kaart geschikt om als *Bürgerkarte* geactiveerd te worden. In dit geval moeten we concluderen dat het gebruik van sectorgebonden identificatoren effectief tot verlies aan gebruiksvriendelijkheid zou kunnen leiden. Ook voor de overheidsdiensten zelf kunnen er opmerkingen gemaakt worden met betrekking tot de gebruiksvriendelijkheid van dit systeem. De problematiek van de gegevenskoppelingen is hier een treffend voorbeeld van.[125]

TRANSPARANTIE - Naast de vraag naar de gebruiksvriendelijkheid van het systeem, willen we ook de transparantie van dit systeem onderzoeken. Er zijn immers zeker een aantal interessante principes te vinden in het Oostenrijkse systeem, zoals onpersoonlijke identificatienummers en partiële identiteiten. Daarnaast is de Oostenrijkse *Datenschutzgesetz* is bijgevolg van toepassing en zal er dus rekening gehouden moeten worden met onder andere het finaliteit- en proportionaliteitsprincipe uit de Richtlijn. De kern van dit systeem is echter de sterke beveiliging. Hoewel zulke beveiliging interessant kan lijken, kan die echter ook een probleem van een andere orde worden. Er dient immers voldoende transparantie naar de burger toe te zijn. De hoge graad van techniciteit van de Oostenrijkse beveiliging, zou er toe kunnen leiden dat de burger wat verloren loopt in het kluwen van PINs, hashfuncties en dergelijke.[126] De overheid zal haar onderdanen dus voldoende moeten informeren over hoe het systeem in zijn werk gaat. Indien de overheid dit niet doet, kan de burger het systeem gaan wantrouwen of kan men zelfs denken aan het probleem van '*security through obscurity*'.[127] Het gebruik van cryptografie als beveiligingsmaatregel kan daarom zeer interessant lijken, maar er dient voldoende ruimte open gelaten te worden voor transparantie en inlichting van de burger. Die eis van transparantie maakt ook een be-

---

[123] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; *www.law.kuleuven.be/icri/frobben,* 4.

[124] Er wordt gerapporteerd dat dit identificatienummer ook buiten de sector van de sociale zekerheid gebruikt wordt: IDABC, "eID Interoperability for PEGS: Update of Country Profiles Study - Austrian Country Profile", *ec.europa.eu/idabc*, 9. De centrale privacyautoriteit heeft zich recent uitgesproken tegen het onnodig gebruik van het identificatienummer van de sociale zekerheid. DATENSCHUTZRAT, „Stellungnahme Zur Untersuchung von Alternativen zur Sozialversicherungsnummer in der Bildungsdokumentation", 25 februari 2010, *www.bka.gv.at*.

[125] Zo is het volgens de Oostenrijkse wet op de e-Government quasi onmogelijk voor een overheidsdienst om gegevens over een burger uit de ene sector te linken aan gegevens over diezelfde burger uit een andere sector. Dit kan de efficiënte werking van die overheidsdiensten ernstig belemmeren. Op deze problematiek zal onder hoofdstuk 2.3.1 van deel II van dit project dieper ingegaan worden.

[126] Ook ondernemingen proberen de sectorgebonden PINs te ontwijken: J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr 2, 52-60; *www.law.kuleuven.be/icri/frobben*, 4.

[127] Hierbij steunt de beveiliging van het systeem op de geheimzinnigheid die er rond hangt. Door die geheimzinnigheid probeert men de zwakke plakken in het systeem te verbergen. Dit staat in contrast met het principe van Kerckhoffs dat vertrouwt op de intrinsieke sterkte van het systeem, ook al wordt alles behalve de sleutel publiek gemaakt. A. KERCKHOFFS, "La Cryptografie Militaire", *Journal des Sciences Militaires*, Vol. IX, 1883, 12.

langrijk deel uit van de privacybescherming. Hoofdstuk II, afdeling IV van Richtlijn 95/46/EC bepaalt immers welke informatie meegedeeld dient te worden aan de betrokkene van die verwerking. Aan het transparantiebeginsel wordt veel belang gehecht en men dient er bijgevolg over te waken dat dit beginsel voldoende wordt nageleefd.[128]

BÜRGERKARTE - Als we de tweede Belgische pijler, de **e-ID**, willen vergelijken met het Oostenrijkse beleid, stoten we op een probleem. Het concept van de *Bürgerkarte* is vrij verschillend van de Belgische e-ID en het is dus maar de vraag of de doelstellingen van beide werkelijk gelijkaardig - en bijgevolg vergelijkbaar - zijn.[129] De e-ID is in de eerste plaats immers een verplicht identiteitsbewijs dat dankzij de huidige technologie een paar nieuwe functies heeft gekregen. Oostenrijk kent wat dat betreft de *Identitätsausweis* voor binnenlandse identificatie. Voor reizen binnen de Schengenlanden is er de *Personalausweis* en voor verdere reizen de *Reisepass*. De Belgische e-ID zou dus veeleer met de *Personalausweis* vergeleken moeten worden.[130] De *Personalausweis* is echter geen werkelijke elektronische kaart zoals de Belgische e-ID. Daar Oostenrijk geen verplichting tot het dragen van een identiteitsbewijs kent, worden de hier aangehaalde identiteitsdocumenten overigens maar zeer occasioneel gebruikt.

AUTHENTIEKE BRONNEN - Wat het gebruik van **gevalideerde authentieke bronnen** betreft zien we dat Oostenrijk dit niet als een algemeen uitgangspunt gebruikt.[131] Verificatie van mandaten en/of kenmerken zal dus via verschillende kanalen kunnen plaatsvinden, waarbij men dus ook de betrouwbaarheid van elk kanaal zal moeten nagaan. Wat betreft de verificatie van bijvoorbeeld mandaten, zien we dat men hiertoe de *Bürgerkarte* kan gebruiken.[132] Men kan bijvoorbeeld mandaten verwerken in een XML bestand en laten ondertekenen door de autoriteit die het register van de *SourcePIN* beheert. Vervolgens wordt het XML bestand opgeslagen op de *Bürgerkarte* en kan het gebruikt worden als een rechtsgeldig mandaat. Waar de Belgische dienstenintegratoren dus authentieke bronnen gebruiken om de geldigheid van mandaten en autorisaties te controleren, steunt het Oostenrijkse systeem op een door een erkende autoriteit ondertekend XML bestand. Ook dit lijkt af te wijken van het Belgisch beleid waar men niet wil steunen op informatie aangereikt door de e-ID of bij uitbreiding door de burger zelf.

DIENSTENINTEGRATOREN - Op het vlak van **dienstenintegratoren** lijkt Oostenrijk wel een enigszins vergelijkbare koers te varen als België. Ook in Oostenrijk ziet men - getuige de opbouw van het e-Government platform - de noodzaak van een verregaande integratie van de verschillende overheidstoepassingen. En ook in Oostenrijk spreekt men over een knooppunt - een zogenaamde *Verzeichnisdienst* - waar de verschillende overheidsdiensten, zowel federaal als lokaal, geïntegreerd worden voor gebruik tussen verschillende overheden, maar ook voor gebruik naar de

[128] Zie het sectoraal comité voor de Federale Overheid dat zegt dat er slechts een eerlijke verwerking van persoonsgegevens is wanneer dit transparant gebeurt. Daarnaast beschouwt het comité de informatieplicht als een hoeksteen van het transparantiebeginsel, SECTORAAL COMITÉ VOOR DE FEDERALE OVERHEID, “Beraadslaging FO nr. 05/2009”, 16 april 2009, *www.privacycommission.be*, randnummer 36. Ook overweging 38 bij de Richtlijn maakt melding van het belang van de informatieplicht.

[129] Zo is de *Bürgerkarte* allereerst een technologieneutraal concept en geen *smartcard*. Daarnaast zien we dat het plaatsen van elektronische handtekeningen is als belangrijkste doel van dit concept wordt gepropageerd.

[130] De Belgische e-ID geldt - zoals de *Personalausweis* - immers ook in de Schengenlanden. België heeft geen identiteitsbewijs dat enkel geldig is in het binnenland, zoals de *Identitätsausweis*.

[131] Er zijn overigens geen plannen tot toenadering tot dit principe. Zie: IDABC, “eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability”, 2007, *ec.europa.eu/idabc*, 69.

[132] IDABC, “eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability”, 2007, *ec.europa.eu/idabc*, 83 en 86. Binnenkort volgt een update van deze studie.

burger toe.[133] Net als de PINs zijn deze diensten sectorgebonden.[134] Deze knooppunten zijn de Oostenrijkse implementatie van een geïntegreerde dienstverlening.[135]

PRIVACYBESCHERMING - De **sectorale comités** zijn iets wat men niet kent in Oostenrijk. Naast een centrale privacycommissie - de *Datenschutzkommission* - die het algemene toezicht op de privacybescherming voert, is er nog een centrale privacyraad, de *Datenschutzrat*. Die raad adviseert op verzoek van de federale en regionale overheden in verband met hun beleid op het gebied van privacybescherming. Hoewel de Oostenrijkse privacycommissie wel de toezichthoudende autoriteit is en dus bevoegd is voor het ontvangen van aanmeldingen tot de verwerking van persoonsgegevens, is dit orgaan niet bevoegd voor het verlenen van machtigingen voor de toegang tot het personenregister. Die bevoegdheid ligt in principe bij de Minister van Binnenlandse Zaken.[136] De Oostenrijkse privacycommissie kan daarom beschouwd worden als een klassieke toezichthoudende autoriteit zoals bepaald in de Europese Richtlijn. Er zijn geen opmerkelijke bijkomende bevoegdheden.

GEEN IDEAAL SYSTEEM - Concluderend moeten we allereerst herhalen dat het net het gebrek aan historische evolutie op het gebied van deze materie was die voor Oostenrijk de weg vrijmaakte om al de geplande veranderingen op deze schaal te implementeren. De implementatie van zulk systeem in een land met een traditie met betrekking tot deze materie zal daarom geen sinecure zijn. Ook is het moeilijk om te zeggen of het overnemen van zulk systeem ook effectief zal werken in zulk land.[137] Het rechtsvergelijkend onderzoek dat we hier voerden, toont overigens aan dat het Oostenrijkse systeem in de praktijk niet zo goed is als oorspronkelijk werd gedacht. Zo tonen recentere studies aan dat het belangrijkste onderdeel van dit systeem, de *Bürgerkarte,* slechts een zeer klein percentage van de bevolking heeft kunnen aanspreken.[138] Ook wat betreft gebruiksvriendelijkheid en transparantie zagen we dat er nog een aantal bedenkingen te maken zijn bij dit systeem. Wat privacybescherming betreft zagen we dat de uitgebreide beveiliging die Oostenrijk hanteert niet kan verhinderen dat de wetgeving met betrekking tot de verwerking van persoonsgegevens van toepassing blijft. Dit leidt ons tot de conclusie dat het Oostenrijkse systeem zeker wel een aantal interessante punten kent, maar dat het systeem in zijn geheel niet als een waardig alternatief kan worden beschouwd voor een land dat al een actief beleid voert met betrekking tot deze materie.

2.2.2. ZWEDEN

ZWEEDSE E-GOVERNMENT - Aangezien Zweden ook een enkele unieke identificator gebruikt, zou dit beleid meer gelijkenissen moeten vertonen met het Belgisch beleid. Daarnaast komt Zweden in

[133] *www.digitales.oesterreich.gv.at.*
[134] Zie de *eHealth Verzeichnisdienst*, opgericht bij artikel 10 van de Gesundheitsreformgesetz 2005, *BGBl. I* Nr. 179/2004. Daarnaast is er een centraal platform voor verdere integratie: *reference.e-government.gv.at.*
[135] Gezien de omvang gaat het hier om meer dan een gewoon portaal. Aangezien het knooppunt voor eHealth ook zelf informatie bewaart, zou men echter kunnen argumenteren dat het hier om gegevensintegratie gaat. De hier bewaarde informatie is echter van te kleine omvang om te kunnen spreken van werkelijke gegevensintegratie.
[136] Artikel 16a Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 - MeldeG), *BGBl.* 9/1992, laatste wijziging in *BGBl.* I 45/2006.
[137] Zoals bij het onderzoek naar het Zweeds beleid zal blijken is de historische en culturele achtergrond van een land hier ook een niet te onderschatten factor.
[138] IDABC, "eID Interoperability for PEGS: Update of Country Profiles Study - Austrian Country Profile", *ec.europa.eu/idabc*, 6.

verschillende studies naar voren als één van de best presterende landen met betrekking tot e-Government.[139] Het algemene uitgangspunt in het Zweedse eGovernment beleid is dat de overheid 24 uur op 24 en zeven dagen op zeven beschikbaar dient te zijn.[140] De overheid heeft hier echter gekozen voor een lichte aanpak. Zo is er bijvoorbeeld geen overkoepelende wet met betrekking tot eGovernment.[141] De reden hiertoe is dat Zweden zeer gedecentraliseerd bestuurd wordt en dat het dus aan de lokale overheden is om de nodige maatregelen te nemen.[142] De centrale overheid houdt zich bijgevolg voornamelijk bezig met de algemene coördinatie.[143]

NATIONAAL IDENTIFICATIENUMMER EN OPENBAARHEID - Zweden kent dus een **enkele unieke identificator**, namelijk het nummer van het personenregister. De structuur van het nummer is zeer gelijkaardig aan die van het Belgisch Rijksregisternummer.[144] Wat de inhoud van het personenregister betreft, zien we dat deze quasi identiek is aan die van het Rijksregister.[145] Het Zweedse personenregister gaat net als het Rijksregister uit van de eenmalige gegevensinzameling. Deze grote gelijkenissen met het Belgisch systeem zorgen er natuurlijk voor dat we ook dezelfde vragen kunnen stellen als over het Belgisch systeem. Zo zullen we moeten kijken hoe Zweden omgaat met de privacybescherming en de verwerking van persoonsgegevens. Daar beide landen een enkele unieke identificator gebruiken, zal er maar weinig efficiëntieverschil merkbaar zijn. Eventueel verschil kan bijgevolg geweten worden aan de verdere bijzonderheden van het betrokken beleid. Op het vlak van transparantie hebben beide landen gemeen dat zij geen systeem met pseudoniemen en bijbehorende ingewikkelde cryptografische bewerkingen nodig hebben en dat het dus al meteen eenvoudiger wordt om te voldoen aan de eis van transparantie. Toch is de Zweedse situatie nog net iets anders. Zoals bleek uit het historisch onderzoek is transparantie voor Scandinavische landen een zeer belangrijk punt in de verhouding tussen de overheid en de burgers. Zweedse burgers eisen daarom volledige transparantie van hun overheid en zijn bijgevolg in ruil bereid om ook zelf hun gegevens meer open te stellen. Historisch gezien kent men in deze landen een minder prangende vraag naar privacybescherming en heerst er een algemene openbaarheid van informatie. Het belang dat de Zweden hechten aan de openbaarheid van informatie, laat zich afleiden uit het feit dat dit principe beschouwd wordt als deel van de Zweedse grondwet.[146] Al in 1766 nam Zweden - als eerste land ter wereld - een wet aan die de persvrijheid moest vrijwaren.[147] Er wordt algemeen aangenomen dat die wet ook het openbaarheidsprincipe (het *Offentlighetsprincipen*) garandeert.[148] Die openbaarheid leidt er ook toe dat

[139] Zie het eUSER project: EUSER, "eGovernment Brief: Sweden", 2005, *www.euser-eu.org*. Zie ook: UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, *E-Government Survey 2008: From E-Government to Connected Governance(ST/ESA/PAD/SER.E/112),* New York, United Nations Publication, 2008, 20+58.
[140] IDABC, "eGovernment Factsheets: Sweden", 2008, *ec.europa.eu/idabc*, 8. Daarnaast kunnen enkele centrale punten teruggevonden worden in: SWEDISH MINISTRY OF FINANCE, "Public Administration in the Service of Democracy: an Action Programme", 2000, *www.sweden.gov.se.*
[141] IDABC, "eGovernment Factsheets: Sweden", 2008, *ec.europa.eu/idabc*, 11.
[142] *www.sweden.gov.se/sb/d/2102.*
[143] IDABC, "eGovernment Factsheets: Sweden", 2008, *ec.europa.eu/idabc*, 9. Zie de nieuwe strategie: IDABC, "eID Interoperability for PEGS: Update of Country Profiles study - Sweden country profile", 2009, *ec.europa.eu/idabc*, 7-9.
[144] NATIONAL TAX BOARD, "Population Registration in Sweden", 2007, *www.skatteverket.se*, 11.
[145] Het Zweedse register maakt echter wel geen melding van het beroep van de persoon.
[146] De Zweedse grondwet bestaat uit vier fundamentele wetten. *www.regeringen.se/sb/d/2707/a/15187.*
[147] Meer over de Zweedse grondwet en de wet met betrekking tot de persvrijheid: *www.riksdagen.se.*
[148] Zie Hoofdstuk 2, artikel 1 van Freedom of the Press Act, *SFS* 1949:105.

het gebruik van het persoonsnummer in principe vrij is.[149] Ook de toegang tot het personenregister zelf is relatief vrij.[150]

OPENBAARHEID EN PRIVACYBESCHERMING - Hoewel dit principe op gespannen voet lijkt te leven met de privacybescherming, kent Zweden toch een vrij sterke traditie met betrekking tot de bescherming van de persoonlijke levenssfeer. Zo werd er in 1973 al een wet met betrekking tot de bescherming van persoonsgegevens aangenomen, lang voordat er sprake was van zulke bescherming op Europees vlak.[151] De nieuwe versie van de wet - de Personal Data Act 1998 - heeft ter implementatie van Richtlijn 95/46/EG een aantal gevoelige aanpassingen aan het Zweedse systeem ingevoerd.[152] Gezien de ruime uitzonderingen die de wet voorziet, zal de werkelijke impact van Richtlijn 95/46/EG op de Zweedse samenleving maar gering zijn. De bedenkingen die we kunnen formuleren bij de Zweedse privacybescherming zullen daarom gelijkaardig zijn aan de bedenkingen bij het Belgisch beleid. De belangrijkste vraag is of het toelaatbaar is dat een algemeen nationaal identificatienummer zo vrij toegankelijk is. Het antwoord is dat het vanuit een puur privacyrechtelijk standpunt inderdaad beter is om het gebruik van dit nummer af te schermen. Het verschil tussen beide landen is dat Zweden een lange traditie van openbaarheid kent. Omdat België zulke traditie niet kent, kunnen we de Zweedse situatie onmogelijk toepassen op België.

ELEKTRONISCHE IDENTITEITSKAART - Het verhaal met betrekking tot de **e-ID** is enigszins anders. Zweden kent immers geen verplicht identiteitsdocument en er zijn bijgevolg verschillende optionele documenten.[153] Sinds oktober 2005 geeft de Zweedse overheid - via de politie - zelf ook optionele identiteitsbewijzen uit.[154] Het gaat hier om een werkelijke nationale elektronische identiteitskaart die ook geldt voor reizen binnen de Schengenzone. Uiterlijk bevat de kaart ongeveer dezelfde gegevens als de Belgische kaart. Wat de chip betreft zijn er echter een aantal verschillen met de Belgische e-ID. Zo bevat de Zweedse kaart allereerst twee chips, een gewone contactchip zoals de Belgische en een contactloze RFID-chip die biometrische data kan bevatten.[155] Wat de beveiliging betreft kunnen we - bij gebrek aan implementatie - vermoeden dat deze quasi identiek zal zijn aan die van de biometrische paspoorten. Sinds juni 2009 is immers *Extended*

[149] Advies van de Tafel 'Personeelsbeleid in het kader van identiteitsmanagement', juni 2002, *www.ejure.nl,* 136. De informatie uit het personenregister wordt via het Navet-systeem doorgegeven aan een ander register, het *Swedish Population and Address* Register (SPAR). Overheidsdiensten kunnen de benodigde informatie uit het SPAR halen.

[150] NATIONAL TAX BOARD, "Population Registration in Sweden", 2007, *www.skatteverket.se*, 3. Toegang tot het register kan beperkt worden. Ook fiscale gegevens zijn vrij toegankelijk. Er wordt bijgevolg geen voorafgaande machtiging vereist. Overheden kunnen de volledige informatie raadplegen, waar particulieren in principe meer beknopte informatie te zien krijgen. Toegang tot de lokale registers is mogelijk bij de plaatselijke belastingdiensten: GENERAL REGISTER OFFICE, "Citizen Information Project. Annex 6: Population Registers Overseas", 2005, *www.gro.gov.uk*, 10-15.

[151] Een onofficiële Engelstalige versie van de wet: *archive.bild.net/dataprSw.htm.*

[152] Art. 22 vereist toestemming van de betrokken persoon Uitzonderingen hierop zijn mogelijk indien het persoonsnummer nodig is voor het doel van de verwerking, in het kader van een veilige identificatie of bij een andere zwaarwichtige reden. Noch 'veilige identificatie', noch 'zwaarwichtige reden' worden verduidelijkt. De uitzonderingen zijn dus zo ruim dat de bescherming uit de wet quasi nihil is. Art. 7 en 8 bepalen dat de wet geen afbreuk doet aan de vrijheid van meningsuiting, de persvrijheid en het openbaarheidsprincipe.

[153] Het gaat hier van bankkaarten en personeelskaarten tot paspoorten, rijbewijzen en identiteitscertificaten. Zie BankID (*www.bankid.com*) en Nordea (*www.nordea.se*). De politie reikt paspoorten uit: *www.polisen.se/Service/Pass-och-id-kort.* De Zweedse belastingsdienst regelt de identiteitskaart: *www.skatteverket.se/idkort.*

[154] Förordning om nationellt identitetskort, 1 september 2009, *SFS* 2005:661. *www.polisen.se/Service/Pass-och-id-kort/Fragor-kring-pass--och-id-kort/Fakta-om-ID-kort.*

[155] Tot op heden zijn er nog geen certificaten aanwezig op de contactchip: IDABC, "eID Interoperability for PEGS: Update of Country Profiles Study - Sweden Country Profile", *ec.europa.eu/idabc*, 13.

Access Control de verplichte standaard voor beveiliging van de contactloze chips in Europese biometrische paspoorten.[156] Dankzij die op cryptografie gesteunde beveiliging kan de data op de chip niet zonder meer uitgelezen worden en zou die beveiliging dus ook de logische keuze voor de contactloze chip op de e-ID zijn. Daarnaast wordt er vermoed dat de e-ID - net als de Belgische kaart - twee certificaten en twee sleutelparen zal gaan bevatten.[157] De Zweedse e-ID zal wellicht ook het nationaal nummer in beide certificaten vermelden.[158]

AUTHENTIEKE BRONNEN - Op dit ogenblik heeft Zweden nog geen officiële beslissing genomen met betrekking tot het gebruik van **gevalideerde authentieke bronnen**.[159] Er wordt wel sterk gesteund op het personenregister. De gegevens in dat register worden ook doorgestuurd naar het zogenaamde SPAR (*Swedish Population and Address Register*).[160] Het SPAR wordt vervolgens door zowel overheden als private actoren gebruikt als authentieke bron ter identificatie van de persoon.[161] Gezien deze *de facto* toenadering tot het principe is het niet ondenkbaar dat Zweden in de toekomst het gebruik van gevalideerde authentieke bronnen ook officieel zal invoeren. We haalden eerder al aan dat Zweden daarnaast ook het principe van de eenmalige gegevensinzameling volgt.

DIENSTENINTEGRATOREN - De vraag is nu op welke manier de verschillende Zweedse overheden met elkaar samenwerken en of Zweden ook gebruik maakt van **dienstenintegratoren**. Het nieuwe plan voor e-Government wil vooral de interne cohesie en coördinatie aanpakken.[162] Hiervoor is de e-delegatie ingesteld met als doel de verdere coördinatie en integratie tussen de verschillende overheidsdiensten.[163] Deze delegatie is vooral samengesteld uit de Directeurs-generaal van verschillende overheidsdiensten.[164] Het belangrijkste verschil met de Belgische Kruispuntbanken is dat de bijbehorende functies in Zweden dus door slechts één centraal orgaan worden uitgevoerd. Zweden streeft hier dus net als België een geïntegreerde dienstverlening na.

PRIVACYBESCHERMING - Het toezicht op de naleving van de wetgeving met betrekking tot privacybescherming en de verwerking van persoonsgegevens gebeurt door de toezichthoudende autoriteit, het zogenaamde *Datainspektionen*. Dit orgaan probeert vooral duidelijk te maken dat privacy een zeer subjectief gegeven is en dat het aan het individu zelf is om uit te maken wat hij of zij wil toelaten.[165] Ondanks de gedecentraliseerde opbouw van de Zweedse Staat is dit orgaan voor het gehele grondgebied en elke sector bevoegd.[166] Er zijn wel nog *Personal Data Represen-*

---

156 Verordening 444/2009 van 28 mei 2009, *Pb.* L 142 van 6 juni 2009.

157 IDABC, "eID Interoperability for PEGS: Update of Country Profiles Study - Sweden Country Profile", *ec.europa.eu/idabc*, 16.

158 De bestaande elektronische identiteitsbewijzen BankID en de versie van Nordea bevatten immers al het national identificatienummer in beide certificaten: IDABC, "eID Interoperability for PEGS: Update of Country Profiles Study - Sweden Country Profile", *ec.europa.eu/idabc*, 16-18.

159 Zie: IDABC, "eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability", 2007, *ec.europa.eu/idabc*, 70-71.

160 NATIONAL TAX BOARD, "Population Registration in Sweden", 2007, *www.skatteverket.se*, 3.

161 Dit volgt uit artikel 1 van de wet (*Lag om det statliga personadressregistret*) van 11 juni 1998, *SFS* 1998/527. Voor de verdere verspreiding van deze informatie naar verschillende overheden toe is er een centraal platform (*Navet).*

162 Een Engelstalige samenvatting van die nieuwe strategie: *www.epractice.eu/en/document/288378.*

163 M. LIND, O. ÖSTBERG, P. JOHANNISSON, "Acting out the Swedish e-Government action plan - Mind and mend the gaps", *International Journal of Public Information Systems,* vol. 2009:2, 57.

164 *www.edelegationen.se/sida/ledamoter-och-experter.*

165 DATA INSPECTION BOARD, "What on earth does the Data Inspection Board do?", *www.datainspektionen.se*, 5.

166 Voor een organigram: DATA INSPECTION BOARD, "We protect your privacy in the information society", 2005, *www.datainspektionen.se,* 5.

tatives. Deze werknemers zien toe op het naleven van de privacywetgeving binnen hun bedrijf. Deze personen kunnen ook het *Datainspektionen* consulteren. Zweden kent met andere woorden geen **sectorale comités**. Aangezien de toegang tot het personenregister en het gebruik van het persoonsnummer relatief vrij is, hoeft deze privacyautoriteit hier geen voorafgaande machtiging toe te verlenen.

GELIJKENISSEN EN VERSCHILLEN - Zoals we zagen zijn er zeer grote gelijkenissen tussen de Zweedse en de Belgische aanpak. Ondanks een aantal bedenkingen in verband met de privacybescherming, kunnen we ook relatief eenvoudige oplossingen voorstellen. Ook zien we dat deze landen minder last hebben van problemen in verband met transparantie en efficiëntie. Wat de e-ID betreft kent Zweden geen verplichting tot het dragen van een identiteitsbewijs. Toch is er ook een door de overheid uitgevaardigde e-ID, die quasi identiek is aan de Belgische kaart. Het Zweedse personenregister kan net als het Rijksregister beschouwd worden als één van de mogelijke authentieke bronnen en de e-delegatie is - ondanks zijn centralisatie - quasi identiek aan de Kruispuntbanken. Wat privacybescherming betreft kent Zweden geen sectorale comités, maar een gecentraliseerde autoriteit. België kent op zijn beurt geen eeuwenlange traditie met betrekking tot het typisch Scandinavische openbaarheidsprincipe. De vraag naar privacy luidt dus anders in beide landen en zal daarom ook in beide landen anders aangepakt moeten worden.

2.2.3. DUITSLAND

FLEXIBILITEIT - Duitsland heeft zich zeer flexibel opgesteld bij het opstellen van haar strategie met betrekking tot e-Government. In plaats van vast te houden aan één grootschalig plan, wordt het bestaande plan voortdurend geëvalueerd en waar nodig aangepast. We zien ook een grote invloed van het Oostenrijks beleid. Het is dan de vraag in hoeverre Oostenrijk gevolgd zal worden en op welke punten Duitsland een eigen weg zal in slaan.

TOENADERING TOT EEN ENKELE UNIEKE IDENTIFICATOR? - Als we dan de eerste pijler van het Belgisch beleid, het gebruik van een **enkele unieke identificator**, willen vergelijken met de Duitse situatie, zien we dat Duitsland geen uniek nationaal identificatienummer kan toekennen aan haar onderdanen.[167] Die houding kan echter nog veranderen. Duitsland wil immers een centraal bevolkingsregister oprichten.[168] Dit register zou in 2010 volledig operationeel moeten worden. Een nationaal identificatienummer zoals het Rijksregisternummer zal hier echter niet bijhoren.[169] Daarnaast zal Duitsland onder invloed van Europese Verordening 763/2008 in 2011 een census

[167] Dit zou in strijd zijn met het grondrecht en de rechtspraak van het hoogste gerechtshof. Zie het historisch overzicht met betrekking tot Duitsland onder deel 1.2.1. in dit onderzoek. Hoewel er wel identificatienummers zijn, kunnen deze nooit werkelijk nationaal of algemeen zijn. Ook het recente *Steuer-Identifikationsnummer* leidde tot protest. § 139b Abgabenordnung van 1 oktober 2002, laatst gewijzigd door artikel 2 Wet 30 juli 2009, *BGBl. I* 2474.

[168] Er zijn nu immers lokale en regionale bevolkingsregisters. Deze wil men nu samenbrengen in één federaal register. BUNDESMINISTERIUM DES INNERN, "IT-Projekte im Überblick: Bundesmelderegister", 2007, *www.deutschland-online.de,* 1. Daarnaast is er bij de gemeenten ook het *Personenstandsbuch*, het register van de burgerlijke stand. Dit register bevat echter maar zeer beperkte gegevens en bevat geen identificatienummer.

[169] *„… keine "Nummer für alle Zwecke" geben wird, denn das wäre datenschutzrechtlich kaum vertretbar"*, BUNDESMINISTERIUM DES INNERN, "IT-Projekte im Überblick: Bundesmelderegister", 2007, *www.deutschland-online.de,* 2.

uitvoeren.[170] Met de komst van het register lijkt Duitsland gewonnen te zijn voor het idee van de eenmalige gegevensinzameling die quasi onmogelijk is zonder enige vorm van centraal register.

ELEKTRONISCHE IDENTITEITSKAART - Een **e-ID** komt er in Duitsland wel. Duitsland kent zelfs de verplichting voor personen ouder dan 16 jaar om een identiteitsbewijs te bezitten.[171] De invoer van een e-ID bleek in Duitsland echter zeer moeilijk te zijn.[172] De belangrijkste reden hiervoor is de vraag naar een uitgebreide beveiliging die op afdoende wijze de privacy zou kunnen beschermen. Wat de technische kant betreft, zien we dat de Duitse kaart in grote lijnen het Oostenrijkse concept volgt.[173] Zo valt allereerst op dat de Duitse kaart uiterlijk meer gegevens bevat dan de Belgische.[174] De contactloze chip bevat echter minder gegevens.[175] De kaart heeft voornamelijk tot doel het identificeren/authentiseren van de burger en het plaatsen van gekwalificeerde elektronische handtekeningen, zowel binnen een overheidscontext als in het kader van e-business. De beveiliging van de Duitse kaart is wel strenger dan die van de Belgische. Zo kunnen de gegevens op de chip niet uitgelezen worden zonder de persoonlijke PIN van de gebruiker in te voeren. Ook bij de certificaten maakt de Duitse kaart gebruik van het zogenaamde PACE (*Password Authenticated Connection Establishment*), wat een meer betrouwbare beveiliging zou moeten zijn dan de standaardbeveiliging BAC (*Basic Access Control)* die normaal toegepast wordt bij RFID-chips. Aangezien de Duitse e-ID op dit moment nog maar in een proefstadium zit, is het moeilijk om dit concept al te beoordelen. Gezien de grote gelijkenissen met het Oostenrijkse systeem, vermoeden we een gelijkaardig scenario, met het verschil dat Duitsland wel een bezitsplicht kent.

TRANSPARANTIEPROBLEMEN - Wat transparantie betreft, kunnen we verwijzen naar de Oostenrijkse situatie. De overheid zal dus voor voldoende openheid moeten zorgen. Ook met betrekking tot privacybescherming kunnen we - net door die grote invloed - naar het Oostenrijkse systeem kijken. De bedenkers van het Duits systeem gaan er graag van uit dat het Duitse systeem zonder meer het meest privacyvriendelijk is. Hier is echter geen onmiddellijke aanleiding toe. Wanneer de Duitse overheid een e-ID uitvaardigt met gegevens die men uit het bevolkingsregister gehaald heeft en later de gegevens op die kaart gebruikt om die persoon toegang te verlenen tot bepaalde toepassingen voor e-Government, dan gaat het immers nog steeds om de verwerking van persoonsgegevens. En ondanks het feit dat Duitsland de privacy van haar burgers zo graag wil beschermen, bevat de Duitse e-ID zowel visueel als op de contactloze chip meer persoonsgegevens dan de tot hier toe besproken landen en is er - net als in Zweden - sprake van het bewaren van biometrische gegevens op de chip. Net als in de overige besproken landen, zal er in Duitsland dus voldoende aandacht dienen te worden besteed aan de bepalingen van de privacywetgeving.

[170] Verordening (EG) nr. 763/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende volks- en woningtellingen, *Pb. L* 218/14 van 13 augustus 2008. Voor de Duitse volkstelling, zie: *www.zensus2011.de.*

[171] § 1 Gesetz über Personalausweise van 19 december 1950, laatst gewijzigd op 20 juli 2007, *BGBl. I* 1566. Let wel dat er in Duitsland enkel de bezitsplicht geldt en geen draagplicht.

[172] Een meer uitgebreide bespreking van de bijzonderheden, de functies en de uitdagingen van de Duitse elektronische identiteitskaart, kan teruggevonden worden bij: G. HORNUNG, A. ROßNAGEL, "An ID card for the Internet – The new German ID card with 'electronic proof of identity'", Computer Law & Security Review, vol. 26, 2010, 151-157.

[173] De Duitse kaart zal echter een fysieke kaart zijn. Verder gebruikt Duitsland uiteraard geen *SourcePIN*.

[174] Zo zijn de lengte van de persoon en het adres visueel aanwezig op de Duitse kaart.

[175] De burger kan gedeeltelijk zelf beslissen hoe gesofisticeerd zijn persoonlijke e-ID zal zijn. Zo kan men bepaalde informatie weren en kan men de functie voor het plaatsen van elektronische handtekeningen gedeactiveerd laten.

AUTHENTIEKE BRONNEN - Duitsland kent het concept '**gevalideerde authentieke bronnen**' niet, of althans niet in dezelfde mate als België. Men kent wel het concept van validatie van gegevens, namelijk in de vorm van *Bürgerportale*.[176] Met dat project wil de overheid een veilig communicatieplatform aanbieden.[177] Een belangrijk onderdeel voor de veiligheid van zulk platform is het gegeven dat de identiteit van de gebruikers onbetwistbaar vast dient te staan. Hiertoe wil men er voor zorgen dat het platform gebruik maakt van gevalideerde authentieke gegevens met betrekking tot de identiteit van de persoon. Hoewel er enige gelijkenissen met de Belgische gevalideerde authentieke bronnen merkbaar zijn, is de Duitse praktijk toch nog enigszins anders. Daarnaast is nu wel de elektronische opslag van data in het register van de burgerlijke stand toegelaten.[178] Met de eerder aangehaalde invoer van een nationaal personenregister is het daarom niet ondenkbaar dat Duitsland toch nog beroep zal doen op het idee van de gevalideerde authentieke bronnen. Aangezien beide registers zouden kunnen dienen als authentieke bron, is er immers al een geleidelijke toenadering tot dit principe merkbaar.

DIENSTENINTEGRATOREN - Ook wat **dienstenintegratoren** betreft, zijn er verschillen merkbaar. Waar de Belgische Kruispuntbanken niveau- of sectorgebonden opgericht worden, lijkt Duitsland wat dit betreft meer te streven naar centralisatie. De DOI (*Deutschland-Online Infrastruktur*) is opgevat als een centraal platform waar de overheden - federaal, regionaal en lokaal - zonder problemen met elkaar kunnen communiceren.[179] Daarnaast loopt er ook een project tot standaardisatie bij communicatie tussen de verschillende overheden.[180] Toch is er ook in Duitsland wel ruimte voor een geïntegreerde dienstverlening, zij het met meer nadruk op het centrale niveau.[181]

PRIVACYBESCHERMING - Ook Duitsland kent geen **sectorale comités**. Er is wel een centrale instantie - de *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* - die waakt over de naleving van de wetgeving in verband met de bescherming van de persoonlijke levenssfeer en ontvangt in die hoedanigheid de aanmeldingen voor de verwerking van persoonsgegevens.[182] Daarnaast kennen de Duitse deelstaten ook hun eigen instantie, de *Landesbeauftragte für den Datenschutz*. Deze niveaus werken samen door op gezette tijdstippen samen te komen.[183] De regio's hebben ook hun eigen privacywetgeving aangenomen.[184] Hoewel er bijgevolg wel controle op verschillende niveaus is, kan ook dit systeem niet als equivalent aan de Belgische sectorale comités worden beschouwd. Organisatorisch is de centrale instantie wel onderverdeeld in verschillende eenheden die men sectoraal zou kunnen noemen. Het gaat hier echter om een

---

176 IDABC, "eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability", 2007, *ec.europa.eu/idabc*, 70.
177 Meer informatie over dit project kan gevonden worden op: *www.cio.bund.de.*
178 Paragraaf 3 (2) Personenstandsgesetz van 19 februari 2007, *BGBl.* I s. 122.
179 *www.deutschland-online.de.*
180 *www.standardisierung.deutschland-online.de.*
181 Meer sectorgebonden initiatieven zijn er echter ook te vinden. Zo is *S.A.F.E.* vooral gericht op de integratie van de componenten en het algemene toegangsbeheer van het justitieapparaat. Zie voor meer informatie: *www.justiz.de.*
182 *www.bfdi.bund.de.*
183 Een overzicht van de resultaten van die bijeenkomsten kan gevonden worden onder DSB-Konferenz op: *www.datenschutz.de.* De federale instantie is bevoegd voor de controle op de federale overheid en privéondernemingen. De regionale instanties zijn bevoegd voor de controle op regionale en lokale overheden, alsook voor het toezicht op de privésector. Merk op dat niet alle regio's automatisch bevoegd zijn voor het toezicht op de privésector. We vinden zulke bevoegdheid bij negen van de zestien '*Länder*' terug.
184 Links naar de verschillende '*Landesdatenschutzgesetze'* zijn te vinden op de Duitstalige Wikipedia.

interne taakverdeling en niet om aparte entiteiten binnen de schoot van de centrale autoriteit, zoals dat bij de Belgische sectorale comités wel het geval is.

GEEN VOORBARIGE CONCLUSIES - Aangezien het Duitse beleid met betrekking tot e-Government op dit moment nog in volle testfase zit, is het onmogelijk om nu al definitieve conclusies te trekken uit de praktische werking van dat beleid. We weten wel dat Duitsland sterk beïnvloed is door het Oostenrijkse beleid. Het zal daarom nog interessant worden om te kijken op welke punten Duitsland zal afwijken van dat voorbeeld en in welke mate dat zal leiden tot een succesvoller systeem.

2.2.4. VERENIGD KONINKRIJK

VOORAFGAANDE PLANNING - Ook het Verenigd Koninkrijk heeft bij het opzetten van een strategie voor e-Government gekozen voor een globaal plan voor de lange termijn. Net als Duitsland is dit land wat later begonnen met het plannen van die strategie, wat er natuurlijk toe leidt dat er al een aantal praktijkvoorbeelden voorhanden waren die als basis gebruikt konden worden. In 2000 werd een eerste versie van de e-Government strategie gepubliceerd. Een groot deel van de toenmalige doelstellingen werd in jaren daarop gerealiseerd. In 2005 werd er een nieuwe strategie voorgelegd.[185] Het gebruik van elektronische identiteitskaarten wordt echter niet vermeld als een directe doelstelling van de strategie voor e-Government. De Britse *Identity Cards Act* uit 2006 kwam er immers voornamelijk vanuit de vraag naar de nationale veiligheid, immigratiecontrole en de angst voor terrorisme.[186] Eind 2009 begint in Manchester het pilootproject van de Britse identiteitskaart.[187] Ondanks het feit dat deze kaart er dus nog niet is en daarnaast ook louter facultatief zal zijn, is er al verschillende jaren een hevig protest aan de gang.[188]

ENKELE UNIEKE IDENTIFICATOR? - Het Verenigd Koninkrijk zal ook een personenregister oprichten, waar de registratie in principe slechts zal gebeuren na expliciete aanvraag door de betrokken burger.[189] Als gevolg van zijn registratie zal de burger een **persoonlijk identificatienummer** toegekend krijgen.[190] Op dit moment is het echter nog onduidelijk wat de precieze functie van dit nummer zal zijn.[191] Het spreekt voor zich dat de bezorgdheid van de burger voor zijn privacy hier niet geheel onterecht is.[192] Wat de efficiëntie van het systeem betreft, zijn er op dit moment te weinig details bekend om een degelijke analyse te maken. Tot op heden blijft het hele beleid

---

[185] CABINET OFFICE, "Transformational Government Enabled by Technology", november 2005, *www.cabinetoffice.gov.uk.*

[186] Het '*Home Office'* beschrijft ook voornamelijk de veiligheidsoverwegingen voorafgaande aan de identiteitskaart: *www.homeoffice.gov.uk/passports-and-immigration.* Zie ook art. 1 (4) Identity Cards Act, 2006, *c.* 15 (Eng.).

[187] Details kunnen gevonden worden op: *www.direct.gov.uk.*

[188] Zie *www.no2id.net.* Ook overheidsonderzoek zelf is niet positief: HOME OFFICE IDENTITY AND PASSPORT SERVICE, "National Identity Service Tracking Research Wave 8: June 2009", 2009, *www.ips.gov.uk,* 6 e.v.

[189] Art. 1 en 2 (1) Identity Cards Act, 2006, *c.* 15 (Eng.). Artikel 2 (4) bepaalt de registratie zonder voorafgaande aanvraag. De omvang van dit artikel is onduidelijk. De *explanatory notes* bij de wet geven ook geen bevredigend antwoord. Ook zal iedereen die een paspoort of identiteitskaart aanvraagt, meteen in het register opgenomen worden.

[190] Artikel 2 Identity Cards Act 2006 (*National Identity Registration Number*) Regulations 2009, *S.I.* 2009 No. 2574 bepaalt dat dit nummer volstrekt onpersoonlijk zal zijn en niet naar andere identificatienummers zal verwijzen.

[191] Door de omvang van het nationaal register, is het niet ondenkbaar dat dit nummer als enkele unieke identificator zal worden gebruikt. Zie bijlage 1 bij de *Identity Cards Act*. Ook kan het register nog worden uitgebreid.

[192] Dit is niet het enige project waarbij de Britse overheid allerhande persoonsgegevens in een centrale databank wil stoppen. Zie *National Health Service National Programme for IT* (NPfIT): *news.bbc.co.uk/2/hi/health/7850619.stm.*

immers baden in een waas van onduidelijkheid. Ook de inwerkingtreding van de relevante wetgeving laat op zich wachten. Dit brengt ons natuurlijk op het punt van transparantie. Zoals uit onderzoek van de overheid zelf al blijkt, leeft er onder de Britten zeer veel onzekerheid en verwarring met betrekking tot de juiste doelstellingen en de omvang van dit project.[193] Aangezien het Britse systeem geen pseudoniemen zal gebruiken, zou het voor de burger net gemakkelijker moeten zijn om de werking van het systeem te begrijpen. Nu dit duidelijk niet het geval is, kunnen we ons afvragen of de overheid wel kan voldoen aan de eis van transparantie.

ELEKTRONISCHE IDENTITEITSKAART - De Britse **e-ID** zal ook enigszins verschillen van de Belgische versie. Allereerst zal de doelstelling van de kaart al zeer verschillend zijn. België kende immers al de verplichte identiteitskaart en voerde de e-ID in als deel van het e-Government beleid. In het Verenigd Koninkrijk is de e-ID echter het product van evoluties op het gebied van staatsveiligheid. De kaart zelf bevat niet veel meer persoonsgegevens dan de Belgische e-ID.[194] Het belangrijkste verschil is dat de chip van de Britse versie niet het nummer van het nationaal register zal bevatten, maar wel biometrische gegevens.[195] Wat de beveiliging betreft, maakt de chip - net als die op de Belgische e-ID - gebruik van de RSA encryptiestandaard.[196] Bepaalde data - zoals de opgeslagen vingerafdrukken - worden extra beveiligd. Verder wordt bij de Britse identiteitskaart een PIN gebruikt wanneer men de gegevens op de chip wil uitlezen. Identificatie en authenticatie zullen daarom de belangrijkste functies van de Britse e-ID worden. Op dit moment is het nog niet duidelijk of de Britse e-ID ook geschikt zal zijn voor het plaatsen van elektronische handtekeningen. De Britse overheid vaardigt op dit moment immers niet zelf de nodige certificaten uit.[197] Wat privacybescherming betreft, is het positief dat de kaart geen onnodige data bevat.[198] Er zijn echter wel biometrische gegevens - namelijk vingerafdrukken - aanwezig. Hoewel vingerafdrukken intussen ook al een vereiste zijn voor het verkrijgen van een paspoort, is er nog steeds veel tegenstand tegen het gebruik van biometrie. Daarnaast zijn er ook de nodige twijfels bij het al dan niet verplicht zijn van de kaart. De wet geeft in artikel 13 immers de mogelijkheid om personen zonder zulke kaart de toegang tot bepaalde openbare diensten te ontzeggen. In zulk geval wordt het bezit van de kaart een *de facto* verplichting. Ook hier is bijgevolg verdere transparantie vereist.

HET PERSONENREGISTER - Een groter privacyprobleem is echter de omvang van het personenregister.[199] Zo zal men erover moeten waken dat er geen ongeoorloofde verwerking van de betrokken persoonsgegevens plaatsvindt en dat de toegang tot het register strikt gereguleerd wordt. Artikelen 17 tot 21 van de wet op het personenregister handelen over de mogelijkheden om toegang tot het register te verkrijgen zonder toestemming van de betrokkene. Deze artikelen laten ruime bevoegdheden aan een commissaris voor het nationaal personenregister (*National Identity Scheme Commissioner*). Onder deel IV van de privacywet (*Data Protection Act*) vinden

---

[193] HOME OFFICE IDENTITY AND PASSPORT SERVICE, "National Identity Service Tracking Research Wave 8: June 2009", 2009, *www.ips.gov.uk,* 12 e.v.

[194] Meer informatie over het uiterlijk van de kaart is te vinden op: *www.ips.gov.uk.*

[195] HOME OFFICE, "Introducing the National Identity Service", 2009, *www.direct.gov.uk,* 15.

[196] De beveiliging van de Britse e-ID is onlangs sterk in opspraak gekomen. S. BOGGAN, "New ID cards are supposed to be 'unforgeable' - but it took our expert 12 minutes to clone one, and programme it with false data", 6 augustus 2009, *www.dailymail.co.uk.*

[197] Dit wordt overgelaten aan een aantal erkende dienstenaanbieders. Zo zijn voor het gebruik van gateway.gov.uk enkel certificaten van Simplysign - van de Britse Kamer van Koophandel - en Equifax erkend. *www.gateway.gov.uk.*

[198] Zo is het nummer van het nationaal register noch visueel, noch digitaal op de kaart aanwezig.

[199] Bijlage één bij de *National Identity Cards Act.* Dit is overigens niet de enige databank die de Britse overheid plant.

we een aantal interessante uitzonderingen op de privacybeschermende normen.[200] Op het eerste zicht lijkt het er op dat de Britse overheid hier met opzet de privacybescherming probeert te omzeilen. Ook het ICO (*Information Commissioner's Office*), de Britse privacyautoriteit, heeft al laten weten zeer bezorgd te zijn over het opzet en het doel van het register. De hoeveelheid persoonsgegevens die men in dit register wil verwerken dient immers nodig te zijn voor het doel, aldus het finaliteitprincipe krachtens artikel 6 van Richtlijn 95/46/EG. Hoewel de toezichthoudende autoriteit het moeilijk vindt om het exacte doel van de Britse wet op de identiteitskaart te omschrijven, is het wel van mening dat de in bijlage 1 van die wet opgenomen persoonsgegevens niet allen nodig zijn indien het doel van de wet de loutere identificatie van personen zou omvatten.[201] De wet bevindt zich met andere woorden in een grijze zone wat de wetgeving betreffende de verwerking van persoonsgegevens betreft. Ook wat betreft de toegang tot het register kunnen er bedenkingen gemaakt worden bij de effectiviteit van de wettelijke bepalingen.[202] In principe zullen enkel overheden toegang krijgen tot het register.[203] Men waarschuwt tot slot ook voor het overmatige loggen van informatie.[204] Op grond van deze bevindingen concluderen we dat het Belgisch Rijksregister en de Belgische e-ID veel transparanter en privacyvriendelijker zijn. De bezorgdheid van de Britten om hun privacy lijkt hier zeker niet ongegrond te zijn.

AUTHENTIEKE BRONNEN - Wat **gevalideerde authentieke bronnen** betreft, zal in de toekomst wellicht het register zelf gebruikt worden.[205] Men wil immers van het register een voldoende betrouwbare bron van informatie maken. Het register kan overigens nog worden uitgebreid, zoals blijkt uit onder meer punt 4 (l) van bijlage 1. We kunnen hier dan denken aan bijvoorbeeld de opname van het registratienummer van artsen.[206] Ook andere overheidsdatabanken kunnen als bron ter validatie van bepaalde persoonsgegevens gebruikt worden.[207] Deze mate van centralisatie gaat lijnrecht in tegen de geest van het Belgisch beleid. We kunnen dit echter wel beschouwen als een zekere toenadering tot het principe van de gevalideerde authentieke bronnen.

DIENSTENINTEGRATOREN - Ook op het vlak van **dienstenintegratoren** zal het register zijn weerslag kennen. De focus van het Belgisch beleid op het gebied van deze materie ligt duidelijk op de integratie van diensten zelf en het vermijden van te verregaande centralisatie van informatie. Het Verenigd Koninkrijk heeft echter gekozen voor een zeer sterke gegevensintegratie en -centralisatie binnen een geïntegreerde dienstverlening. Het register is echter onderdeel van de

[200] Belangrijk is dat deze uitzonderingen overeenkomen met de doelstellingen uit de *National Identity Cards Act*.
[201] INFORMATION COMMISSIONER, "Response to the Government's Consultation on Legislation on Identity Cards", *www.ico.gov.uk,* 3-4.
[202] De wet bepaalt in artikel 22 wel dat er een commissaris aangesteld zal worden, die zal waken over de naleving van de wet en de vertrouwelijkheid van het register. Artikel 22 (4) beperkt al meteen de bevoegdheden van deze persoon.
[203] INFORMATION COMMISSIONER, "Response to the Government's Consultation on Legislation on Identity Cards", *www.ico.gov.uk,* 2. Zie ook artikelen 17 tot 21 van de *National Identity Cards Act.* Artikel 21 legt voorwaarden op om informatie uit het register zonder toestemming door te geven. Deze voorwaarden zijn echter vrij onduidelijk geformuleerd.
[204] INFORMATION COMMISSIONER, "The Identity Cards Bill: The Information Commissioner's Concerns", *www.ico.gov.uk,* 2-3.
[205] Dit is de horizontale integratie van informatie waarvan sprake in: IDABC, "eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability", 2007, *ec.europa.eu/idabc*, 71.
[206] Men mag pas het beroep van arts uitoefenen indien men geregistreerd is. Vanaf november 2009 dienen artsen zich te registreren alsook een licentie aan te vragen. *www.gmc-uk.org/register.*
[207] IDABC, "eID Interoperability for PEGS: Update of Country Profiles - United Kingdom Country Profile", *ec.europa.eu/idabc,* 18.

plannen op het gebied van staatsveiligheid en immigratiebeleid en staat bijgevolg los van de integratie van de diensten zelf, wat onderdeel is van de nieuwe strategie met betrekking tot e-Government. Het doel is om verschillende overheidsdiensten samen aan te bieden.[208] Het hiertoe opgerichte '*Common Infrastructure Board'* zal de verschillende overheidsdiensten begeleiden en adviseren bij het opzetten van zulk gemeenschappelijk platform.[209] Daarnaast probeert men ook te komen tot meer integratie van de back-offices.[210] Deze verschillende vormen van gedeelde diensten worden gecoördineerd door het *Cabinet Office*.[211] Samen met de centrale platformen '*DirectGov'* en '*Government Gateway'* is het duidelijk dat deze initiatieven centraal gerealiseerd worden. Het Verenigd Koninkrijk kent bijgevolg geen sector- of niveaugebonden dienstenintegratoren zoals de Belgische Kruispuntbanken. Men streeft met andere woorden wel naar een geïntegreerde dienstverlening, maar probeert dit te bereiken door middel van een verregaande centralisatie van gegevens. Dit systeem staat daarom haaks op de Belgische dienstenintegratie.

PRIVACYBESCHERMING - Zoals al vermeld heeft de wetgeving op de privacybescherming een toezichthoudende autoriteit aangesteld, die dus ook bevoegd is voor het ontvangen van aanmeldingen tot de verwerking van persoonsgegevens zoals volgt uit de Richtlijn.[212] Voor het verlenen van toegang tot de gegevens in het personenregister is echter een andere persoon aangesteld door de Minister van Binnenlandse Zaken. De naleving van de privacywetgeving wordt dus in principe centraal gecontroleerd, hoewel er ook nog regionale instanties zijn voor Wales, Schotland en Noord-Ierland.[213] Deze regionale instanties zijn opgericht binnen de centrale autoriteit, net zoals de Belgische **sectorale comités**, maar zijn dus regionaal gericht en niet sectorgebonden. Het Verenigd Koninkrijk kent bijgevolg geen sectorale comités.

BEDENKINGEN BIJ DIT BELEID - We kunnen hier concluderen dat het Verenigd Koninkrijk - ondanks het feit dat het door dit latere optreden al een aantal landen als praktijkvoorbeeld kon volgen - hier een volledig eigen weg uitgegaan is. Het is intussen wel duidelijk dat we deze weg zeker niet kunnen verkiezen boven de eerder besproken systemen en het zal aan de toekomst zijn om uit te wijzen wat de gevolgen zullen zijn van deze zeer verregaande aanpak. Wat ook opmerkelijk is, is het feit dat het register en de e-ID hier geen deel zijn van het e-Government beleid, maar een onderdeel van de staatsveiligheid en immigratiecontrole. Daarnaast zien we ook dat de overdreven uitgebreidheid van het register, de onduidelijkheid in verband met de toegang en de precieze omvang van het register, de vele confrontaties met de privacywetgeving en -autoriteit en de vele mogelijkheden tot fraude het Britse systeem niet bepaald tot een lovenswaardig voorbeeld maken.

2.2.5. PORTUGAL

[208] CABINET OFFICE, "Transformational Government Enabled by Technology", november 2005, *www.cabinetoffice.gov.uk,* 12-14.
[209] Een voorbeeld is '*Government Connect'* dat de lokale en centrale overheden met elkaar wil verbinden over een gemeenschappelijk netwerk. *www.govconnect.gov.uk.*
[210] Zie het '*country-report'* over het Verenigd Koninkrijk bij de 40ste conferentie van het '*International Council for Information Technology in Government* Administration' (ICA), 2006, *www.ica-it.org/conf40,* 6-7.
[211] *www.cabinetoffice.gov.uk/cio/shared_services.aspx*.
[212] Zie art. 6 Data Protection Act 1998, *c.* 29.
[213] *www.ico.gov.uk/about_us/regional_offices.aspx.*

IDENTIFICATOREN, SECTOREN EN REGIONALISERING - Het laatste land dat we in dit rechtsvergelijkend onderzoek willen opnemen, is Portugal. De reden hiertoe is dat Portugal een aantal verschillende unieke identificatoren naast elkaar gebruikt. We willen daarom onderzoeken hoe dit in de praktijk verloopt en wat de gevolgen van dit systeem zijn. We zien ook dat het Portugese beleid zeer regionaal georiënteerd is, wat zich uit in het '*Cidades Digitais*' project.[214] Dit project was de eerste stap van het Portugese beleid met betrekking tot e-Government en heeft tot doel het ontwikkelen van een digitale structuur van de steden en regio's uit. Net als in het Zweedse beleid zien we hier dus een regionale focus. Op centraal niveau is er sinds 2005 een technisch plan voor de verdere opbouw van infrastructuren voor e-Government.[215]

SECTORGEBONDEN IDENTIFICATOREN - Portugal hanteert in principe geen nationale **enkele unieke identificator**. Net als in Duitsland is het gebruik van een nationaal identificatienummer grondwettelijk verboden.[216] Men gebruikt daarom verschillende identificatienummers, zoals onder meer een nummer voor de sociale zekerheid, een nummer voor de gezondheidszorg en een fiscaal identificatienummer. Het gebruik van deze nummers is in principe vrij.[217] Toch kent Portugal ook een persoonlijk identificatienummer voor het personenregister. Het gebruik van dit nummer is echter niet vrij, dit om te verhinderen dat dit nummer als nationaal identificatienummer zou worden gebruikt.[218] In het dagelijkse leven worden daarom in principe enkel de sectorgebonden identificatoren als identificatiemiddel gebruikt. Ondanks het feit dat Portugal net als Oostenrijk en Duitsland sectorgebonden identificatoren hanteert, zijn er toch zeer grote verschillen tussen deze landen. Zo wordt er in Portugal binnen een bepaalde sector steeds dezelfde sectorgebonden identificator gebruikt, waar er in Oostenrijk en in Duitsland *ad hoc* identificatoren gegenereerd kunnen worden. Dit heeft tot gevolg dat Portugal geen nood heeft aan de ingewikkelde beveiliging die deze Germaanse landen kennen, wat er toe leidt dat Portugal ook niet dezelfde problemen met betrekking tot de gebruiksvriendelijkheid en de transparantie zal kennen. Ook wat betreft de privacybescherming lijken er aan deze aanpak minder nadelen verbonden te zijn dan aan de Duitse en Oostenrijkse systemen. De Portugese wetgeving met betrekking tot de bescherming van de privacy in verband met de verwerking van persoonsgegevens blijft echter ook van toepassing op het gebruik van de niet-beschermde identificatoren, maar Portugal vereist in principe geen voorafgaande machtiging voor het gebruik van deze nummers.

GEÏNTEGREERDE ELEKTRONISCHE IDENTITEITSKAART - Ook wat betreft identiteitsdocumenten zien we dat dit gelijk loopt met het net besproken gebruik van unieke identificatoren. Voor elk identificatienummer bestond er vroeger een aparte kaart.[219] Voor algemene identificatie was er een standaard 'papieren' identiteitskaart. Opmerkelijk is dat Portugal niet enkel de vroegere identiteitskaart wil vervangen door een elektronisch exemplaar, maar dat alle vroegere identificatiekaarten geïntegreerd zullen worden in één enkele '*cartão de cidadão*'. Deze kaart geldt met andere

[214] *www.cidadesdigitais.pt.*
[215] *www.planotecnologico.pt.*
[216] Artikel 35, 5) van de Portugese grondwet verbiedt het toewijzen van een enkel nationaal identificatienummer. IDABC, "eID Interoperability for PEGS: Portuguese Country Profile", *ec.europa.eu/idabc,* 6.
[217] IDABC, "eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability", 2007, *ec.europa.eu/idabc*, 48-49. Merk op dat zulke unieke identificatoren wel nog steeds als persoonsgegevens in de zin van Richtlijn 95/46/EG beschouwd kunnen worden. De privacywetgeving zal daarom van toepassing blijven op deze identificatoren, ongeacht of hun gebruik vrij is of niet.
[218] IDABC, "eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability", 2007, *ec.europa.eu/idabc*, 43.
[219] Merk op dat Portugal een bezitsplicht kent voor burgers vanaf zes jaar.

woorden als gewone identiteitskaart, maar bevat ook het identificatienummer van de sociale zekerheid, de gezondheidszorg en het fiscaal nummer. De '*cartão de cidadão'* is ook een volwaardige **e-ID**, die een contactchip met gegevens in digitale vorm bevat, alsook twee certificaten waarvan het ene voor authenticatie en het andere voor het plaatsen van elektronische handtekeningen.[220] Wat de beveiliging van de gegevens op de kaart betreft zien we dat de gebruikte standaarden gelijkaardig zijn aan die van de Belgische e-ID. Hoewel het vreemd kan lijken om al die verschillende identificatoren te bundelen op één enkele kaart, is er hier echter maar weinig bezwaar tegen in te brengen. Het gebruik van deze nummers is immers in principe vrij.[221] Aangezien de Portugese e-ID zelf geen medische gegevens en dergelijke zal bevatten, kunnen we het gebruik van deze nummers als verdedigbaar beschouwen.[222] De kaart zal daarnaast wel enige biometrische gegevens bevatten. Zo zal naast de klassieke foto ook de lengte van de persoon en zijn vingerafdrukken bewaard worden.[223] De '*cartão de cidadão'* zal tot slot ook gelden als reisdocument binnen de Europese Unie. De Portugese versie van de e-ID lijkt daarom zeer sterk op de Belgische identiteitskaart.[224] De belangrijkste verschillen zijn het gebruik van verschillende identificatoren en biometrische gegevens. Wanneer de Belgische e-ID binnenkort echter ook als identificatiemiddel voor de sociale zekerheid zal dienen, zien we dat de verschillen tussen de Belgische en de Portugese identiteitskaart zeer minimaal worden.

GEVAREN VAN DE INTEGRATIE - Portugal betreedt hier echter wel een moeilijk terrein. Zoals we in Oostenrijk al zagen, is het gebruik van sectorgebonden identificatoren niet altijd even geliefd bij de burger. Men probeert daarom de gegenereerde ssPINs te vermijden door enkel nog één bepaald nummer te gebruiken. Men creëert hier dus een *de facto* enkele unieke identificator. We moeten wel onthouden dat deze praktijk in Oostenrijk voornamelijk het gevolg is van het gebrek aan gebruiksvriendelijkheid en transparantie in het systeem. Men probeert dan niet zozeer de sectorgebonden identificator te ontwijken, dan wel de ingewikkelde beveiliging die er mee gepaard gaat. Aangezien Portugal zulke beveiliging niet zal gebruiken, bestaat er nog een kans dat het daar niet zulke vaart zal lopen. Daarnaast zien we ook dat Portugal een vaststaand identificatienummer voor een bepaalde sector hanteert, waar men in Oostenrijk in principe ssPINs kan blijven genereren. Ook dit is een belangrijke reden waarom de Oostenrijkse burgers in praktijk de ssPINs proberen te ontwijken.

GEGEVENSKOPPELINGEN - De toekomst zal moeten uitwijzen wat er met de Portugese identificatoren zal gebeuren wanneer de e-ID algemeen ingevoerd is. De wet op de identiteitskaart meldt echter wel dat mogelijke gegevenskoppelingen door gebruik van één van de op de kaart aanwezige nummers slechts mogelijk is krachtens wettelijke verplichtingen of bij toestemming van de nationale privacyautoriteit.[225] Een *de facto* evolutie naar het veralgemeend gebruik van een enkel identificatienummer in de publieke sector – ondanks de grondwettelijke afkeer van zulk

[220] *www.cartaodecidadao.pt.* Het certificaat voor elektronische handtekeningen kan vanaf de leeftijd van zestien jaar op vraag van de burger geactiveerd worden.
[221] Gegevenskoppelingen op basis van deze nummers lijken in de wet op de '*cartão de cidadão'* wel strikter geregeld te worden. Zo bepaalt artikel 16 van die wet dat de daar opgesomde identificatienummers enkel gekoppeld of uitgewisseld mogen worden indien toegestaan door de wet of door de toezichthoudende autoriteit, Lei n.o 7/2007 van 5 februari 2007 Cria o cartão de cidadão e rege a sua emissão e utilização, *Diário da República 1*, nr. 25, 942..
[222] Ook in België zullen de gegevens op de huidige SIS-kaart in 2011 verhuizen naar de e-ID.
[223] Opmerkelijk is dat dit voor de Portugezen geen nieuwigheid is. Ook de vroegere 'papieren' identiteitskaart bevatte al deze gegevens.
[224] Wat uiteraard niet verwonderlijk is aangezien de firma Zetes sterk betrokken is bij beide projecten.
[225] Artikel 16, 2 Lei n.o 7/2007 van 5 februari 2007 Cria o cartão de cidadão e rege a sua emissão e utilização, *Diário da República 1*, nr. 25, 942.

nummer – lijkt daarom niet *a priori* uitgesloten. Uit de praktijk blijkt intussen ook dat er binnen de Portugese publieke sector steeds meer gebruik gemaakt wordt van een enkel identificatienummer voor de identificatie van de burger.[226] Het principiële grondwettelijke verbod op het toewijzen van een enkel nationaal identificatienummer wordt omzeild door de sectorgebonden identificatoren te behouden, naast het gebruik van één bepaalde identificator als veralgemeend identificatienummer. Door meerdere identificatoren te behouden – ook al wordt één ervan als algemene identificator gebruikt – is er immers geen sprake van het toewijzen van een enkel nationaal identificatienummer.

AUTHENTIEKE BRONNEN - Wat betreft het gebruik van **gevalideerde authentieke bronnen** zien we dat Portugal - net als de meeste andere landen die we hier besproken hebben - dit principe nog niet officieel aanvaard heeft, maar dat er wel enige toenadering is tot het principe. We kunnen daarom spreken van een informele aanvaarding van het principe van de gevalideerde authentieke bronnen. Portugal kent immers een centrale databank die allerlei attributen over de houders van identiteitskaarten bevat. Dit wordt beschouwd als authentieke informatie over de betrokken burgers en het is daarom ook deze informatie die gebruikt wordt in het authenticatiecertificaat voor de '*cartão de cidadão'*. De op de e-ID opgenomen identificatienummers worden rechtstreeks bij de betrokken overheidsdienst gehaald, dit om ook hier de nodige authenticiteit te verzekeren. Door de informatie met betrekking tot de sectorgebonden identificatoren bij de bevoegde autoriteiten te laten, vermijdt men een te gecentraliseerde gegevensopslag. Portugal lijkt daarnaast ook het principe van de eenmalige gegevensinzameling te respecteren door de algemene informatie met betrekking tot de persoon - zoals zijn geboorte, zijn nationaliteit en dergelijke - door een centrale autoriteit te laten beheren. Hierdoor vermijdt men immers dat de persoon deze gegevens aan iedere sector afzonderlijk zou moeten meedelen. Het Portugese beleid is wat dit betreft daarom niet zo erg verschillend van het Belgisch beleid en het lijkt ook niet ondenkbaar dat Portugal het gebruik van gevalideerde authentieke bronnen ooit nog officieel zal aanvaarden.

DIENSTENINTEGRATOREN - Een ander belangrijk punt in het Portugese beleid is de geïntegreerde dienstverlening. Zo is er een centraal overheidsportaal waar de burger toegang kan krijgen tot de verschillende overheidsdiensten.[227] Ook de e-ID zelf kan gebruik maken van een aantal kanalen voor geïntegreerde dienstverlening. Door verschillende instrumenten voor identificatie in één enkele kaart te verenigen, is de e-ID op zich ook al een voorbeeld van de integratie van diensten die Portugal nastreeft. Zoals we bij de gevalideerde authentieke bronnen al zagen, wordt sectorgebonden informatie ook in die sector bewaard. De integratie van gegevens is bijgevolg geen doelstelling van de Portugese overheid. Dit alles sluit aan bij de geest van de Belgische **dienstenintegratoren**. Het grote verschil is dat Portugal hier echter geen sectorgebonden instanties voor hanteert. Er is wel een centraal orgaan, het '*Agência para a Modernização Administrativa'*, dat verschillende projecten voor e-Government beheert. Een van die projecten is het opzetten van een algemeen kader voor openbare diensten. Net als in Duitsland wil men hier een gemeenschappelijk platform creeëren waar alle overheidsdiensten geïntegreerd worden, waar

[226] We merken hierbij op dat het hier dan gaat om het identificatienummer van het personenregister. Het nummer van de identiteitskaart zelf is uniek voor die specifieke kaart. Indien de burger met andere woorden een nieuwe identiteitskaart verkrijgt, zal die kaart dus ook een ander nummer dragen. Een dergelijk variabel nummer lijkt ongeschikt voor gebruik als enige unieke identificator binnen de publieke sector.

[227] *www.portaldocidadao.pt.*

er gewerkt wordt met de laatste gangbare standaarden en waar men de burger een goede beveiliging kan garanderen.[228]

PRIVACYBESCHERMING - We zagen al dat in Portugal het gebruik van de sectorgebonden identificatoren niet geregeld is. Dit wil zeggen dat er geen voorafgaande machtiging vereist is om deze nummers te kunnen gebruiken. Omdat deze sectorgebonden identificatoren nog steeds te beschouwen zijn als persoonsgegevens, blijft het gebruik echter wel nog onderworpen aan de bepalingen van Richtlijn 95/46/EG en de Portugese wet betreffende de privacybescherming. De Portugese toezichthoudende autoriteit, de *'Comissão Nacional de Protecção de Dados',* is opgericht als een onafhankelijke autoriteit binnen het Portugese parlement. Het gaat hier om een klassieke toezichthoudende autoriteit zoals bepaald in de Richtlijn. De belangrijkste bevoegdheden zijn het toezien op het naleven van de regels in verband met privacy, het ontvangen en onderzoeken van aanmeldingen tot de verwerking van persoonsgegevens, het adviseren, en dergelijke. Deze commissie kent geen opmerkelijke bijkomende bevoegdheden. Hoewel Portugal gekozen heeft voor sectorgebonden identificatoren, zien we dat het toezicht op de naleving van de regels in verband met de privacybescherming op centraal niveau gebeurt. Er zijn dus geen **sectorale comités**.

EEN UNIEKE COMBINATIE MET BEKENDE ELEMENTEN - We zagen dat Portugal net als Duitsland in principe geen nationale enkele unieke identificator kan toewijzen. Daarom wordt er gebruik gemaakt van verschillende sectorgebonden identificatienummers. Wat de gebruiksvriendelijkheid en transparantie van dit systeem betreft, kunnen we al concluderen dat de vaste sectorgebonden nummers allicht minder problemen zullen kennen dan het Oostenrijks of Duits systeem waar er voortdurend *ad hoc* unieke identificatoren gegenereerd kunnen worden. Wat betreft de privacybescherming zagen we dat het gebruik van de sectorgebonden identificatoren steeds moet voldoen aan de bepalingen uit de Richtlijn, ook al is er geen voorafgaande machtiging vereist voor zulk gebruik. Zeer opmerkelijk is dat Portugal de bestaande identificatoren samen wil brengen op één enkele smartcard, de Portugese e-ID. Door deze gegevens samen te brengen blijkt echter nu al een evolutie plaats te vinden naar een *de facto* enkele unieke identificator. De toekomst zal uitwijzen hoe dit verder zal evolueren wanneer de nieuwe elektronische identiteitskaart volledig ingevoerd wordt. Net als bijna elk ander land dat in deze studie onderzocht werd, zien we dat Portugal het concept 'gevalideerde authentieke bronnen' nog niet officieel heeft aanvaard. Ook hier zijn er echter duidelijke sporen van toenadering tot dit principe merkbaar. Hier blijkt ook dat Portugal de principes van gedecentraliseerde gegevensopslag en eenmalige gegevensinzameling volgt. Ook wat het gebruik van dienstenintegratoren betreft zien we dat Portugal wel een orgaan kent dat een geïntegreerde dienstverlening helpt op te bouwen en dat men gegevensintegratie wenst te vermijden. Portugal kent hier echter enkel één centraal orgaan en kent dus geen sectorgebonden dienstenintegratoren. De Portugese privacyautoriteit is ook goed vergelijkbaar met eerder besproken voorbeelden. Het gaat hier om een klassieke toezichthoudende autoriteit in de zin van Richtlijn 95/46/EG. Er is geen sectorgebonden toezicht.

2.2.6. CONCLUSIE

UNIEKE IDENTIFICATOREN - In dit onderzoek hebben we getracht de vijf belangrijkste bouwstenen uit het Belgisch beleid met betrekking tot e-Government terug te vinden in het beleid van een

[228] Dit is wat men noemt het '*Framework de Serviços Comuns*', *www.ama.pt.*

aantal Europese landen. Wat het gebruik van **unieke identificatoren** betreft, zagen we dat het Oostenrijkse - en wellicht ook het Duitse - systeem van sectorgebonden identificatoren niet aan de verwachtingen lijkt te beantwoorden. Het systeem is zo ingewikkeld dat het bijna onmogelijk wordt om voldoende gebruiksvriendelijk te behouden. Ook kan de verregaande beveiliging en onvoldoende communicatie door de overheid leiden tot een gebrek aan transparantie. Wat betreft de gebruiksvriendelijkheid en transparantie zouden we daarom opteren voor een enkele unieke identificator. We zagen dat dit niet noodzakelijk een probleem vormt voor de privacybescherming, mits men gebruikt maakt van technieken als de voorafgaande machtiging. Wat dit laatste betreft merken we op dat België het enige land is dat de privacyautoriteit - althans de sectorale comités - betrekt bij zulk proces. Hoewel het Portugese systeem door de vaste sectorgebonden identificatoren het gebruik van een verregaande beveiliging kan vermijden, merken we toch op dat ook dit systeem een aantal *caveats* kent. Men zal er voornamelijk voor moeten opletten dat men door de geïntegreerde identiteitskaart niet een *de facto* enkele unieke identificator zal willen hanteren. Dit zou immers het grondwettelijke verbod op het gebruik van zulk algemeen identificatienummer omzeilen. We willen hier echter wel benadrukken dat uit deze bevindingen niet volgt dat het gebruik van sectorgebonden identificatoren volstrekt ontoelaatbaar is. We zagen dat zulke systemen zeker interessante punten bevatten, maar dat het systeem als een geheel niet geschikt lijkt om in te voeren in een land dat al een systeem in voege heeft, zoals België. Men zou er echter wel aan kunnen denken om bepaalde elementen uit het systeem van de sectorgebonden identificatoren over te nemen. Zulk hybride systeem vereist echter wel nog bijkomend onderzoek naar de technische haalbaarheid er van.

ELEKTRONISCHE IDENTITEITSKAARTEN - Wat de **e-ID** betreft, komt de Belgische e-ID als het best ingeburgerde en meest gebruikte voorbeeld uit de bus. Hoewel technologieneutrale oplossingen zoals de *Bürgerkarte* en de *BankID* zeer interessant kunnen zijn, zorgt het gebrek aan traditie betreffende het dragen van identiteitsbewijzen er voor dat die concepten in bepaalde landen toch niet op grote schaal geïmplementeerd raken. Wat betreft de Portugese geïntegreerde identiteitskaart, die de belangrijkste identificatienummers verzamelt op een enkele kaart, kunnen we herhalen dat deze evolutie zich ook in België zal laten voelen. Zo zullen binnenkort de identificatiegegevens voor de sociale zekerheid opgenomen worden op de e-ID. Ook hier verwijzen we naar de beperkingen die er zouden moeten heersen op het verspreiden van het nationaal identificatienummer. Voor België wil dit zeggen dat het gebruik van het Rijksregisternummer op beide certificaten bijgevolg maar moeilijk verdedigbaar is. Wat de beveiliging van de Belgische e-ID betreft kunnen we niet anders dan concluderen dat deze aan de verwachtingen voldoet.[229]

AUTHENTIEKE BRONNEN - Hoewel van de hier besproken landen tot op heden enkel België het gebruik van **gevalideerde authentieke bronnen** officieel aanvaard heeft, zien we dat ook Zweden, het Verenigd Koninkrijk, Portugal en - zij het zeer behoedzaam - Duitsland deze richting lijken in te slaan. Enkel Oostenrijk lijkt dit concept niet toe te passen. Het gebruik van gevalideerde authentieke bronnen kan nochtans positief onthaald worden. Zo helpt het de eenmalige gegevensopslag, leidt het tot minder centralisatie en kan het een voldoende zekerheid bieden bij identificatie en authenticatie. Centralisatie van informatie zoals vooropgesteld door het Britse personenregister zou best vermeden worden.

[229] De Belgische e-ID is tot op heden nog niet gekraakt. Daarnaast wordt de middleware voortdurend verder ontwikkeld. Zie onder meer het persbericht uitgegeven door ESAT van 13 juni 2008, *esat.kuleuven.be.*

DIENSTENINTEGRATOREN - Het gebruik van **dienstenintegratoren** kan helpen de verdere coördinatie en integratie van verschillende diensten te regelen. We zagen dat alle landen hier wel een orgaan toe aangesteld hebben, zij het niet altijd niveau- of sectorgebonden. Verder dienen we voor het doel van deze vergelijking een onderscheid te maken tussen integratie van diensten en integratie van gegevens. Krachtens het proportionaliteitsbeginsel uit de Richtlijn, mogen er niet meer gegevens verwerkt worden dan strikt noodzakelijk is voor het doel van de verwerking. Men kan dan argumenteren dat er bij loutere gegevensintegratie meer gegevens verwerkt worden dan bij de Belgische vorm van dienstenintegratie, waar de Kruispuntbanken in de regel niet zelf over gegevens beschikken. Toegepast op dit probleem zou dat willen zeggen dat gegevensintegratie pas toegelaten zou zijn indien het beoogde doel niet louter door middel van dienstenintegratie kan worden bereikt.[230]

PRIVACYBESCHERMING – SECTORALE COMITÉS - Tot slot zijn er de Belgische **sectorale comités**. De hier besproken landen hebben allen wel centrale of regionale privacyautoriteiten die bevoegd zijn voor het ontvangen van aanmeldingen voor de verwerking van persoonsgegevens. Een werkelijke verdeling van deze taken aan verschillende instanties die elk voor een eigen sector bevoegd zijn, is echter een typisch Belgisch unicum. De creatie van de sectorale comités is het gevolg van de wet van 26 februari 2003. De wetgever wou hiermee tegemoet komen aan een aantal institutionele problemen waardoor het werk van de Commissie in gedrang kwam. Hierbij werd enerzijds de werking van de Commissie gewijzigd en werden anderzijds de sectorale comités in het leven geroepen. Deze veranderingen werden echter niet unaniem positief onthaald. Zo was er de vrees dat deze versnippering van de bevoegdheden zou leiden tot een gebrek aan een globale visie en coherentie in het beleid van de privacyautoriteit.[231] Hoewel we moeten vaststellen dat een sectorgebonden toezicht zeker wenselijk kan zijn, mogen we daarom niet vergeten dat er nog steeds nood is aan een sterke overkoepelende centrale autoriteit – wat België met de Commissie voor de bescherming van de persoonlijke levenssfeer ook lijkt te hebben.

PRIVACYBESCHERMING – VOORAFGAANDE MACHTIGING - Een tweede unicum in de Belgische situatie met betrekking tot de privacybescherming, is de praktijk van de voorafgaande machtigingen tot toegang tot het Rijksregister of tot gebruik van het Rijksregisternummer. Bij de overige hier besproken landen lijkt de centrale privacyautoriteit zich – naast de gewone bevoegdheden als nationale privacyautoriteit krachtens de Privacyrichtlijn – vooral bezig te houden met een meer algemene en adviserende functie, het ontvangen van klachten en het informeren van de burger. Op de Belgische positie met betrekking tot de voorafgaande machtigingen tot het gebruik van het Rijksregisternummer komen we verder nog terug.

PROBLEMEN - Wanneer we alles samen beschouwen moeten we concluderen dat het Oostenrijkse systeem - en wellicht zal hetzelfde gelden voor het Duitse systeem - over een aantal interessante punten beschikt, maar dat het geheel toch een aantal problemen kent in verband met de transparantie en de gebruiksvriendelijkheid ervan. Hoewel het Portugese systeem het wat deze punten betreft beter lijkt te doen dan Oostenrijk en Duitsland, is dit systeem nog onvoldoende in de praktijk geïmplementeerd om er al definitieve conclusies uit af te leiden. Het Britse sys-

---

[230] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr. 2, 52-60; *www.law.kuleuven.be/icri/frobben,* 6.

[231] Voor een complete bespreking van de hervormingen van de wet van 26 februari 2003 en de mogelijke gevolgen voor de Privacycommissie, zie: D. DE BOT, "De Commissie voor de Bescherming van de Persoonlijke Levenssfeer: "Tussen droom en daad staan er niet alleen wetten in de weg, maar vooral praktische problemen", *T.B.B.R.*, 2003, 384-402.

teem kunnen we door de onduidelijkheid en het verregaande register niet als een goede evolutie beschouwen. Het Zweedse systeem voor het gebruik van een enkele unieke identificator lijkt minder problemen met betrekking tot transparantie en gebruiksvriendelijkheid te ervaren. Dit beleid steunt echter op de typisch Scandinavische openbaarheid van informatie. Het zal daarom geen vanzelfsprekendheid zijn om dit systeem zonder meer in te voeren in een ander land. Zo kennen West-Europese landen vaak een grotere vraag naar een afdoende graad van bescherming van de privacy tegen de verwerking van persoonsgegevens. We kunnen uiteraard wel een aantal elementen uit dit systeem in het achterhoofd houden. Een systeem dat steunt op transparantie en openbaarheid en dat geëvolueerd is naar een systeem waar het nationale identificatienummer gebruikt wordt mits expliciete en ondubbelzinnige toestemming van de betrokkene, mag immers niet a priori uitgesloten worden.

VRIJ OF GEREGULEERD GEBRUIK VAN DE ENKELE UNIEKE IDENTIFICATOR? - Het grote verschil tussen het Belgisch en het Zweeds beleid is uiteraard het gegeven dat het gebruik van het Zweeds nationaal identificatienummer in principe vrij is. Bij het rechtsvergelijkend onderzoek naar het Zweeds beleid gaven we al aan dat dit identificatienummer goed ingeburgerd is in de Zweedse maatschappij. Het *Personnummer* wordt werkelijk in alle aspecten van het dagelijks leven gebruikt, tot banken en fitnessclubs toe. Recente overheidsenquêtes tonen aan dat de meerderheid van de Zweedse burgers tevreden is met het ongereguleerd gebruik van dit identificatienummer.[232] Het vrij gebruik van het nationaal identificatienummer – hoewel dit in Zweden voornamelijk het gevolg is van het Zweedse openbaarheidsprincipe – kent bijgevolg toch een duidelijke maatschappelijke aanvaarding. Hoewel men zich hier vanuit het standpunt van de privacybescherming bedenkingen bij zou kunnen maken, kan er geargumenteerd worden dat de problemen in verband met het vrij gebruik van zulk identificatienummer ook niet overschat mogen worden.[233] Het is echter niet het doel van deze studie om de definitieve keuze te maken tussen het vrij en het gereguleerd gebruik van het nationaal identificatienummer.[234] We pleiten er echter wel voor dat een gemaakte keuze consequent opgevolgd wordt. Wat België betreft merken we daarom op dat het verspreiden van het Rijksregisternummer via de certificaten op de e-ID op enigszins gespannen voet staat met het gereguleerd gebruik van dat nummer.

CONCLUSIES VOOR HET HUIDIG BELGISCH BELEID - Het gereguleerd gebruik van een enkele unieke identificator kan daarom zeker verdedigd worden indien de toegang tot het register en de verspreiding en het gebruik van het nationaal identificatienummer voldoende geregeld worden. Het lijkt ons voor een land als België daarom niet meteen opportuun om het bestaande systeem volledig te vervangen door een ander systeem. Uit het historisch onderzoek onthouden we overigens dat het bestaande systeem in landen zoals België en Zweden vaak het product is van een lange evolutie met betrekking tot deze materie. We zagen ook dat het net die evolutie is die er toe geleid heeft dat deze systemen veel meer ingeburgerd en aanvaard zijn dan de systemen die landen zoals Oostenrijk en Duitsland nu proberen te implementeren. We pleiten er in deze studie daarom niet voor om het huidig Belgisch systeem volledig te vervangen, maar om te onderzoeken of

[232] X, 'Skyddet för den personliga integriteten del II - kartläggning och analys', *SOU* 2007:22, bijlage 6 bij bijlage 4, 1.
[233] Ook in België tonen de jaarverslagen van de CBPL aan dat er maar weinig klachten zijn in verband met het gebruik van het Rijksregisternummer. Men spreekt hier in 2008 over 31 behandelde klachten, wat ongeveer een 1,5% vormt van de in die periode behandelde klachten, CBPL, 'Jaarverslag 2008', *www.privacycommission.be*, 65.
[234] Dit onderzoek werd immers voornamelijk gevoerd met het oog op de privacybescherming. Vanuit deze ooghoek kan het huidig gereguleerd gebruik verdedigd worden. Andere ooghoeken – zoals onder meer de efficiëntie van overheidsprocessen – zouden echter gebaat kunnen zijn met een meer vrij gebruik van deze identificator. Het zou ons daarom nog bijkomend onderzoek vereisen vooraleer we hier een duidelijke positie wensen in te nemen.

het kan worden aangevuld met interessante factoren uit andere systemen, zoals de systemen voor sectorgebonden identificatoren.

UITBREIDING TOT BUITEN DE OVERHEIDSCONTEXT? - In die context kunnen we dan ook denken aan het gebruik van een sectorgebonden nummer buiten de overheidssector. Een bank zou bijvoorbeeld gebaat kunnen zijn bij een identificator, die op zekere wijze de identiteit van de persoon kan staven en die gebonden is aan die bepaalde sector. De reden waarom we in de niet-publieke context aan een sectorgebonden nummer kunnen denken, is dat het toepassen van een machtigingsregime - zoals dat onder het huidige Belgisch beleid binnen de overheidscontext nodig is - daar niet praktisch haalbaar is. Het zou daarom een interessante denkpiste zijn om dit idee verder te onderzoeken.

3. AANBEVELINGEN VOOR BELGIË

3.1. UITGANGSPUNT

AANWEZIGHEID VAN HET RIJKSREGISTERNUMMER - Zoals aangegeven in paragraaf 2.1.2, is de veralgemeende aanwezigheid van het Rijksregisternummer niet overal strikt nodig. Dit nummer wordt op de buitenkant van elke elektronische identiteitskaart geprint, en is ook in het identiteitsbestand, het authentiseringscertificaat en het handtekencertificaat opgenomen. Niettegenstaande het feit dat er bij de introductie van de eID-kaart goede redenen waren om dit nummer op al deze plaatsen op te nemen, wordt vooral de aanwezigheid van het Rijksregisternummer in het authentiseringscertificaat als een privacybedreiging ervaren. Telkens een burger zich authentiseert met zijn eID-kaart, wordt dit nummer vrijgegeven. De aanwezigheid van het Rijksregisternummer aan de buitenkant, in het identiteitsbestand en in het handtekencertificaat is minder problematisch, en zelfs noodzakelijk om gebruikers van de eID-kaart de nodige garanties te kunnen bezorgen over de identiteit van de kaarthouder.

WAAR HET RIJKSREGISTERNUMMER NODIG IS … - De aanwezigheid van het Rijksregisternummer op de eID-kaart en in het identiteitsbestand dat op de chip ervan bewaard wordt kan bezwaarlijk worden aangevochten omdat dit bestand de correctheid beveiligt van het nummer dat geprint wordt op de buitenkant. Daarnaast kan het Rijksregisternummer ook niet uit het handtekencertificaat gehaald worden, omdat dit de mogelijkheid zou bemoeilijken om te bevestigen dat handtekeningen die met verschillende handtekencertificaten overeenkomen uitgaan van dezelfde kaarthouder, bijvoorbeeld als de kaarthouder een nieuwe eID-kaart gebruikt.

… EN WAAR HET NIET NODIG IS - De vermelding van het Rijksregisternummer in het authentiseringscertificaat is echter niet strikt nodig. Dit nummer werd in het authentiseringscertificaat opgenomen om de server waartegenover een kaarthouder zich authentiseert toe te laten de fysieke persoon te koppelen aan eerder geregistreerde gegevens, bijvoorbeeld een dossier, klantengegevens, enz.

HET AUTHENTICERINGSCERTIFICAAT … - Aangezien de eID-kaart oorspronkelijk hoofdzakelijk bedoeld was om een burger met de overheid te laten communiceren, en de overheid vaak gemachtigd is om in het kader van het algemene belang het Rijksregisternummer te gebruiken, werd dit nummer in het authentiseringscertificaat opgenomen. De private sector is na verloop van tijd het gebruik van de eID-kaart echter ook aantrekkelijk gaan vinden, waardoor de vraag zich opdringt of het nog opportuun is om het Rijksregisternummer in een authentiseringscertificaat te behouden, aangezien vele actoren uit de private sector geen machtiging hebben om dit nummer te gebruiken, en er heerst onduidelijkheid betreffende de mate waarin dit nummer `gebruikt' kan worden.

… ZONDER IDENTIFICATIENUMMER - Het is mogelijk om het Rijksregisternummer niet meer in een authentiseringscertificaat op te nemen, maar te vervangen door een ander (willekeurig gekozen) nummer, of zelfs helemaal weg te laten. Er kunnen zich twee situaties voordoen: een partij die gemachtigd is om het Rijksregisternummer te gebruiken ontvangt het niet meer automatisch samen met het authentiseringscertificaat zelf. Het is ook mogelijk dat een burger die zijn eID-kaart gebruikt nog niet gekend is door de partij bij wie de burger zich wil authentiseren. Dit in de veronderstelling dat elke nieuwe eID-kaart van een burger een authentiseringscertificaat bevat dat refereert aan een ander uniek nummer dan het Rijksregisternummer.

3.2. NAAR EEN MOGELIJKE OPLOSSING

TWEE VOORWAARDEN - Vanuit een praktisch standpunt, kan het Rijksregisternummer in een authentiseringscertificaat alleen weggelaten of vervangen worden door een ander nummer op twee voorwaarden. Ten eerste moeten de al bestaande toepassingen uit de private en de publieke sector met minimale aanpassingen gewoon kunnen blijven verder werken. Dit houdt in dat toepassingen die terecht nood hebben aan het Rijksregisternummer zonder meer over dit nummer moeten kunnen beschikken, terwijl toepassingen die het Rijksregisternummer niet mogen verwerken, dit nummer niet zullen ontvangen. Ten tweede moet het mogelijk zijn om te bepalen of twee verschillende authentiseringscertificaten die bij eenzelfde burger horen inderdaad bij elkaar horen. Dit is nodig omdat een burger zich anders opnieuw moet registreren met zijn of haar nieuwe eID-kaart.

NOOD AAN VERDER ONDERZOEK - In de tweede fase van deze studie zal een technische implementatie ontwikkeld worden waarbij aangetoond wordt dat aan beide voorwaarden kan voldaan worden, en wel zonder performantieverlies of onnodige complexiteit in te voeren.

EERSTE VOORWAARDE - Deze implementatie zal het gebruikelijke protocol waarmee de geldigheid van een authentiseringscertificaat wordt nagegaan, uitbreiden zodat de partij die een burger authentiseert te weten komt of het gebruikte authentiseringscertificaat nog geldig is, en tegelijk ook het Rijksregisternummer van deze burger zal ontvangen, uiteraard op voorwaarde dat deze partij gemachtigd is om dit nummer te kennen of te gebruiken. Dit zorgt ervoor dat aan de eerste voorwaarde voldaan wordt.

HET OCSP-PROTOCOL - Standaard werkt dit protocol als volgt: als een burger zijn of haar authentiseringscertificaat gebruikt om zich te authentiseren ten opzichte van een derde partij, zal deze laatste de geldigheidsstatus van het gebruikte authentiseringscertificaat nagaan door bij een online server de certificaatstatus op te vragen. Deze controle gebeurt aan de hand van een OCSP-aanvraag te versturen met het Online Certificate Status Protocol (OCSP). De Certificatieautoriteit die het te controleren certificaat heeft uitgegeven baat de server uit die deze OCSP-aanvragen beantwoordt. Er bestaan drie mogelijke antwoorden. Het eerste antwoordtype geeft aan dat het certificaat geldig is. Het tweede dat het niet geldig is, en het derde geeft aan dat het niet mogelijk is een uitspraak te doen over het bewuste certificaat. Dit laatste antwoord treedt bijvoorbeeld op als een OCSP-aanvraag wordt verstuurd naar een OCSP server in verband met een certificaat dat niet werd uitgegeven door de Certificatieautoriteit die de OCSP server uitbaat. Telkens een dienstenleverancier de geldigheid van een authentiseringscertificaat wil controleren, wordt dit protocol uitgevoerd.

UITBREIDING VAN HET PROTOCOL - De uitbreiding van dit protocol die in de tweede fase van deze studie zal ontwikkeld worden bouwt op het gewone Online Certificate Status Protocol, waarbij de OCSP-aanvraag ondertekend wordt door de aanvrager. Nadat de OCSP server heeft gecontroleerd of de handtekening die de aanvrager heeft berekend correct is, en de OCSP-server ook heeft nagaan of de aanvrager gemachtigd is om het Rijksregisternummer te gebruiken, zal de OCSP server naast een van de drie klassieke antwoorden ook nog bijkomende informatie terugsturen naar de aanvrager. Deze bijkomende informatie bestaat uit het Rijksregisternummer dat hoort bij de gebruiker van het authentiseringscertificaat.

GEVOLGEN VOOR BETROKKEN PARTIJEN - Deze uitbreiding stelt partijen in staat om op een efficiënte wijze over het Rijksregisternummer te beschikken, en biedt de garantie dat alleen partijen die gemachtigd zijn om dit nummer te gebruiken het Rijksregisternummer ontvangen. Partijen die niet gemachtigd zijn om het Rijksregisternummer te gebruiken krijgen alleen het standaard OCSP-antwoord. Zij kunnen uiteraard ook de gewone, niet-getekende OCSP-aanvragen versturen, aangezien ze toch geen bijkomende informatie zullen ontvangen.

TWEEDE VOORWAARDE - Aan de tweede voorwaarde om het Rijksregisternummer van een authentiseringscertificaat te kunnen vervangen door een uniek nummer kan voldaan worden door ook de OCSP-aanvraag uit te breiden. Met deze uitbreiding wordt de OCSP-aanvraag ook gehandtekend door de aanvrager, zoals hierboven beschreven, maar wordt de aanvraag ook voorzien van een referentie aan het authentiseringscertificaat waarvan vermoed wordt dat het hoort bij dezelfde burger die hoort bij het te controleren authentiseringscertificaat. Nadat de OCSP server heeft nagegaan of de OCSP-aanvraag correct gehandtekend werd, en de aanvrager gemachtigd is om de link te kunnen leggen tussen verschillende authentiseringscertificaten, wordt het OCSP-antwoord teruggestuurd naar de aanvrager. Dit antwoord bevat het klassieke OCSP-antwoord, samen met de bevestiging of de ontkenning dat het gecontroleerde authentiseringscertificaat hoort bij dezelfde burger als het authentiseringscertificaat waaraan gerefereerd wordt in de OCSP-aanvraag. Ook deze uitbreiding stelt alle partijen in staat om op een efficiënte wijze de link te leggen tussen twee verschillende authentiseringscertificaten die horen bij eenzelfde burger.

COMBINATIE VAN BEIDE UITBREIDINGEN - Beide uitbreidingen kunnen uiteraard gecombineerd worden, zodat een partij die voldoende gemachtigd is met een enkele gehandtekende OCSP-aanvraag te weten kan komen of twee verschillende authentiseringscertificaten overeenkomen met eenzelfde burger, en welk Rijksregisternummer aan deze burger werd toegekend. Om het aantal interacties met de machtigingsserver beperkt te houden kan de OCSP server bijvoorbeeld in een databank bij houden of een aanvrager gemachtigd is om zowel het Rijksregisternummer te kennen als de link te leggen tussen twee verschillende authentiseringscertificaten. Dit zorgt ervoor dat de OCSP server maar een enkele keer de machtiging moet controleren van de aanvrager.

3.3. OPMERKINGEN BIJ DEZE OPLOSSING

CAVEATS - Uiteraard kunnen er de nodige bedenkingen geformuleerd worden bij een dergelijke oplossing. Hoewel de hier voorgestelde oplossing zich nog in een erg vroeg stadium bevindt en later nog verder ontwikkeld zal moeten worden, konden we toch al een aantal voorwaarden formuleren waar een uiteindelijke oplossing voor het hier voorliggende probleem aan zal moeten voldoen. Om te verzekeren dat er bij de ontwikkeling van het uiteindelijke voorstel tot oplossing voldoende rekening gehouden wordt met de zwakke punten die de slaagkansen van een dergelijk voorstel zouden kunnen aantasten, willen we hier een overzicht bieden van een aantal van de belangrijkste opmerkingen die geformuleerd zouden kunnen worden bij een dergelijk voorstel.

WET VAN 25 MAART 2003 - Men zou kunnen argumenteren dat de wetswijziging van 25 maart 2003 de aanwezigheid van het Rijksregisternummer in beide certificaten positief geëvalueerd heeft door dit identificatienummer in beide certificaten te behouden. Hierbij wordt dan echter wel over het hoofd gezien dat er niet voldaan werd aan de verwachtingen van de Privacycommissie en de Raad van State. Zo ging de Privacycommissie in haar advies van 17 april 2001 wel akkoord met de vermelding van het Rijksregisternummer op de identiteitskaart – zowel visueel als elektronisch – maar dit slechts onder de voorwaarden dat de toegang tot de gegevens op de kaart goed beveiligd zou worden en dat er een onpersoonlijk nummer gebruikt zou worden. Bovendien haalden zowel de Privacycommissie als de Raad van State aan dat het Rijksregisternummer enkel toegankelijk zou mogen zijn voor de overheden, instellingen of personen die gemachtigd zijn om dit nummer te gebruiken. Het gros van de parlementaire besprekingen was echter gericht op de kostprijs van de invoer van een elektronische identiteitskaart en met de voorwaarden voorgesteld in de adviezen van de Privacycommissie en de Raad van State blijkt in de praktijk geen rekening gehouden te worden.[235] Het feit dat men op dat moment gekozen heeft – zij het dan op zeer impliciete wijze – voor de aanwezigheid van het Rijksregisternummer in deze certificaten wil met andere woorden niet zeggen dat men vroegere en huidige bedenkingen hierover zonder meer kan negeren. Zij zullen minstens onderzocht moeten worden.

DE AANWEZIGHEID VAN HET RIJKSREGISTERNUMMER IN DE CERTIFICATEN - De vraag is dan wat de precieze reden is waarom men het Rijksregisternummer wou opnemen in de certificaten van de e-ID, ondanks het protest tegen zulke opname. Uit de parlementaire voorbereidingen van de Wet van 25 maart 2003 blijkt dat men de visuele en elektronische aanwezigheid van het Rijksregisternummer op de e-ID noodzakelijk vond omdat de burger dit nummer onder bepaalde voorwaarden zal moeten aanwenden in zijn relaties met de overheden en instellingen die gemachtigd zijn om het Rijksregisternummer te gebruiken. Hoewel we dit doeleinde zeker kunnen steunen, blijkt de praktische uitwerking van deze bepaling enigszins andere resultaten op te leveren. Onder de huidige stand van zaken kan immers iedereen met een kaartlezer kennis nemen van het Rijksregisternummer van de houder van de kaart en is er geen manier om een onderscheid te maken tussen wie gemachtigd is om dit nummer te gebruiken en wie daar niet toe gemachtigd is. Het is duidelijk dat deze praktijk verder gaat dan het vooropgestelde doel.

[235] Zo werd er trouwens ook aangegeven dat men binnen afzienbare termijn zou evolueren naar het gebruik van een onpersoonlijk nummer. Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/001, 7.

REGISTRATIEAUTORITEIT - Daarnaast zou men ook kunnen opmerken dat er rekening gehouden moet worden met de registratieautoriteit (RA).[236] Deze autoriteit vormt een belangrijke bouwsteen binnen een publieke sleutelinfrastructuur zoals de e-ID. Hij staat immers in voor de band tussen de identiteit van de burger en het certificaat dat de certificatieautoriteit aan hem uitreikt. Bijgevolg krijgt hij alle persoonsgegevens en de volledige identiteit van de gebruikers te zien. Wanneer men zoekt naar een manier om te verhinderen dat de volledige identiteit en de bijhorende attributen van de burger onmiddellijk doorgegeven worden, bestaat er het risico dat men de procedure voor de werkelijke authenticatie aan een andere instantie zal willen doorgeven, waarbij men niet dezelfde garanties zou kunnen leveren als een registratieautoriteit. Hierbij moet worden opgemerkt dat de hier voorgestelde oplossing de taak van de registratieautoriteit in principe niet aantast. Deze partij zal immers nog steeds de link tussen de identiteit en het certificaat kunnen garanderen gedurende het productie- en uitreikingsproces van de identiteitskaart. Eenmaal deze link is vastgesteld, is de functie van de registratieautoriteit vervuld. De latere controle van de geldigheid van het certificaat zal in de regel gebeuren door de certificatieautoriteit op basis van een OCSP-verzoek of via *Certificate Revocation Lists*.

UITLEZEN VAN DE KAART - Men zou ook kunnen stellen dat het uitlezen van de gegevens op de e-ID niet zo verregaand is. Het visueel tonen van de kaart – waarbij het Rijksregisternummer dus ook zichtbaar is – geeft immers toegang tot een gelijkaardige set gegevens als die men zou verkrijgen door het uitlezen van de chip van de kaart en het authentiseringscertificaat. Daarnaast is de derde die de gegevens op de kaart uitleest onder geen beding ontslaan van zijn plicht om de wetgeving met betrekking tot de bescherming van de persoonlijke levenssfeer na te leven. De aldus verkregen gegevens kan men bijgevolg slechts verwerken in overeenstemming met wat de Richtlijn en de Privacywet voorschrijven. Op deze manier zou een afdoende bescherming van de privacy alsnog gegarandeerd worden, ongeacht het feit dat het Rijksregisternummer vrijgegeven werd. Een dergelijke zienswijze kan echter maar moeilijk gevolgd worden. Wanneer men er immers van uitgaat dat er bij het uitlezen van de e-ID gegevens verwerkt worden, geeft men toe dat hierbij ook het Rijksregisternummer verwerkt wordt. Het gebruiken of verwerken van het Rijksregisternummer zonder voorafgaande toestemming door het sectoraal comité van het Rijksregisternummer is echter verboden. Daarnaast moet er gewezen worden op de toename van het gebruik van de e-ID in de private sector en de ruime verspreiding van kaartlezers. Deze evolutie leidt ertoe dat de gegevens op de e-ID steeds vaker uitgelezen en mogelijk ook verwerkt worden en dit zonder dat hierbij steeds aangifte gedaan wordt bij de Privacycommissie. Vanuit het standpunt van de privacywetgeving en de beschermde status van het Rijksregisternummer kan deze positie met andere woorden niet volgehouden worden.

PROPORTIONALITEIT - Een andere opmerking ter verdediging van de aanwezigheid van het Rijksregisternummer in het authentiseringscertificaat van de e-ID is dat zulke aanwezigheid proportioneel zou zijn. Men argumenteert dan dat de e-ID op vrijwillige basis gebruikt wordt, dat de kaart een beveiligde toegang naar online diensten toelaat en dat er toch een zekere graad van transparantie voor de dienstverleners mogelijk gemaakt wordt. Deze feiten stelt men dan tegenover de algemene toestand in het dagelijkse leven – voornamelijk op het internet – waar men voortdurend sporen van persoonsgegevens nalaat, waar allerlei gegevens onbeveiligd gecommuniceerd worden, waar onder bepaalde omstandigheden zelfs geen sprake is van transparantie en

[236] Binnen de structuur van de Belgische e-ID wordt de rol van RA uitgevoerd door het Rijksregister, bijgestaan door de gemeenten.

waar met andere woorden de privacy voortdurend met de voeten getreden wordt, zonder de mogelijkheid zich hiertegen te verzetten. Men beschouwt dan de huidige onvolmaaktheden van de e-ID als proportioneel ten opzichte van het doel van de e-ID, namelijk het aanbieden van een veilig identificatiemiddel. Hierbij kan uiteraard een discussie gevoerd worden naar de juiste draagwijdte van zulke proportionaliteit, naar het precieze doel van de e-ID, en dergelijke. Hoewel het niet de bedoeling van dit onderzoek is om zich te mengen in zulk debat, kunnen we enkel maar aanhalen dat een dergelijk debat vermeden kan worden door het Rijksregisternummer te verwijderen uit het authentiseringscertificaat.

DELEGATIE VAN BEVOEGDHEDEN? - Een meer fundamentele vraag naar de mogelijkheid van de hier voorgestelde oplossing is de vraag of de beheerder van de gegevens uit het Rijksregister – de Algemene Directie Instellingen en Bevolkingen binnen de FOD Binnenlandse Zaken – het gebruikers- en toegangsbeheer met betrekking tot het gebruik van het Rijksregisternummer mag overdragen aan een certificatiedienstverlener. Dit zou bijvoorbeeld mogelijk zijn voor het verwezenlijken van een opdracht van algemeen belang. Men zou dan kunnen argumenteren dat er geen wettelijke bepaling bestaat die toelaat dat een certificatiedienstverlener de bevoegdheid krijgt om te controleren of een betrokkene gemachtigd is om het Rijksregisternummer te gebruiken en om hem in voorkomend geval dit nummer mee te delen. De certificatiedienstverlener zou op basis van de gegevens die hij verwerkt ook profielen kunnen opstellen van de gebruikers van de ene of de andere dienst. Een dergelijke verwerking van persoonsgegevens moet uiteraard vermeden worden. Deze vraag naar een mogelijke delegatie van bevoegdheden is zeker niet onterecht en moet verder worden onderzocht.

CERTIPOST - Het OCSP-verzoek dat wordt vermeld in de hier voorgestelde oplossing moet uiteraard gericht worden aan de certificatieautoriteit die het betrokken certificaat uitgaf. Voor de Belgische e-ID worden het authentiseringscertificaat en het handtekeningcertificaat uitgegeven door Certipost.[237] Naast het uitgeven van de certificaten kan Certipost deze uiteraard ook controleren door middel van een OCSP-verzoek of door middel van *Certificate Revocation Lists*. Volgens de hier voorgestelde oplossing zou de OCSP-server naast het standaard takenpakket ook controleren of de aanvrager gemachtigd is om het Rijksregisternummer te gebruiken en om hem dit nummer – in voorkomend geval – mee te delen. De vraag is dan of een certificatiedienstverlener als Certipost gemachtigd is om het Rijksregisternummer op dergelijke manier te gebruiken en mee te delen en of zulks werkelijk een bevoegdheidsoverdracht van de administratie van het Rijksregister naar Certipost inhoudt.

DE CERTIFICATIEDIENSTVERLENER EN HET RIJKSREGISTER - Het spreekt voor zich dat Certipost gemachtigd is om het Rijksregisternummer te verwerken: het is immers de taak van deze certificatiedienstverlener om de gekwalificeerde certificaten te genereren en het Rijksregisternummer maakt onder de huidige stand van het recht deel uit van deze certificaten. Deze toelating tot het gebruik van het Rijksregisternummer is opgenomen onder artikel 6, §5 van de Wet van 19 juli 1991.[238] De administratie van het Rijksregister is bovendien krachtens artikel 9 van de Wet op

[237] Certipost werd opgericht als een *joint-venture* tussen Belgacom en De Post. Intussen heeft Belgacom haar aandelen verkocht en is De Post enige aandeelhouder. Belgacom werd oorspronkelijk aangewezen om de continuïteit van de certificatiedienstverlening te verzekeren. In de Ministerraad van 26 september 2008 werd deze taak overgedragen aan De Post.

[238] Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.* 3 september 1991.

het Rijksregister aangewezen als de tussenpersoon tussen de geaccrediteerde certificatiedienstverlener en de andere instanties die betrokken zijn bij de uitgave van een elektronische identiteitskaart, zij zal immers de certificatiedienstverlener de nodige gegevens moeten verschaffen. Daarnaast is er ook voorzien in een wettelijke controle op de certificatiedienstverlener. Zo bepaalt artikel 16, 7° van de Wet op het Rijksregister dat het sectoraal comité van het Rijksregister toezicht houdt op de procedure van de aanmaak en afgifte van deze certificaten. Ook moet het sectoraal comité krachtens artikel 16, 8° aan de burger de mogelijkheid bieden om de status van de certificaten na te gaan.

TAKEN VAN DE CERTIFICATIEDIENSTVERLENER - We weten nu dus al dat er een wettelijke gegevensoverdracht is tussen de certificatiedienstverlener en het Rijksregister. We weten ook dat de certificatiedienstverlener het Rijksregisternummer kan gebruiken binnen de aan deze instantie wettelijk toebedeelde taken. We moeten dan vaststellen wat deze taken precies inhouden. Artikel 6ter van de Wet van 19 juli 1991 bepaalt dat de certificatiedienstverlener op vraag van de burger de elektronische functies van de kaart kan schorsen of intrekken. Krachtens artikel 6bis moet de certificatiedienstverlener zijn hulp verlenen bij het bijwerken van het Register van de Identiteitskaarten dat door de FOD Binnenlandse Zaken bijgehouden wordt. De belangrijkste taak vinden we echter terug in artikel 6, wat handelt over de elektronische identiteitskaart zelf. Deze taak kan samengevat worden als het aanleveren van de certificaten voor authenticatie en voor het plaatsen van elektronische handtekeningen. We zagen al eerder dat het Rijksregisternummer oorspronkelijk opgenomen werd in de certificaten van de e-ID om ervoor te zorgen dat de overheden, instellingen en personen die gemachtigd zijn om dit nummer te gebruiken, zonder problemen kennis zouden kunnen nemen van het Rijksregisternummer van de houder van de kaart. De certificatiedienstverlener moet met andere woorden gebruik maken van het Rijksregisternummer om dit nummer op te nemen in de certificaten die zij uitvaardigt om er op die manier voor de zorgen dat dit nummer meegedeeld kan worden aan zij die gemachtigd zijn om dit nummer te gebruiken.

GEEN DELEGATIE NODIG - Uit het voorgaande blijkt dat er hier niet noodzakelijk sprake is van een onwettige delegatie van bevoegdheden. In de hier voorgestelde oplossing vervult de certificatiedienstverlener immers enkel een onderdeel van de aan deze instantie toegewezen taken uit de Wet van 19 juli 1991 – namelijk het doorgeven van het Rijksregisternummer aan de overheden, instellingen of personen die gemachtigd zijn om dit nummer te gebruiken. Het Rijksregisternummer zal dan echter niet meer rechtstreeks via het authentiseringscertificaat meegedeeld worden, maar via de omweg van het OCSP-verzoek. Aangezien de machtigingen tot het gebruik van het Rijksregisternummer steeds gepubliceerd moeten worden, maakt het beroep van de certificatiedienstverlener op deze machtigingen geen schending uit van de privacybescherming of van de wettelijk toegewezen bevoegdheden. Men zou voor de realisatie van dit deel van de hier voorgestelde oplossing nog kunnen denken aan een mogelijk beroep op het *ex ante* register van de verleende machtigingen, een figuur die in het kader van het Kadaster van Verbindingen onder deel II van dit onderzoek verder uitgediept zal worden. We kunnen daarom argumenteren dat de certificatiedienstverlener krachtens de aan deze instantie wettelijk toegewezen taken wel de bevoegdheid zou hebben om te controleren of een betrokkene gemachtigd is om het Rijksregisternummer te gebruiken en om hem in voorkomend geval dit nummer mee te delen. Dit strookt immers met zowel de initiële bedoeling van de wetgever toen hij besloot om het Rijksregisternummer op te nemen in de certificaten van de e-ID als met de opmerkingen die de Privacycommissie en de Raad van State formuleerden bij dit voorstel.

DELEGATIE WEL MOGELIJK? - Hoewel uit het voorgaande volgt dat een delegatie van bevoegdheden van de administratie die belast is met het beheer van het Rijksregister naar de certificatiedienstverlener niet strikt noodzakelijk is, loont het toch de moeite om de mogelijkheidsvoorwaarden voor een dergelijke bevoegdheidsdelegatie te onderzoeken. Allereerst moeten we Certipost plaatsen als een dochteronderneming van De Post. Krachtens artikel 6, 4° van het vierde beheerscontract tussen de Staat en De Post N.V. van publiek recht moet De Post instaan voor de dienstverlening voor het certificeren van berichten.[239] Het gaat hier om een taak van openbare dienst en kan dus beschouwd worden als een opdracht van algemeen belang. Deze taak wordt echter uitbesteed aan Certipost, wat tot gevolg heeft dat de certificatiedienstverlening van Certipost al tot op zekere hoogte beschouwd kan worden als de uitvoering van een opdracht van algemeen belang. Daarnaast zien we dat de overheid in 2002 het contract voor de levering van identificatie- en handtekeningencertificaten en de levering van certificatiediensten aan Belgacom toegekend heeft. Dit contract werd in 2004 overgedragen aan Certipost, waarbij er van Belgacom gevraagd werd om in te staan voor de continuïteit van de levering van de identiteitskaarten. Bij het overdragen van de aandelen die Belgacom aanhield in Certipost aan De Post, werd daarom ook die verantwoordelijkheid overgedragen. De precieze omvang van de taken die krachtens deze raamovereenkomst aan Certipost toegewezen zijn, is te vinden in Bijzonder Bestek RRN 006/2001 van 14 november 2002. Algemeen kan de taak van Certipost worden omschreven als het leveren van de certificaten en de certificatiediensten voor de e-ID. Hierbij moet worden opgemerkt dat de "Verklaring met betrekking tot de certificatiepraktijk" van de Citizen-CA – dit is Certipost – duidelijk aangeeft dat certificatiediensten openbare diensten zijn.[240] Uit de functionele betekenis van het begrip openbare dienst volgt dat Certipost als certificatiedienstverlener bijgevolg een opdracht van algemeen belang uitvoert. Een eventuele delegatie van een deel van de bevoegdheden van de administratie die belast is met het beheer van het Rijksregister naar de certificatiedienstverlener kan dan plaatsvinden uit hoofde van de opdracht van algemeen belang waarmee de certificatiedienstverlener belast is.

DELEGATIE OF TOEWIJZING? - We moeten ons bovendien bewust zijn van het onderscheid tussen de delegatie van bevoegdheden en de toewijzing van bevoegdheden. Van delegatie is immers enkel sprake indien een administratief orgaan zelf over zijn bevoegdheden beschikt. Dit zou inderdaad het geval zijn indien de administratie die belast is met het beheer van het Rijksregister zelf de beslissing neemt om bepaalde aspecten van het gebruikers- en toegangsbeheer van het Rijksregister over te dragen aan de certificatiedienstverlener. In dit geval moet er rekening gehouden worden met een aantal restrictieve voorwaarden, zoals onder meer de bepaling dat zulke delegatie moet kaderen binnen een opdracht van algemeen belang. De federale wetgever kan echter een dergelijke bevoegdheid ook rechtstreeks toewijzen aan de certificatiedienstverlener. In dit geval kan men de problematiek van de opdrachten van algemeen belang vermijden.

STOPZETTING VAN DE DIENSTVERLENING - Een laatste opmerking bij het toekennen van de hier voorgestelde taak aan de certificatiedienstverlener gaat uit naar de problemen die zouden kunnen ontstaan indien de huidige certificatiedienstverlener vervangen wordt door een andere certificatiedienstverlener. Hier kan artikel 15 van de Wet van 9 juli 2001 betreffende het juridisch kader voor elektronische handtekeningen en certificatiediensten soelaas bieden. Dit artikel bepaalt

[239] Merk op dat artikel 8 van het beheerscontract bepaalt dat de hier vermelde opdracht van openbare dienst slechts gewaarborgd wordt door De Post na het sluiten van een uitdiepingsovereenkomst met de Staat.

[240] CITIZEN CA, "Verklaring met betrekking tot de certificatiepraktijk – Certification Practice Statement", *www.certipost.be*, 55. Certificatiediensten worden omschreven als de diensten die verbonden zijn met de levenscyclus van de certificaten. Hierbij hoort onder meer het valideren van de geldigheid van de certificaten.

immers dat indien een certificatiedienstverlener zijn activiteiten stopzet, hij ervoor moet zorgen dat zijn activiteiten overgenomen worden door een andere certificatiedienstverlener die eenzelfde kwaliteits- en veiligheidsniveau kan waarborgen. Indien hij hier niet voor kan zorgen, zal hij de door hem uitgevaardigde certificaten moeten herroepen. Conform bijlage 2, i) van de wet moeten de gekwalificeerde certificaten geregistreerd worden gedurende de nuttige termijn van dertig jaar. Indien Certipost de taak van certificatiedienstverlener zou stopzetten, kan dit bedrijf geen nieuwe certificaten meer uitreiken en is het bedrijf bijgevolg niet langer gemachtigd om het Rijksregisternummer te gebruiken. Daarnaast verbiedt de regelgeving met betrekking tot de privacybescherming de bewaring van persoonsgegevens voor een langere duur dan nodig is voor het bereiken van het doel van de verwerking. Bij het stopzetten van de certificatiedienstverlening zal Certipost bijgevolg alle persoonsgegevens moeten verwijderen die voor de uitvoering van de wettelijk toegekende taak bewaard werden. Tot slot moet worden opgemerkt dat De Post garanties moet leveren voor de continuïteit van deze dienstverlening.

OCSP - Tot slot wordt opgemerkt dat het gebruik van het *Online Certificate Status Protocol* niet overal ingeburgerd is. De hier aangehaalde verificatie gebeurt veelal op basis van een *Certificate Revocation List* (CRL) die aangeeft welke certificaten ingetrokken zijn. Bij het verder uitwerken van de hier voorgestelde oplossing zal er dus moeten aangetoond worden dat het gebruik van het OCSP geen verlies aan efficiëntie betekent voor de overheidsdiensten en dat het gebruik van dit protocol evenmin bijkomende kosten met zich meebrengt. Hierbij zal ook een alternatieve oplossing geanalyseerd worden. In deze alternatieve oplossing wordt het Rijksregisternummer in het authentiseringscertificaat vervangen door een ander identificatienummer dat door middel van een databank bij het Rijksregister gelinkt wordt aan een specifieke burger. Hierdoor blijft het certificaat uniek voor elke identiteitskaart en kan men ervoor zorgen dat wie gemachtigd is om het Rijksregisternummer te gebruiken, dit nummer ook zal ontvangen. In dit voorstel wordt echter wel melding gemaakt van een dubbel OCSP-verzoek. Aangezien er gevreesd wordt dat een enkel OCSP-verzoek al tot een overbodig complexe procedure zou leiden, kan een voorstel dat gebruik maakt van een dubbel OCSP-verzoek uiteraard geen meerwaarde bieden.

4. CONCLUSIE

KEUZE TUSSEN UNIEKE IDENTIFICATOREN - Zoals uit het historisch onderzoek bleek, kan de keuze tussen een enkele unieke identificator enerzijds en sectorgebonden identificatoren anderzijds in bepaalde landen het gevolg zijn van een jarenlange evolutie. Het door deze landen gehanteerde systeem zit daarom vaak sterk in de nationale cultuur ingebakken en het zal voor deze landen wellicht geen sinecure zijn om zonder meer het gehele bestaande systeem te vervangen door een ander systeem. Uit het rechtsvergelijkend onderzoek bleek bovendien dat het - net door onder meer die culturele verschillen - ook niet altijd mogelijk zal zijn om een vreemd systeem zonder meer in te voeren in een land met een andere culturele en historische achtergrond. We herhalen echter wel dat dit niet wil zeggen dat men niet bepaalde elementen uit de systemen die andere landen hanteren kan overnemen om het eigen systeem aan te vullen en te verbeteren.

PROBLEMEN IN ANDERE LANDEN - Bij de verdere analyse van het beleid van een aantal Europese landen bleek dat het Oostenrijks systeem - ondanks de vele lofbetuigingen die dit land al heeft mogen ontvangen - toch nog een aantal niet te onderschatten problemen kent in verband met de transparantie en de gebruiksvriendelijkheid ervan. Gelet op de sterke overeenkomsten tussen het in Duitsland geplande systeem en het Oostenrijks systeem, kunnen we vermoeden dat Duitsland nog met gelijkaardige problemen geconfronteerd zal worden. Ook het Portugese systeem kent nog een aantal problemen, ondanks het feit dat dit land al de belangrijkste problemen die het Oostenrijks en Duits systeem bedreigen, heeft kunnen vermijden. Wat betreft het systeem dat in het Verenigd Koninkrijk ingevoerd zal worden, kunnen we niet anders dan concluderen dat dit systeem niet kan voldoen aan de verwachtingen met betrekking tot transparantie en de bescherming van de persoonlijke levenssfeer. Zoals we zagen zijn transparantie en de bescherming van de persoonlijke levenssfeer hier erg belangrijke elementen, die bepalend zullen zijn voor het uiteindelijke succes van het systeem. Zweden - een land dat net als België een enkele unieke identificator hanteert - kent door het openbaarheidsprincipe allicht geen gebrek aan transparantie. Het is echter ook dat openbaarheidsprincipe dat er voor zorgt dat het Zweedse systeem niet gemakkelijk te implementeren zal zijn in een land dat een sterkere vraag naar privacybescherming kent. We concludeerden daarom dat het Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer zeker verdedigd kan worden in het licht van Richtlijn 95/46/EG. Dit is het gevolg van een voldoende graad aan transparantie en van een afdoende privacybescherming door onder meer het gebruik van voorafgaande machtigingen.

PROBLEMEN IN BELGIË - Dit wil echter niet zeggen dat er geen opmerkingen te maken zijn bij het huidig Belgisch beleid. Zo kan het sterk veralgemeende gebruik van het Rijksregisternummer op de e-ID - en dan vooral het gebruik van dit nummer in beide certificaten - maar moeilijk verdedigd worden. Het leek ons daarom interessant om een meer technisch georiënteerd onderzoek te voeren, waar er getracht zou worden om praktische aanbevelingen te formuleren om het Belgisch beleid verder op punt te stellen.

AANBEVELINGEN - Wat de aanbevelingen uit het technisch onderzoek betreft, zagen we dat het niet strikt nodig is dat het Rijksregisternummer opgenomen wordt in het authentiseringscertificaat. Dit nummer kan vervangen worden door een ander uniek nummer of zelfs verwijderd. Hiertoe zijn er echter twee voorwaarden. De bestaande toepassingen in zowel de publieke als de private sector moeten met minimale aanpassingen kunnen blijven werken en het moet mogelijk zijn om te bepalen of twee verschillende authentiseringscertificaten die bij eenzelfde burger horen ook effectief bij deze burger horen. Dit kan gebeuren door het protocol waarmee de geldigheid van een authentiseringscertificaat nagegaan wordt uit te breiden zodat men te weten kan komen of dit certificaat nog geldig is en tegelijk – indien men hiertoe gemachtigd is – het Rijksregisternummer van de burger kan ontvangen. Men kan daarnaast ook de OCSP-aanvraag uitbreiden. Ook dit stelt immers de betrokken partijen in staat om efficiënt twee verschillende authentiseringscertificaten die bij eenzelfde burger horen aan elkaar te linken. In dit deel van het project is er al een eerste aanzet gegeven wat betreft deze aanbeveling. Het hier geformuleerde voorstel zal in de loop van dit project nog verder onderzocht en uitgewerkt worden.

AANZET TOT VERDER ONDERZOEK - Deze resultaten zullen dienen als basis voor het tweede deel van dit project, het kadaster van verbindingen. Er zal dan onderzocht worden hoe zulk kadaster technisch, organisatorisch en juridisch georganiseerd moet worden. Het hier gevoerde rechtsvergelijkend onderzoek zal ons helpen te onderzoeken hoe andere Europese landen zulk concept invullen. Ook de bevindingen uit het hier gevoerde technisch onderzoek - we denken dan aan de uitbreiding van het protocol waarmee de geldigheid van authentiseringscertificaten gecontroleerd wordt – zullen later in dit project nog verder ontwikkeld worden. Uit dit deel van het project onthouden we voornamelijk dat het gebruik van een nationale enkele unieke identificator zoals het Rijksregisternummer verdedigd kan worden vanuit het standpunt van de privacybescherming. In wat volgt zullen er twee pistes onderzocht worden om op die manier het huidige Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer meer consequentie mee te geven. Indien we het huidige geregelde gebruik willen aanhouden, zal het onderzoek naar de uitbreiding van het OCSP kunnen dienen als middel om het gebruik van dit identificatienummer in de e-ID enigszins te temperen. Indien men er echter voor zou opteren om meer aansluiting te zoeken bij het Zweeds beleid van het vrij gebruik van zulk nummer, zal er gezocht worden naar hoe men de transparantie betreffende het gebruik van het Rijksregisternummer nog kan verbeteren. Enige transparantieverhoging zal hier nodig zijn om het Zweeds openbaarheidsprincipe te benaderen.

DEEL II: HET KADASTER VAN VERBINDINGEN

1. INLEIDING

HET VERALGEMEEND GEBRUIK VAN HET RIJKSREGISTERNUMMER - In het eerste luik van dit project hebben we het veralgemeend gebruik van het Rijksregisternummer binnen de overheidscontext onderzocht. We gaven eerst een overzicht van de belangrijkste bouwstenen voor het Belgisch beleid met betrekking tot e-Government, waaronder het gebruik van unieke identificatoren en de elektronische identiteitskaart. Vervolgens hebben we getracht deze bouwstenen terug te vinden in het beleid dat een aantal Europese landen er op na houden. Waar deze landen niet dezelfde bouwstenen hanteerden, werd er gezocht naar een enigszins equivalent punt in het beleid van deze landen. Dit rechtsvergelijkend onderzoek stelde ons in staat om zowel de pluspunten als de minpunten van het huidige Belgisch beleid in kaart te brengen. Daarnaast kon deze rechtsvergelijking ons meteen duidelijk maken of de in andere landen gehanteerde oplossingen al dan niet een meerwaarde zouden kunnen bieden voor het Belgisch beleid. We concludeerden dat het gebruik van sectorgebonden identificatoren – zoals we dit zagen in Oostenrijk en Duitsland – een aantal interessante punten met zich mee brengt, maar dat het niet opportuun is om zulk systeem in zijn geheel in België te willen implementeren. We willen echter wel de interessante punten van zulk systeem in het achterhoofd houden als eventuele suggestie ter verbetering van het huidige Belgisch beleid.

HET ONLINE CERTIFICATE STATUS PROTOCOL - Hoewel we het Belgisch gebruik van het Rijksregisternummer als enige unieke identificator doorheen de hele overheidssector zeker kunnen verdedigen vanuit het standpunt van de privacybescherming met betrekking tot de verwerking van persoonsgegevens, merkten we op dat er toch ook mindere punten verbonden waren aan het huidige beleid. In een meer technisch gericht onderzoek werden er daarom suggesties geformuleerd om dit beleid verder op punt te stellen. Zo stelden we voor om het Rijksregisternummer niet meer in het authentiseringscertificaat op te nemen. Een voorgestelde manier om dit te kunnen bereiken – de uitbreiding van het *Online Certificate Status Protocol* – zal verder in dit project nog verder ontwikkeld worden. De in het eerste luik opgeleverde resultaten zullen dan ook dienen als basis voor het onderzoek in het kader van het technisch luik van dit project.

HET KADASTER VAN VERBINDINGEN - Het tweede luik van het project gaat uit naar het Kadaster van Verbindingen. We zullen zien dat we het idee voor zulk kadaster kunnen vinden in de Wet op het Rijksregister, maar dat dit begrip nergens gedefinieerd of geconcretiseerd wordt.[241] Het Kadaster van Verbindingen is bijgevolg onder de huidige stand van het recht slechts een begrip zonder inhoud. Het doel van dit luik van het project is om het Kadaster van Verbindingen nader te onderzoeken. Onder hoofdstuk 2 zal er daarom onderzoek gevoerd worden naar de invulling van het concept zelf. We zullen trachten het begrip 'Kadaster van Verbindingen' duidelijk af te bakenen. Er zal ook onderzocht worden of andere Europese landen een gelijkaardig concept kennen en hoe zij dit invullen. De resultaten van het rechtsvergelijkend onderzoek uit het eerste luik van het project zullen hier als basis dienen. Er zal ook onderzocht worden welke informatie er in zulk kadaster opgenomen moet worden en hoe dit in zijn werk hoort te gaan. Wanneer we

[241] Wet tot regeling van een Rijksregister van de natuurlijke personen, 8 augustus 1983, *B.S.* 21 april 1984.

enige invulling gegeven hebben aan het concept zelf, zullen we onderzoeken hoe zulk Kadaster van Verbindingen in de praktijk opgezet zou moeten worden. Er zullen immers bij het opzetten van dit systeem ongetwijfeld een aantal juridische, organisatorische en technische problemen opduiken. Het praktijkonderzoek voor het Kadaster zal uitgewerkt worden onder hoofdstuk 3 van dit onderzoek. Het doel van dit onderzoek is om een aantal praktische aanbevelingen te kunnen formuleren. Die praktische aanbevelingen zullen onder hoofdstuk 4 worden samengevat tot een conclusie voor deze conceptstudie met betrekking tot de oprichting van het Kadaster van Verbindingen. Gelet op het tijdsbestek en de omvang van deze studie is het echter onrealistisch om een volledig uitgewerkt projectplan op te leveren. Dit onderzoek zal zich daarom richten op het formuleren van een meer conceptueel – zij het praktijkgericht – plan.

2. HET CONCEPT 'KADASTER VAN VERBINDINGEN'

BEGRIPSAFBAKENING - Zoals uit de korte inleiding al bleek, is er in de Wet op het Rijksregister sprake van een 'kadaster van netwerkverbindingen'. Dit begrip wordt echter nergens verder gedefinieerd of concreter ingevuld. In dit hoofdstuk zullen we daarom dit concept proberen uit te diepen. We onderzoeken allereerst waarom zulk Kadaster van Verbindingen nodig zou zijn (2.1). Vervolgens zullen we trachten dit begrip af te bakenen en het enigszins te definiëren (2.2). Door middel van een rechtsvergelijkend onderzoek (2.3) zullen we kijken of dit begrip een Belgisch unicum is of dat andere Europese landen ook zulk concept kennen. Indien dit concept ook in andere landen gekend is, zullen we onderzoeken hoe het daar ingevuld wordt. Daarna zal er onderzocht worden wat de precieze inhoud van het Kadaster zou moeten worden (2.4). We zullen onderzoeken welke informatie er in het Kadaster bewaard moet worden, voor hoe lang die informatie bewaard moet worden, wie er toegang toe heeft, en dergelijke. Tot slot zullen al deze bevindingen samengevat worden in een conclusie (2.5) om zo voldoende inzicht te verwerven in wat het concept 'Kadaster van Verbindingen' inhoudt.

2.1. WAAROM EEN KADASTER VAN VERBINDINGEN?

RIJKSREGISTERNUMMER EN PRIVACYBESCHERMING - Zoals we in het eerste luik van dit project al zagen, rijzen er een aantal vragen bij het veralgemeend gebruik van het Rijksregisternummer. Zo kan men bij het gebruik van zulke veralgemeende enkele unieke identificator vragen stellen in verband met de bescherming van de privacy. We zagen immers dat een nationaal identificatienummer moet worden beschouwd als een persoonsgegeven in de zin van Richtlijn 95/46/EG.[242] Er werd daarom geconcludeerd dat het gebruik van zulk nummer wel aanvaard kan worden, mits er voldoende garanties zijn voor de bescherming van de burger in verband met de verwerking van zijn persoonsgegevens. Voor België concludeerden we dat het systeem van voorafgaande machtigingen tot het gebruik van het Rijksregisternummer of tot toegang tot het Rijksregister door het sectoraal comité van het Rijksregister een voldoende bescherming kan bieden. Het Belgisch gebruik van het Rijksregisternummer als enkele unieke identificator in de hele overheidssector kan bijgevolg verdedigd worden vanuit het standpunt van de privacybescherming.

[242] Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.* L van 23 november 1995, 31-50. Hierna: de Richtlijn.

PRINCIPES VAN PRIVACYBESCHERMING - Dit wil echter niet zeggen dat er automatisch voldaan wordt aan alle principes van Richtlijn 95/46/EG en de Belgische Privacywet.[243] Zo zal men er nog steeds over moeten waken dat er voldaan wordt aan onder meer het finaliteitsprincipe, de proportionaliteitsregel en het transparantieprincipe.[244] Vooral de naleving van dit laatste principe is een zeer belangrijk punt in de geest van de Richtlijn. Men kan immers argumenteren dat er geen sprake kan zijn van de in artikel 6 van de Richtlijn bepaalde eerlijke en rechtmatige verwerking wanneer die verwerking niet voldoende transparant gebeurt.[245] Om tot voldoende transparantie bij de verwerking van persoonsgegevens te komen, zal men er dus voor moeten zorgen dat er voldaan wordt aan onder meer de informatieplicht, het toegangsrecht en de aanmeldingsplicht.[246] Het louter regelen van de toegang tot het personenregister en van het gebruik van het nationaal identificatienummer is dus niet zonder meer voldoende om een correcte naleving van de wetgeving met betrekking tot de verwerking van persoonsgegevens te garanderen.

NOOD AAN MEER TRANSPARANTIE - De naleving van de principes die voor de transparantie zo belangrijk zijn, blijkt in de praktijk echter vrij problematisch. De reden hiervoor is dat de eenvoudige toepassing van de relevante wettelijke bepalingen op zich niet automatisch leidt tot voldoende transparantie. Zo wordt de burger vaak geïnformeerd over de verwerking van zijn persoonsgegevens door middel van algemene voorwaarden en/of standaardclausules. Hoewel dit strikt genomen kan voldoen aan de wettelijk bepaalde informatieplicht, spreekt het voor zich dat deze praktijk de burger niet noodzakelijk wijzer maakt. Ook aan de aanmeldingsplicht kan voldaan worden door de vereiste informatie te laten opnemen in het publiek register van de verwerkingen. Het is echter niet zeker dat de burger ook effectief geholpen is door deze zeer beperkte informatie. Tot slot is ook het recht op toegang een recht met zeer beperkte inhoud. We onderscheiden hierbij nog de actieve en passieve openbaarheid. De actieve openbaarheid houdt in dat de verantwoordelijke voor de verwerking zelf de betrokkene op de hoogte moet brengen van de vereiste informatie.[247] Passieve openbaarheid betekent dan dat de burger zelf zijn informatie mag gaan halen bij de verantwoordelijke van de verwerking.[248] Ondanks het feit dat al deze regels dus bedoeld lijken om de burger meer transparantie te verschaffen bij de verwerking van zijn persoonsgegevens, zien we dat de loutere naleving van deze principes niet voldoende is om tot effectieve transparantie te leiden. Daarnaast dient men te onthouden dat er op de informatieplicht en op het recht van toegang een aantal relatief ruime uitzonderingen bestaan voor verwerkingen in het kader van de uitvoering van overheidstaken. We zullen daarom moeten zoeken naar verdere regels om voor meer transparantie te zorgen.

---

[243] Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992, *B.S.* 18 maart 1993. Hierna: de Privacywet

[244] Deze principes werden kort besproken onder hoofdstuk 1.2.7 van deel 1 van dit project. Voor een meer diepgaande bespreking, zie: D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 32-52; J. DUMORTIER, *ICT-Recht*, Leuven, Acco, 2009, 98-116.

[245] Die redenering wordt gevolgd door het sectoraal comité voor de Federale Overheid. Daarnaast beschouwt het comité de informatieplicht als een hoeksteen van het transparantiebeginsel, SECTORAAL COMITÉ VOOR DE FEDERALE OVERHEID, "Beraadslaging FO nr. 05/2009", 16 april 2009, *www.privacycommission.be*, randnummer 36. Ook overweging 38 bij de Richtlijn maakt melding van het belang van de informatieplicht.

[246] Zie voetnoot 244.

[247] Zie artikel 9 Privacywet. Merk op dat de hier vermelde informatie slechts zeer beperkt is.

[248] Zie artikel 10 Privacywet. De hier omvatte informatie is ruimer dan artikel 9 maar vereist dus een meer actieve houding van de betrokkene zelf.

MEER AANDACHT VOOR DE BURGER - De burger zal er immers van op de hoogte willen zijn wie zijn gegevens verwerkt en voor welke doeleinden dit gebeurt. Men zal er ook van op de hoogte willen zijn welke gegevens er verwerkt worden en hoe men eventueel bepaalde gegevens van zulke verwerking kan uitsluiten. We weten immers dat de Belgische overheden van het sectoraal comité voor het Rijksregister machtiging kunnen verkrijgen om de gegevens van de burger in het Rijksregister te consulteren en om het Rijksregisternummer van de burger als veralgemeend identificatiemiddel te gebruiken doorheen de verschillende overheidsdiensten. Voldoende transparantie zou dan vereisen dat de burger hiervan op de hoogte gebracht kan worden. Vroeger was dit niet gemakkelijk te realiseren, maar met de komst van de technologieën van de digitale maatschappij is het echter perfect mogelijk om te registreren – we spreken dan veelal over 'loggen' – wie toegang tot het register verkregen heeft en om dit vervolgens door middel van een gebruikerstoepassing toegankelijk te maken voor de burger.[249]

TRANSPARANTIE NAAR DE BURGER TOE - Deze vraag naar meer inspraak voor de burger met betrekking tot de verwerking van zijn persoonsgegevens en gegevenskoppelingen op basis van identificatienummers zoals het Rijksregisternummer, is zeker geen onbekend gegeven. Ook binnen de private sector kan men immers de afgelopen jaren een duidelijke groei vaststellen van de vraag naar transparantie naar de burger toe. Door de burger meer inspraak in het beheer van zijn persoonsgegevens te geven, kan men de transparantie van mogelijke verwerkingen en gegevenskoppelingen aanzienlijk verhogen. In zulk systeem gaat het meestal om het creëren en beheren van digitale deelidentiteiten, waarbij de burger kan bepalen welke van zijn persoonsgegevens door welke deelidentiteiten vrijgegeven kunnen worden. Het aan de burger inzage bieden van de gelogde gegevens is daarom een belangrijk hulpmiddel bij het beschermen van de persoonlijke levenssfeer van de burger, alsook voor het verhogen van de transparantie van de verwerking van zijn persoonsgegevens. Er zijn daarom al verschillende onderzoeksprojecten gewijd aan hoe men de burger meer inspraak kan geven in het verwerken van zijn persoonsgegevens.[250]

KADASTER VAN NETWERKVERBINDINGEN - Zoals net al aangehaald werd, zien we dat het Rijksregisternummer – net door de status van nationale enkele unieke identificator – doorheen de gehele overheidssector gebruikt wordt om gegevens over de betrokken burger uit te wisselen en met elkaar te koppelen. Artikel 8 van de Wet op het Rijksregister bepaalt dat men in de aanvraag van een machtiging tot gebruik van het Rijksregisternummer – die in de regel vereist is indien men het Rijksregisternummer wil gebruiken – moet vermelden welke netwerkverbindingen er kunnen voortvloeien uit het gebruik waarvoor men de machtiging vraagt. Die netwerkverbindingen ontstaan dus wanneer een overheid – die gemachtigd is om het Rijksregisternummer te gebruiken – dit nummer gebruikt in haar communicatie met een andere gemachtigde overheid.[251] Het artikel bepaalt verder dat het sectoraal comité van het Rijksregister dit kadaster van netwerkverbindingen moet publiceren. De term 'netwerkverbindingen' wordt hier echter niet verduidelijkt. In haar advies uit 1998 spreekt de Commissie voor de bescherming van de persoonlijke levenssfeer van een "*kadaster* […] *van de koppelingen van bestanden of gegevens die door middel van het Rijksregisternummer gemaakt mogen worden; dit kadaster zou door de Commissie kun-*

[249] België kent al zulk initiatief: de toepassing 'MijnDossier' van het Rijksregister. Verder in dit onderzoek zal dieper ingegaan worden op deze toepassing.
[250] Het meest bekende project over deze materie is PRIME, *www.prime-project.eu.*
[251] D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 189.

nen gehouden worden, parallel aan het register van de geautomatiseerde verwerkingen."[252] De Commissie stelde hier ter concretisering van de veiligheidsmaatregelen voor dat elke instelling die persoonsgegevens meedeelt of ontvangt door middel van een identificatiemiddel een lijst moet houden van de gegevensstromen die ontstaan via het identificatiemiddel. Vervolgens moet er een spoor bewaard worden van de aldus uitgevoerde overheidsopdrachten.[253]

ARTIKELS 8 EN 12 VAN DE WET OP HET RIJKSREGISTER - We moeten echter aanhalen dat het kadaster in de Wet op het Rijksregister maar een vrij recente toevoeging is. In 2003 werd bij de planning van de e-ID een wetsontwerp ingediend tot wijziging van de Wet op het Rijksregister. De voor dit onderwerp belangrijkste wijziging bestond erin het sectoraal comité op te richten en om deze instantie de bevoegdheid tot het verlenen van machtigingen toe te kennen. Tot voordien werden machtigingen immers verleend bij koninklijk besluit, na advies door de Commissie voor de bescherming van de persoonlijke levenssfeer. De wetgever heeft echter de teksten van artikelen 8 en 12 wat ongelukkig geformuleerd. Zo gaat artikel 8 over het net aangehaalde kadaster waarin het sectorale comité de netwerkverbindingen publiceert die het terugvindt in de aanvragen tot machtiging. Hoewel dit een belangrijke regel kan zijn voor de verhoging van de transparantie van de verwerking van persoonsgegevens, zagen we net dat dit artikel vrij onduidelijk geformuleerd is en geen verder gevolg geeft aan het vernoemde kadaster van netwerkverbindingen. Artikel 12 geeft de Commissie voor de bescherming van de persoonlijke levenssfeer ook nog een taak met betrekking tot de transparantie van het Rijksregister: alle machtigingen tot gebruik van het Rijksregisternummer of tot toegang tot het Rijksregister moeten door de Commissie worden gepubliceerd in een publiek register.[254] Het advies van de Commissie uit 1998 lijkt dus maar gedeeltelijk gevolgd te worden, met de teleurstellende teksten van artikelen 8 en 12 tot gevolg. Indien we deze wetswijziging dieper bekijken, kunnen we artikel 12 wel verklaren. Onder de vroegere wet werden de adviezen tot machtiging samen met de Koninklijke besluiten tot machtiging gepubliceerd.[255] Men kan het nieuwe artikel 12 dan beschouwen als een logische opvolger van de publicatie van de machtigingen. Dit register kan de burger dus een overzicht geven van welke verwerkingen en gegevenskoppelingen hij met betrekking tot zijn Rijksregisternummer mag verwachten. Waar artikel 12 zich richt op een openbaar register met de verleende machtigingen, richt artikel 8 zich dus meer specifiek op een overzicht van de gegevenskoppelingen door middel van het Rijksregisternummer die door de verleende machtigingen verwacht mogen worden.

EEN TRANSPARANTIEVERHOGEND MIDDEL - Het Kadaster van Verbindingen zou dan een manier kunnen worden om de burger in staat te stellen om enige controle uit te oefenen op de verwerking van zijn persoonsgegevens. Het kan daarom een zeer belangrijk instrument worden om de verwerking van persoonsgegevens meer transparant te maken. We zagen immers dat het transparantieprincipe een zeer belangrijk principe is en dat er geen sprake kan zijn van een eerlijke en rechtmatige verwerking van persoonsgegevens indien er niet is voldaan aan dit principe. Daarnaast zagen we dat de regels die de Richtlijn en de Privacywet zelf aangeven om tot meer transparantie te komen – namelijk de informatieplicht, het toegangsrecht en de aanmeldingsplicht –

[252] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, Advies 30/1998 van 25 september 1998, *www.privacycommission.be*, 4.
[253] D. DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 190.
[254] Art. 12, §1 Wet tot regeling van een Rijksregister van de natuurlijke personen, 8 augustus 1983, *B.S.* 21 april 1984.
[255] Aldus artikel 8 van de Wet op het Rijksregister voor de wijziging door de wet van 25 maart 2003, *B.S.* 28 maart 2003, 15921 e.v.

op zich niet automatisch leiden tot werkelijke transparantie. De Richtlijn voorziet immers – onder meer in artikel 11 (2) en in artikel 13 – in een aantal ruime uitzonderingen die de naleving van het transparantieprincipe *de facto* quasi geheel uitsluiten voor verwerkingen door overheidsdiensten in het kader van hun werkzaamheden.[256] Een reden hiertoe is dat de burger geacht wordt de wet te kennen en bijgevolg verondersteld zou kunnen worden te weten waarom de overheid welke verwerkingen moet verrichten. Het spreekt echter voor zich dat de burger nooit werkelijk op de hoogte kan zijn van de wettelijke basis voor al deze verwerkingen.[257] Deze uitzonderingen in de Richtlijn leiden met andere woorden tot een situatie waar er geen sprake kan zijn van werkelijke transparantie. Aangezien werkelijke transparantie inhoudt dat de burger toch enigszins op de hoogte is van wat er precies met zijn persoonsgegevens gebeurt, moeten we zoeken naar een ander instrument dat ons hier bij zou kunnen helpen. De burger moet immers kunnen controleren wie zijn gegevens heeft gebruikt en waar ze voor gebruikt worden. Ook wanneer zijn gegevens doorgegeven worden aan een andere overheidsdienst, zal de burger dit spoor willen blijven volgen. Het kadaster van netwerkverbindingen, bekeken vanuit het standpunt van de Commissie voor de bescherming van de persoonlijke levenssfeer in haar advies uit 1998, zou dit instrument kunnen zijn.

HET KADASTER ALS MIDDEL VOOR EFFECTIEVE TRANSPARANTIE - We zien dat het Kadaster van Verbindingen een belangrijk instrument zou kunnen zijn voor het bereiken van effectieve transparantie bij de verwerking van persoonsgegevens. Gelet op de nood aan zulke effectieve transparantie, is het belangrijk om dit Kadaster verder te definiëren en om er een werkelijke inhoud aan te geven. Nu we al een eerste idee hebben over wat het Kadaster is en waarom dit nodig is, kunnen we overgaan tot de verdere definiëring.

2.2. HET BEGRIP 'KADASTER VAN VERBINDINGEN'

VERDERE BEGRIPSAFBAKENING - Uit het voorgaande volgt dat het Kadaster van Verbindingen zeker een interessant instrument kan zijn voor de privacybescherming. Om dit Kadaster in de praktijk te kunnen toepassen, is er echter nog bijkomend onderzoek nodig. Zo zagen we al dat het Kadaster de burger in staat zou moeten kunnen stellen om op de hoogte te blijven van de verwerkingen van zijn persoonsgegevens. Het Kadaster zou dan een soort portaal worden, dat toegang geeft tot wat we het best kunnen omschrijven als een logboek waarin bijgehouden wordt wie de betrokken persoonsgegevens gebruikt en aan wie deze worden doorgegeven. Meer specifiek gaat het hier om een weergave van de koppelingen van bestanden of gegevens die men door middel van het Rijksregisternummer maakt.[258] Hoewel dit ons al een eerste idee geeft over wat het Kadaster moet voorstellen, moeten we het begrip 'Kadaster van Verbindingen' nog verder afbakenen en definiëren alvorens we kunnen overgaan tot de werkelijke invulling ervan.

EX ANTE OF EX POST BENADERING? - De korte definitie die de Commissie voor de bescherming van de persoonlijke levenssfeer aan dit begrip gaf, zegt immers maar weinig over hoe het Kadaster er in de praktijk zou uitzien. Wanneer we gaan zoeken naar een meer praktijkgerichte definitie, sto-

[256] FIDIS, "D16.1: Conceptual Framework for Identity Management in eGovernment", 2008, *www.fidis.net*, 40.
[257] FIDIS, "D16.1: Conceptual Framework for Identity Management in eGovernment", 2008, *www.fidis.net*, 40.
[258] We hanteren hier de invulling die de Commissie voor de bescherming van de persoonlijke levenssfeer hanteerde in haar advies van 25 september 1998. COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, Advies 30/1998 van 25 september 1998, *www.privacycommission.be*, 4.

ten we echter op problemen. We kunnen immers twee verschillende opvattingen over de precieze werking van dit Kadaster aanduiden. Zo kan men het Kadaster zien als een portaal dat de burger toegang biedt tot het register dat de gegevens bevat van wie er gemachtigd is om welbepaalde gegevens uit te wisselen met andere gemachtigde instanties. Aangezien het Kadaster volgens deze opvatting enkel toegang geeft tot het overzicht van de gemachtigde personen en de gegevens die zij tussen elkaar mogen uitwisselen – en dus geen overzicht geeft van de koppelingen en verwerkingen die effectief plaatsgevonden hebben – kunnen we deze opvatting beschouwen als een *ex ante* benadering. De tweede opvatting die we kunnen aanduiden in verband met de precieze werking van het Kadaster, is dan de logische tegenpool van de *ex ante* benadering: de *ex post* benadering. Volgens deze laatste benadering moet het Kadaster toegang geven tot een werkelijk logboek, waarin melding gemaakt wordt van alle verwerkingen en koppelingen aangaande de persoonsgegevens van de betrokken persoon. Zulk Kadaster zou zich dus enkel richten op de verwerkingen die al effectief hebben plaatsgevonden. Deze *ex post* benadering sluit aan bij het probleem van het gegevensspoor.[259] Het gaat hier immers om het probleem van het loggen van wat er met de persoonsgegevens van de burger gebeurt. Deze problematiek zal de rode draad vormen in dit onderzoek.

BEIDE BENADERINGEN ZIJN NUTTIG … - Zowel de *ex ante* benadering als de *ex post* benadering kunnen echter nuttig zijn voor het verhogen van de transparantie naar de burger toe. Zo kan men de *ex ante* benadering verdedigen omdat deze de burger onmiddellijk een overzicht kan geven van wat hij mag verwachten. Hij zal meteen weten wie toegang heeft tot welke gegevens en aan wie deze gegevens doorgegeven mogen worden. Hij zal dus al op voorhand weten welke gegevenskoppelingen er met betrekking tot zijn persoonsgegevens mogelijk zijn. Dit is uiteraard een belangrijk gegeven en heeft daarom een aantal eigenschappen gemeen met het principe achter de bepaling met betrekking tot de informatieplicht die de Richtlijn en de Privacywet op de verantwoordelijke voor de verwerking leggen.[260] De informatieplicht zal immers normaal vervuld worden bij de gegevensinzameling voor de verwerking zelf. Men brengt de betrokkene bijgevolg op de hoogte van de verwerkingen en koppelingen die kunnen plaatsvinden en niet van welke al plaatsgevonden hebben. De *ex post* benadering heeft echter ook zijn nut. Hoewel het zeker tot meer transparantie kan leiden indien men de burger goed op de hoogte brengt van welke verwerkingen en koppelingen hij mag verwachten, is het zeker niet ondenkbaar dat de burger ook op de hoogte zal willen zijn van welke verwerkingen en koppelingen er effectief hebben plaatsgevonden. De persoonlijke levenssfeer van de burger zal immers pas geschonden kunnen worden door een onrechtmatige verwerking van persoonsgegevens indien zulke verwerking ook effectief heeft plaatsgevonden. Ook de *ex post* benadering kan daarom beschouwd worden als een interessante benadering om de transparantie van de verwerking toe te verhogen. Deze benadering vertoont gelijkenissen met het recht op toegang uit de Richtlijn en de Privacywet. Dit recht op toegang zal zich immers ook voornamelijk *ex post* uiten.

… EN KUNNEN CUMULATIEF TOEGEPAST WORDEN - We zien dus dat zowel de *ex ante* als de *ex post* benadering nuttig kunnen zijn om de transparantie van de verwerking te verhogen. Hoewel beide benaderingen elkaars tegenpolen zijn, zou het toch een goed idee kunnen zijn om deze benaderingen cumulatief trachten toe te passen. De burger zou op die manier voor de verwerking op de

[259] Men gebruikt eerder de termen 'audit trail', 'data trail' of 'data log' dan de term 'gegevensspoor'.
[260] Ook hier wensen we nog eens de uitzonderingen op de informatieplicht in het geval van een indirecte inzameling van gegevens of in het geval van een verwerking in het kader van een wettelijke bepaling aan te stippen. Hoewel de informatieplicht zeker een interessante bepaling is, blijft er door deze ruime uitzonderingen weinig transparantie over naar de burger toe.

hoogte gebracht worden van de verwerkingen en koppelingen die hij mag verwachten. Vervolgens zou hij na de verwerking op de hoogte gebracht worden van de verwerkingen en koppelingen die ook effectief hebben plaatsgevonden. Hoewel elk van beide benaderingen al een goede evolutie voor de privacybescherming zou kunnen betekenen, zou een combinatie van beide benaderingen uiteraard voor een nog hoger niveau van privacybescherming kunnen zorgen. De *ex ante* benadering kan in principe al bereikt worden dankzij artikel 12 van de Wet op het Rijksregister. Dit artikel bepaalt immers dat de Commissie voor de bescherming van de persoonlijke levenssfeer een register moet bijhouden waarin het melding moet maken van alle machtigingen die het sectoraal comité van het Rijksregister verleend heeft. Omdat dit register enkel de verleende machtigingen – en dus niet de verwerkingen die effectief plaatsgevonden hebben – vermeld, vertoont dit grote gelijkenissen met de *ex ante* benadering. Men zou er dan voor kunnen opteren om het Kadaster van Verbindingen voornamelijk de *ex post* benadering te laten volgen, om dan tot een hoger niveau van transparantie te komen door het gebruik van zowel het register uit artikel 12 als het Kadaster uit artikel 8 van de Wet op het Rijksregister. Men zou er echter ook voor kunnen opteren om ook het *ex ante* register onder te brengen in het Kadaster van Verbindingen. Het Kadaster zou dan enerzijds toegang bieden tot een *ex ante* register en anderzijds ook toegang bieden tot een *ex post* logging.

WAT ZEGT DE WETGEVER? - Om het voorstel om het Kadaster van Verbindingen enkel een *ex post* benadering of zowel de *ex ante* als de *ex post* benadering te laten volgen mogelijk te maken, moeten we eerst onderzoeken of dit wel strookt met de geest van artikel 8 van de Wet op het Rijksregister. Het artikel zelf lijkt immers voornamelijk de *ex ante* benadering na te streven, getuige het feit dat het sectoraal comité de netwerkverbindingen moet zoeken in de aanvragen tot machtiging. Het gaat immers om mogelijke netwerkverbindingen die de aanvrager voorstelt op het moment dat hij de machtiging aanvraagt en dus zulke gegevenskoppelingen nog niet heeft kunnen uitvoeren. Ook eventuele wijzigingen in die beoogde netwerkverbindingen moeten voorafgaandelijk ter goedkeuring aan het sectoraal comité voorgelegd worden. Laat dit artikel dan nog wel ruimte voor een *ex post* benadering? Uit de parlementaire stukken blijkt alleszins van wel.

WAT ZEGT DE WETGEVER? – ONTWERP EN ADVIES CBPL - Hoewel de voorgestelde tekst van artikel 8 betreffende het kadaster van netwerkverbindingen niet gewijzigd werd tijdens de wetgevende procedure, tonen de parlementaire stukken echter wel verschillende interpretaties van deze tekst. Zo toont de memorie van toelichting bij het wetsontwerp aan dat men met deze tekst het gebruik van het Rijksregisternummer enigszins wou liberaliseren. De achterliggende gedachte hier was dat men vaststelt dat het gebruik van het Rijksregisternummer op zich niet onmiddellijk grote problemen stelt in verband met de privacybescherming. Ongebreidelde gegevenskoppelingen op basis van het gebruik van dit identificatienummer vormen echter wel een bedreiging voor de privacybescherming. Daarom werd er, op voorstel van de Commissie voor de bescherming van de persoonlijke levenssfeer, besloten dat een nieuwe procedure voor het verlenen van machtigingen tot het gebruik van het Rijksregisternummer zeker de publicatie van de beoogde netwerkverbindingen op basis van het gebruik van het Rijksregisternummer moet omvatten.[261] Deze memorie wijst ook uitdrukkelijk op het feit dat het kadaster zou bestaan uit de netwerk-

[261] Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/001, 15.

verbindingen "*waarvoor dit nummer zal worden gebruikt*".[262] In dit stadium werd met andere woorden een duidelijke *ex ante* benadering nagestreefd. Op dit wetsontwerp volgde advies 19/2002 van de privacycommissie waar enerzijds het *ex ante* karakter van het beoogde kadaster bevestigd wordt en anderzijds ook sprake is van een *ex post* controle op de rechtmatigheid van de voorgestelde gegevenskoppelingen.[263]

WAT ZEGT DE WETGEVER? – ADVIES RAAD VAN STATE EN KAMER - Advies 33.962/2 van de Raad van State keert echter terug naar de *ex ante* benadering, door te stellen dat wijzigingen van de netwerkverbindingen ter fine van de beslissing van het sectoraal comité moeten worden voorgelegd.[264] In een volgende stap, het verslag namens de Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt, gooit men het weer over een andere boeg. Hier spreekt men over het Kadaster van netwerkverbindingen door middel van het gebruik van het Rijksregisternummer als de mogelijkheid voor de burger om te raadplegen wie de voorafgaande zes maanden zijn persoonlijk dossier geraadpleegd of bijgewerkt heeft.[265] Het gaat hier met andere woorden om wat we kennen als de toepassing 'MijnDossier' en volgt dus duidelijk een *ex pos*t benadering.[266]

WAT ZEGT DE WETGEVER? - SENAAT - Na deze lezing werd het ontwerp door de Kamer goedgekeurd en overgemaakt aan de Senaat. Hier volgde geen amendering en werd er niet dieper ingegaan op het Kadaster.[267] Het ontwerp werd terug overgemaakt aan de Kamer waar het op 25 maart 2003 bekrachtigd werd. Uit deze korte bespreking van de parlementaire procedure blijkt dus dat er inderdaad een aantal verschillende opvatting bestaan met betrekking tot het voorgestelde Kadaster van Verbindingen. Het is echter wel duidelijk dat men zowel de *ex ante* als de *ex post* benadering kan verdedigen als basis voor het Kadaster.

WAT ZEGT DE WETGEVER? - CONCLUSIE - We zien dus dat men de *ex ante* benadering op verschillende plaatsen kan implementeren. Dit register kan immers zowel een aparte entiteit zijn als een onderdeel van het Kadaster. Het lijkt wel aanbevelingswaardig dat het Kadaster van Verbindingen

---

[262] Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/001, 16.

[263] Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/002, 18.

[264] Merk op dat de Raad van State spreekt van een advies. De Raad meende immers dat het sectoraal comité slechts een adviserende bevoegdheid zou mogen krijgen, waarbij de eindbeslissing bij de Koning of de Minister zou blijven. Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/003, 15.

[265] Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/005, 4.

[266] Op 'MijnDossier' zal onder hoofdstuk 2.4.1 e.v. nog dieper worden ingegaan.

[267] Wetsontwerp tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Senaat 2002-03, nrs. 2-1494/2 en 2-1494/3.

toegang zal bieden tot zowel de *ex ante* als de *ex post* benadering. Volgens deze benadering zou het Kadaster van Verbindingen enerzijds een overzicht bieden van de verwerkingen en gegevenskoppelingen die men door gebruik van het Rijksregister mag verwachten en anderzijds een toegang geven tot het logboek dat een overzicht geeft van alle verwerkingen en koppelingen die al plaatsgevonden hebben. Er rest dan nog de vraag welke gegevens er nu juist gelogd moeten worden, wie toegang moet krijgen tot die loggings, tot op welk niveau de specifieke ambtenaar die de verwerking uitvoerde geïdentificeerd moet kunnen worden, en dergelijke. Deze vragen zullen onder hoofdstuk 2.4 verder onderzocht worden. We zullen onder hoofdstuk 2.3 eerst kijken of er wat dit onderwerp betreft nog iets te leren valt uit het beleid van een aantal andere Europese landen.

HET NUT VAN ARTIKEL 8? - Uit voorgaande bespreking van de totstandkoming van het nieuwe artikel 8 van de Wet op het Rijksregister volgt dat de wetgever zelf niet goed wist wat hij met de vage bewoordingen van dit artikel moest aanvangen. Quasi elke betrokken vergadering of adviserende instantie hield er immers een eigen interpretatie van dit artikel op na. Hoewel we – zoals uit voorgaande analyse blijkt – uit de voorbereidende werkzaamheden zeker kunnen afleiden dat het Kadaster zowel de *ex ante* als de *ex post* benadering zou moeten volgen, zijn er uiteraard ook nog andere denkpistes mogelijk. Zo werd immers al vaker het nut van een dergelijk vaag artikel in vraag gesteld. Wat het *ex ante* register betreft, kan men bovendien argumenteren dat de publicatie van de machtigingen – vroeger in het Belgisch Staatsblad, nu op de website van de Privacycommissie – krachtens artikel 12 van de Wet op het Rijksregister al kan volstaan als een overzicht van de situaties waarin een organisatie gemachtigd is om het Rijksregisternummer te gebruiken of om de gegevens uit het Rijksregister in te kijken. Deze machtigingen – en dan voornamelijk de vroegere machtigingen bij koninklijk besluit – geven echter geen duidelijk beeld van de gegevenskoppelingen die deze gemachtigde organisaties effectief maken door gebruik te maken van dat Rijksregisternummer. Indien het Kadaster van Verbindingen bedoeld is als een transparantieverhogende maatregel die de burger op gestructureerde wijze inzicht wil bieden in de gegevenskoppelingen die er gemaakt worden door gebruik te maken van zijn Rijksregisternummer, dan kan het inderdaad vreemd lijken dat een dergelijk Kadaster beroep doet op een register van machtigingen dat maar weinig kan vertellen over die gegevenskoppelingen.

ALTERNATIEVEN OP ARTIKEL 8? - Vanuit de zonet aangehaalde denkpiste zou men kunnen argumenteren dat de *ex ante* benadering van het Kadaster van Verbindingen geen noodzakelijk onderdeel vormt van een centraal portaal dat de burger inzicht verschaft in de gegevenskoppelingen die gemaakt werden door gebruik te maken van zijn Rijksregisternummer. Men zou zich dan enkel kunnen richten op de *ex post* loggings van de precieze gegevenskoppelingen die er effectief plaatsgevonden hebben. Hier wordt dan een toepassing voorgesteld waar de burger, bijvoorbeeld, kan raadplegen welke van zijn persoonsgegevens Organisatie A meegedeeld heeft aan Organisaties B, C en D. Vervolgens kan de burger kijken welke van die gegevens door Organisatie B verder verspreid werden aan organisaties C, E en F. Op deze manier zou de burger in staat gesteld worden om het hele gegevensspoor van de koppelingen van zijn persoonsgegevens te traceren. Hierbij moeten we wel opmerken dat er voor de implementatie van zulk systeem wellicht beroep gedaan zal worden op een zeer complex datamodel. Voor het verdere verloop van dit onderzoek zullen we ons echter blijven richten op het Kadaster van Verbindingen zelf. Een *ex post* benadering zal hier zonder twijfel deel van moeten uitmaken. Op die manier kan het Kadaster de burger immers op gestructureerde wijze inzicht bieden in de logs met betrekking tot de gegevenskoppelingen die gemaakt werden door gebruik van zijn Rijksregisternummer. Om het hier gevoerde onderzoek een ruimere draagwijdte mee te geven, zal ook de *ex ante* benadering onderzocht worden.

EX ANTE OF EX POST BENADERING? - CONCLUSIE - Bij het definiëren van het begrip ‘Kadaster van Verbindingen’ stellen we dus vast dat er hier twee belangrijke benaderingen onderscheiden kunnen worden. De *ex ante* benadering gaat uit van een register dat alle mogelijke verwerkingen en verbindingen op voorhand vastlegt. De *ex post* benadering gaat dan uit van een logboek dat bijhoudt welke verwerkingen en verbindingen er werkelijk hebben plaatsgevonden. Beide benaderingen zijn interessant, maar met het oog op het bereiken van een maximale transparantie bij de verwerking van persoonsgegevens van de persoon, lijkt het interessanter om beide benaderingen tezelfdertijd te hanteren. Het Kadaster zou dan kunnen uitgaan van zowel de *ex ante* als de *ex post* benadering. Daar de combinatie van beide benaderingen voor een maximale impact op de transparantie kan zorgen, zal het wellicht interessanter zijn om beide benaderingen op dezelfde plaats - dus in het Kadaster - te implementeren. In een later stadium van dit onderzoek zullen we de precieze inhoud van het Kadaster verder trachten in te vullen

BEGRIPSAFBAKENING - CONCLUSIE - Wanneer we dan enige invulling of definitie proberen te geven aan het begrip ‘Kadaster van Verbindingen’, dan kunnen we stellen dat het Kadaster een portaal zal worden dat toegang biedt tot een gegevensbank die de burger in staat moet stellen om na te gaan welke van zijn persoonsgegevens er aan elkaar gekoppeld kunnen worden door het gebruik van zijn Rijksregisternummer. Deze gegevensbank zal dan de loggings bevatten van de verwerkingen en gegevenskoppelingen die al plaatsgevonden hebben. Mogelijk kan deze gegevensbank tezelfdertijd ook een voorafgaand overzicht bieden van alle verwerkingen en gegevenskoppelingen die met betrekking tot de door de burger meegedeelde persoonsgegevens toegelaten zijn.

2.3. BELGISCH UNICUM OF EUROPESE BEKENDE?

NOOD AAN RECHTSVERGELIJKEND ONDERZOEK - We hebben nu al een idee van wat het Kadaster van Verbindingen ongeveer zou moeten voorstellen. Vooraleer we gaan proberen om nog wat meer invulling te geven aan dit begrip en om te onderzoeken wat het Kadaster nu precies zou moeten omvatten, gaan we eerst onderzoeken of er al een praktijkvoorbeeld bestaat. Indien een ander land een gelijkaardig Kadaster zou kennen, zouden we dit als voorbeeld kunnen gebruiken bij de verdere uitwerking van het Belgisch Kadaster van Verbindingen. We zullen daarom nu een rechtsvergelijkend onderzoek voeren naar het Kadaster van Verbindingen in een aantal andere Europese landen. Indien we een gelijkaardig fenomeen vinden, zullen we analyseren hoe men dit begrip invult in dat land. Indien we geen equivalent vinden, zullen we trachten aan te geven hoe men deze problematiek in dat land dan wel aanpakt. We zullen de resultaten van het rechtsvergelijkend onderzoek uit deel I van dit project gebruiken als basis voor het huidige onderzoek. We onderzoeken daarom ook dezelfde landen als onder deel I van het project.

2.3.1. OOSTENRIJK

HET OOSTENRIJKS SYSTEEM - Het Oostenrijks systeem lijkt op het eerste geen volledig aan het Belgisch beleid gelijkwaardig Kadaster van Verbindingen te kennen. We zagen immers dat het Belgische Kadaster draait om de verwerkingen en de gegevenskoppelingen die door middel van het

Rijksregisternummer tot stand gekomen zijn. Het Oostenrijkse systeem heeft zich echter duidelijk gekant tegen het gebruik van een nationale enkele unieke identificator en heeft een zeer uitgebreid systeem voor het gebruik van sectorgebonden identificatoren ingesteld. Oostenrijk wil met andere woorden net vermijden dat er zulke gegevenskoppelingen kunnen plaatsvinden door middel van een nationaal identificatienummer. In het rechtsvergelijkend onderzoek onder deel I van het project zagen we dat Oostenrijk in principe wel een identificatienummer voor het nationaal personenregister kent, maar dat dit nummer – het ZMR-nummer – strikt geheim gehouden wordt. Om gebruik te kunnen maken van de Oostenrijkse *Bürgerkarte* zal er wel een *SourcePIN* gegenereerd worden, die niet kan worden teruggekoppeld aan het oorspronkelijke ZMR-nummer. Deze *SourcePIN* kan bewaard worden in een *SourcePIN* Register, dat beheerd wordt door de centrale privacycommissie. Ook dit nummer mag in principe niet gebruikt worden voor gegevenskoppeling. Artikel 8 van de Oostenrijkse wet met betrekking tot e-Government bepaalt dat de burger binnen de verschillende overheidssectoren enkel geïdentificeerd mag worden op basis van zijn sectorgebonden PIN, de zogenaamde ssPIN.[268] Zulke ssPIN kan in principe enkel door de burger zelf – met behulp van de *Bürgerkarte* – gegenereerd worden.[269]

GEGEVENSKOPPELINGEN - Uit het voorgaande volgt dat het overheidsorgaan dat bevoegd is voor een bepaalde sector een burger binnen diezelfde sector enkel zal kunnen identificeren door middel van de voor die specifieke sector bedoelde ssPIN. Datzelfde overheidsorgaan is dus in principe niet gemachtigd om de ssPIN van een andere sector te gebruiken om die burger te identificeren.[270] Wanneer het bevoegde overheidsorgaan van sector A bepaalde data met betrekking tot de burger uit sector B wil raadplegen, zal hij dus de machtiging moeten vragen om de ssPIN van die burger voor sector B te gebruiken.[271] Die machtiging moet worden verleend door de autoriteit die bevoegd is voor het *SourcePIN* Register, de centrale privacycommissie. Indien het overheidsorgaan uit sector A dan de machtiging krijgt om een ssPIN uit sector B te gebruiken, zal deze ssPIN echter versleuteld worden zodat enkel het bevoegde overheidsorgaan uit sector B deze zal kunnen ontcijferen.[272] Het bevoegde overheidsorgaan uit sector A zal dus nog steeds geen kennis kunnen nemen van de werkelijke ssPIN van de burger voor sector B. Het zal voor de overheidsdiensten daarom zeer moeilijk zijn om gegevens met betrekking tot de burger voor de ene sector te koppelen aan gegevens uit een andere sector. Zulk systeem kan uiteraard wel ernstige gevolgen hebben voor de efficiënte werking van de overheidsdiensten.

[268] §8 Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl.I* Nr. 10/2004.

[269] §10 (1) en (2) Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl.I* Nr. 10/2004.

[270] §9 (1) Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl.I* Nr. 10/2004.

[271] §10 (2) Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl.I* Nr. 10/2004.

[272] §13 (2) Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl.I* Nr. 10/2004. Hoe dit precies in zijn werk moet gaan, wordt gespecificeerd onder hoofstuk 3 van de Verordnung des Bundeskanzlers, mit der Tätigkeiten der Stammzahlenregisterbehörde betreffend das Stammzahlenregister nach dem E-Government-Gesetz näher geregelt werden (Stammzahlenregisterverordnung – StZRegV), 2 maart 2005, *BGBl. II* Nr. 57/2005.

PRIVACYCOMMISSIE - Belangrijk hier is dat de centrale privacycommissie een log zal bijhouden van de verschillende stappen in de procedure van de verwerking.[273] Deze log zal met andere woorden een overzicht geven van de gegevenskoppelingen die er tussen de verschillende overheidsdiensten en –sectoren plaatsvonden op basis van een identificatienummer. Men heeft hier dus duidelijk gekozen voor een *ex post* benadering. Het belangrijkste verschil tussen Oostenrijk en België is dan dat er in Oostenrijk sectorgebonden nummers gehanteerd worden en dat de bevoegde overheid uit een bepaalde sector in principe geen kennis zal kunnen nemen van het sectorgebonden identificatienummer dat een burger in een andere sector hanteert. De in Oostenrijk gehanteerde werkwijze kan echter niet verhinderen dat er toch nog gegevenskoppelingen zullen plaatsvinden, wat meteen de reden is voor de *ex post* logging. We kunnen ons wel vragen stellen naar de invloed van zulk systeem op de efficiëntie van de overheidsdiensten.

2.3.2. ZWEDEN

EEN NATIONALE ENKELE UNIEKE IDENTIFICATOR … - Zoals we onder deel I al zagen, gebruikt Zweden net als België een nationale enkele unieke identificator. De gegevenskoppelingen tussen de verschillende overheidsdiensten en –sectoren in Zweden zullen dus gelijkaardig zijn aan de koppelingen die plaatsvinden door het gebruik van het Belgische Rijksregisternummer. Door het Zweedse openbaarheidsprincipe is het gebruik van het Zweedse nationale identificatienummer echter relatief vrij. Het nummer wordt immers door elk overheidsorgaan in alle sectoren gebruikt als algemeen identificatienummer. Ook binnen de private sector wordt dit nummer als algemene identificator gebruikt. Wat betreft het hier voorliggende probleem van de gegevenskoppeling, kunnen we dus al vermoeden dat men hier in Zweden minder strikt op toekijkt dan in andere landen.

… DIE VRIJ TE GEBRUIKEN IS - Het vrij en veralgemeend gebruik van dit identificatienummer in zowel de publieke als de private sector, leidt er immers toe dat men door gebruik van dit ene identificatienummer toegang kan krijgen tot quasi alle informatie die er bestaat met betrekking tot die persoon. Loggen van de gegevenskoppelingen die door het gebruik van dit identificatienummer plaatsvinden, zal bijgevolg een zeer moeilijke taak zijn. Het bijhouden van een logboek, zoals dat waar het Belgische Kadaster van Verbindingen toegang toe zou moeten bieden, is immers maar werkbaar indien het gebruik van het betrokken identificatienummer enigszins overzichtelijk blijft. Bij een onbeperkt gebruik in de private sector, zoals in Zweden, zullen er zo veel gegevenskoppelingen plaatsvinden door het gebruik van dit nummer, dat het loggen van deze koppelingen in die sector praktisch onhaalbaar wordt. Het loggen van de gegevenskoppelingen door middel van dat nummer in de publieke sector, zou echter wel nog mogelijk moeten zijn.

GEEN GELIJKWAARDIG ALTERNATIEF - Zweden kent met andere woorden geen aan het Belgische Kadaster van Verbindingen gelijkwaardig alternatief. Net door zowel het vrij gebruik van het nationaal identificatienummer als door de relatief vrije toegang tot de gegevens van het personenregister, voelt Zweden niet de nood om de burger de mogelijkheid te bieden om de loggegevens met betrekking tot de gegevenskoppelingen die plaatsvinden door middel van het gebruik van het nationaal identificatienummer in te kijken. Het loggen van zulke transacties in de publieke

---

[273] §§13-16 Stammzahlenregisterverordnung verwijzen immers naar het artikel uit de Oostenrijkse privacywet dat handelt over de beveiliging van de verwerking (§14 Datenschutzgesetz 2000 (DSG 2000), *BGBl. I* Nr. 165/1999). Dit artikel vereist het bijhouden van logs.

sector zelf zal echter als gevolg van de verplichtingen die volgen uit onder meer de Richtlijn en artikel 8 van het Europees Verdrag van de Rechten van de Mens wel nog steeds moeten plaatsvinden.

2.3.3. DUITSLAND

VERSCHILLEN MET OOSTENRIJK - Ondanks de grote gelijkenissen tussen het Duits en het Oostenrijks systeem, lijken we hier te stoten op een belangrijk verschil tussen het beleid van beide landen. Oostenrijk kent immers een identificatienummer voor het personenregister en een *SourcePIN*. Deze twee identificatienummers – of enkel het laatste daar het ZMR-nummer geheimgehouden wordt– zorgen er voor dat er in Oostenrijk in principe wel algemene identificatienummers bestaan. We zagen echter wel dat het voor de gegevenskoppelingen tussen de diensten van verschillende overheidssectoren niet deze algemene identificatienummers zijn die gebruikt worden, maar de sectorgebonden identificatoren.

CENTRAAL PERSONENREGISTER - Duitsland is momenteel een centraal personenregister aan het opbouwen. Dit register zal als gevolg van het grondwettelijk verbod geen identificatienummer uitreiken aan de burgers. In Duitsland kan men bijgevolg in principe onmogelijk overgaan tot gegevenskoppeling door middel van een nationaal identificatienummer. We zagen dat er echter wel sectorgebonden identificatienummers bestaan in Duitsland, maar dat deze meestal ook maar op kleine schaal toegepast worden. Deze sectorgebonden identificatienummers zijn bijgevolg in principe niet geschikt voor algemene identificatie buiten hun sector en zullen daarom ook minder vaak gebruikt worden bij gegevenskoppelingen dan een nationaal identificatienummer. We zouden kunnen concluderen dat er hier daarom een minder sterke nood is aan transparantieverhogende mechanismes, maar dit wil echter niet zeggen dat deze sectorgebonden identificatoren helemaal niet gebruikt worden bij gegevenskoppelingen. Ook hier zal er dus nog enige nood zijn aan middelen tot het bereiken van werkelijke transparantie. Onder de huidige stand van zaken lijkt er in Duitsland echter geen waardig alternatief te bestaan op wat het Belgisch Kadaster van Verbindingen zou moeten worden. Wat Duitsland betreft lijkt het er dus op dat gegevenskoppeling door middel van identificatienummers een vrij moeilijke opgave is. Naam, geboortedatum en geboorteplaats zijn de meest interessante persoonsgegevens voor identificatie.[274] Het zullen dan ook deze gegevens zijn die hoofdzakelijk gebruikt zullen worden voor eventuele gegevenskoppelingen.

DUITSE IDENTITEITSKAART - Ook de Duitse elektronische identiteitskaart lijkt ons hier niet verder te helpen. Hoewel deze identiteitskaart wel *ad hoc* pseudoniemen kan genereren, lijkt het gebruik van deze pseudoniemen zeer anders te verlopen dan wat we in Oostenrijk zagen. Ook deze lijken daarom niet geschikt voor gegevenskoppeling. De Duitse e-ID is momenteel uiteraard nog niet operationeel, dus de tijd zal uitwijzen hoe Duitsland deze materie in de praktijk zal aanpakken.

2.3.4. VERENIGD KONINKRIJK

[274] IDABC, "eID Interoperability for PEGS: Update of Country Profiles – German Country Profile", 2009, *ec.europa.eu/idabc*, 19.

IDENTIFICATIENUMMER VAN HET PERSONENREGISTER - Net als in België, Zweden en Oostenrijk zal er in het Verenigd Koninkrijk een identificatienummer verbonden worden aan het nationaal personenregister.[275] Dit leidt er toe dat dit identificatienummer in principe gebruikt zou kunnen worden bij gegevenskoppeling. Het register zelf is op dit moment echter nog niet functioneel en over de precieze functie van het identificatienummer van het register bestaat momenteel ook nog grote onduidelijkheid. Het is daarom zeer moeilijk om op dit moment al een antwoord te geven op de vraag hoe men in het Verenigd Koninkrijk zal omgaan met gegevenskoppelingen door gebruik van het identificatienummer van het nationaal personenregister.

OMVANGRIJK REGISTER - De bevindingen uit het rechtsvergelijkend onderzoek van deel I van het project scheppen echter wel enige verwachtingen. Gezien de geplande omvang van het Britse personenregister kunnen we al zeker stellen dat dit register door quasi alle overheidsorganen zal worden gebruikt als algemene bron aan informatie met betrekking tot de burger. Het precieze gebruik van het identificatienummer van het register is echter nog niet bekend.[276] We kunnen wel aanhalen dat het Verenigd Koninkrijk op het eerste zicht geen specifiek register zal oprichten dat een gelijkaardige functie kent als wat we verwachten van het Belgische Kadaster van Verbindingen. Dit wil echter niet zeggen dat de gegevenskoppelingen hier niet gelogd zullen worden. De eerste bijlage bij de wet op de nationale identiteitskaart bepaalt immers dat er melding gemaakt kan worden van elk moment waarop er aan iemand informatie met betrekking tot de gegevens van een persoon uit het register verschaft wordt, alsook van de gegevens van de persoon of instantie aan wie zulke informatie verschaft werd en van de bijzonderheden met betrekking tot deze informatieoverdracht zelf.[277] In de verklarende tekst bij deze wet wordt dit aangeduid als het '*audit log'*, wat zoveel betekent als de eerder besproken *ex post* benadering.[278]

BRITSE IDENTITEITSKAART - De Britse wet op de nationale identiteitskaart maakt ook melding van de mogelijkheden om toegang te krijgen tot de gegevens die opgenomen zijn in het register.[279] Hoewel de wet al een eerste indruk kan geven van wie er onder welke voorwaarden toegang tot deze gegevens kan krijgen, wordt er toch nog een duidelijke discretionaire bevoegdheid overgelaten aan de Minister van Binnenlandse Zaken. Er bestaat met andere woorden geen exhaustief overzicht van de personen of instanties die toegang tot het register kunnen krijgen. Het Verenigd Koninkrijk streeft bijgevolg niet de *ex ante* benadering na.

2.3.5. PORTUGAL

GEEN NATIONAAL IDENTIFICATIENUMMER - Zoals we al zagen, heeft Portugal net als Duitsland het gebruik van een enkel nationaal identificatienummer grondwettelijk verboden. Portugal hanteert dus sectorgebonden identificatoren voor de identificatie en authenticatie van de burger binnen

[275] In tegenstelling tot het Belgische en Zweedse identificatienummer, zal het hier gaan om een onpersoonlijk nummer: The Identity Cards Act 2006 (National Identity Registration Number) Regulations 2009, S.I. 2009 No. 2574.
[276] Gezien de centralisatie die men met het geplande register lijkt na te streven, zou men kunnen vermoeden dat het identificatienummer van dit register als nationale enkele unieke identificator zal dienen. Anderzijds zal dit identificatienummer niet vermeld worden op de geplande e-ID, wat het gebruik van dit nummer als nationale enige unieke identificator dan weer minder vanzelfsprekend maakt.
[277] Paragraaf 9, Bijlage 1, Identity Cards Act 2006 (c. 15).
[278] Paragraaf 229, Explanatory Notes Identity Cards Act 2006 (c. 15).
[279] Vooral artikelen 17 tot 21 zijn hier van belang.

die bepaalde sectoren. Hoewel er het risico bestaat dat men in de private sector het identificatienummer van de nieuwe geïntegreerde identiteitskaart als *de facto* nationale enkele unieke identificator zal gebruiken om het grondwettelijk verbod te omzeilen, zal de publieke sector dit identificatienummer allicht niet gebruiken voor gegevenskoppeling.

STRENGE VOORWAARDEN TOT GEGEVENSKOPPELING - Wanneer we het Portugese beleid met betrekking tot de materie van gegevenskoppeling vergelijken met dat van de eerder besproken landen, zien we dat Portugal een vrij streng systeem hanteert. Zo zien we dat persoonsgegevens enkel gekoppeld mogen worden indien hier een wettelijke basis toe is of indien men hiertoe de toestemming van de nationale privacyautoriteit verkregen heeft.[280] Zulke gegevenskoppeling moet bovendien noodzakelijk zijn vanuit de wettelijke of legitieme belangen van de verantwoordelijke voor de verwerking, mag niet discrimineren – of op een andere manier de rechten en vrijheden van de betrokkene schenden – en moet gepaard gaan met veiligheidsmaatregelen die afgestemd zijn op de te koppelen gegevens.[281] Het gaat hier dus om een voorafgaande machtiging, vergelijkbaar met het Belgische principe van de voorafgaande machtiging tot toegang tot het register of tot gebruik van het Rijksregisternummer. Hoewel zulke machtigingen gepubliceerd worden, is er geen sprake van een werkelijk register dat melding maakt van alle personen en instanties die toelating verkregen hebben tot gegevenskoppeling. We kunnen hier dus niet echt spreken van een met de Belgische *ex ante* benadering vergelijkbare situatie.[282]

CONCLUSIE - Door het grondwettelijke verbod op het gebruik van een algemeen nationaal identificatienummer, haalden we al aan dat we het identificatienummer van het personenregister en het identificatienummer van de geïntegreerde identiteitskaart niet kunnen gebruiken voor gegevenskoppeling. Het gebruik van de sectorgebonden identificatoren valt bijgevolg onder de net besproken algemene regels van de privacywetgeving.[283]

2.3.6. CONCLUSIE

BELGISCH UNICUM - Uit dit kort rechtsvergelijkend onderzoek kunnen we alleen concluderen dat het Kadaster van Verbindingen een Belgisch unicum zou worden. Geen van de hier onderzochte landen maakt gebruik van een kadaster dat specifiek opgericht is om de burger een weergave te bieden gegevenskoppelingen door middel van de gehanteerde identificatienummers. Dit wil uiteraard zeggen dat er geen gegevens gelogd worden. Wat de loggings in de onderzochte landen betreft, zal het veeleer gaan om een loutere *ex post* vastlegging van de gegevenskoppelingen die al plaatsgevonden hebben en slechts zelden om een *ex ante* vastgestelde lijst van mogelijke gegevenskoppelingen. Enkel Portugal lijkt er een zekere *ex ante* benadering op na te houden dankzij het gebruik van de techniek van de voorafgaande machtiging. De overige landen streven en-

[280] Artikel 9, eerste lid, Lei da protecçao de dados pessoais van 26 oktober 1998, nr. 67/98, *DDR* I-A nr. 247, 5538.
[281] Artikel 9, tweede lid, Lei da protecçao de dados pessoais van 26 oktober 1998, nr. 67/98, *DDR* I-A nr. 247, 5538.
[282] Merk op dat de Portugese wet ter implementatie van Richtlijn 2006/24/EG – de Dataretentierichtlijn – wel spreekt over een register bij de toezichthoudende autoriteit dat een overzicht biedt van wie toegang heeft tot de krachtens die wet opgeslagen gegevens. Artikel 8 Lei Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relative à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações van 17 juli 2008, nr. 32/2008, *DDR* I-A nr. 137, 4456-4457.
[283] Artikel 16 Lei cria o cartão de cidadão e rege a sua emissão e utilização van 5 februari 2007, nr. 7/2007, *DDR* I-A nr. 25, 942.

kel een *ex post* benadering na. Dit kan gebeuren door de privacyautoriteit – zoals in Oostenrijk – of door zulk logboek in te bouwen in het personenregister – zoals in het Verenigd Koninkrijk. Het Kadaster van Verbindingen, als een centraal portaal waar men de burger inzage biedt tot zowel de toegelaten gegevenskoppelingen als de effectief uitgevoerde gegevenskoppelingen, kan met andere woorden enkel in België teruggevonden worden.

2.4. WAT OMVAT HET KADASTER?

INHOUD VAN HET KADASTER VAN VERBINDINGEN - Nu we een idee hebben over wat we mogen verstaan onder het 'Kadaster van Verbindingen' en nu we weten hoe andere landen dit probleem aanpakken, kunnen we kijken naar wat de concrete invulling van dit kadaster moet worden. We haalden echter al aan dat de *ex post* benadering van het Kadaster in de praktijk neerkomt op het aan de burger inzicht verschaffen in wat men noemt het 'audit trail'. Hoewel we voor dit onderzoek vertrokken zijn van de term 'Kadaster van Verbindingen', zien we dat die term nergens terug te vinden is dan in de Wet op het Rijksregister. Het 'Kadaster van Verbindingen' kunnen we daarom aanduiden als een specifieke term die men gegeven heeft aan wat we ons moeten voorstellen als een portaal waar de burger inzage krijgt in het audit trail dat binnen de context van gegevenskoppeling door middel van het gebruik van het Rijksregisternummer bijgehouden wordt. Daarom hebben we in het voorgaand rechtsvergelijkend onderzoek ook enkel gekeken naar hoe een aantal andere Europese landen de gegevensstroom met betrekking tot het gebruik van hun nationale enkele unieke identificator of hun sectorgebonden identificatoren regelen. Nu we de precieze inhoud van de logs in dit Kadaster willen bepalen, lijkt het ons aangeraden om onderzoek te voeren naar de inhoud die men gebruikelijk aan een audit trail geeft, ongeacht de sector of context waarbinnen dit audit trail functioneert. Het probleem van de gegevenskoppeling en het volgen van de gegevensstroom beperkt zich immers niet enkel tot de context van het gebruik van het Rijksregisternummer. We kunnen in dit licht daarom ook kijken hoe andere overheidssectoren dit probleem proberen aan te pakken.

2.4.1. HET AUDIT TRAIL

HET AUDIT TRAIL - Om de voorgaande redenen zullen we daarom kort het begrip 'audit trail' analyseren om beter te begrijpen wat we hieronder mogen verstaan. Zoals we al konden afleiden uit het onderzoek naar het begrip 'Kadaster van Verbindingen', is het audit trail te omschrijven als een logboek dat vermeldt wanneer bepaalde gebeurtenissen of transacties plaatsvonden. Het International Organization for Standardization (ISO) omschrijft audit trail als "*the aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information management system*."[284] Het kan daarom een overzicht bieden van onder meer het oneigenlijk gebruik van een informatiesysteem door een onbevoegd persoon, kan het aansprakelijk stellen van de verantwoordelijke personen voor hun handelingen vergemakkelijken, en dergelijke. Door bepaalde gegevens te loggen en door deze logs gedurende een bepaalde periode te bewaren, kan men dankzij het audit trail ook voldoen aan bepaalde verplichtingen zoals de beveiligingsverplichting van de verantwoordelijke van de verwerking. De burger kan in principe deze logs inkijken op grond van het beginsel van openbaarheid van be-

[284] ISO/TR 15801:2004, 33.

stuur.[285] De logs zijn immers te beschouwen als informatie waarover een administratieve overheid beschikt en die dus toegankelijk is voor alle geïnteresseerde partijen voor zover dit geen schending van de persoonlijke levenssfeer van de betrokkenen uitmaakt.

INSTRUMENT TOT VERHOGING VAN DE TRANSPARANTIE - Voor de context van de privacybescherming met betrekking tot de verwerking van persoonsgegevens betekent het de burger op gestructureerde wijze inzage bieden in het audit trail dus een zekere verhoging van de transparantie. Ook wat betreft het naleven van de proportionaliteitsregel kan het audit trail helpen. Men kan door middel van de bijgehouden logs immers controleren of men wel enkel de informatie uitwisselde die strikt nodig was voor het bereiken van het doel van de betrokken verwerking. Door middel van deze *ex post* controle kan men dan te weten komen of de wettelijke bepalingen in verband met de verwerking van persoonsgegevens al dan niet geschonden zijn.[286] Omdat deze logs zullen dienen als bewijs, zal men er over moeten waken dat deze correct en onweerlegbaar zijn. We mogen overigens ook niet vergeten dat er in de logs bepaalde data opgeslagen zullen worden die gekwalificeerd kunnen worden als persoonsgegevens. De activiteit van het loggen zelf zal met andere woorden ook aan bepaalde voorwaarden en regels moeten voldoen en men zal er over moeten waken dat het audit trail zelf niet de regelgeving met betrekking tot de verwerking van persoonsgegevens gaat schenden. Zo zal men bijvoorbeeld van elke consultatie van het audit trail ook een log moeten bijhouden om latere controle op deze verwerking mogelijk te maken.

NOOD AAN MEER ONDERZOEK - Het audit trail is dus zeker geen kant-en-klaar begrip. Hoewel er zeker al wel redelijk wat onderzoek gevoerd is naar de precieze inhoud van de betrokken logs, naar hoe lang deze bewaard moeten worden en dergelijke, bestaat er toch nog veel onduidelijkheid over de omvang van dit begrip. Op de meer juridisch-organisatorische aard van het audit trail - en bij uitbreiding dus ook het Kadaster van Verbindingen - gaan we dieper in onder hoofdstuk 3. Nu zal er eerst dieper ingegaan worden op de inhoud van het audit trail, de periode van bewaring en de vraag of de logs geanonimiseerd moeten worden.

PRAKTIJKVOORBEELDEN IN DE OVERHEIDSSECTOR - Het biedt uiteraard een meerwaarde voor het onderzoek indien we een aantal praktijkvoorbeelden zouden kunnen bespreken om zo te leren uit hun positieve en negatieve kenmerken. In de overheidssector staat het gebruik van een portaal om de burger op gestructureerde wijze inzicht te bieden in de logs echter nog in de kinderschoenen. Hoewel er al wel een aantal overheidsdiensten zij die onderzoek gevoerd hebben naar het opzetten van zulke toepassing binnen de eigen dienst, hebben nog maar zeer weinig van zulke onderzoeken ook tot de effectieve invoering van zulk portaal geleid. Binnen de overheidssector kunnen we de applicatie 'MijnDossier' aanduiden als het meest interessante praktijkvoorbeeld. Het gaat hier om een website, opgezet binnen de FOD Binnenlandse Zaken, waar de burger – na authenticatie door middel van zijn e-ID – toegang krijgt tot informatie met betrekking tot zijn gegevens in het Rijksregister. Zo krijgt men een overzicht van de gegevens die opgenomen zijn in het Rijksregister, een overzicht van de aan hem uitgereikte identiteitsdocumenten, en dergelijke. Men kan ook bepaalde documenten genereren, zoals een uittreksel uit het bevolkingsregis-

[285] Op grond van artikel 32 van de Grondwet en de Wet van 11 april 1994 betreffende de openbaarheid van bestuur, *B.S.* 30 juni 1994, 17662.

[286] Hoewel het bij het audit trail voornamelijk gaat om het *ex post* loggen van gebeurtenissen, kunnen een aantal principes ook van toepassing zijn op het *ex ante* register van verleende machtigingen. Zo zal men ook bij zulk register melding moeten maken van onder meer het doel van de verwerking en de betrokken organisatie. Ook het verhullen van betrokken persoonsgegevens zal nodig zijn.

ter of een getuigschrift van inschrijving.[287] De voor het onderwerp van deze studie meest interessante functie van 'MijnDossier' is echter de historiek van de consultatie. Deze historiek is toont een overzicht van wie deze gegevens uit het Rijksregister gedurende de afgelopen zes maanden geconsulteerd heeft. Deze historiek geeft een overzicht van de datum en het tijdstip van de consultatie, de naam van de consulterende persoon of instantie en een korte beschrijving van de consultatie. We zullen verder nog zien dat deze toepassing in haar huidige vorm zeker niet perfect genoemd kan worden, maar dat het binnen de overheidscontext momenteel wel het meest lovenswaardige initiatief is met betrekking tot het gebruik van een audit trail.[288] Andere initiatieven tot op heden zijn veel beperkter in hun opzet. We kunnen wel een aantal diensten aanhalen die de burger toelaten zijn dossier online in te kijken, maar het gebruik van een werkelijk audit trail blijft hier meestal vrij beperkt.[289]

PRAKTIJKVOORBEELDEN IN DE PRIVATE SECTOR - Ook de private sector lijkt intussen meer overtuigd te worden van het belang van meer controle door de gebruiker. Nu de gevaren van bepaalde technologieën en toepassingen voor de bescherming van de persoonlijke levenssfeer steeds vaker in de media komen, kunnen bedrijven niet anders dan een passende oplossing te bieden voor dit probleem. Bedrijven als Google en Facebook hebben de laatste jaren veel kritiek mogen verwerken met betrekking tot hun privacybeleid. Beide bedrijven zijn daarom actief bezig met het uitwerken van een meer op de noden van de gebruiker afgestemd beleid. De gebruiker zou dan meer inzicht krijgen in welke persoonsgegevens hij aan deze bedrijven en derden meedeelt en welke verwerkingen hij dus kan verwachten. Belangrijk is dat men de gebruiker ook toelaat om actief de meegedeelde persoonsgegevens in te perken of af te schermen van andere gebruikers. Google lanceerde hiertoe 'Google Dashboard'. Op deze website kunnen gebruikers zien over welke informatie Google – en diensten die zoals YouTube tot Google behoren – beschikt met betrekking tot deze gebruiker. De gebruiker kan dan op elk moment deze informatie aanpassen. Hoewel dit een interessante eerste stap naar een ruimere privacybescherming genoemd kan worden, is het bezwaarlijk te beschouwen als een degelijk audit trail. De gebruiker krijgt immers enkel een overzicht van de informatie die hij zelf aan Google gegeven heeft. Er is geen log dat melding maakt van wie deze informatie kan inkijken en welke gegevenskoppelingen er plaatsvinden. Ook Facebook heeft stappen ondernomen om haar gebruikers meer zicht te bieden op de toegankelijkheid van hun persoonsgegevens. Gebruikers kunnen er dan voor zorgen dat bepaalde gegevens niet zichtbaar zijn voor bepaalde andere gebruikers. Hoewel deze veranderingen zeker een verbetering zijn voor de bescherming van de persoonsgegevens naar derden toe, is er echter maar weinig verbetering merkbaar in verband met de bescherming van de persoonsgegevens naar Facebook zelf toe. Een werkelijke transparantieverhoging is hier dus zeker nog niet geïmplementeerd.

2.4.2. WAT WORDT ER GELOGD?

[287] Deze documenten kunnen door de burger bewaard worden als een XML bestand. Belangrijk is dat de gemeente dit uittreksel minstens moet ondertekenen. De reden hiertoe is dat het Rijksregister zelf geen geldige uittreksels kan afleveren.

[288] Er wordt met betrekking tot deze toepassing voornamelijk kritiek geuit op het beperkte detail van de identificatie van de consulterende persoon of instantie en de vage beschrijving van de consultatie. Zoals we verder nog zullen zien, kan men door slechts een aantal eenvoudige ingrepen de transparantie van deze toepassing aanzienlijk verhogen.

[289] Een voorbeeld is de KISS databank van de VDAB waar sollicitanten hun curriculum vitae kunnen plaatsen en kunnen volgen door wie deze bekeken wordt.

INHOUD VAN HET AUDIT TRAIL - Nu we enig idee hebben van wat het Kadaster van Verbindingen zal moeten worden, kunnen we gaan onderzoeken wat de logs waar het Kadaster toegang toe zou bieden precies moeten gaan inhouden. We weten al dat zulke log een *ex post* overzicht moet bieden van wie de betrokken persoonsgegevens geconsulteerd heeft en van welke gegevens-koppelingen er plaatsvinden. Daarnaast zou er ook rekening gehouden moeten worden met de mogelijkheid van een *ex ante* register. Dit register zou de burger een eerste idee kunnen geven van de gegevenskoppelingen en de verwerkingen waar hij zich aan mag verwachten. De vraag is dan hoe men dit moet weergeven. Het spreekt voor zich dat men niet zonder meer allerlei data kan gaan loggen. Er zal een duidelijke selectie gemaakt moeten worden van data die relevant is voor het bereiken van het doel van het audit trail. Men zal ook rekening moeten houden met de wettelijke bepalingen met betrekking tot dit onderwerp. Als uitgangspunt kunnen we hier kijken naar onder meer de gegevens die opgenomen zijn in de historiek van consultatie in 'MijnDossier'. Belangrijk is dat de logs aan de burger een antwoord bieden op de vraag: Wie heeft met betrekking tot mijn persoonsgegevens wat gedaan, met welke reden en op welk moment? In het geval van een *ex ante* register blijft de vraag hetzelfde. Het zal dan nog steeds gaan om de vraag naar de identiteit van de verwerkende persoon of instantie, de mogelijke koppelingen en verwerkingen, en de doelstelling waaronder zulke koppelingen en verwerkingen zouden worden toegelaten.

BEPAALDE TRANSACTIES - Het gaat hier in de eerste plaats om het loggen van bepaalde transacties, zoals het consulteren of wijzigen van bepaalde gegevens. Gelet op het doel van audit trails in deze context – namelijk het verhogen van de transparantie van de verwerking van persoonsgegevens – lijkt het ons aangewezen om alleen, of toch minstens hoofdzakelijk, data te loggen over de gebeurtenissen in verband met de verwerking van persoonsgegevens. Dit kan beperkt blijven tot een vage omschrijving van de transactie, zoals in 'MijnDossier', maar het kan ook ruimer zijn. Men zou zelfs de hele inhoud van de transactie kunnen loggen, hoewel dit niet altijd wenselijk kan zijn. Wanneer men immers de precieze inhoud van de gegevenskoppeling in de log opneemt, loopt men immers het risico dat hier ook een disproportioneel aantal persoonsgegevens bij betrokken zijn. Het spreekt voor zich dat men zeer voorzichtig moet omspringen met het loggen van persoonsgegevens, iets waar we verder nog op zullen terugkomen. Uiteraard zal er hier toch wel enig detail vereist zijn. De transparantie naar de burger toe wordt immers maar weinig verhoogd indien hij alleen maar weet dat iemand zijn gegevens geconsulteerd heeft. Hij zal ook willen weten waarom die persoon zijn gegevens geconsulteerd heeft en of die consultatie wel rechtmatig was. Een degelijke omschrijving van de transactie is daarom onontbeerlijk in een audit trail. Het omschrijven van het precieze doel van de verwerking kan ook van belang zijn, maar zal echter niet in elke stap van de gegevensstroom geregistreerd moeten worden. Op dit laatste komen we later nog terug.

BEWIJSKRACHT VAN LOGS - De logs die men dankzij het audit trail kan bijhouden, geven dus een *ex post* overzicht van bepaalde gebeurtenissen met betrekking tot de persoonsgegevens van een betrokken burger. Indien deze burger door middel van de logs vaststelt dat er een onrechtmatige verwerking van zijn persoonsgegevens heeft plaatsgevonden, zal hij daar iets aan willen doen. De logs zullen dan moeten dienen als bewijs van die onrechtmatige verwerking. Om hiertoe bijkomende zekerheid te bieden en om latere discussie met betrekking tot de correctheid van deze gegevens uit te sluiten, kan men daarom de oorsprong, de integriteit en de non-repudiation van de in de logs opgenomen gegevens proberen aan te tonen. Deze gegevens mogen immers na het loggen niet gewijzigd of herroepen worden.

TIMESTAMP - Om de bewijskracht van de logs bijkomend te verzekeren, kan ook de precieze datum en het tijdstip van de gelogde gebeurtenis worden vastgesteld. Daarom kan men een zogenaamde *timestamp* toekennen aan de gelogde gebeurtenissen, om op die manier een bijkomende garantie te bieden dat die bepaalde gebeurtenis ook effectief op dat bepaalde tijdstip plaatsvond. Men zal daarom een vertrouwde derde partij (*trusted third party*) moeten aanduiden als *timestamping authority* (TSA) om deze logs te voorzien van een dergelijke *timestamp*.[290] Het vastleggen van het precieze tijdstip zal veelal in verschillende stadia verlopen. Zo zal het vaak niet alleen het tijdstip van verzending zijn dat van belang is, maar ook het tijdstip van ontvangst. Ook ontvangstberichten – alsook het verzenden en ontvangen ervan – zullen gelogd kunnen worden. Deze *timestamp* kan onder bepaalde voorwaarden ook de oorsprong, integriteit en non-repudiation van de gelogde gebeurtenis garanderen.[291]

IDENTIFICATIE VAN DE VERANTWOORDELIJKE AMBTENAAR - Uiteraard zal ook de verantwoordelijke ambtenaar geïdentificeerd moeten worden. Enige actie die de betrokkene wenst te ondernemen als gevolg van een onrechtmatige verwerking van zijn persoonsgegevens zal immers gericht zijn tegen de ambtenaar die deze onrechtmatige verwerking uitvoerde. Die persoon zal bijgevolg geïdentificeerd moeten worden. Wanneer men vervolgens de identiteitsgegevens van die persoon wil opnemen in een log, is men echter zelf persoonsgegevens aan het verwerken. Het audit trail – een instrument om de transparantie bij de verwerking van persoonsgegevens te verhogen – wordt aldus zelf een potentieel gevaar voor de privacybescherming. Gezien de gevoeligheid van dit probleem, zullen we er onder hoofdstuk 2.4.3 dieper op ingaan.

2.4.3. AFSCHERMEN VAN GEGEVENS

LOGGEN EN DE VERWERKING VAN PERSOONSGEGEVENS - Zoals we al aanhaalden, kunnen er problemen opduiken wanneer we de inhoud van een verwerking van persoonsgegevens of de precieze identiteitsgegevens van de verantwoordelijke ambtenaar willen opnemen in de logs. De inhoud van een verwerking kan immers persoonsgegevens bevatten en het spreekt voor zich dat ook de identiteit van de ambtenaar – zelfs al beperkt men zich tot het vaststellen van zijn naam – persoonsgegevens in de zin van de Privacywet en de Richtlijn omvat.[292] De activiteit van het loggen zelf kan immers beschouwd worden als een verwerking van persoonsgegevens en zal daarom ook de geldende regels in verband met de privacybescherming moeten volgen. Zo haalden we bijvoorbeeld al aan dat men van elke consultatie van het audit trail eveneens een log zal moeten bijhouden om latere controle op deze verwerking van persoonsgegevens mogelijk te maken. Men zal bij het loggen dus rekening moeten houden met onder meer de proportionaliteitsregel. Deze bepaalt dat men niet meer persoonsgegevens mag verwerken dan strikt noodzakelijk is voor het bereiken van het doel van de verwerking. Wanneer we de volledige inhoud van de transacties gaan loggen en indien die inhoud ook persoonsgegevens bevat, kan dit dus leiden tot

[290] Dit kan verlopen volgens de RFC3161 standaard, of de nieuwere ANSI ASC X9.95 standaard. Deze laatste standaard biedt meer zekerheid met betrekking tot de integriteit van de log. Zo wordt er gebruikt gemaakt van het RSA algoritme.

[291] De ANSI ASC X9.95 standaard is hiertoe geschikt.

[292] We herhalen nog dat we in dit onderzoek met 'Privacywet' bedoelen de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992, *B.S.* 18 maart 1993. Met 'Richtlijn' bedoelen we Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.* L van 23 november 1995, 31-50.

een disproportionele verwerking van persoonsgegevens. Dit zal men uiteraard moeten vermijden.

IDENTIFICATIE VAN DE VERANTWOORDELIJKE ORGANISATIE - Men kan er dan ook aan denken om zulke gegevens slechts in zeer beperkte mate op te nemen in de logs. We kunnen hier naar het voorbeeld van 'MijnDossier' kijken. De historiek van deze toepassing geeft slechts een beknopte beschrijving van de betrokken transactie weer. Hierdoor zou de burger al minstens op de hoogte gebracht kunnen worden van het doel van de transactie. De beschrijvingen die men in 'MijnDossier' aan de transactie kan geven, zijn echter steeds maar zeer abstract en geven de burger geen werkelijk inzicht in wat er gebeurd is en waarom. Ook de rechtmatigheid van de transactie is door zulke abstracte omschrijvingen onmogelijk te beoordelen. Hetzelfde probleem geldt voor de identificatie van de consulterende organisatie. De meeste organisaties worden slechts geïdentificeerd op het niveau van de overkoepelende organisatie. Een meer gedetailleerde identificatie per suborganisatie zou wenselijk zijn.[293] Deze toepassing toont dus aan dat men de transparantie van de verwerking wel gevoelig kan verhogen door in de logs een relatief beknopte omschrijving van het doel van deze verwerking alsook een meer algemene identificatie op niveau van de organisatie op te nemen. We zien echter ook dat die omschrijving en identificatie niet te vaag of algemeen mogen zijn.

OMSCHRIJVING VAN HET DOEL VAN DE VERWERKING - Wat betreft de omschrijving van het doel van de verwerking, kan men het voorbeeld van 'MijnDossier' volgen. Zo kan men vooraf een lijst opstellen van mogelijke transacties. De verantwoordelijke ambtenaar moet dan uit die lijst de voor de betrokken transactie meest toepasselijke omschrijving kiezen. Indien zulke lijst van mogelijke transacties met zorg opgesteld is, kan deze voor elke verwerking een vrij betrouwbare omschrijving van het doel van die verwerking geven. Het spreekt ook voor zich dat zulke lijst niet veralgemeend mag worden, maar dat iedere betrokken organisatie of suborganisatie een eigen lijst met de door die organisatie meest uitgevoerde transacties zal moeten opstellen. In zulke lijst kan men dan ook een overzicht bieden van gegevens die doorgaans opgevraagd worden bij de betrokken transacties, zonder hierbij in detail te treden. Op die manier kan men een degelijk overzicht bieden van welke gegevens er betrokken zijn bij een specifieke verwerking, alsook van wat het doel van die verwerking is. Dit zou voldoende moeten zijn om de transparantie van de verwerking naar de burger toe gevoelig te verhogen. Meer gedetailleerde informatie opnemen in zulke lijst zou kunnen leiden tot het opnemen van persoonsgegevens in de uiteindelijke logs, iets wat men allicht zal willen vermijden. Het is dan aan de beheerders van het audit trail om met alle betrokken organisaties te overleggen om zulke – op de noden van die organisatie afgestemde – lijst op te stellen.

NOOD AAN AFDOENDE SPECIFICATIE … - De identificatie van de verantwoordelijke ambtenaar is een moeilijker onderwerp. In de analyse van 'MijnDossier' zagen we dat identificatie op het niveau van de werkelijke overheidsdienst die verantwoordelijk is voor de verwerking al een idee kan geven van wie de betrokken transactie uitvoerde. Men moet er hier wel voor zorgen dat die organisatie voldoende gespecificeerd is. Identificatie op niveau van een overkoepelende organisatie kunnen we immers maar moeilijk als een voldoende identificatie beschouwen. Enige specifi-

[293] Zo worden alle onderdelen van de Kruispuntbank van de Sociale Zekerheid onder deze overkoepelende noemer geplaatst. Een aparte noemer voor bijvoorbeeld de Kruispuntbank van de Sociale Zekerheid zelf en voor suborganisaties zoals de Rijksdienst voor Sociale Zekerheid of de Rijksdienst voor Arbeidsvoorziening zou meer wenselijk zijn met het oog op het verhogen van de transparantie van de verwerking.

catie met betrekking tot de precieze suborganisatie of de precieze eenheid binnen de overkoepelende organisatie lijkt hier op zijn plaats. De vraag is dan of identificatie op niveau van de (sub)organisatie kan volstaan, of dat men werkelijk de specifieke ambtenaar die de verwerking uitvoerde, moet identificeren. Dit is uiteraard geen eenvoudige vraag. Wanneer de burger door middel van logs een onrechtmatige verwerking van zijn persoonsgegevens ontdekt, zal hij de persoon die verantwoordelijk gesteld kan worden voor die verwerking willen aanspreken. Indien dan enkel de betrokken organisatie geïdentificeerd wordt, zal het nog steeds niet duidelijk zijn wie nu precies die onrechtmatige verwerking uitvoerde. Daarom zou het voor zowel de burger als de betrokken organisatie interessanter zijn indien de verwerkende ambtenaar al geïdentificeerd wordt in de logs zelf. Men kan dan meteen de juiste persoon aanspreken en sanctioneren in het geval van een onrechtmatige verwerking. Dit zou natuurlijk de transparantie van de verwerking enkel maar ten goede komen.

… MAAR VERBOD OP OVERDREVEN SPECIFICATIE - Zoals we al aanhaalden, kan men de identificatie van de verwerkende ambtenaar echter niet bereiken zonder op enige manier zelf persoonsgegevens te verwerken in de logs. Dit is echter niet zonder gevolgen. We zagen dat het audit trail een hulpmiddel kan zijn om de transparantie van de verwerking van persoonsgegevens te verhogen. Men zou kunnen stellen dat het daarom een aanvulling vormt op het recht op toegang. Dit laatste is echter geen absoluut recht. De Richtlijn bepaalt immers dat het recht op toegang beperkt kan worden indien dat noodzakelijk is voor de vrijwaring van de bescherming van de rechten en vrijheden van anderen.[294] Het recht op toegang – en dus ook het audit trail dat een aanvulling kan vormen op dit recht – mag met andere woorden niet zo ver gaan dat het de privacybescherming van een andere zou schenden. Aangezien het loggen zelf in principe een verwerking van persoonsgegevens is, spreekt het overigens voor zich dat men de geldende principes uit deze regelgeving – zoals het finaliteitsprincipe, de proportionaliteitsregel en het transparantieprincipe – zal moeten naleven. Daarom zou men er in het licht van de privacybescherming aan kunnen denken om de identificatie van de individuele verwerkende ambtenaar in de logs achterwege te laten.

DE MENING VAN DE CBPL … - Deze zienswijze wordt gedeeld door de Commissie voor de bescherming van de persoonlijke levenssfeer. Zo is de Commissie van mening dat de mededeling van de identiteit van de verwerkende ambtenaar geen informatie kan geven over het doel en de rechtmatigheid van de verwerking en dat "*bijgevolg* […] *de mededeling van de naam van de ambtenaar, rekening houdend met deze doeleinden, als overmatig beschouwd* [moet] *worden in het licht van artikel 4, § 1, 3°, WVP*".[295] De Commissie meent daarom dat het volstaat om de organisatie die verantwoordelijk is voor de betrokken verwerking op te nemen in zulke logs. De Commissie meent ook dat dit "*de nauwkeurige vermelding van de dienst van de gemachtigde van waaruit de raadpleging is gebeurd en de contactpersoon tot wie men zich kan richten voor nadere informatie*" vereist.[296] Het is dan aan de organisatie die verantwoordelijk is voor de verwerking om voldoende controle uit te oefenen op haar werknemers, onder meer door te trach-

[294] Artikel 13, eerste lid, g) Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.* L van 23 november 1995, 31-50.

[295] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 12/2009 van 29 april 2009, *www.privacycommission.be,* 6-7.

[296] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 12/2009 van 29 april 2009, *www.privacycommission.be,* 7-8.

ten om misbruik van de aan die organisatie verleende machtigingen te voorkomen of door proactief op te treden wanneer een werknemer abnormaal veel verwerkingen zou uitvoeren.[297]

… VERSUS DE MENING VAN HET EHRM - Ook het Europees Hof van de Rechten van de Mens besloot in de zaak I v. Finland dat het bijhouden van logs met betrekking tot de consultaties van persoonsgegevens essentieel is voor de bescherming van de persoonlijke levenssfeer.[298] Volgens het Hof rust er op de overheid de positieve verplichting om er voor te zorgen dat de persoonlijke levenssfeer van haar onderdanen afdoende beschermd wordt en dat de overheid er dus voor moet zorgen dat zulke logs bijgehouden worden. Het Hof is echter wel van mening dat het loggen van de identiteit van de voor de verwerking verantwoordelijke organisatie niet voldoende is en dat de individuele verantwoordelijke ambtenaar minstens identificeerbaar moet zijn om een afdoende bescherming van de persoonlijke levenssfeer van de burger te garanderen.

ABSTRACTIE ALS GULDEN MIDDENWEG - De uitspraak van het Hof van de Rechten van de Mens kan gevolgd worden in de zin dat men ervoor zou kunnen zorgen dat de verwerkende ambtenaar niet direct geïdentificeerd wordt, maar dat hij in het geval van misbruik wel op enige manier identificeerbaar is. Het arrest specificeert immers niet of de betrokken burger zelf die identiteitsgegevens mag inkijken, of dat de beheerder van de logs hem toegang moet geven tot een versie waar deze identiteitsgegevens verborgen of weggelaten zijn. Zo zou men bijvoorbeeld de identiteit van die ambtenaar wel kunnen loggen, maar op zulke manier dat de burger er geen toegang toe heeft. De toegang tot die identiteit wordt dan voorbehouden aan de bevoegde autoriteiten of de dienst waar de ambtenaar werkzaam is. Men kan hier ook de zienswijze van de Commissie voor de bescherming van de persoonlijke levenssfeer volgen en de identificatie van de verwerkende ambtenaar laten gebeuren door de voor de verwerking verantwoordelijke organisatie. Door middel van interne controle, zowel *ex ante* als *ex post*, zou men dan in staat moeten zijn om de verwerkende ambtenaar te identificeren. De geabstraheerde logs lijken ons meer zekerheid te kunnen bieden. We concluderen hier daarom dat het in ieder geval aangewezen is om de verwerkende ambtenaar niet rechtstreeks te identificeren tegenover de burger. Men kan er echter wel aan denken om die identiteit te loggen om vervolgens de burger toegang te geven tot een geabstraheerde log waar de identiteit van de verwerkende ambtenaar verhuld wordt. Op die manier is de ambtenaar niet geïdentificeerd, maar wel identificeerbaar.

2.4.4. HET BEWAREN VAN LOGS

GEEN ONBEPERKTE BEWARING - Een andere belangrijke vraag is hoelang men deze logs moet bewaren. Het spreekt voor zich dat de burger voldoende tijd moet krijgen om de logs in te kijken. Anderzijds zal men die logs ook niet eeuwig willen bewaren. Juridisch gezien zou men daar bezwaren tegen kunnen uiten in het licht van de privacybescherming en technisch gezien zou dit enorme opslagmogelijkheden vereisen. Om te bepalen hoelang logs bewaard moeten worden, zullen we dus moeten kijken welke bewaartermijnen men kent onder de huidige stand van het recht en welke het meest toepasbaar is op de figuur van het audit trail.

[297] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 12/2009 van 29 april 2009, *www.privacycommission.be,* 8.
[298] EHRM, *I v. Finland*, 2008.

MOGELIJKE BEWAARTERMIJNEN - In het voorbeeld van 'MijnDossier' worden de gegevens uit de historiek gedurende zes maanden bewaard. De Commissie voor de bescherming van de persoonlijke levenssfeer gaf in een advies uit 1998 aan dat logs met betrekking tot de raadpleging van het Centraal Strafregister minimaal zes maanden bewaard moeten blijven en dat deze termijn verlengd zou moeten worden naar drie jaar.[299] In een ander advies in verband met gegevens uit het Rijksregister sprak de Commissie zelfs over een bewaartermijn van vijf jaar.[300] Daarnaast kunnen we de tienjarige verjaringstermijn voor persoonlijke rechtsvorderingen van artikel 2262bis van het Burgerlijk Wetboek aanhalen. We zagen immers dat de logs veelal gebruikt zullen worden om eventuele onrechtmatige verwerkingen van persoonsgegevens op te sporen. Zulke onrechtmatige verwerking kan dan aanleiding geven tot een persoonlijke rechtsvordering. We herhalen hier nog dat indien we naar de huidige privacywetgeving kijken, we zien dat de Privacywet aangeeft dat gegevens niet langer bewaard mogen worden dan strikt noodzakelijk is voor het bereiken van het doel van de verwerking. Dit houdt de betrokken partijen er toe gehouden zijn om de logs te verwijderen na het verstrijken van de bewaartermijn.

DE DATARETENTIERICHTLIJN - Naast al deze verschillende bewaartermijnen is er nog de problematiek van de Dataretentierichtlijn.[301] Hoewel we het in dit onderzoek bedoelde audit trail niet kunnen beschouwen als iets wat binnen de werkingssfeer van deze richtlijn valt, kan het wel interessant zijn om eens naar deze principes te kijken. Het is immers zeer opvallend dat er volgens deze richtlijn wel een aantal persoonsgegevens bewaard moeten worden.[302] Als bewaartermijn geeft deze richtlijn een minimum van zes maanden en een maximum van twee jaar aan.[303] Wat betreft de gegevensbescherming en het toezicht verwijst de richtlijn naar de principes van de Privacyrichtlijn.[304]

2262BIS BURGERLIJK WETBOEK - Wanneer we al deze bewaartermijnen naast elkaar leggen, zien we dat niemand een bewaartermijn korter dan zes maanden aanraadt. Wat de maximumduur betreft, zien we dat de Commissie voor de bescherming van de persoonlijke levenssfeer een termijn van drie tot vijf jaar aanbeveelt. Indien we de mogelijkheid van de burgerlijke rechtsvordering voor ogen houden, kunnen we echter niet anders dan de tienjarige bewaartermijn uit artikel 2262bis van het Burgerlijk Wetboek te respecteren.

2.4.5. CONCLUSIE

SAMENVATTING VAN HET ONDERZOEK NAAR DE INHOUD - Om de inhoud te bepalen van de logs waarin het Kadaster van Verbindingen de burger inzage wil geven, hebben we gekeken naar de meer algemene problematiek van het audit trail. Het Kadaster kan immers beschouwd worden als een specifiek portaal voor de inzage in het audit trail van gegevenskoppelingen door middel van het

[299] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 28/98 van 25 september 1998, *www.privacycommission.be.*
[300] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 26/2003 van 12 juni 2003, *www.privacycommission.be.*
[301] Richtlijn 2006/24/EG van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *Pb.* L 105 van 13 april 2006, 54-63.
[302] Zoals naam en adres, zie artikel 5 Richtlijn 2006/24/EG.
[303] Artikel 6 Richtlijn 2006/24/EG.
[304] Artikelen 7-9 Richtlijn 2006/24/EG.

Rijksregisternummer. We zagen al onmiddellijk dat het audit trail kan leiden tot een verhoging van de transparantie van de verwerking van persoonsgegevens naar de burger toe, maar dat deze figuur zelf ook tot een aantal problemen in verband met de privacybescherming kan leiden. Als we gaan kijken naar wat er gelogd moet worden in een audit trail, zien we immers dat we al snel op persoonsgegevens stoten. Het loggen is zelf ook al een verwerking van persoonsgegevens en zal daarom moeten voldoen aan de voorwaarden die vervat liggen in de Richtlijn. Het is daarom van kapitaal belang om zorgvuldig af te wegen welke gegevens er gelogd moeten worden en welke niet. Het uitgangspunt is dat het audit trail een antwoord biedt op de vraag: Wie heeft met betrekking tot mijn persoonsgegevens wat gedaan, met welke reden en op welk moment? Indien het audit trail hiertoe in staat is, kunnen we spreken van een verhoging van de transparantie van de verwerking indien de burger op gestructureerde wijze inzage geboden kan worden in de gegevens die het audit trail bevat. We kunnen ook aanraden dat de logs een degelijke *timestamp* meekrijgen om de logs met meer zekerheid aan derden tegenwerpbaar te maken. Minder vanzelfsprekend was het probleem van de identificatie van de verantwoordelijke voor de verwerking enerzijds en het omschrijven van het doel van de verwerking anderzijds. Wat het doel betreft zagen we dat men kan volstaan met een relatief bondige omschrijving. Deze mag niet te uitgebreid zijn, want dan zou zij ook persoonsgegevens bevatten. De omschrijving mag ook niet te vaag zijn, want dan mist zij het doel van de verhoging van de transparantie. Wat de identificatiegegevens betreft zagen we dat het niet wenselijk is dat de individuele verwerkende ambtenaar direct geïdentificeerd wordt tegenover de burger. Het kan volstaan om de voor de verwerking verantwoordelijke organisatie te identificeren. Men moet echter wel de juiste suborganisatie of de juiste eenheid binnen de overkoepelende organisatie identificeren. Wat betreft de verwerkende ambtenaar zelf zagen we dat deze wel identificeerbaar, maar niet geïdentificeerd zou moeten zijn. Tot slot kunnen we een wat de bewaartermijn betreft de redenering van de persoonlijke rechtsvordering volgen. Een tienjarige bewaartermijn zal dan aan de orde zijn.

2.5. CONCLUSIE

HET KADASTER IS NODIG - In het begin van dit onderzoek werd duidelijk dat het Kadaster van Verbindingen onder de huidige stand van het recht slechts een inhoudsloos begrip is. Daarom hebben we in dit hoofdstuk getracht om dit begrip af te bakenen en om er enige invulling aan te geven. We hebben allereerst onderzocht waarom een Kadaster van Verbindingen nodig zou zijn. Zo bleek dat de bestaande regels in het domein van de privacybescherming vaak niet in staat zijn om een effectieve transparantie van de verwerking van persoonsgegevens te garanderen. Er is daarom nood aan aanvullende regels of een aanvullend mechanisme om tot zulke effectieve transparantie te komen. Men zou dit kunnen bereiken door de burger op gestructureerde wijze inzage te verschaffen in logs waarin weergegeven wordt welke verwerkingen of gegevenskoppelingen er kunnen plaatsvinden – of hebben plaatsgevonden – met betrekking tot zijn persoonsgegevens. De Wet op het Rijksregister biedt ons de mogelijkheid om een portaal voor zulke inzage op te richten. Het is dan de bedoeling dat de inzage in de betrokken logs de burger op effectieve wijze een inzicht kunnen bieden in wat er met zijn persoonsgegevens gebeurt of kan gebeuren. Dit moet dan leiden tot een hogere transparantie bij de verwerking van persoonsgegevens.

TWEE MOGELIJKE BENADERINGEN - Hoewel het voorgaande ons al enig inzicht kan verschaffen in hoe het Kadaster er ongeveer zou moeten uitzien, moeten we het begrip zelf nog duidelijker afbakenen en invullen. Wat de begripsafbakening betreft stootten we op twee verschillende benaderingen. Volgens de *ex ante* benadering zou het Kadaster een overzicht bieden van wie er gemachtigd is om welbepaalde gegevens uit te wisselen met andere gemachtigde instanties. Dit overzicht wordt dan vastgesteld voor er enige verwerking heeft plaatsgevonden. De *ex post* benadering geeft op haar beurt een overzicht van de verwerkingen en gegevenskoppelingen die al hebben plaatsgevonden. We argumenteerden dat beide benaderingen op zich al kunnen bijdragen tot een verhoging van de transparantie van de verwerking van persoonsgegevens, maar dat het interessanter zou zijn om beide benaderingen – ondanks het feit dat zij schijnbare tegenpolen zijn – samen toe te passen. Op die manier zouden we komen tot een volwaardig overzicht dat een overzicht biedt van de gegevenskoppelingen die men kan verwachten alsook van de gegevenskoppelingen die al plaatsgevonden hebben. We concludeerden dat het Kadaster daarom best beide benaderingen combineert door toegang te bieden tot zowel een *ex ante* als een *ex post* register.

BELGISCH UNICUM - Vooraleer we het begrip hebben proberen in te vullen, werd er een kort onderzoek gevoerd naar hoe een aantal andere Europese landen deze problematiek aanpakken. Uit dit onderzoek bleek dat er geen ander land is dat een met het Belgisch Kadaster van Verbindingen vergelijkbare benadering nastreeft. Het loggen van gegevenskoppelingen zelf is uiteraard wel aanwezig in de meeste van de onderzochte landen. Zo zagen we dat Portugal zich voornamelijk richt op de *ex ante* benadering. Oostenrijk en het Verenigd Koninkrijk hielden er een sterke *ex post* benadering op na. Oostenrijk kende de verantwoordelijkheid voor deze logs toe aan de centrale privacyautoriteit. Het Verenigd Koninkrijk zal het register waar gegevenskoppelingen worden gelogd opnemen in het centrale personenregister. Een centraal portaal dat de burger inzage verschaft in de bestaande loggings, is echter afwezig in de onderzochte landen.

HET AUDIT TRAIL ALS MIDDEL TOT BEGRIPSVERRUIMING - Voor de precieze invulling van het begrip werd het onderzoek verbreed tot het probleem van het audit trail. Het Kadaster van Verbindingen kan immers worden opgevat als een portaal dat de burger op gestructureerde wijze inzage verschaft in het audit trail dat specifiek bedoeld is voor de context van de gegevenskoppelingen door middel van het Rijksregisternummer. We zagen dat het audit trail kan worden opgevat als een logboek dat vermeldt wanneer en waarom bepaalde gebeurtenissen of transacties plaatsvonden met betrekking tot de in een informatiesysteem bewaarde informatie. Door de burger toegang te geven tot deze logs, krijgt hij een werkelijk inzicht in wat er met zijn persoonsgegevens gebeurt. Het audit trail is daarom een instrument om de transparantie van de verwerking van persoonsgegevens aanzienlijk te verhogen. Het audit trail helpt daarom ook bij het naleven van de proportionaliteitsregel en kan helpen bij het opsporen van onrechtmatige gegevensverwerkingen. Wat Belgische praktijkvoorbeelden betreft werd er besloten voornamelijk de toepassing 'MijnDossier' te hanteren als leidraad voor de verdere ontwikkeling van het Kadaster van Verbindingen.

HET AUDIT TRAIL EN DE LOGGINGS - Wat de inhoud van het audit trail betreft, werd er allereerst onderzocht welke informatie er in de loggings opgenomen moet worden. Zo zagen we dat het belangrijk is dat de logs een antwoord bieden op de vraag: Wie heeft met betrekking tot mijn persoonsgegevens wat gedaan, met welke reden en op welk moment? Hiertoe moet men in de eerste plaats de transacties loggen die betrekking hebben op persoonsgegevens. De transacties zelf moeten kort omschreven worden. Belangrijker dan die omschrijving is dat de logs een duidelijke weergave geven van het doel van de gebeurtenis of de transactie. Daarnaast moeten deze logs kunnen dienen als rechtsgeldig bewijs in het geval van een onrechtmatige verwerking van persoonsgegevens. Het is daarom aanbevelingswaardig dat de logs de oorsprong, de integriteit en de non-repudiation van de in de logs opgenomen gegevens aantonen. Men kan hiertoe denken aan het gebruik van degelijke *timestamps*.

DE INHOUD VAN DE LOGGINGS - Hoewel het audit trail als onderdeel van het Kadaster van Verbindingen in de eerste plaats moet dienen als een instrument om de transparantie van de verwerking van persoonsgegevens te verhogen, zagen we dat het loggen zelf als een verwerking van persoonsgegevens kan worden beschouwd. Het is daarom belangrijk om ervoor te zorgen dat er niet buitensporig veel persoonsgegevens verwerkt worden bij het loggen zelf. Met betrekking tot de omschrijving van het doel van de verwerking, verwezen we naar het voorbeeld van 'MijnDossier'. Een vooraf bepaalde lijst met doeleinden waaruit de verantwoordelijke ambtenaar de op die bepaalde verwerking meest toepasbare optie aanduidt, lijkt ons het meest aangewezen. Zulke lijst moet echter wel met voldoende zorg opgesteld worden en moet overeenstemmen met de noden van de instantie die verantwoordelijk is voor de verwerking. Men zal dus voor elke betrokken instantie een aparte lijst moeten opstellen, wat uiteraard wel enige organisatie zal vereisen. Wat de identificatie betreft van de instantie die verantwoordelijk is voor de verwerking volgen we het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. De rechtstreekse identificatie van de verantwoordelijke ambtenaar tegenover de burger moet hier als overmatig worden beschouwd. Het kan daarom volstaan om de verantwoordelijke voor de verwerking op het niveau van de organisatie te identificeren. Belangrijk is wel dat hier de juiste suborganisatie of de juiste eenheid binnen een overkoepelende organisatie aangeduid wordt. Men kan bijvoorbeeld wel de identiteit van de verantwoordelijke ambtenaar loggen om vervolgens de burger toegang te geven tot geabstraheerde logs. Op deze manier is de ambtenaar niet direct geïdentificeerd tegenover de burger, maar wel identificeerbaar. Wat het bewaren van logs betreft zagen we dat er een grote verscheidenheid aan bewaartermijnen bestaat. Indien we de adviezen van de Commissie voor de bescherming van de persoonlijke levenssfeer volgen, komen we op een bewaartermijn van drie tot vijf jaar. We haalden echter aan dat we hier ook de verjaringstermijn voor persoonlijke rechtsvorderingen uit artikel 2262bis van het Burgerlijk Wetboek kunnen volgen. Indien een log gebruikt kan worden als bewijs bij zulke persoonlijke rechtsvordering, spreekt het voor zich dat de logs bewaard moeten worden tot wanneer zulke vordering verjaart. Een bewaringstermijn van tien jaar lijkt dan aangewezen.

HET KADASTER AFGEBAKEND EN INHOUDELIJK INGEVULD - We hebben nu het begrip 'Kadaster van Verbindingen' proberen af te bakenen en er – door ons te richten op de algemene problematiek van het audit trail – enige inhoud aan trachten te geven. Hoewel deze begripsafbakening en inhoudelijke invulling ons al een goed beeld kunnen geven van wat het Kadaster in de praktijk zal moeten voorstellen, rijzen er toch nog een aantal vragen bij de praktische implementatie van dit alles. We zullen daarom verder onderzoeken hoe het Kadaster van Verbindingen er in de praktijk zal uitzien. In dit praktijkonderzoek zullen we een aantal juridische, organisatorische en technische vragen met betrekking tot de realisatie van het Kadaster van Verbindingen van naderbij bekijken.

3. PRAKTIJKONDERZOEK

NA HET BEGRIPSMATIG EN INHOUDELIJK ONDERZOEK … - Onder hoofdstuk 2 hebben we allereerst getracht het begrip 'Kadaster van Verbindingen' enigszins af te bakenen. We onderzochten waarom zulk kadaster nodig zou zijn om de transparantie van de verwerking van persoonsgegevens naar de betrokkene toe te verhogen. Vervolgens hebben we het begrip trachten te definiëren en werd er een rechtsvergelijkend onderzoek gevoerd. Tot slot werd er gezocht naar wat de concrete invulling van het Kadaster van Verbindingen zou moeten worden. We hebben ons in dat onderzoek gericht op de problematiek van het audit trail, om een ruimer beeld te kunnen vormen van wat de mogelijkheden voor deze materie zijn. Men zou het Kadaster immers kunnen opvatten als portaal dat de burger inzage verschaft tot een audit trail in de specifieke context van de gegevenskoppelingen door middel van het Rijksregisternummer. Deze begripsverruiming heeft ons geleid tot gelijkaardige initiatieven zoals de toepassing 'MijnDossier'. Aangezien er veel te leren valt uit zulke praktijkvoorbeelden, zullen we deze begripsverruiming aanhouden.

… HET JURIDISCH EN ORGANISATORISCH ONDERZOEK - Hier zal er allereerst een onderzoek gevoerd worden naar hoe men het Kadaster van Verbindingen in de praktijk zou moeten realiseren. Het spreekt voor zich dat er zich een aantal juridische, technische en organisatorische vragen opstapelen. We zullen daarom onder dit hoofdstuk trachten om een juridisch, organisatorisch en technisch kader te schetsen voor de realisering van het Kadaster van Verbindingen.

3.1. (DE)CENTRALISATIE

DE GECENTRALISEERDE BENADERING - Allereerst moeten we ons afvragen op welk niveau een audit trail binnen de overheidscontext moet bijgehouden worden. Zo zou men kunnen denken aan een centraal logboek waar alle verschillende overheidsdiensten melding kunnen maken van de verwerkingen van persoonsgegevens en de gegevenskoppelingen die zij uitvoeren. Op die manier zouden al de persoonsgegevens die de overheid met betrekking tot de persoon van de burger bewaart, alsook van wat er met al die persoonsgegevens gebeurt op een enkele plaats bewaard worden.

DE GEDECENTRALISEERDE BENADERING - In de plaats van een gecentraliseerde databank waar de logs van alle overheidsdiensten op eenzelfde plaats opgeslagen worden, kan men ook denken aan een gedecentraliseerd systeem. Er zouden dan aparte audit trails – waar ook hier ruimte kan zijn voor zowel de *ex post* als de *ex ante* benadering – bijgehouden worden door elke overheidsdienst. Deze methode kan een aantal voordelen bieden ten opzichte van het gebruik van een gecentraliseerde opslag. Zo kunnen we in de eerste plaats denken aan de schaalproblemen die men zou ervaren bij het opzetten van een centrale gegevensopslag. De kleinere schaal die men bereikt met het opzetten van een apart audit trail voor iedere overheidsdienst kan allicht een aantal organisatorische en technische problemen vermijden. Ook juridisch gezien kan het audit trail op kleinere schaal voordelen bieden, gelet op de vele vragen die men zich kan stellen bij het oprichten van de gecentraliseerde gegevensbank die de gecentraliseerde gegevensopslag onvermijdelijk met zich meebrengt.

PRAKTIJKVOORBEELDEN IN NEDERLAND - In dit deel van het onderzoek willen we daarom bepalen welke van beide benaderingen aanbeveling verdient voor de Belgische situatie. We zullen hiertoe eerst zoeken naar bestaande praktijkvoorbeelden, zowel nationaal als internationaal. Op internationaal vlak kunnen we het Nederlandse voorstel van de 'digitale kluis' als belangrijkste voorbeeld aanhalen. Het gaat hier om een project waarbij alle persoonsgegevens van de burger cryptografisch beveiligd opgeslagen zouden worden in een digitale kluis. Het zou hier gaan om zowel de persoonsgegevens waarover de overheid al beschikte als informatie die de burger zelf aan-brengt, zoals medische dossiers en dergelijke. Door al die gegevens op één plaats samen te brengen, zou de burger op eenvoudige wijze kunnen aangeven welke gegevens hij met welke personen of instanties zou willen delen, dit uiteraard zonder afbreuk te doen aan wettelijke verplichtingen tot het meedelen van bepaalde gegevens. De voornaamste kritiek op dit voorstel ging uit naar het probleem van de beveiliging van zulke centrale gegevensbank en de last die het beheer van zulke 'kluis' met zich zou meebrengen voor de burger. Het voorstel is daarom nooit effectief ingevoerd. Er bestaan echter wel een aantal particuliere initiatieven die het basisidee van dit voorstel behouden, zoals Lockertje.nl of de digitale kluis die de ABN-AMRO bank aanbiedt als deel van haar dienst voor internetbankieren. Sinds 2008 loopt echter wel het project 'MijnOverheid.nl', een centraal platform voor verschillende overheidsdiensten en gemeenten. Ook hier kan de burger toegang krijgen tot de persoonsgegevens waarover de aangesloten diensten en gemeenten met betrekking tot zijn persoon beschikken. Door het relatief beperkte aantal aangesloten gemeenten en het zeer lage gebruikersaantal in die gemeenten, kunnen we deze dienst op dit moment nog geen succes noemen.[305] Wantrouwen tegenover de gebruikte methode van authenticatie en het centraal overheidsportaal zijn hier de belangrijkste redenen toe. In tegenstelling tot de digitale kluis kan 'MijnOverheid.nl' niet onmiddellijk beschouwd worden als een voorbeeld van een gecentraliseerde gegevensopslag, maar het is wel een illustratie van het wantrouwen dat men kan ondervinden indien men een te gecentraliseerd beheer van gegevens nastreeft. De afkeer van de burger tegen eerdere projecten als de digitale kluis blijft immers duidelijk nazinderen.

PRAKTIJKVOORBEELDEN IN BELGIË - In België bestaat er op dit moment geen gecentraliseerde databank die logs bevat met betrekking tot de gegevenskoppelingen op basis van zijn Rijksregisternummer. De bestaande voorbeelden – zoals 'MijnDossier' voor het Rijksregister of MyMinfin voor de FOD Financiën – zijn allen gedecentraliseerde toepassingen die toegang geven tot informatie die binnen een bepaalde overheidsdienst worden bijgehouden. Bij de Federale Overheidsdienst voor Informatie- en Communicatietechnologie (Fedict) loopt er momenteel een voorstudie naar het concept van de digitale kluis.

PROBLEMEN VAN CENTRALISATIE - ORGANISATORISCH - Het samenbrengen van alle persoonsgegevens van de burger op een centrale plaats is uiteraard geen sinecure. Organisatorisch gezien zal men een databank moeten oprichten waar alle verschillende overheidsdiensten de gegevens waarover zij al beschikken kunnen samenbrengen. Technisch gezien zal men uiteraard aandacht moeten besteden aan de beveiliging van het systeem. Men zal zulke centrale gegevensbank moeten kunnen beschermen tegen aanvallen van buitenaf. Daarnaast zal men ook rekening moeten houden met ongeoorloofde handelingen van binnenuit. Men zal er immers voor moeten zorgen dat de verschillende overheidsdiensten enkel de informatie te zien krijgen die zij gemachtigd zijn te zien. Zoals al aangehaald zullen kleinschaligere projecten – audit trails op het niveau van de verschillende overheidsdiensten – daarom een grotere haalbaarheid tonen op technisch en organisatorisch vlak.

PROBLEMEN VAN CENTRALISATIE - JURIDISCH - Ook op juridisch vlak brengt een gecentraliseerde gegevensopslag de nodige problemen met zich mee. Door een gecentraliseerde aanpak zouden immers alle logs uit de overheidssector samengebracht worden in één enkele gegevensbank. Het spreekt voor zich dat dit op gespannen voet leeft met de privacywetgeving. Zo kan men zich onder meer afvragen of zulke centrale gegevensopslag nog te verenigen valt met het doel van het

[305] E.-J. HAMEL, "MijnOverheid.nl bereikt doelgroep niet", 7 juli 2009, *webwereld.nl*.

Kadaster, namelijk het verhogen van de transparantie van de verwerking. Door het hele proces van het loggen meer gecompliceerd te maken door informatie op een centrale plaats te bewaren, lijkt het al niet meer zo vanzelfsprekend dat zulke centrale databank nog zou bijdragen tot het verhogen van de transparantie van de verwerking.[306] Daarnaast zagen we al dat het loggen op zich ook een verwerking van persoonsgegevens uitmaakt en dat men bijgevolg ervoor zal moeten zorgen dat het loggen in regel verloopt met de privacywetgeving. Indien we dan besluiten dat een centrale databank allicht meer informatie zal bevatten dan wat strikt noodzakelijk is voor het bereiken van het doel van het Kadaster van Verbindingen – namelijk het verhogen van de transparantie van die verwerking – dan kunnen we niet anders dan besluiten dat de gecentraliseerde gegevensopslag niet beantwoordt aan de proportionaliteitsregel.[307] Een gecentraliseerde opslag van deze informatie mag dus alleen een optie zijn indien de gedecentraliseerde opslag – met doorgifte zonder opslag op centraal vlak – niet op redelijke wijze haalbaar is.

VOORDELEN VAN DECENTRALISATIE - Uit het voorgaande kunnen we afleiden dat gedecentraliseerde loggings per overheidsdienst een meer interessante werkwijze vormen dan een gecentraliseerde gegevensopslag. Een gedecentraliseerd systeem zal immers gemakkelijker te organiseren zijn en zal ook minder gevoelig liggen bij de burger omdat het op minder gespannen voet zal staan met de bestaande privacywetgeving. Ook voor de betrokken overheidsdiensten zelf zal het wellicht interessanter zijn om een eigen audit trail op te kunnen richten in plaats van deze bevoegdheid te moeten delegeren aan een centrale instantie.[308] Het gevolg van de gedecentraliseerde aanpak is immers dat iedere overheidsdienst verantwoordelijk is voor het bijhouden van de eigen gegevens die noodzakelijk zijn voor het reconstrueren van de gegevensstroom die heeft plaatsgevonden. Iedereen is met andere woorden verantwoordelijk voor zijn eigen aandeel in de keten en zal op deze manier dan ook beschikken over de nodige bewijsstukken in het geval van een controle op de door die dienst uitgevoerde gegevensverwerkingen en –koppelingen. Voor de burger kan er daarnaast nog steeds ruimte zijn voor een centraal platform waar hij de informatie uit deze decentraal opgeslagen logs kan consulteren. Het Kadaster wordt dan nog steeds een centraal platform voor de consultatie van het 'end-to-end' audit trail, maar zal in dit geval niet hoeven te steunen op een gecentraliseerde databank.

DE KEUZE VOOR DECENTRALISATIE - We kunnen daarom concluderen dat een gedecentraliseerde gegevensopslag te verkiezen valt boven het gebruik van een enkele centrale databank. Door een gedecentraliseerde aanpak houden de verschillende overheidsdiensten de verantwoordelijkheid voor hun eigen audit trail. Er zal dan echter wel voldoende aandacht geschonken moeten worden aan de interoperabiliteit van de verschillende audit trails die de verschillende diensten en administraties hanteren en de effectieve wisselwerking tussen deze diensten. Zulke interoperabiliteit en wisselwerking zijn immers nodig om de burger de mogelijkheid te bieden om het volledige 'end-to-end' audit trail te reconstrueren. Hiertoe kan men dan gebruik maken van een centrale gebruikerstoepassing – wat het Kadaster van Verbindingen zal worden – waar de relevante gegevens uit de logs van de betrokken overheidsdiensten samengebracht worden om de burger een overzicht te geven van het gehele gegevensspoor. We zullen daarom verder onder-

[306] Het centraal bewaren van al deze informatie gaat trouwens rechtstreeks in tegen een aantal kernpunten van het Belgisch beleid, zie de analyse van het Belgisch beleid onder deel I van dit project.
[307] Art. 6, lid 1, c) van de Richtlijn en art. 4, §1, 3° van de Privacywet.
[308] Dit wordt door onder meer W3C en een studie van Eurécom omschreven als choreografie. A. SVIRKAS, et. al., 'Compliance Proofs for Collaborative Interactions using Aspect-Oriented Approach', 2007, www.eurecom.fr, 1; W3C, 'Web Services Choreography Description Language Version 1.0', 2005, *www.w3.org/TR/ws-cdl-10*.

zoek voeren naar hoe zulk gedecentraliseerd systeem voor het gebruik van audit trails in de overheidscontext verder uitgewerkt zal moeten worden.

3.2. DE BETROKKEN ACTOREN

NOOD AAN SAMENWERKING TUSSEN … - Het spreekt voor zich dat het voor het reconstrueren van het volledige 'end-to-end' audit trail noodzakelijk is dat er een zekere vorm van samenwerking of minstens een akkoord bestaat tussen de verschillende betrokken actoren. We zagen al dat het volledige audit trail maar gereconstrueerd kan worden indien de logs die de verschillende overheidsdiensten bijhouden enigszins samenhangen en onderling compatibel zijn. We zullen later nog bepalen hoe zulke samenwerking zou moeten verlopen. Hier zullen we eerst trachten de betrokken actoren te identificeren en een beeld te vormen van hun taak in het geheel.

… DE BETROKKEN ACTOREN - Algemeen genomen kunnen we een onderscheid maken tussen de back office actoren en de front office actoren. De burger zal zijn vraag voor informatie met betrekking tot de verwerking en de koppelingen van zijn persoonsgegevens in de eerste plaats richten aan de front office actoren. Deze zullen die vraag doorgeven aan de back office actoren. Het zijn immers de back office actoren die de gevraagde informatie beheren en zij kunnen hier bijgevolg aangeduid worden als het bronsysteem. Wanneer de front office actoren al de benodigde informatie verzameld en verwerkt hebben, geven zij deze door aan de burger die de aanvraag indiende. De front office actoren zijn met andere woorden de doelsystemen die verantwoordelijke zijn voor het verlenen van een degelijk 'end-to-end' audit trail. In het gedecentraliseerde systeem dat we eerder voorstelden, kunnen we dus de verschillende overheidsdiensten die een eigen audit trail bijhouden in de regel aanduiden als back office actoren. Een derde groep actoren die we kunnen aanduiden, zijn de tussenpersonen. Deze slaan een brug tussen de front office actoren en de back office actoren. Zij kunnen de verschillende actoren tegenover elkaar identificeren en authentiseren, zij brengen de verschillende schakels in de informatieketen met elkaar in contact, en dergelijke.

3.2.1. FRONT OFFICE ACTOREN

DOELSYSTEMEN - Zoals we al aangaven kunnen we de front office actoren in deze materie aanduiden als de doelsystemen. Zij zijn immers de actoren die in eerste instantie in contact zullen komen met de burger – of met een rechtspersoon – om een aanvraag tot het consulteren van het audit trail te ontvangen en te verwerken. Het zijn dan ook deze actoren die de aanvraag doorgeven aan de back office actoren die over de opgevraagde informatie beschikken om die informatie vervolgens weer te ontvangen, te verwerken en te presenteren aan de aanvrager. Net omdat het de front office actoren zijn die in contact komen met de aanvrager, zullen zij ook de partij zijn die perfect op de hoogte is van het precieze doel van de aanvraag tot het consulteren van het audit trail. We herhalen hier dat het consulteren van een audit trail immers zelf een verwerking van persoonsgegevens inhoudt. Zulke consultatie zal bijgevolg ook moeten voldoen aan de principes uit de privacywetgeving. We denken hier dan weer aan onder meer het finaliteitsprincipe, de proportionaliteitsregel en het transparantieprincipe. De verwerking zal dan ook aangegeven moeten worden bij de toezichthoudende autoriteit.

BELANGRIJKE VERANTWOORDELIJKHEID VOOR HET GEHEEL - Hoewel we zagen dat in een gedecentraliseerd systeem in principe iedere partij verantwoordelijk is voor de verwerkingen van persoonsgegevens die zij zelf uitvoeren, moeten we hier bij opmerken dat het de front office actoren zullen zijn die de bijkomende verantwoordelijkheid dragen voor de invulling van de principes van finaliteit en proportionaliteit. Ook eventuele regelingen met betrekking tot de bewaartermijn en de eventuele verdere doorgifte van de hier verstrekte informatie zal onder de bevoegdheid van de front office actoren vallen. We wensen wel nog te benadrukken dat deze bijkomende verantwoordelijkheid van de doelsystemen echter geen afbreuk doet aan de algemene verplichtingen die rusten op elke betrokken partij als verantwoordelijke voor de eigen verwerking van persoonsgegevens. Zo zal iedere betrokken partij zelf de verantwoordelijkheid dragen voor het indienen van een machtigingsaanvraag bij het bevoegde sectoraal comité indien de verwerking die zij wensen uit te voeren zulke machtiging vereist.

3.2.2. BACK OFFICE ACTOREN

BRONSYSTEMEN - Hoewel de front office actoren dus naast hun gewone verantwoordelijkheden ook nog een bijkomende verantwoordelijkheid dragen met betrekking tot de werking van het Kadaster, beschikken zij zelf niet over de benodigde informatie. Die informatie wordt in een systeem van gedecentraliseerde gegevensopslag immers bijgehouden door de back office actoren, die we daarom kunnen aanduiden als de bronsystemen. We kunnen dus stellen dat het hier gaat om authentieke bronnen, een figuur die we onder deel I van dit project al bespraken. Deze back office actoren dragen in ieder geval wel de verantwoordelijkheid voor de eigen verwerkingen en koppelingen van persoonsgegevens. Zij zullen er dus voor moeten zorgen dat de privacywetgeving nageleefd wordt bij de eigen verwerkingen en zullen binnen hun dienst immers een audit trail bijhouden van de verwerkingen en koppelingen van persoonsgegevens die plaatsvonden met betrekking tot de gegevens waarover hun dienst beschikt.

AUTHENTIEKE BRONNEN - We zagen al dat het principe van de eenmalige gegevensinzameling bepaalt dat een overheidsdienst de burger niet om gegevens mag vragen die hij al eens meegedeeld heeft aan de overheid. De betrokken overheidsdienst zal deze gegevens dan moeten halen bij de organisatie die wel over die gegevens beschikt. In het kader van de realisatie van e-Government in België heeft men het principe van de eenmalige gegevensinzameling bevestigd door te verklaren dat bepaalde informatie enkel bij authentieke bronnen kan worden verkregen. Deze authentieke bronnen bevatten dan informatie die de overheid met betrekking tot haar onderdanen ingezameld heeft en waarvan de juistheid, de volledigheid en de actualiteit vaststaat. De overheidsdienst die de gegevens waarover een authentieke bron beschikt wil raadplegen, zal dan moeten worden geauthentiseerd en zal een wettige reden moeten aantonen, alsook dat er voldaan wordt aan onder meer het finaliteitsprincipe van deze verwerking van persoonsgegevens.

CONSULTATIE IS OOK VERWERKING VAN PERSOONSGEGEVENS - Hoewel men dit laatste kan begrijpen vanuit het standpunt van de bescherming van deze gegevens in het kader van de privacybescherming en de verwerking van persoonsgegevens, moeten we toch concluderen dat dit kan leiden tot een moeilijke situatie. Het doelsysteem zal volgens deze redenering immers niet zonder meer informatie kunnen opvragen bij de bronsystemen, maar zal allerlei gegevens – waaronder allicht persoonsgegevens – moeten meedelen met die bronsystemen vooraleer de opgevraagde gegevens te verkrijgen. Het audit trail – op zich al een verwerking van persoonsgegevens – geeft op deze manier aanleiding tot nog een verdere verwerking van persoonsgegevens. Het spreekt voor zich dat we zulke situatie onmogelijk als wenselijk kunnen beschouwen. Met de bespreking van het Belgisch beleid onder deel I van dit project in gedachten, komen we dan tot de figuur van de dienstenintegrator – de kruispuntbanken – die kan dienen als een neutrale tussenpersoon tussen de doelsystemen en de bronsystemen. We zullen de mogelijkheid van een tussenpersoon in deze transactie daarom verder onderzoeken.

NOOD AAN VOLDOENDE IDENTIFICATIE EN AUTHENTICATIE - We concluderen daarom dat de back office actoren als bronsystemen beschouwd moeten worden als authentieke bronnen. Zij beheren de informatie die de audit trails ons kunnen verschaffen en kunnen de juistheid, volledigheid en actualiteit van die informatie garanderen. De rol van de bronsystemen in het audit trail bestaat er bijgevolg in om de opgevraagde gegevens door te geven aan de doelsystemen voor verdere verwerking en mededeling aan de aanvrager van de consultatie. De doelsystemen zullen echter op afdoende wijze geauthentiseerd moeten worden vooraleer ze toegang krijgen tot de informatie waarover de bronsystemen beschikken. Zij zullen ook informatie moeten verlenen met betrekking tot de precieze reden en het doel van hun aanvraag. Omdat dit laatste echter op gespannen voet staat met de geldende privacywetgeving, lijkt het hier aangewezen om te onderzoeken of er hier geen neutrale tussenpersoon bij te pas kan komen.

3.2.3. TUSSENPERSONEN

DE NEUTRALE DERDE - Hoewel men zou kunnen denken dat het gedecentraliseerd systeem perfect zou kunnen werken door de loutere samenwerking tussen de front office en back office actoren, zagen we net dat zulke samenwerking toch op een aantal beperkingen stoot. Het is daarom geen slecht idee om te onderzoeken of er niet de mogelijkheid bestaat om een neutrale tussenpersoon tussen de bron- en doelsystemen te plaatsen. Deze tussenpersoon dient dan als doorgeefluik van informatie tussen beide actoren. Daarnaast kan de tussenpersoon ook de bron- en doelsystemen tegenover elkaar authentiseren, zorgen dat de overdracht van de betrokken gegevens voldoende beveiligd wordt en garanties vragen voor de eerlijke en rechtmatige verwerking van de betrokken persoonsgegevens. Dit laatste kunnen zij doen door onder meer te controleren of wel enkel de voor die verwerking strikt noodzakelijke gegevens uitgewisseld worden. Het belangrijkste uitgangspunt hier is dat de tussenpersoon slechts mag dienen als doorgeefluik en dat deze bijgevolg zelf geen informatie bewaart.

HET NUT VAN DE TUSSENPERSOON - Hoewel uit het voorgaande blijkt dat de tussenpersoon zeker een interessante toevoeging kan zijn voor het hier voorgestelde systeem, kan men argumenteren dat een extra betrokkene in de keten deze infrastructuur onnodig zou kunnen belasten. We moeten daarom eerst onderzoeken of de toevoeging van de tussenpersoon in de infrastructuur werkelijk nodig is om de goede werking van het audit trail te garanderen en om zo tot effectieve transparantie te komen. Zo zou de tussenpersoon allereerst kunnen zorgen voor de interne cohesie van de infrastructuur. We zagen immers al dat het in kaart brengen van het gehele gegevensspoor kan leiden tot een complexe structuur. Het is dan uiteraard belangrijk dat er een partij aangewezen wordt als algemene coördinator van de gegevensstroom tussen de front office en back office actoren. De tussenpersoon kan een dergelijke rol waarnemen. Daarnaast kan de tussenpersoon er ook voor zorgen dat enkel de noodzakelijk gegevens worden doorgegeven van de back office actoren naar de front office actoren. De back office actoren bewaren hun gegevens immers op een gestandaardiseerde wijze. Zij maken geen onderscheid voor wat betreft de gegevens die nodig zijn voor een specifieke verwerking. Het is dan de taak van de tussenpersoon om ervoor te zorgen dat de front office actoren enkel de specifieke gegevens verkrijgen die zij in die bepaalde situatie nodig hebben. Hoewel het kan lijken dat de toevoeging van een tussenpersoon de hier voorgestelde structuur onnodig zou belasten, blijkt dat de tussenpersoon net voor vereenvoudiging kan zorgen. Zo kan de tussenpersoon optreden als coördinator en kan hij ervoor zorgen dat enkel de strikt noodzakelijke gegevens doorgegeven worden van de back office actoren naar de front office actoren. De aanwezigheid van de tussenpersoon in een dergelijke structuur kan dus zeker verdedigd worden.

DUALE VERANTWOORDELIJKHEID - De tussenpersoon verkrijgt dus een tweeledige verantwoordelijkheid. Tegenover de bronsystemen zal hij ertoe gehouden zijn om in te staan voor een degelijke authenticatie van de doelsystemen en voor het beveiligen van de gegevensoverdracht. Hiertoe zullen de nodige afspraken tussen beide actoren gemaakt moeten worden. Ook zullen er garanties gegeven moeten worden dat de tussenpersoon zelf geen inhoudelijke gegevens zal bewaren. Tegenover de doelsystemen zal hij er dan toe gehouden zijn om te garanderen dat de geleverde gegevens afkomstig zijn van de juiste gevalideerde authentieke bron. De vraag is dan welke figuur het meest geschikt is om de taak van zulke neutrale tussenpersoon op zich te nemen. We kunnen hier denken aan de figuur van de vertrouwde derde partij.[309] Deze figuur is in de rechtsleer al vaker besproken. Zo stelde het Observatorium van de Rechten op het Internet al in 2004 voor om een juridisch statuut te voorzien voor deze figuur.[310] Uiteindelijk hebben deze en andere aanbevelingen geleid tot de wet op de verleners van vertrouwensdiensten.[311] Deze wet regelt een aantal basisregels – zoals de neutraliteit en vertrouwelijkheidsplicht – voor zulke dienstverleners. Hoewel de wet zeker niet alomvattend is – veel zaken zullen immers nog voor iedere dienstverlening *ad hoc* moeten ingevuld worden – kunnen we dit toch al beschouwen als een goede juridische erkenning van de figuur van de vertrouwde derde partij. De wet zelf is intussen in werking getreden, maar de tijd die voorzien was voor het aannemen van uitvoeringsbesluiten is intussen ruim verstreken. De wet op de verleners van vertrouwensdiensten blijft daarom grotendeels zonder gevolg.

DIENSTENINTEGRATOREN ALS TUSSENPERSONEN - Binnen de overheidscontext kunnen we voornamelijk denken aan de dienstenintegratoren als tussenpersonen. Hoewel dit niet expliciet in de wet op de verleners van vertrouwensdiensten is opgenomen, kunnen we deze dienstenintegratoren toch beschouwen als een vertrouwde derde partij. Bij gebrek aan een werkelijke vertrouwde derde partij in de overheidscontext is het immers geen verrassing dat men zich hiertoe tot de dienstenintegratoren richt. Bij de bespreking van de dienstenintegratoren onder deel I van dit project zagen we immers dat zij in principe zelf geen inhoudelijke gegevens bewaren, maar enkel instaan voor een vlotte en correcte uitwisseling van gegevens tussen verschillende diensten. Het zijn net die eigenschappen die ervoor zorgen dat de dienstenintegratoren de ideale tussenpersoon zouden zijn bij het verwerken van aanvragen tot consultatie van audit trails. We mogen ook niet vergeten dat dienstenintegratoren – als deel van de overheid – onderworpen zijn aan een aantal wettelijke bepalingen zoals de beginselen van behoorlijk bestuur en de openbaarheid van bestuur. Principes zoals het gelijkheidsbeginsel, het redelijkheidsbeginsel en het rechtsze-

[309] In het jargon van de cryptografie spreekt men veelal van '*trusted third party*' (TTP).

[310] OBSERVATORIUM VAN DE RECHTEN OP HET INTERNET, 'Advies nr. 3 betreffende denkpistes om het vertrouwen in de elektronische handel te versterken', 2004, *www.internet-observatory.be*, 23-26.

[311] Wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten, *B.S.* 17 juli 2007, 38587-38591.

kerheidsbeginsel zullen dus gerespecteerd moeten worden bij het uitvoeren van de taak als tussenpersoon.

De tussenpersoon als noodzaak voor het audit trail - We concluderen hier daarom dat neutrale tussenpersonen een noodzaak zijn voor de goede werking van een gedecentraliseerd systeem voor audit trails. Gelet op hun taak binnen de overheid en de figuur van de vertrouwde derde partij kunnen we dienstenintegratoren aanduiden als de perfecte kandidaat voor de positie van tussenpersoon in zulk gedecentraliseerd systeem. We zien echter wel dat er tussen de betrokken partijen de nodige afspraken gemaakt moeten worden voor de vlotte werking van het systeem. Ook zullen de front office en back office actoren enerzijds en de tussenpersonen anderzijds de nodige garanties van elkaar verlangen. We zullen daarom nog verder ingaan op die specifieke problematiek.

3.2.4. AFSPRAKEN TOT SAMENWERKING

Nood aan afspraken tussen de betrokken actoren - We zagen dat de drie actoren in het gedecentraliseerd systeem – de front office en back office actoren en de tussenpersonen – nauw zullen moeten samenwerken om de consultatie van de logs door de burger vlot en rechtmatig te doen verlopen. Om zulke samenwerking mogelijk te maken is het onontbeerlijk dat er voldoende afspraken gemaakt worden tussen deze actoren. We zagen immers dat de tussenpersoon beschouwd kan worden als een vertrouwde derde partij. Er zullen dan allereerst voldoende garanties geboden moeten worden op de betrouwbaarheid van die tussenpersoon. We zullen daarom kijken naar wat de belangrijkste afspraken zijn die de partijen onderling moeten maken om een vlotte samenwerking tussen deze partijen tot stand te doen komen. We zullen daarbij ook kijken naar welke garanties er geboden moeten worden voor die samenwerking. Tot slot zullen we rekening houden met de verdeling van de aansprakelijkheid. Elke partij heeft immers zijn verantwoordelijkheden, wat wil zeggen dat men zal willen verhinderen dat de ene partij haar aansprakelijkheid afschuift op de andere.

Taakverdeling - Het spreekt voor zich dat er een aantal afspraken gemaakt zullen moeten worden om zulk gedecentraliseerd systeem op te richten. We zullen daarom onderzoeken welke afspraken er gemaakt moeten worden. Die afspraken kunnen zowel *ad hoc* als via een kaderovereenkomst gemaakt worden. Een eerste onderdeel waar men de nodige afspraken over zal moeten maken, is de taakverdeling en de garanties tot samenwerking. De taakverdeling in deze materie is vrij vanzelfsprekend. De doelsystemen staan als front office in voor het ontvangen van de aanvraag tot consultatie. Zij zullen die aanvraag verwerken en doorgeven aan de aangewezen tussenpersoon. Op het einde van de procedure zullen zij de verkregen gegevens verwerken en doorgeven aan de aanvrager. De tussenpersonen krijgen van de front office actoren de opdracht om de gevraagde gegevens bij de juiste back office actoren op te halen. Hoewel we nog zullen zien dat er nog enige opmerkingen te maken zijn bij de positie van de tussenpersoon, zien we wel dat deze actoren als doorgeefluik slechts een zo beperkt mogelijke rol zullen spelen. De back office actoren beschikken over de gevraagde informatie en zullen deze doorgeven aan de tussenpersonen.

Garanties op de goede werking - Deze taken kunnen uiteraard niet uitgevoerd worden zonder de nodige garanties op de goede werking van iedere partij. Zo zagen we al dat de back office actoren de gegevens waarover zij beschikken slechts zullen doorgeven nadat de aanvragende partij voldoende geauthentiseerd is en indien zij een geldige reden en een voldoende omschrijving van het doel van zulke aanvraag verkregen hebben. Het wordt dan de taak van de tussenpersonen om te garanderen dat aan deze voorwaarden voldaan is. De bronsystemen en de tussenpersonen zullen dus onderlinge afspraken moeten maken om vast te leggen hoe men zulke garanties moet leveren, hoe sterk de authenticatie moet zijn, en dergelijke. De tussenpersonen zullen daarnaast moeten garanderen dat zij zelf ook effectief geen inhoudelijke gegevens opslaan. Tot slot zullen zij de nodige garanties moeten leveren dat het doelsysteem de voorwaarden voor het gebruik van de geleverde gegevens zal naleven. De tussenpersonen zullen die voorwaarden dus tegenwerpelijk moeten maken aan de doelsystemen. De doelsystemen zullen op hun beurt ook de nodige garanties vragen van de tussenpersonen. Zo zullen deze laatste moeten garanderen dat de geleverde gegevens juist en volledig zijn. Hoewel de taak van de tussenpersonen dus in principe relatief beperkt blijft, zien we dat deze toch net die garanties moeten leveren die de werking van het systeem mogelijk maken. Zij zullen echter zelf ook een aantal garanties willen verkrijgen. De doel- en bronsystemen zullen moeten garanderen dat zij de privacywetgeving zullen naleven bij het uitoefenen van hun taken. Indien de opgevraagde gegevens geen betrekking hebben op de aanvrager, maar op een derde, dan zal er beroep gedaan worden op de uitzondering van de noodzakelijkheid voor de behartiging van een gerechtvaardigd belang van de aanvrager.[312] Men zal dan moeten nagaan of de rechten van de betrokkene in balans zijn met de belangen van de derde-aanvrager.

AANSPRAKELIJKHEID - Een ander belangrijk onderdeel van de afspraken die men zal moeten maken, gaat over de verdeling van de aansprakelijkheid. Aangezien het hier gaat om een vrij gevoelige materie – de privacy en de verwerking van persoonsgegevens – is het niet zo vreemd dat de betrokken actoren elkaar willen wijzen op de verantwoordelijkheden die elk van hen draagt. We zagen immers al dat zowel de front office actoren als de back office actoren persoonsgegevens zullen verwerken bij de uitoefening van hun taken. Deze actoren dragen bijgevolg de verantwoordelijkheid om tijdens de uitvoering van hun taken erover te waken dat de principes van de privacywetgeving met betrekking tot de verwerking van persoonsgegevens nageleefd worden en zij zijn bovendien de verantwoordelijken voor die verwerkingen. Daarnaast haalden we ook al aan dat de front office actoren als doelsystemen de eindverantwoordelijkheid dragen voor het bepalen van de principes van finaliteit, proportionaliteit, transparantie, en dergelijke in de hele procedure tot consultatie van het audit trail. Ook eventuele regelingen met betrekking tot de bewaartermijn en de eventuele verdere doorgifte van de hier verstrekte informatie zal onder de bevoegdheid van de front office actoren vallen. Zij dragen immers een belangrijke verantwoordelijkheid met betrekking tot de goede uitoefening van het ‘end-to-end’ audit trail. Dit zal dan ook voldoende uit de onderlinge akkoorden moeten blijken.

EEN SPECIAAL STATUUT VOOR DE TUSSENPERSOON – De verantwoordelijkheden van de tussenpersonen in het systeem zullen in principe beperkter zijn dan die van de andere actoren. In een aantal situaties zullen de front office en back office actoren immers de verantwoordelijken voor de verwerkingen zijn, in welk geval de tussenpersonen in principe beschouwd kunnen worden als verwerkers. Zij dienen dan in de eerste plaats slechts als doorgeefluiken voor de betrokken gegevens en zullen dus zelf in principe geen persoonsgegevens bewaren. Net door die positie als doorgeefluik en doordat zij in de regel niet zelf gegevens bewaren, kunnen we in zulke gevallen de aansprakelijkheid van de tussenpersonen enigszins tot een minimum herleiden. Het zullen dus beide uiteinden van de ‘end-to-end’ keten zijn die de belangrijkste aansprakelijkheden op

[312] Art. 7, f) Richtlijn en art. 5, f) Privacywet.

zich moeten nemen. Hiertoe zullen echter ook de nodige afspraken gemaakt worden tussen de verantwoordelijken voor de verwerkingen en de verwerkers. Hoewel we zagen dat de tussenpersonen een aantal garanties moeten leveren aan zowel de bronsystemen als de doelsystemen, benadrukken we dat men zal moeten afspreken dat zij toch niet aansprakelijk gesteld kunnen worden voor het niet naleven van de door andere partijen geleverde garanties, afspraken en wettelijke bepalingen door de bron- en doelsystemen. De tussenpersonen horen door hun positie in het geheel slechts aansprakelijk te zijn voor eigen opzet, zware fout of nalatigheid.

3.2.5. ORGANISATIE VAN SAMENWERKING

NA DE AFSPRAAK VOLGT DE ORGANISATIE - We zagen intussen dat er een aantal afspraken gemaakt moeten worden ten behoeve van de samenwerking tussen de verschillende actoren die betrokken zijn bij een centraal portaal voor de inzage van de decentraal opgeslagen logs. Het spreekt voor zich dat er ook de nodige aandacht zal moeten worden besteed aan de organisatie van zulke samenwerking. We zullen daarom kort een aantal punten aanhalen die van belang zullen zijn bij het organiseren van zulke samenwerking. Op de hier aangehaalde punten zal in een later stadium van het onderzoek nog dieper worden ingegaan.

HOE DE SAMENWERKING TE ORGANISEREN? - Allereerst moeten we ons afvragen hoe we ons de samenwerking tussen de front en back office actoren en de tussenpersonen organisatorisch moeten voorstellen. We zagen immers al dat de verschillende actoren tegenover elkaar geauthentiseerd moeten worden. Daarnaast zagen we ook dat de tussenpersonen ervoor moeten zorgen dat de doorgifte van de gegevens voldoende beveiligd wordt. Er zal dus een systeem moeten worden opgezet dat toelaat dat de betrokken partijen zich veilig tegenover elkaar authentiseren en dat een beveiligde gegevensoverdracht – al dan niet door middel van cryptografische bewerkingen – kan garanderen. Het doel van zulke beveiligde constructie – alsook een reden voor het gebruik van tussenpersonen – is om ervoor te zorgen dat de bron- en doelsystemen in verband met een aanvraag tot inzage in de logs niet meer informatie te weten komen dan strikt noodzakelijk is voor het uitoefenen van hun eigen taak binnen het geheel. Anderzijds moet men er wel voor zorgen dat de burger wel in staat gesteld wordt om het gehele gegevensspoor te reconstrueren. We zouden hier kunnen denken aan het gebruik van een gefedereerd systeem op basis van vertrouwenskringen. Deze figuur zal onder hoofdstuk 3.3 nog verder onderzocht worden.

NOOD AAN EEN WETTELIJK KADER? - Men kan zich ook afvragen wat het precieze juridische kader is voor zulke samenwerking. We zagen al dat de betrokken partijen de nodige afspraken zullen moeten maken en dat zij elk wel onderworpen zijn aan een aantal wettelijke bepalingen, zoals de privacywetgeving. Ook zagen we dat er al een wettelijk kader voor de figuur van de vertrouwenspersoon voorgesteld werd, maar dat dit kader in principe niet bedoeld is voor het hier voorgestelde gebruik. De vraag is dan of er geen nood is aan een wettelijk kader dat de specifieke problemen kan aanpakken die we in verband met deze materie ervaren. Zulk wettelijk kader zal onder hoofdstuk 3.4 nog verder onderzocht worden. In het kader van dat onderzoek zullen we ook bekijken wie het meest geschikt is om het gedecentraliseerd systeem te beheren. Er zal onderzocht worden of het kan volstaan om de front office actoren – door hun bijzondere verantwoordelijkheid in de procedure – aan te stellen als beheerder van dit proces of dat er een onafhankelijke beheerder nodig is.

3.3. FEDERATIE OP BASIS VAN VERTROUWENSKRINGEN

ZOEKEN NAAR EEN GESCHIKT SYSTEEM - Uit het voorgaande blijkt dat loutere onderlinge afspraken tussen de betrokken actoren wellicht niet voldoende zullen zijn om de vlotte werking van het systeem van gedecentraliseerde gegevensopslag te garanderen. Er is daarom nood aan een systeem dat ervoor kan zorgen dat de partijen zich veilig en betrouwbaar tegenover elkaar kunnen authentiseren en dat de gegevensoverdracht voldoende beveiligd wordt. Het is immers belangrijk dat de bron- en doelsystemen enkel de informatie te zien krijgen die strikt noodzakelijk is voor de uitoefening van hun taken binnen deze procedure. Het is in principe de taak van de tussenpersonen om hier voor te zorgen. Men zal dus een systeem moeten oprichten waarmee men zulke beveiligde gegevensoverdracht kan garanderen. Een manier om dit te doen, is door middel van het gebruik van een gefedereerd systeem op basis van vertrouwenskringen.

DE FEDERATIE OP BASIS VAN VERTROUWENSKRINGEN - Het model van de federatie op basis van vertrouwenskringen is immers uitermate geschikt voor een systeem met gedecentraliseerde opslag van persoonsgegevens.[313] Dit model houdt in dat er tussen de betrokken partijen afspraken gemaakt worden met betrekking tot het gebruikers- en toegangsbeheer.[314] Op die manier kan men de nodige authenticaties en verificaties vastleggen en kan men aanduiden wie de verantwoordelijkheid en de aansprakelijkheid draagt hiervoor. Men kan dan ook bepalen hoe gegevens uitgewisseld zullen worden tussen de verschillende partijen, alsook welke partij toegang krijgt tot welke gegevens. Op die manier kan men vermijden dat de eindpunten van de procedure – de bron- en doelsystemen – informatie met betrekking tot persoonsgegevens te weten komen die niet strikt noodzakelijk is voor de uitoefening van hun taken. De burger zal uiteindelijk wel in staat gesteld worden om het volledige spoor van verwerkingen en koppelingen te traceren. Wat het gebruikersbeheer betreft zal men de benodigde kenmerken, mandaten en autorisaties moeten registreren in het systeem. Dit is nodig voor de latere authenticatie van de betrokken actoren op basis van bijvoorbeeld de e-ID. Men zal er op die manier voor kunnen zorgen dat de gegevens die binnen het systeem verwerkt worden afgeschermd zijn van derden. Het toegangsbeheer zal dan regelen wie toegang krijgt tot welke gegevens. Dit zal gebeuren door middel van de registratie en de verificatie van autorisaties.[315]

FEDERATIE EN DE IDENTIFICATIE VAN DE VERANTWOORDELIJKE VOOR DE VERWERKING - Het model van het gefedereerd systeem kan ook helpen bij het probleem van de identificatie van de ambtenaar die de verwerking uitvoert in opdracht van de voor de verwerking verantwoordelijke organisatie in de logs. Zoals we onder hoofdstuk 2.4.3 zagen, is het niet opportuun om de verantwoordelijke ambtenaar zonder meer te identificeren in de logs. Dit zou immers een bijkomende verwerking van persoonsgegevens inhouden die we als overmatig kunnen beschouwen voor het bereiken van het doel van het Kadaster van Verbindingen. Een overmatige verwerking van persoonsgegevens is uiteraard een schending van het principe van de proportionaliteit dat we kennen uit de wetgeving met betrekking tot de verwerking van persoonsgegevens. We concludeerden daarom dat de identificatie van de verwerkende ambtenaar in de logs niet nodig is en dat men kan volstaan met de identificatie op het niveau van de voor die verwerking van persoonsgegevens ver-

[313] J. DUMORTIER, F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerrecht*, 2009, nr. 2, 52-60; *law.kuleuven.be/icri/frobben*, 4.

[314] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, 'aanbeveling 01/2008', 24 september 2008, *www.privacycommission.be,* 4.

[315] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, 'aanbeveling 01/2008', 24 september 2008, *www.privacycommission.be,* 9.

antwoordelijke organisatie. Hoewel men – zoals de Commissie voor de bescherming van de persoonlijke levenssfeer – kan argumenteren dat de identificatie van de organisatie in plaats van de persoon te verkiezen valt vanuit het standpunt van de privacybescherming, zien we dat er toch een duidelijke vraag is naar identificatie van de verwerkende ambtenaar zelf. Uit een arrest van het Europees Hof van de Rechten van de Mens volgt dat de verwerkende persoon minstens identificeerbaar moet zijn. Het is duidelijk dat er dan wel een conflict kan rijzen tussen de belangen van de betrokkene en het recht op privacy van de verwerkende derde. Om dit op te lossen gaven we al aan dat het aan te bevelen is dat de verwerkende ambtenaar wel geïdentificeerd wordt, maar dat zijn identiteitsgegevens afgeschermd worden. Op die manier blijft zijn persoonlijke levenssfeer in eerste instantie beschermd. Zijn identiteit kan pas onthuld worden indien hij betrokken was bij een onrechtmatige verwerking van persoonsgegevens. De federatie op basis van vertrouwenskringen kan hiervoor zorgen. Men zou dan de identiteit van de verwerkende ambtenaar – eventueel in versleutelde vorm – kunnen afschermen van de actoren die niet gemachtigd zijn om deze te zien. Die identiteit zou in eerste instantie voor alle actoren verborgen kunnen blijven, maar zal aan de hiertoe aangewezen partij vrijgegeven worden in het geval van een onrechtmatige gegevensverwerking.

PRAKTIJKONDERZOEK - Het gefedereerd systeem op basis van vertrouwenskringen wordt in de praktijk al langer onderzocht. De Liberty Alliance groep voert al jaren onderzoek naar open standaarden om de privacy van burgers en bedrijven beter te beschermen bij online transacties.[316] De standaarden en modellen die door deze groep tot stand gebracht zijn, worden wereldwijd door bedrijven uit alle sectoren, alsook door overheden, gebruikt. Ook zij baseren hun model voor gebruikers- en toegangsbeheer op het idee van het gefedereerd systeem en vertrouwenskringen. Het door hen voorgestelde '*Liberty Identity Federation Framework*' (ID-FF) is intussen opgegaan in de '*Security Assertion Markup Language 2.0*' (SAML 2.0) standaard. Een ander voorbeeld is de '*Shibboleth*' standaard die onder meer door de K.U.Leuven gebruikt wordt.[317] Net door het feit dat het hier gaat om open standaarden, is het mogelijk om de voor het hier voorliggende probleem van het gedecentraliseerd systeem voor audit trails meest geschikte standaard te zoeken en om deze waar nodig aan te passen.

EEN GESCHIKT MODEL - Op grond van het hier gevoerde onderzoek concluderen we dat het model van de federatie op basis van vertrouwenskringen zeker geschikt is voor gebruik in het kader van een gedecentraliseerd systeem voor audit trails. Dit model biedt immers de mogelijkheden met betrekking tot gebruikers- en toegangsbeheer die zulke gedecentraliseerd model nodig heeft. Men kan door het gebruik van een federatie op basis van vertrouwenskringen vermijden dat de bron- en doelsystemen persoonsgegevens verkrijgen die niet strikt noodzakelijk zijn voor het uitoefenen van hun taak. Anderzijds kan men er met dit model – mits een aantal andere benodigde technische maatregelen uitgevoerd werden – wel voor zorgen dat de burger in staat gesteld wordt om na authenticatie, bijvoorbeeld op basis van zijn e-ID, het gehele spoor van gegevens met betrekking tot gegevensverwerkingen en –koppelingen te reconstrueren. Daarnaast zien we dat het model van de federatie op basis van vertrouwenskringen ook geschikt is voor gebruik in een systeem tot het afschermen van de identiteit van de verwerkende ambtenaar. Men kan op die manier garanderen dat hij niet rechtstreeks geïdentificeerd zal worden naar de betrokken actoren en de burger toe, maar dat hij in geval van een onrechtmatige gegevensverwerking wel geïdentificeerd kan worden.

[316] *www.projectliberty.org.*
[317] *shibboleth.internet2.edu.*

3.4. HET WETTELIJK KADER

NOOD AAN EEN WETTELIJK KADER? - In het voorgaande zijn we tot de conclusie gekomen dat we voor de organisatie van het audit trail best kunnen opteren voor een gedecentraliseerde aanpak. Vervolgens hebben we de verschillende actoren in zulk systeem besproken en hebben we onderzocht hoe de samenwerking tussen deze verschillende actoren geregeld zou moeten worden. We kwamen daar tot de conclusie dat er nog verder onderzocht moet worden hoe we ons het Kadaster van Verbindingen organisatorisch en juridisch moeten voorstellen. Wat het organisatorisch aspect betreft concludeerden we dat we de voorkeur kunnen geven aan een gefedereerd systeem op basis van vertrouwenskringen. In dit deel zullen we dan het wettelijk kader van zulk systeem onderzoeken. We kunnen ons immers nog vragen stellen in verband met de mogelijkheden van de samenwerkingsovereenkomst tussen de bij een systeem van gedecentraliseerde gegevensopslag betrokken actoren, die zoals we al zagen ertoe gehouden zijn bepaalde wettelijke bepalingen – zoals de privacywetgeving – na te leven. Aansluitend zagen we dat er in principe al een wettelijk kader bestaat voor de figuur van de vertrouwenspersoon. De vraag is dan in hoeverre er voor de tussenpersoon in het Kadaster van Verbindingen al een wettelijk kader bestaat. Indien dit niet het geval is, zal er onderzocht worden hoe we ons zulk kader zouden moeten voorstellen. Tot slot zal er ook worden stilgestaan bij het beheer van het Kadaster. Kan het volstaan dat één van de betrokken actoren het beheer in handen neemt of is er nood aan een onafhankelijk beheerder?

ACTOREN GEBONDEN AAN DE WET - PRIVACYWETGEVING - Bij het bespreken van de verschillende actoren die betrokken zijn bij een systeem van gedecentraliseerde gegevensopslag, merkten we al op dat zij allen gebonden zijn aan een aantal wettelijke bepalingen. Zo is er de privacywetgeving, die door elke betrokken partij nageleefd zal moeten worden bij het uitvoeren van haar taken binnen het systeem. We zagen ook dat de betrokken organen deel uitmaken van de overheid. Zij zijn bijgevolg gehouden tot het naleven van de regelgeving in verband met de beginselen van behoorlijk bestuur en de openbaarheid van bestuur. Bij het aangaan van onderlinge overeenkomsten, zullen de betrokken actoren er dus voor moeten zorgen dat zulke overeenkomsten niet zullen leiden tot een inbreuk op hun wettelijke verplichtingen. Wat betreft de privacywetgeving herhalen we dat het bijhouden van logs en de consultatie ervan onvermijdelijk ook een verwerking van persoonsgegevens inhoudt en dat men bijgevolg ervoor zal moeten zorgen dat de principes van finaliteit, proportionaliteit en transparantie nageleefd worden. Hoewel in principe iedere betrokken partij gehouden is tot het naleven van die principes bij de uitvoer van de eigen taken binnen het systeem, zagen we dat de front office actoren als doelsystemen een bijkomende verantwoordelijk dragen voor het naleven van een aantal van die principes, alsook voor het bepalen van de bewaartermijn en dergelijke.

ACTOREN GEBONDEN AAN DE WET - BEHOORLIJK EN OPENBAAR BESTUUR - Wat betreft het behoorlijk bestuur en de openbaarheid van bestuur kunnen we denken aan de beginselen van gelijkheid, rechtszekerheid en redelijkheid. Daarnaast moeten de handelingen van deze actoren voldoende gemotiveerd worden. Die motivatieplicht geldt zowel op materieel als op formeel vlak.[318] De openbaarheid van bestuur houdt in dat de gegevens waarover de overheidsorganen beschikken

[318] Voor een verder bespreking van deze beginselen, zie: J. DE STAERCKE, 'Algemene beginselen van behoorlijk burgerschap. Naar een wederkerig bestuursrecht?', *jura falconis 2001-2002*, vol. 38, nr. 4, 505-535.

in principe openbaar en voor geïnteresseerde partijen toegankelijk moeten zijn.[319] Dit geldt bijgevolg ook voor het Kadaster van Verbindingen, dat openbaar toegankelijk is tenzij zulke openbare toegang in conflict zou komen met het recht op privacybescherming van de betrokkene. Dit laatste toont al aan dat er soms conflicten kunnen rijzen tussen de verschillende wettelijke bepalingen die op deze actoren rusten. Men zal er bijgevolg bij het opstellen van de overeenkomsten tussen de actoren over moeten waken dat deze overeenkomsten niet leiden tot verdere conflicten met – of inbreuken op – deze wettelijke bepalingen.

NOOD AAN EEN APART WETTELIJK KADER … - Deze mogelijke conflicten tussen verschillende wettelijke bepalingen en de soms moeizame wisselwerking van die wettelijke bepalingen met de overeenkomsten die de betrokken actoren onderling sluiten, zijn illustratief voor de moeilijkheden die men kan ondervinden bij het oprichten van een platform als het Kadaster van Verbindingen binnen de overheidscontext. Het zou daarom een interessante denkpiste kunnen zijn om een onderzoek te voeren naar de mogelijkheid van een wettelijk kader voor dit Kadaster. Met zulk kader zouden een aantal van de tot hier toe geformuleerde moeilijkheden onmiddellijk kunnen worden aangepakt. Men zou op die manier ook alle relevante bepalingen op een enkele plaats kunnen samenbrengen, wat de algemene transparantie van deze materie enkel maar ten goede zou komen. We zullen daarom in eerste instantie onderzoeken of er al niet een wettelijk kader bestaat dat toepasbaar zou zijn op de hier voorliggende materie. We kunnen in de eerste plaats kijken naar het eerder aangehaalde wettelijk kader voor de figuur van de vertrouwenspersoon.[320] De Wet tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten regelt immers een aantal basisregels voor de vertrouwenspersonen. Hoewel dit kader al een mooie aanzet zou zijn tot de werkelijke aanvaarding en codificatie van de figuur van de vertrouwenspersoon, zagen we dat de wet toch nog een aantal lacunes bevat die bijgevolg voor elke situatie op een *ad hoc* wijze zullen moeten worden ingevuld.

… BIJ GEBREK AAN TOEPASBAAR KADER - We zagen daarnaast ook dat het juridisch kader voor de vertrouwenspersoon geen melding maakt van de mogelijke toepassing van dit kader op een vertrouwenspersoon die deel uitmaakt van de overheid, zoals de tussenpersonen in het Kadaster van Verbindingen zouden zijn. Ondanks de grote gelijkenissen tussen de figuur van de tussenpersoon die we in het Kadaster zouden terugvinden en de figuur van de vertrouwenspersoon krachtens de betrokken wet, is het met andere woorden niet zeker dat we het wettelijk kader voor deze laatste figuur kunnen toepassen op de andere. Daarnaast zou het wettelijk kader voor de vertrouwenspersoon uiteraard ook enkel relevant zijn voor de tussenpersoon in het Kadaster van Verbindingen en niet op het gehele Kadaster zelf. Er zou dan nog steeds nood zijn aan een wettelijk kader voor de andere actoren en voor het Kadaster van Verbindingen op zich. Tot slot heeft de inwerkingtreding van deze wet voor een aantal problemen gezorgd die ertoe leiden dat deze wet allicht zonder gevolg blijft. Onder de huidige stand van het recht lijkt er daarom geen wettelijk kader te bestaan dat toegepast kan worden op de gehele figuur van het Kadaster van Verbindingen of op de actoren binnen deze figuur. Men zal daarom een apart wettelijk kader moeten ontwikkelen voor de figuur van het Kadaster. We zullen hier een aantal mogelijkheidsvoorwaarden toe onderzoeken.

[319] Merk op dat het hier slechts gaat om een passieve openbaarheid, zoals die uit artikel 10 van de Privacywet. Zie hoofdstuk 2.1 voor een meer uitgebreide bespreking van deze materie.

[320] Wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten, *B.S.* 17 juli 2007, 38587-38591. Merk op dat we al eerder aanhaalden dat er nog problemen zijn met betrekking tot de inwerkingtreding van deze wet.

DE BEVOEGDE OVERHEID IS … - Voor we overgaan tot het onderzoeken van de precieze inhoud van een wettelijk kader voor het Kadaster van Verbindingen, moeten we eerst kijken naar het niveau waarop zulk kader aangenomen zou moeten worden. We zoeken hier met andere woorden naar de autoriteit die bevoegd is om het Kadaster op enigszins bindende manier te regelen. Indien men binnen de overheidssector het gebruik van logs wil veralgemenen, zal men er immers voor moeten zorgen dat men alle overheidsdiensten – of preciezer: alle verantwoordelijken voor de verwerking van persoonsgegevens binnen de overheidssector – kan verplichten om deel te nemen aan zulk project. Het spreekt voor zich dat het Kadaster van Verbindingen zijn doel volledig mist indien de burger niet het volledige gegevensspoor kan reconstrueren omdat een aantal overheidsdiensten daar niet aan willen meewerken. Wat België betreft zien we dat zowel de federale overheid – bij wet – als de gemeenschappen en gewesten – bij decreet of ordonnantie – bevoegd zijn om transparantieverplichtingen op te leggen. Het Kadaster van Verbindingen kan, zoals eerder al werd geargumenteerd, beschouwd worden als een maatregel die de transparantie van de verwerking van persoonsgegevens kan verhogen. De Belgische federale overheid en de overheden van de gemeenschappen en de gewesten zijn dus bevoegd om het bijhouden van logs en het op gestructureerde wijze aanbieden van deze logs via een centraal platform als het Kadaster van Verbindingen op te leggen aan de overheidsdiensten.[321] Men zou kunnen argumenteren dat de verplichting tot het bijhouden van logs niet rechtstreeks af te leiden valt uit Richtlijn 95/46/EG en dat zulke verplichting dus verder gaat dan wat de Europese Unie haar lidstaten oplegt. Aangezien Richtlijn 95/46/EG in de eerste plaats een minimumniveau aan privacybescherming wou garanderen en dus geen volledige harmonisatie voor ogen had, is er echter geen enkel probleem met lidstaten die zwaardere normen wensen te hanteren. De Richtlijn laat immers zelf al ruimte over voor de inbreng van de lidstaten, bijvoorbeeld door hen op te roepen om passende waarborgen te nemen in het geval van een uitzondering op de informatieplicht bij onrechtstreekse gegevensinzameling.[322]

… MINSTENS DE FEDERALE OVERHEID - Het spreekt in deze materie wel voor zich dat het Kadaster van Verbindingen op zowel federaal als op het niveau van de gemeenschappen en gewesten geregeld moet worden. Een regeling op slechts één van beide niveaus geeft immers geen garantie dat de betrokken overheden op het andere niveau ook zullen deelnemen aan dit project. Zoals we al aanhaalden, kan het in bepaalde gevallen noodzakelijk zijn dat alle overheidsdiensten en –niveaus aan dit project deelnemen, om op die manier te garanderen dat de burger het volledige gegevensspoor zal kunnen reconstrueren. We concluderen daarom allereerst dat een wettelijk kader voor het oprichten van het Kadaster van Verbindingen nodig is om alle overheidsdiensten op alle niveaus te verplichten om deel te nemen aan dit project. Het Kadaster van Verbindingen kan immers pas nuttig zijn indien het de burger de mogelijkheid biedt om het hele spoor van verwerkingen en koppelingen van zijn persoonsgegevens kan traceren. Indien bepaalde overheden niet meewerken, zal een reconstructie van het 'end-to-end' gegevensspoor niet mogelijk zijn. Uit deze conclusie volgt dan dat het wettelijk kader van het Kadaster van Verbindingen binnen de Belgische federale structuur zowel op federaal als op deelstatelijk vlak geregeld moet

[321] Voor de gemeenschappen en gewesten zou zulke beslissing moeten kaderen binnen een aangelegenheid die tot hun bevoegdheid hoort en voor zover zulke beslissing geen inbreuk maakt op de bevoegdheden van de federale regering of op internationaalrechtelijke normen. De gemeenschappen en gewesten kunnen met andere woorden het beschermingsniveau dat opgelegd wordt door de federale overheid wel verhogen, maar kunnen niet verlagen. Zie AH 19 januari 2005, nr. 16/2005 en RvS 28 mei 2004, advies 37.288/3.

[322] Zie artikel 11 (2) Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.* L van 23 november 1995, 31-50.

worden. Ook hier is de reden daartoe dat men alle overheidsdiensten en –niveaus zal moeten betrekken in dit project. We kunnen dan denken aan een overkoepelend wettelijk kader op federaal niveau, met ruimte voor eventuele afwijkingen – binnen de toegestane grenzen – voor de gemeenschappen en gewesten. Dit strookt met de positie van het Grondwettelijk Hof en de Raad van State betreffende deze materie. De decreetgever mag dan specifieke regelgeving uitvaardigen ter verhoging van de transparantie van de verwerking van persoonsgegevens door overheidsdiensten, voor zover het beschermingsniveau dat door de federale wetgever gewaarborgd wordt hiermee niet verlaagd wordt. Gelet op het belang van deze materie voor alle beleidsniveaus zou een samenwerkingsakkoord een interessante oplossing kunnen bieden.

De inhoud van het wettelijk kader - Nu we weten op welk niveau het wettelijk kader zou moeten aangenomen worden, kunnen we kijken naar wat zulk kader precies zou moeten regelen. Uit het voorgaande volgt dat het wettelijk kader er in de eerste plaats voor zal moeten zorgen dat alle overheidsdiensten op alle niveaus verplicht worden tot het meewerken aan het Kadaster van Verbindingen. Vervolgens zou het wettelijk kader de betrokken actoren moeten identificeren en een aantal basisprincipes vastleggen. Zo kan er gewezen worden op de individuele verantwoordelijkheden die op de betrokken actoren rusten, zoals hun verplichtingen onder de privacywetgeving en hun verplichtingen met betrekking tot de openbaarheid van bestuur en de beginselen van behoorlijk bestuur. Wat betreft de tussenpersonen kunnen een groot aantal van de verplichtingen die op hen rusten al teruggevonden worden in de Wet op de vertrouwenspersoon, in zoverre deze wet ooit enige praktische weerslag zal kennen.

Beperkingen op het wettelijk kader - We mogen echter niet vergeten dat de betrokken actoren nog onderlinge afspraken zullen moeten maken. Het wettelijk kader mag dus niet van zulke aard zijn dat het de mogelijkheden tot het sluiten van onderlinge overeenkomsten tussen de actoren volstrekt onmogelijk maakt. Hoewel een wettelijk kader dus zeker nodig zal zijn voor de goede werking van het Kadaster, zal het zich dus echter wel moeten beperken tot het aanreiken van een algemeen kader waarbinnen de actoren hun audit trail opzetten. Het wettelijk kader zal daarom niet verder moeten gaan dan het verplichten van de overheidsdiensten tot medewerking, het identificeren van de betrokken actoren, het aanhalen van een aantal basisprincipes– voornamelijk met verwijzing naar bestaande regelgeving zoals de privacywet, de beginselen van behoorlijk bestuur en de openbaarheid van bestuur – en het opsommen van een aantal basisverantwoordelijkheden die de betrokken actoren zullen moeten dragen. Enkel op die manier kan er voldoende rekening gehouden worden met de bijzonderheden van bepaalde overheidsdiensten. Zo kent bijvoorbeeld elke authentieke bron wel een aantal bijzonderheden die deze bron onderscheiden van andere authentieke bronnen. Wanneer zulke authentieke bron zal dienen als bronsysteem in een systeem van gedecentraliseerde gegevensopslag, dan zal men in de onderlinge overeenkomsten tussen de betrokken actoren uiteraard rekening moeten houden met die bijzonderheden. Het spreekt voor zich dat het wettelijk kader de betrokken actoren hun autonomie om hun eigen specifieke modaliteiten tot samenwerking te bepalen niet volledig mag ontnemen. We kunnen daarom denken aan het eerder aangehaalde samenwerkingsakkoord. Hierbij kunnen alle beleidsniveaus – federaal en deelstatelijk – betrokken worden bij deze materie om de deelname van alle lagen van de overheid aan dit project te garanderen. Het akkoord kan dan ook voldoende ruimte geven tot het verder specificeren van onderlinge afspraken door de actoren zelf, alsook het bepalen van de vorm waarin zulke afspraken gemaakt moeten worden. Wanneer dit samenwerkingsakkoord minstens bij koninklijk besluit bekrachtigd wordt, zal het een voldoende wettelijke basis kunnen bieden.

HET BEHEER VAN HET KADASTER VAN VERBINDINGEN – KUNNEN DE BESTAANDE ACTOREN VOLSTAAN? - Tot slot moet er ook onderzocht worden wie het Kadaster van Verbindingen en de logs waartoe het Kadaster toegang verschaft zal beheren. We zagen al eerder dat de betrokken actoren hun eigen verantwoordelijkheden dragen binnen de uitvoering van hun taak binnen het geheel en bijgevolg ook aansprakelijk zijn indien zij die verantwoordelijkheden niet naleven. Daarnaast zagen we ook al dat de front office actoren als doelsystemen een zwaardere taak opgelegd krijgen. Zij zullen immers een bijkomende verantwoordelijkheid dragen voor het naleven van onder meer de principes van finaliteit, proportionaliteit en transparantie, alsook voor het regelen van de bewaartermijn en eventuele verdere doorgifte van de hier verstrekte informatie. De vraag is dan of het volstaat dat de front office actoren zulke bijkomende verantwoordelijkheid dragen voor het goede verloop van het 'end-to-end' gegevensspoor of dat het nodig zou zijn om beroep te doen op een onafhankelijke beheerder van de hele procedure.

HET BEHEER VAN HET KADASTER VAN VERBINDINGEN – IS ER NOOD AAN EEN ONAFHANKELIJKE BEHEERDER? - Het feit dat er tussen de betrokken actoren onderlinge afspraken gemaakt zijn met betrekking tot de werking van het systeem en de verdeling van de verantwoordelijkheden en aansprakelijkheid met betrekking tot dit systeem, alsook het feit dat de front office actoren bijzondere verantwoordelijkheden opnemen, kan zeker een eerste vorm van interne controle bieden. Ook de aanwezigheid van de tussenpersonen kan er voor zorgen dat zij voor hun deel van de transacties kunnen toezien voor de goede werking van de gegevenssporen. Dit wil echter nog niet onmiddellijk zeggen dat er geen nood is aan een bijkomende beheerder voor de transacties binnen het audit trail. De taken van de tussenpersonen, hoe belangrijk deze ook mogen zijn, zijn immers ook maar beperkt tot een deel van de procedure. Voor het beheer van het audit trail is er echter nood aan een instantie die de gehele procedure kan overzien. Het principe van de scheiding der machten – wat nog steeds de belangrijkste basis vormt voor onze rechtstaat – vereist daarnaast dat de partij die instaat voor het toezicht op het systeem niet zelf een belanghebbende partij in datzelfde systeem mag zijn. Zolang er geen erkende tussenpersoon bestaat die krachtens de wet een duidelijke opdracht tot onafhankelijk toezicht verkregen heeft, zal er dus wel nood zijn aan een beheerder die buiten de betrokken partijen staat en die aldus op onafhankelijke wijze toezicht kan houden. Het uiteindelijke Kadaster– het portaal waar men de burger inzage verschaft in deze logs – zal daarnaast ook een eigen beheerder nodig hebben.

HET BEHEER VAN DE LOGS EN HET KADASTER VAN VERBINDINGEN – NAAR EEN ROL VOOR HET SECTORAAL COMITÉ VAN HET RIJKSREGISTER? - We mogen niet vergeten dat het loggen zelf te beschouwen is als een verwerking van persoonsgegevens. De Commissie voor de bescherming van de persoonlijke levenssfeer zal dus moeten toekijken op de werking van het gegevensspoor. De basis hiervoor vinden we in artikel 32 van de Belgische Privacywet. Dit artikel handelt over de bevoegdheden waarover de Commissie kan beschikken in het kader van de *ex post* controle op de naleving van de bepalingen uit deze wet. Zulke controle door de privacyautoriteit kan belangrijke waarborgen bieden met betrekking tot de kwaliteit en de volledigheid van het gegevensspoor waartoe het Kadaster toegang verschaft. Uit het voorgaande volgt daarnaast dat de actoren in het systeem zelf al een zekere vorm van controle op elkaars werking uitvoeren. Het gaat dan voornamelijk om de controle die uitgevoerd wordt door de tussenpersonen, wat meteen ook wil zeggen dat deze controle beperkt is tot de transacties waar de tussenpersonen bij betrokken zijn. Het lijkt ons daarom meer opportuun om de uiteindelijke controle over de logs over te laten aan een onafhankelijke beheerder, zoals bijvoorbeeld de centrale privacycommissie. Deze instantie bevindt zich immers – net door die positie van centrale toezichthoudende autoriteit – in de perfecte positie om controle uit te oefenen op alle logs binnen de overheidscontext, ongeacht de precieze sector waarin deze bijgehouden worden. We concluderen daarnaast ook dat het uiteindelijke Kadaster als centraal portaal waar de burger inzage in de logs aangeboden wordt, ook een eigen beheerder nodig zal hebben. Het wettelijk kader bij het Kadaster van Verbindingen zou dan kunnen aangeven op welke aspecten van het systeem er bijkomende controle door de centrale beheerder nodig zal zijn. Bij het beheer van het Kadaster van Verbindingen als centraal portaal op zich, denken we uiteraard aan het sectoraal comité van het Rijksregister. Het is immers deze instantie die krachtens artikel 8 van de Wet op het Rijksregister de taak toegewezen gekregen heeft om een dergelijk kadaster op te richten.

3.5. HET KADASTER IN DE PRAKTIJK BRENGEN

DE THEORIE VERSUS DE PRAKTIJK - In al het voorgaande onderzoek hebben we het audit trail – en bij uitbreiding ook het Kadaster van Verbindingen – voornamelijk vanuit een juridische en theoretische invalshoek bekeken. Nu we ons een beeld kunnen vormen van wat het Kadaster van Verbindingen inhoudt en hoe we het juridisch zouden moeten organiseren, kunnen we even stilstaan bij een aantal praktische problemen. De theorie kan immers zeer mooi klinken, het zal uiteindelijk de praktische haalbaarheid van het project zijn die bepalend is voor de effectieve realisatie ervan. Daarom zullen we nu een aantal van de voor het Kadaster van Verbindingen meest prangende praktische problemen aanhalen.

HET AUDIT TRAIL EX NUNC - Allereerst moeten we in acht nemen dat het audit trail waarin het Kadaster inzage biedt niet zonder meer *ex nunc* te regelen zal zijn. Het loggen van de gegevenskoppelingen en de verwerkingen om een *ex post* controle mogelijk te maken kan uiteraard wel slechts van start gaan vanaf het ogenblik dat het systeem voor het loggen van zulke transacties operationeel wordt. Een groter probleem ligt echter bij de *ex ante* benadering. Hier zal men er enerzijds voor moeten zorgen dat de toekomstige machtigingen opgenomen worden in het systeem, maar zullen anderzijds de vroeger verleende machtigingen eveneens in het systeem opgenomen moeten worden. Wat de toekomstige machtigingen betreft is er geen probleem. Men zou men die machtigingen immers via een afgesproken standaard kunnen opstellen.[323] Op deze manier kunnen de voor het audit log benodigde gegevens met een relatief kleine inbreng doorgegeven worden aan het register en hoeft hier enkel bijkomend personeel bij te pas te komen om deze machtigingen om te zetten in een formaat dat in het register opgenomen kan worden. Wat die gegevens betreft kunnen we verwijzen naar hoofdstuk 2.4.2. De *ex post* logs moeten immers een antwoord bieden op de vraag: Wie heeft met betrekking tot mijn persoonsgegevens wat gedaan, met welke reden en op welk moment? Het spreekt dan voor zich dat de gegevens in het *ex ante* register van de beoogde gegevenskoppelingen dan een gelijkaardig patroon zullen moeten volgen. Het gaat hier over de identiteit van de verantwoordelijke ambtenaar, het aanduiden van de persoonsgegevens waarvoor de machtiging verleend is, het doel van de verwerking, de voorwaarden waar de verwerking aan moet voldoen, de periode waarover de verwerking loopt en de beoogde gegevenskoppelingen.

HET AUDIT TRAIL EX TUNC - PROBLEEMSTELLING - De vroeger verleende machtigingen zullen echter voor een aantal probleem zorgen. Deze machtigingen volgden uiteraard niet de vaste structuur die we voor toekomstige machtigingen kunnen aanbevelen. Het invoeren van deze machtigingen in het audit trail systeem zal bijgevolg niet geautomatiseerd kunnen verlopen en zal dan een zeer

[323] Men kan hier bijvoorbeeld gebruik maken van de veelgebruikte XML standaard.

intensieve opdracht worden voor de ambtenaren die hiermee belast worden. Daarnaast is er het probleem van de publicatie. Een systematische en geordende publicatie op een publiek toegankelijke website is pas een in voege gekomen met de oprichting van het sectoraal comité van het Rijksregister in 2003. De vroegere machtigingen bij koninklijk besluit zijn weliswaar in het Staatsblad gepubliceerd, maar er lijkt nergens een officieel systematisch overzicht van al die bestaande koninklijke besluiten te bestaan. Men zal hier dus handmatig moeten proberen om alle verleende machtigingen die nu nog gelden in kaart te brengen om deze vervolgens handmatig in te voeren in het audit trail systeem.

HET AUDIT TRAIL EX TUNC - GEVOLGEN VOOR DE PRAKTIJK - Het is onmogelijk om in het kader van dit onderzoek een correcte weergave te bieden van de precieze omvang van het aantal koninklijke besluiten dat handmatig in kaart gebracht zou moeten worden en het aantal machtigingen – zowel bij koninklijk besluit als door het sectoraal comité – dat handmatig ingevoerd zou moeten worden, maar we kunnen wel met enige zekerheid zeggen dat het hier om een niet te onderschatten werklast gaat.[324] Deze werklast wordt nog verhoogd door de tekst van deze machtigingen zelf. Hoewel de machtigingen verleend door het sectoraal comité een gelijkaardig stramien volgen, zien we dat het dispositief van deze machtigingen voor het doeleinde en de voorwaarden steeds naar de tekst van de beraadslaging verwijzen. Ook de teksten volgen een herkenbaar patroon, maar zijn onderling te verschillend om zonder aandachtige lezing in een systeem voor audit trails opgenomen te worden. De machtigingen bij koninklijk besluit gaan echter nog veel verder. Die teksten stammen immers uit een tijd waar er nog veel restrictiever omgegaan werd met het verlenen van zulke machtigingen en worden daarom gekenmerkt door hun wel zeer omslachtige formuleringen. De ingewikkelde constructies die men in deze besluiten moest opnemen om tot het verlenen van een machtiging te komen, laten zich dus niet zonder meer vertalen in een systeem dat deze machtigingen op gestructureerd geordende wijze wil opnemen in een gegevensbank.[325]

EEN MOEIZAME SAMENWERKING - VAN ALLEENSTAAND PROBLEEM … - Een tweede punt dat de oprichting van het Kadaster van Verbindingen in de praktijk enigszins kan bemoeilijken, is de samenwerking tussen de verschillende overheidsdiensten. Zoals we al aangaven, zullen al de verschillende diensten met betrekking tot de gegevens die zij bewaren een log moeten bijhouden van enerzijds de door hen verleende machtigingen tot verwerking van die gegevens, en anderzijds van de gegevenskoppelingen en verwerkingen die plaatsgevonden hebben. Uiteraard vereist dit een zekere graad van samenwerking tussen de verschillende overheidsdiensten. Als we kijken naar het voorbeeld van 'MijnDossier', zagen we al dat er gebruik gemaakt wordt van een vooraf be-

---

[324] Ter illustratie: In alleen al de editie van 19 december 1986 van het Staatsblad vinden we zeven koninklijke besluiten tot machtiging tot het gebruik van het Rijksregisternummer terug. Een korte raadpleging van de wetgevingsdatabank Juridat brengt ons op ongeveer 150 machtigingen bij koninklijk besluit en dit is allicht geen volledige lijst. Daar moeten vervolgens nog de machtigingen door het sectoraal comité bijgeteld worden. Voor enkel het jaar 2008 maakt het jaarverslag van de Commissie voor de bescherming van de persoonlijke levenssfeer melding van 56 aanvragen waarover het sectoraal comité voor het Rijksregister beraadslaagd heeft. Voor het precieze aantal effectief verleende machtigingen is echter een analyse van elk van deze 56 dossiers vereist. De lijst opgesteld door Dirk De Bot biedt allicht het meest complete overzicht. De vraag is dan of deze lijst aanvaarden kan worden of niet. D.DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 427-463.

[325] Een mooi voorbeeld: Koninklijk besluit van 5 december 1986 tot regeling van de toegang tot de informatiegegevens en van het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen in hoofde van instellingen die, in het kader van de wetgeving betreffende de ziekte- en invaliditeitsverzekering, opdrachten van algemeen belang vervullen, *B.S.* 19 december 1986, 17351.

paalde lijst met mogelijke transacties. Wanneer bijvoorbeeld de Kruispuntbank van de Sociale Zekerheid het Rijksregister consulteert, zal de verwerkende ambtenaar uit die lijst de optie kiezen die het meest aansluit bij de transactie in kwestie. We zagen ook dat het gebruik van het Kadaster maar kan bijdragen tot het verhogen van de transparantie van de verwerking van persoonsgegevens indien in de beheerders van de binnen dit portaal aangeboden logs de door hen gebruikte lijsten met de nodige zorg opstellen. Zo zal er voldoende aandacht moeten worden besteed aan de identificatie van de verantwoordelijke voor de verwerking en aan het specificeren van de reden voor de verwerking. Om zulke lijst voldoende specifiek te maken, zal men echter de betrokken instanties moeten raadplegen. In het kader van 'MijnDossier' betekent dit dan dat het Rijksregister alle organisaties en personen die voor hun verwerkingen gebruik maken van het Rijksregister of het Rijksregisternummer zal moeten aanspreken om een op de noden van die organisatie of persoon afgestemde lijst op te stellen. De betrokken overheidsdienst moet dan wel bereid gevonden worden om zulke lijst op te stellen.

Een moeizame samenwerking - … tot structureel probleem - Indien echter verschillende overheidsdiensten los van elkaar gelijkaardige initiatieven beginnen te ontwikkelen, kunnen er problemen ontstaan in verband met de interoperabiliteit van deze initiatieven. Het risico bestaat dan dat elk systeem een voor dat systeem specifieke lijst wil hanteren, wat betekent dat de betrokken overheidsdiensten voor al die initiatieven een aparte lijst zouden moeten opstellen. Uiteraard gaan zij hier niet toe bereid gevonden worden. Net zoals tegenover de burger het principe van de eenmalige gegevensinzameling gehanteerd wordt, zullen ook de betrokken overheidsdiensten zulke lijst slechts eenmalig willen opstellen voor gebruik door andere overheidsdiensten in hun logs. Het spreekt voor zich dat er hier dus een duidelijke nood is aan enige interoperabiliteit. Op die manier zou elke verantwoordelijke voor de verwerking slechts een enkele lijst moeten opstellen met de door die organisatie of persoon meest uitgevoerde transacties. Die lijst zou dan door alle overheidsdiensten die een audit trail bijhouden gebruikt moeten worden. Hoewel dit het probleem van conflicten tussen de logs van verschillende overheidsdiensten kan vermijden en de algemene last van de oprichting van het Kadaster van Verbindingen kan reduceren, zien we dat ook deze interoperabiliteit niet gemakkelijk te bereiken zal zijn. Er moeten immers afspraken gemaakt worden tot het vastleggen van bepaalde standaarden. Bepaalde diensten zouden dan voor hen nieuwe standaarden opgedrongen kunnen krijgen. Andere diensten die al logs bijhouden en die de burger al een gestructureerde inzage in deze logs aanbieden, zullen hun systeem misschien moeten aanpassen aan die nieuwe standaarden. De onderhandelingen om tot de hier voorgestelde interoperabiliteit te komen, zullen daarom wellicht lang en moeizaam zijn. We kunnen daarom aanbevelen dat het wettelijk kader – dat zoals we al zagen in ieder geval nodig zal zijn voor het functioneren van het Kadaster van Verbindingen – deze problematiek opvangt. Dit kader kan – door middel van een samenwerkingsakkoord – de betrokken partijen verplichten tot medewerking aan dit systeem. Verder kan zulk wettelijk kader de koning de bevoegdheid verlenen tot het bepalen van de benodigde standaarden. Dit zou de hier aangehaalde gevaren van de onderhandelingen tussen de betrokken overheidsdiensten al enigszins kunnen opvangen.

Interoperabiliteit en integratie in bestaande systemen - We zagen ook dat er tussen de actoren in het systeem voor gedecentraliseerde opslag van de logs een aantal afspraken gemaakt zullen moeten worden. Hoewel de verantwoordelijkheden en de aansprakelijkheid van de actoren grotendeels gedicteerd wordt door de rol die zij binnen het systeem waarnemen, zagen we dat er aan de betrokken actoren voldoende ruimte gelaten moet worden om zelf hun taak binnen het geheel in te vullen. Dit leidt er echter toe dat het dan ook hier geen sinecure zal zijn om de verschillende overheidsdiensten op dezelfde lijn te krijgen. Het lijkt ons daarom aangewezen om het gegevensspoor zoveel mogelijk binnen bestaande platformen – waar overheidsdiensten al tot overeenstemming gekomen zijn – op te richten.[326] Op die manier kan men al een aantal structurele onenigheden vermijden en zullen de betrokken partijen enkel nog tot overeenstemming moeten komen met betrekking tot de precieze details van het project. Door het gegevensspoor zoveel mogelijk te integreren binnen bestaande platformen, kan men ook vermijden dat de overheidsdiensten die al initiatieven ondernomen hebben tot de invoer van een gegevensspoor de door hen geleverde inspanningen verloren zien gaan. Er zal dan immers maar zo weinig mogelijk overgestapt moeten worden op nieuwe platformen. Hoewel dit de initiële oprichting van het Kadaster kan vereenvoudigen, is deze oplossing moeilijker op lange termijn te verdedigen. De integratie in bestaande systemen kan er immers toe leiden dat de burger geen volledig beeld krijgt van wat er nu precies aan de gang is. Op termijn zal men daarom nood hebben aan een *de facto* standaard, of aan een integrator die ermee belast wordt om de nodige interoperabiliteit te voorzien. Een dergelijke *de facto* standaard zou dan bestaan uit een centraal platform op federaal vlak. Ook hier zou men kunnen denken aan het uitbreiden van een bestaand platform zoals 'MijnDossier' als alternatief voor de creatie van een geheel nieuw platform.

INTEGRATIE IN BESTAANDE SYSTEMEN EN HET EX ANTE REGISTER - Ook in verband met het probleem van het opsporen en analyseren van de machtigingen die al verleend zijn voor opname in het *ex ante* register, kan de integratie van het Kadaster van Verbindingen binnen bestaande platformen tot initiële voordelen leiden. Wanneer bijvoorbeeld een instelling in de sociale zekerheidssector ooit een machtiging tot het gebruik van het Rijksregisternummer verkregen heeft, is het mogelijk dat die machtiging al in die sector opgenomen is in een register.[327] Dankzij de interoperabiliteit zou die machtiging dan doorgegeven kunnen worden aan het *ex ante* register bij het Rijksregister. Indien die machtiging al opgesteld is in een formaat dat geschikt is voor gebruik in een portaal dat de inzage van zulke machtigingen door de burger mogelijk maakt, dan zal deze machtiging dus niet opnieuw handmatig moeten worden ingevoerd.

INTEGRATIE IN BESTAANDE SYSTEMEN – PRAKTIJKVOORBEELD - Wat de realisatie van het Kadaster van Verbindingen betreft, moeten we uiteraard verwijzen naar de bestaande toepassing 'MijnDossier' binnen de structuur van het Rijksregister. Deze toepassing omvat immers al een platform waar de burger – na authenticatie door middel van zijn e-ID – toegang kan krijgen tot onder meer een gestructureerd overzicht van wie er om welke reden zijn gegevens in het Rijksregister geraadpleegd heeft gedurende de laatste zes maanden. Een dergelijk bestaand platform zou daarom uitgebreid kunnen worden om de burger ook een overzicht te bieden van de gegevenskoppelingen die gemaakt werden door gebruik te maken van zijn Rijksregisternummer. Voor het bereiken van effectieve transparantie zal het immers al een belangrijke stap zijn indien de verantwoordelijken voor de verwerkingen van persoonsgegevens en iedere betrokken tussenpersoon – of dienstenintegrator – een publiek toegankelijk overzicht kan bieden van de gegevensuitwisselingen die hij uitvoerde met derde partijen die gemachtigd zijn om het Rijksregisternummer te gebruiken en van de precieze persoonsgegevens die daarbij uitgewisseld werden. Een dergelijk overzicht zou door iedere verantwoordelijke voor de verwerking van persoonsge-

[326] Denk bijvoorbeeld aan eBirth, dat geïntegreerd wordt binnen de structuur van het bestaande eHealth platform op initiatief van Fedict.
[327] Hiermee bedoelen we een zogenaamd "Policy Information Point", zoals gebruikt in een generiek policytoepassingsmodel.

gevens binnen de kortst mogelijke tijd gepubliceerd moeten worden om op die manier de realisatie van effectieve transparantie niet afhankelijk te laten worden van de uitbouw van een centraal platform zoals hier voorgesteld wordt.

PRAKTISCHE PROBLEMEN – EX TUNC LOGGINGS - We kunnen voor dit deel concluderen dat de invoer van het Kadaster van Verbindingen in de praktijk nog op een aantal problemen kan stoten. Het opzetten van de *ex post* logging van de transacties en het opleggen van een vaste structuur voor de machtigingen met het oog op de geautomatiseerde invoer van deze machtigingen in het *ex ante* register, zouden niet voor noemenswaardige problemen mogen zorgen. De technieken voor zulke systemen zijn immers al beschikbaar en er bestaan binnen de overheidscontext al gelijkaardige initiatieven. Het invoeren van al de vroeger verleende machtigingen in een gestructureerde gegevensbank, zal echter voor een aantal problemen zorgen. Allereerst laten die machtigingen zich niet automatisch invoeren in het voorgestelde systeem en is er dus nood aan een handmatige analyse en invoer. Daarnaast zijn die machtigingen niet systematisch geordend, wat wil zeggen dat al de nog geldende machtigingen eerst in kaart gebracht zullen moeten worden. Dit leidt tot een zekere werklast die de totale kostprijs van het systeem uiteraard niet ten goede zal komen. Om de omvang van dit probleem beter in te kunnen schatten, werd er een apart onderzoek gevoerd waarbij er allereerst getracht werd om een standaardformaat voor toekomstige machtigingen te ontwikkelen. Vervolgens werd er getracht om een aantal vroeger verleende machtigingen – zowel bij koninklijk besluit als door het sectoraal comité – om te zetten naar dit standaardformaat. De resultaten van dat onderzoek zijn toegevoegd als bijlage 1 bij dit rapport.

PRAKTISCHE PROBLEMEN – SAMENWERKING TUSSEN DE OVERHEIDSDIENSTEN - Een tweede punt dat voor praktische problemen kan leiden, is de samenwerking tussen de verschillende overheidsdiensten. Hier zien we dat er zeker een nood is aan voldoende interoperabiliteit – bijvoorbeeld door het gebruik van gemeenschappelijke standaarden – om te verzekeren dat de verschillende overheidsdiensten voldoende en op effectieve wijze met elkaar kunnen samenwerken. Om deze samenwerking enigszins te vergemakkelijken, kan men proberen om het Kadaster van Verbindingen initieel zoveel mogelijk te integreren in bestaande platformen. Over bestaande systemen bestaan immers al akkoorden, wat er toe leidt dat men dan enkel nog met betrekking tot een aantal details tot een overeenstemming zal moeten komen. Dit zal zeker de uitvoering van het Kadaster van Verbindingen vergemakkelijken en zorgt ervoor dat het bereiken van effectieve transparantie niet afhankelijk wordt van het bereiken van een akkoord over de oprichting van het centrale gebruikersplatform dat hier als einddoel vooropgesteld wordt. Ook wat het uiteindelijke centrale platform betreft, kunnen we de uitbreiding van een bestaande toepassing zoals 'MijnDossier' voorstellen. Hiermee vermijdt men de kosten die gepaard zouden gaan met de oprichting van een geheel nieuw platform.

3.6. DE OMVANG VAN HET KADASTER

KUNNEN DE INDIVIDUELE OVERHEIDSDIENSTEN VOLSTAAN … - In dit deel wensen we dieper in te gaan op wat de precieze omvang van het Kadaster van Verbindingen moet worden. In het voorgaande hadden we het immers over een bijhouden van logs op het niveau van een individuele overheidsdienst, zoals de toepassing 'MijnDossier' toegang biedt tot logs bijgehouden bij het Rijksregister. Deze toepassing werd opgericht binnen die bepaalde overheidsdienst en richt zich dan ook enkel op de transacties met betrekking tot de persoonsgegevens in het Rijksregister en het gebruik van het Rijksregisternummer. Men kan door middel van deze toepassing wel te weten komen welke organisatie of persoon de vermelde transacties uitvoerde, maar daarmee weet de burger niet of dit het volledige gegevensspoor is. Hij zal dan moeten kijken of de organisatie of persoon die verantwoordelijk was voor een bepaalde transactie ook zulk systeem bijhoudt, om daar te gaan kijken of er nog andere organisaties of personen betrokken zijn bij dit gegevensspoor. Om op deze manier het gegevensspoor werkelijk van het begin tot het einde van de gegevenskoppeling te kunnen volgen, zou minstens elke betrokken overheidsdienst een gelijkaardige toepassing moeten hanteren. De vraag is dan of het aan de burger inzage bieden in de logs die op het niveau van de individuele overheidsdienst bijgehouden worden werkelijk kan volstaan voor het bereiken van het 'end-to-end' gegevensspoor of dat er nood is aan meer.

... OF IS ER NOOD AAN ENIGE CENTRALISATIE? - In het voorgaande haalden we al aan dat het voor de verschillende overheidsdiensten nodig is dat er binnen de overheidscontext een zekere graad van interoperabiliteit bereikt wordt. Ook de overheidsdiensten zelf zullen immers niet bereid gevonden worden om dezelfde informatie meermaals aan verschillende instanties door te geven en zullen willen dat een aantal zaken – zoals het opstellen van een lijst met meest frequent voorkomende transacties – slechts eenmalig uitgevoerd moeten worden, om deze vervolgens door al de verschillende overheidsdiensten te laten gebruiken. Die interoperabiliteit kan op zich bereikt worden door het gebruik van afgesproken standaarden binnen de overheidssector en door het Kadaster van Verbindingen zoveel mogelijk te integreren in bestaande platformen. Anderzijds zou men ook kunnen denken aan een zekere graad van centralisatie binnen het systeem van gedecentraliseerde opslag van de logs. Men zou dan de eigenlijke logs kunnen laten beheren door de verschillende overheidsdiensten zelf, met een rol voor de Commissie voor de bescherming van de persoonlijke levenssfeer als algemeen beheerder van dergelijke logs. Zij dienen dan als bronsysteem in het systeem. De bestaande dienstenintegratoren zoals de Kruispuntbank van de Sociale Zekerheid kunnen dan dienen als tussenpersonen. Als doelsysteem kunnen we denken aan een gecentraliseerde toepassing onder de hoede van het sectoraal comité van het Rijksregister. Op die manier worden de logs niet centraal bewaard – wat zoals we al zagen belangrijk is voor de privacybescherming – en is er toch een centrale instantie die kan instaan voor een werkelijk en volledig 'end-to-end' gegevensspoor. We haalden al eerder aan dat het Kadaster van Verbindingen zulk centraal portaal kan worden dat de burger op gestructureerde wijze inzage verschaft in de logs die gedecentraliseerd bijgehouden worden door de betrokken overheidsdiensten.

VOORDELEN VAN EEN CENTRALE INSTANTIE - Die centrale instantie kan ervoor zorgen dat het systeem naar de burger toe gepresenteerd wordt als een coherent geheel, terwijl er voor de individuele overheidsdiensten toch nog enige ruimte blijft om hun registers en loggings naar eigen wens – maar indachtig de voor het systeem afgesproken standaarden – te organiseren. Door het gebruik van een centraal doelsysteem kan men immers de bronsystemen relatief vrij laten in de ontwikkeling van hun eigen aandeel in het gegevensspoor. Dit is nodig voor bepaalde authentieke bronnen die nood hebben aan strengere regels, bijvoorbeeld om te zorgen dat het geheim van een onderzoek gerespecteerd wordt. Zoals we zagen zullen de tussenpersonen ervoor zorgen dat de bronsystemen de identificaties en authenticaties verkrijgen die zij vereisen. Een centraal doelsysteem zou bijgevolg zowel voor de burger als voor de betrokken overheidsdiensten zelf een interessantere keuze kunnen zijn dan een systeem waarbij alle overheidsdiensten er relatief los van elkaar aparte toepassingen op na houden.

PRAKTIJKVOORBEELD - We kunnen dit illustreren met een eenvoudig voorbeeld. Bij het openen van een bankrekening zal de bank een aantal persoonsgegevens van deze klant willen bewaren. De elektronische identiteitskaart wordt uitgelezen waardoor – zoals uitvoerig behandeld in deel I van dit project – ook het Rijksregisternummer van de klant wordt meegegeven. Nu de bank over het Rijksregisternummer van de klant beschikt, kan zij dit nummer hanteren als identificatienummer voor die persoon en kan zij dit nummer gebruiken voor gegevenskoppelingen met betrekking tot deze persoon. De klant zal dan willen weten wat de bank met zijn Rijksregisternummer kan doen. Het gebruik van dit nummer is immers niet vrij en elk gebruik van dit nummer door de bank zonder voorafgaande machtiging door het sectoraal comité van het Rijksregister, zal bijgevolg in principe onrechtmatig zijn. Via de toepassing 'MijnDossier' kan de burger wel nakijken of de bank iets met zijn gegevens in het Rijksregister gedaan heeft, maar daar houdt het dan ook wel bij op. Om een werkelijk 'end-to-end' gegevensspoor te bereiken, zal dit dus niet voldoende zijn.[328] Er wordt immers enkel melding gemaakt van de verbindingen tussen de bank en het Rijksregister en niet van de koppelingen die de bank met andere organisaties uitvoert op basis van het Rijksregisternummer. Aangezien er hier dus geen sprake is van een werkelijk en volledig 'end-to-end' gegevensspoor, kunnen we besluiten dat een systeem waarbij de verschillende overheidsdiensten elk hun eigen gegevensspoor hanteren niet kan volstaan. Er is dus nood aan een zekere centralisatie op het vlak van de presentatie van het gehele gegevensspoor aan de burger. Een centraal doelsysteem onder de hoede van het sectoraal comité van het Rijksregister zou hier geschikt voor kunnen zijn.

OOK IN DE PRIVATE SECTOR? - Het voorgaande handelde voornamelijk over de omvang van een portaal voor de presentatie van het gegevensspoor binnen de overheidscontext. Met het voorbeeld van de bank haalden we echter al aan dat inzage in een gegevensspoor ook in de private sector ingang zou kunnen vinden. Het is niet het doel van dit project om een volledige analyse te maken over de mogelijkheidsvoorwaarden van het gebruik van het audit trail binnen de private sector. We wensen echter wel aan te stippen dat zulk onderzoek nodig zal zijn als gevolg van het veralgemeend gebruik van het Rijksregisternummer dat al een tijd aan de gang is binnen de overheidssector en zich zou kunnen uitbreiden tot de private sector. Wat private initiatieven tot het gebruik van een vorm van audit trail betreft, kunnen we verwijzen naar de bespreking onder hoofdstuk 2.4.1.

3.7. CONCLUSIE

EEN GEDECENTRALISEERD OPGERICHT SYSTEEM - Onder dit hoofdstuk hebben we getracht een antwoord te bieden op een aantal vragen met betrekking tot de juridische, organisatorische en technische problemen die zich zouden kunnen stellen wanneer men het Kadaster van Verbindingen in de praktijk wil brengen. We hebben ons allereerst afgevraagd op welk niveau we ons het Kadaster moeten voorstellen. Uit dat onderzoek bleek dat het ten behoeve van de privacybescherming niet aan te raden is om de gegevens uit de logs centraal te bewaren. Een systeem waarbij er een centraal logboek bijgehouden wordt waar alle overheidsdiensten de gegevens met betrekking tot hun logs bewaren, moet bijgevolg vermeden worden. We gaven daarom de

[328] Merk op dat we bestaande initiatieven als 'MijnDossier' zeker kunnen aanbevelen als vertrekpunt bij de uitbouw van de hier voorgestelde structuur. Hierdoor zal het bereiken van effectieve transparantie niet afhankelijk moeten worden van de praktische realisatie van een centraal platform. Als langetermijndoelstelling stellen we echter wel de realisatie van een centraal platform voorop.

voorkeur aan een gedecentraliseerd systeem, waarbij de verschillende overheidsdiensten elk hun eigen logs bijhouden.[329] Omdat deze aanpak leidt tot een gegevensopslag op een veel kleinere schaal rijzen er minder problemen op het gebied van de privacybescherming en de organisatie van zulk systeem. We concludeerden daarom dat een gecentraliseerde gegevensopslag enkel een optie zou mogen zijn indien de gedecentraliseerde opslag van de logs – met eventuele doorgifte zonder opslag op centraal vlak – niet op redelijke wijze haalbaar is. Het Kadaster van Verbindingen binnen de overheidscontext zal dus moeten steunen op gegevens die in gedecentraliseerde gegevensbanken bewaard worden. Dit zal de meest interessante optie vormen voor zowel de burger als voor de betrokken overheidsdiensten zelf. Wat de burger betreft merkten we in dit stadium wel al op dat er voldoende aandacht zal moeten worden besteed aan de samenwerking tussen de verschillende overheidsdiensten. De logs die zij bijhouden zullen dan enigszins op elkaar afgestemd moeten worden. Onderlinge compatibiliteit en samenhang zullen immers nodig zijn om de burger een volledige reconstructie van het 'end-to-end' audit trail aan te bieden.

ACTOREN MET DUIDELIJK AFGEBAKENDE TAKEN EN VERANTWOORDELIJKHEDEN - DOELSYSTEMEN - Om een beter beeld te krijgen van hoe we ons zulk gedecentraliseerd systeem moeten voorstellen, hebben we eerst een onderzoek gevoerd naar de betrokken actoren. We zagen dat de burger zijn vraag tot consultatie van een gegevensspoor zal richten tot de front office actoren, ook de doelsystemen genaamd. Deze zullen de aanvraag van de burger verwerken en zullen de benodigde gegevens opvragen bij de betrokken overheidsdiensten. Wanneer zij de opgevraagde gegevens ontvangen, zullen zij deze verwerken en het resultaat aan de burger presenteren. Net omdat zij omgaan met de aanvrager van de consultatie van het gegevensspoor, zullen de doelsystemen een bijkomende verantwoordelijkheid dragen voor het naleven van een aantal principes – zoals finaliteit, proportionaliteit, en dergelijke – binnen de gehele procedure. Zij zullen ook de bewaartermijn en de eventuele verdere doorgifte van de verstrekte gegevens bepalen.

ACTOREN MET DUIDELIJK AFGEBAKENDE TAKEN EN VERANTWOORDELIJKHEDEN - BRONSYSTEMEN - De tegenpool van de front office actoren zijn uiteraard de back office actoren. Zoals we al zagen gaat het hier om de overheidsdiensten die logs bijhouden. Zij beschikken over de gegevens die nodig zijn voor de reconstructie en de consultatie van het gegevensspoor. De doelsystemen zullen de voor de aanvraag benodigde informatie dus moeten gaan opvragen bij deze bronsystemen. De back office actoren kunnen we aanduiden als authentieke bronnen. Zij staan garant voor de juistheid, de volledigheid en de actualiteit van de door hen bewaarde gegevens en zullen ook niet zonder meer vrije toegang tot deze gegevens willen verlenen. Daarnaast zien we ook dat het gevaarlijk wordt wanneer de bron- en doelsystemen te veel informatie over de precieze aanvraag met elkaar uitwisselen. Het consulteren en reconstrueren van het gegevensspoor is immers een verwerking van persoonsgegevens en zal dus moeten voldoen aan de regels van de privacybescherming. Net om de naleving van die regels te garanderen, besloten we dat er nood is aan een derde partij.

[329] Merk bovendien op dat de verschillende overheidsdiensten als gevolg van allerlei wettelijke verplichtingen op dit moment al vaak zulke logs zullen bijhouden. De publicatie van die logs kan dan vrijwel onmiddellijk plaatsvinden zonder bijkomende kost of werklast. Zulke publicatie van de logs die door de verschillende overheidsdiensten worden bijgehouden, kan al een belangrijke eerste stap vormen om tot effectieve transparantie te komen. Pas in een volgend stadium zullen deze logs geïntegreerd worden in bestaande gebruikerstoepassingen om uiteindelijk geïntegreerd te worden in een centraal platform, wat het einddoel van het Kadaster van Verbindingen is.

ACTOREN MET DUIDELIJK AFGEBAKENDE TAKEN EN VERANTWOORDELIJKHEDEN - TUSSENPERSONEN - De derde partij in dit systeem zou een neutrale tussenpersoon – ook wel genaamd 'de vertrouwde derde partij' – moeten vormen tussen de bron- en doelsystemen. De tussenpersoon is dan een doorgeefluik van informatie tussen deze actoren en kan ook instaan voor een afdoende identificatie en authenticatie van beide partijen tegenover elkaar. Belangrijk is dat deze tussenpersonen zelf geen inhoudelijke gegevens zullen bewaren en dat zij er over waken dat enkel de voor de verwerking strikt noodzakelijke gegevens doorgegeven worden. Zij dragen daarom een belangrijke verantwoordelijkheid tegenover de andere partijen. Binnen de overheidscontext kunnen de dienstenintegratoren als het ideale voorbeeld van een vertrouwde derde partij beschouwd worden. Vervolgens zagen we dat er tussen deze drie partijen voldoende afspraken tot samenwerking gemaakt zullen moeten worden. Zo zullen er afspraken gemaakt moeten worden met betrekking tot de taakverdeling, de aansprakelijkheid, de garanties die de betrokken partijen aan elkaar moeten bieden, en dergelijke. Wat deze afspraken betreft concludeerden we dat het belangrijk is dat de partijen enigszins vrij gelaten worden om deze afspraken onderling te regelen. Daarbij mag niet vergeten worden dat de aansprakelijkheid van de tussenpersonen zoveel mogelijk beperkt moet blijven en dat de front office actoren bijkomende verantwoordelijkheden voor de degelijke werking van het gegevensspoor dragen. Tot slot zagen we dat er ook een aantal afspraken gemaakt moeten worden in verband met de organisatie van de samenwerking tussen deze actoren. Enerzijds is er de nood aan een systeem dat de actoren toestaat zich op betrouwbare wijze tegenover elkaar te identificeren en authentiseren, waarmee gegevens veilig uitgewisseld kunnen worden en dat de burger in staat stelt om het gehele gegevensspoor te reconstrueren. Anderzijds is er ook nood aan een wettelijk kader dat een basis voor deze samenwerking kan vastleggen.

EEN FEDERATIE OP BASIS VAN VERTROUWENSKRINGEN - Voor het systeem dat zorgt voor een veilige identificatie, authenticatie en gegevensoverdracht kunnen we denken aan het gefedereerd systeem op basis van vertrouwenskringen. Het gebruik van zulke federatie binnen het hier voorgestelde systeem kan er door middel van het gebruikers- en toegangsbeheer voor zorgen dat de betrokken actoren slechts die gegevens te zien krijgen die strikt noodzakelijk zijn voor de uitvoering van hun taak binnen het geheel. Op die manier kan men er voor zorgen dat onder meer het proportionaliteitsprincipe gehandhaafd blijft en dat men de burger toch nog in staat kan stellen om het volledige gegevensspoor in te kijken. We merkten ook op dat dankzij het gefedereerd systeem de identiteit van de verwerkende ambtenaar bewaard kan worden; maar dat die identiteit aanvankelijk afgeschermd zal worden van de gebruikers. Enkel in het geval van betrokkenheid bij een onrechtmatige verwerking van persoonsgegevens zal de identiteit aan de bevoegde instanties vrijgegeven worden.

EEN DUIDELIJK OMLIJND WETTELIJK KADER - Wat het wettelijk kader betreft zagen we dat er onder de huidige stand van het recht geen juridisch kader is dat we volledig kunnen toepassen op de hier voorgestelde figuur van het Kadaster van Verbindingen. We zagen immers dat het kader voor de figuur van de vertrouwenspersoon – onder meer – niet geschikt is voor gebruik in de overheidscontext. Het wettelijk kader voor het gedecentraliseerd systeem voor de inzage van loggings binnen de overheidscontext zou in de eerste plaats moeten verwijzen naar een aantal andere wettelijke bepalingen, zoals de privacywetgeving en de wetgeving in verband met de beginselen van behoorlijk bestuur en openbaar bestuur. Men zal immers willen voorkomen dat deze bepalingen en de taken van de partijen – of de afspraken tussen de partijen – binnen het systeem met elkaar in conflict komen. Verder zal het wettelijk kader de betrokken actoren moeten identificeren en een aantal basisprincipes – zoals de taken en verantwoordelijkheden van deze partijen – moeten vastleggen, maar dat er anderzijds toch nog voldoende ruimte aan de betrokken actoren gelaten moet worden tot het sluiten van onderlinge overeenkomsten. Er zal immers rekening gehouden moeten worden met de specifieke bijzonderheden van een aantal authentieke bronnen. Wat betreft het niveau waarop zulk wettelijk kader aangenomen zou moeten worden, dachten we binnen de Belgische context aan het federaal niveau. Op deze manier kunnen alle overheidsdiensten en –niveaus verplicht worden mee te werken aan het project. Een werkelijk 'end-to-end' gegevensspoor zal immers de betrokkenheid van alle overheidsdiensten vereisen. Om zulke betrokkenheid te garanderen kan men gebruik maken van een samenwerkingsakkoord tussen de betrokken overheden. Wat betreft het beheer van de logs waar het het Kadaster van Verbindingen inzicht in zal verschaffen, zagen we dat de betrokken actoren al elk hun eigen verantwoordelijkheden voor hun aandeel in de procedure dragen. Daarnaast dragen de front office actoren een bijkomende verantwoordelijkheid met betrekking tot de goede werking van het 'end-to-end' gegevensspoor. De vraag is dan of dit kan volstaan of dat er nood is aan een aparte en onafhankelijke beheerder. Uit het onderzoek naar de verantwoordelijkheden van de betrokken actoren blijkt dat deze verantwoordelijkheden – vastgelegd door middel van onderlinge overeenkomsten – al een zekere controle kunnen uitoefenen op de werking van het systeem, maar dat zulke controle geen voldoende garantie kan bieden op de effectieve werking van het geheel. Daarom lijkt het meer opportuun om een controlefunctie te geven aan de centrale privacycommissie als algemeen beheerder van de logs. Er zal dan geen nood zijn aan een nieuwe instantie als controleorgaan. De Commissie kan deze *ex post* controle uitoefenen op grond van haar bevoegdheden krachtens artikel 32 van de Privacywet. Bijkomende specificaties met betrekking tot de precieze omvang van de controle door de Commissie, kan geregeld worden binnen het algemeen wettelijk kader voor het Kadaster van Verbindingen. Voor het beheer van het Kadaster van Verbindingen als centraal portaal zelf denken we – op grond van artikel 8 van de Wet op het Rijksregister – aan het sectoraal comité van het Rijksregister.

PRAKTISCHE MOEILIJKHEDEN - Naast het voorgaande theoretisch onderzoek hebben we het Kadaster van Verbindingen ook vanuit een meer praktische ooghoek bekeken. Uit dit onderzoek bleek dat er een aantal problemen zijn wanneer we het Kadaster in de praktijk zouden willen toepassen. Wat de *ex post* loggings betreft zagen we dat er relatief weinig problemen rijzen. De techniek hiertoe bestaat al en een aantal overheidsdiensten kennen al gelijkaardige systemen. Wat het *ex ante* register van de verleende machtigingen tot verwerking en gegevenskoppeling betreft, stoten we echter op een aantal problemen. Allereerst zal men voor de toekomstige machtigingen een standaard moeten afspreken die toelaat om deze machtigingen op quasi-geautomatiseerde wijze op te nemen in het register. Wat de vroeger verleende machtigingen betreft, zien we dat men deze bij gebrek aan een officiële geordende publicatie eerst in kaart zal moeten brengen. Verder zal men deze machtigingen – en dan voornamelijk de machtigingen bij koninklijk besluit – handmatig moeten analyseren en invoeren, wat een niet te onderschatten werklast met zich meebrengt. Daarnaast zien we dat de eerder besproken samenwerking tussen de verschillende overheidsdiensten ook nog een zekere moeilijkheidsgraad met zich mee kan brengen. Zo zal men immers een bepaalde graad van interoperabiliteit tussen de logs van de verschillende overheidsdiensten moeten bereiken, onder meer door een aantal standaarden af te spreken. Om deze interoperabiliteit gemakkelijker te bereiken, lijkt het ons aanbevelingswaardig om het Kadaster initieel waar mogelijk te integreren in bestaande systemen, daar er over die bestaande systemen al akkoorden bereikt zijn. Op die manier vermijdt men ook dat diensten die al dergelijke initiatieven genomen hebben hun inspanningen verloren zien gaan. Men vermijdt op deze manier ook dat het bereiken van effectieve transparantie afhankelijk gesteld wordt van het bereiken van een akkoord over het oprichten van een centraal platform. Wanneer de verschillende overheidsdiensten de logs die zij bijhouden publiceren en deze integreren in toepassingen zoals 'MijnDossier', is er immers al een belangrijke eerste stap genomen in de richting van het bereiken van effectieve transparantie. Op termijn zal men hier echter wel voor een meer definitieve oplossing moeten zorgen, zoals bijvoorbeeld de uitbreiding van een bestaande toepassing zoals 'MijnDossier' tot een centraal platform op federaal niveau.

SAMENWERKING EN COMPATIBILITEIT - Tot slot werd er dieper ingegaan op de precieze omvang van het Kadaster van Verbindingen. Uit eerder onderzoek bleek al dat het doel van het Kadaster er in bestaat dat de burger het volledige 'end-to-end' gegevensspoor moet kunnen traceren. Wanneer iedere overheidsdienst er een eigen log op na houdt en er geen sprake is van samenwerking tussen deze verschillende diensten, dan kan het moeilijk worden om dat doel te bereiken. Hoewel we het al eerder aanhaalden, wensen we daarom andermaal te benadrukken dat er een duidelijke nood is aan samenwerking en compatibiliteit tussen de verschillende overheidsdiensten. In dit opzicht kunnen we dan de overheidsdiensten die de logs bijhouden aanduiden als back office actoren. De dienstenintegratoren – de Belgische Kruispuntbanken – zijn dan de geschikte tussenpersonen. Als doelsysteem stellen we een centraliseerde toepassing voor, waar de burger op één plaats inzage kan krijgen in het gehele gegevensspoor. Zulke gecentraliseerde toepassing zou dan onder de hoede kunnen komen te staan van het sectoraal comité van het Rijksregister, met een bijzondere rol voor de Commissie voor de bescherming van de persoonlijke levenssfeer als algemeen beheerder van de logs zelf.

NAAR CONCRETE AANBEVELINGEN - Het voorgaande illustreert het onderzoek naar hoe we ons het Kadaster van Verbindingen juridisch, organisatorisch en technisch zouden moeten voorstellen. In het volgend hoofdstuk zullen onze bevindingen samengevat worden in een aantal concrete en praktische aanbevelingen die een aanzet kunnen geven tot het oprichten van het Kadaster van Verbindingen.

4. CONCLUSIE

TERUGKOPPELING AAN DEEL I - In het eerste deel van dit project onderzochten we het veralgemeend gebruik van het Rijksregisternummer binnen de overheidscontext. Omdat we zagen dat het gebruik van dit nummer beschermd is en dat er tegen het gebruik van zulke nationale enkele unieke identificator toch nog een aantal opmerkingen in verband met de privacybescherming geuit kunnen worden, werd er daarom in dit tweede deel van het project dieper ingegaan op de problematiek van de gegevenskoppelingen die tot stand komen door middel van het gebruik van dat Rijksregisternummer. We stootten bij dit onderzoek op het Kadaster van Verbindingen. Omdat dit concept nergens gedefinieerd wordt, werd allereerst het begrip zelf onderzocht om vervolgens te onderzoeken of het mogelijk zou zijn om hiervoor een juridisch kader vast te leggen. Dit onderzoek zou dan moeten leiden tot praktische aanbevelingen die kunnen bijdragen tot de realisatie van het concept 'Kadaster van Verbindingen.' Gelet op het tijdsbestek van dit project werd geopteerd om voornamelijk een praktijkgerichte conceptstudie na te streven. Een volledig uitgewerkt en gedetailleerd projectplan zou binnen het kader van dit project immers onhaalbaar zijn. In deze conclusie worden eerst alle onderzoeksresultaten samengebracht om vervolgens tot de aangekondigde praktijkgerichte aanbevelingen te komen.

4.1. OVERZICHT VAN BEVINDINGEN

HET CONCEPT EN HET NUT VAN HET KADASTER VAN VERBINDINGEN - Zoals we al aangaven, werd er eerst een onderzoek gevoerd naar de precieze draagwijdte en de invulling van het concept ‘Kadaster van Verbindingen’. We vertrokken vanuit de vaststelling dat de loutere naleving van de bestaande principes op het gebied van privacybescherming vaak niet voldoende zijn om tot effectieve transparantie te leiden. Die effectieve transparantie zal nodig zijn omdat de burger beter op de hoogte gehouden zal willen worden van de mogelijke verwerkingen en gegevenskoppelingen die met betrekking tot zijn persoonsgegevens uitgevoerd worden. Een mogelijke manier om tot zulke transparantieverhoging te komen, is door middel van het kadaster van netwerkverbindingen uit de Wet op het Rijksregister. Dit kadaster kan de burger immers meer inspraak geven, wat leidt tot een verhoogde transparantie bij de verwerking van persoonsgegevens.

BEGRIPSMATIGE INVULLING - Het Kadaster van Verbindingen kan dus een belangrijk instrument worden voor het bereiken van effectieve transparantie. Toch lijkt dit begrip nergens verder uitgediept of gedefinieerd te worden. We hebben in deze studie daarom eerst getracht dit begrip verder af te bakenen en te definiëren. Zo merkten we allereerst op dat er hier twee opvatting bestaan. Men kan het Kadaster immers beschouwen als een platform dat de burger toegang biedt tot een *ex ante* register dat een overzicht biedt van de mogelijke verwerkingen en gegevenskoppelingen. Anderzijds kan het Kadaster toegang geven tot de loutere *ex post* loggings van de verwerkingen en gegevenskoppelingen die effectief hebben plaatsgevonden. We merkten op dat beide benaderingen nuttig kunnen zijn voor de verhoging van de transparantie van de verwerking naar de burger toe. Omdat beide benaderingen ook cumulatief toegepast kunnen worden, leek het ons de meest interessante optie om het Kadaster van Verbindingen te richten op zowel de *ex ante* als de *ex post* benadering. Dit sluit aan bij de parlementaire besprekingen van de wijzigingen aan de Wet op het Rijksregister uit 2003.

BELGISCH UNICUM - Hoewel het probleem van het gebrek aan effectieve transparantie zich zeker niet enkel in België stelt, bleek uit een rechtsvergelijkend onderzoek met een aantal andere Europese lidstaten dat België momenteel wel het enige land is dat het oprichten van een centraal portaal dat toegang biedt tot een register dat de gegevenskoppelingen door middel van bepaalde identificatienummers nastreeft. We merkten wel op dat als er enige vorm van een register van gegevenskoppelingen aanwezig is, het meestal gaat om een *ex post* logging. Een werkelijk *ex ante* register zoals hier voor België voorgesteld wordt kent geen buitenlandse equivalenten.

KADASTER EN AUDIT TRAIL - Na het afbakenen van het begrip ‘Kadaster van Verbindingen’, werd er onderzoek gevoerd naar de precieze invulling van dit concept. Om de problematiek van het registreren en loggen van verwerkingen van persoonsgegevens en gegevenskoppelingen beter te kunnen begrijpen, werd er gezocht naar praktijkvoorbeelden. We zijn daarom in de eerste plaats het begrip ‘audit trail’ gaan onderzoeken. In een later stadium zouden de conclusies met betrekking tot de invulling en de realisatie van het audit trail dan toegepast kunnen worden op de specifieke situatie van het Kadaster van Verbindingen binnen de context van gegevenskoppelingen door middel van het Rijksregisternummer. Het audit trail zou dan onder meer een overzicht bieden van het oneigenlijk gebruik van een informatiesysteem door een onbevoegd persoon, het verantwoordelijk stellen van bevoegde personen voor hun handelingen en dergelijke. Het verhogen van de effectieve transparantie naar de burger toe is hier dus nog steeds de belangrijkste doelstelling.

INHOUD - Na de begripsverruiming werd er gezocht naar de precieze inhoud van de logs waar het Kadaster van Verbindingen toegang toe wil bieden. We haalden hier aan dat het Kadaster in de eerste plaats een antwoord zou moeten bieden op de vraag: "Wie heeft er met betrekking tot welke van mijn persoonsgegevens welke verwerkingen of gegevenskoppelingen verricht, met welk doel en op welk moment?" Hoewel deze vraag in de context van het Kadaster haast intuïtief vanuit de *ex post* benadering geformuleerd wordt, zagen we dat dit ook een overzicht biedt van de gegevens die relevant zijn voor een *ex ante* register. Wat de *ex post* loggings betreft zagen we dat men hier ook voldoende aandacht moet schenken aan de bewijskracht van deze logs. Omdat de gegevens in de logs na het loggen immers niet gewijzigd of herroepen mogen worden, zien we dat men de oorsprong, de integriteit en de non-repudiation van de in de logs opgenomen gegevens kan proberen aan te tonen om de bewijskracht van deze logs te verzekeren. Dit kan men bereiken door ondermeer het gebruik van *timestamps*.

VERHULLEN VAN IDENTITEITSGEGEVENS - Een belangrijke *caveat* bij het loggen van verwerkingen van persoonsgegevens en gegevenskoppelingen is dat het loggen zelf een verwerking van persoonsgegevens is. Het loggen zelf zal daarom ook moeten voldoen aan de voorwaarden uit de wetgeving met betrekking tot de verwerking van persoonsgegevens. Van elke consultatie van de logs zal bijgevolg ook een log bijgehouden moeten worden. Net om te voldoen aan de proportionaliteitsregel uit deze wetgeving, zullen we bepaalde persoonsgegevens moeten weren uit de logs, of deze minstens verhullen. Het grootste probleem zien we bij het identificeren van de verantwoordelijke voor de verwerking. Enerzijds moet de organisatie die verantwoordelijk is voor de verwerking afdoende gespecificeerd worden. Identificatie op het niveau van de overkoepelende organisatie zal hierbij niet afdoende zijn. Men moet dus de werkelijke organisatie of suborganisatie aanduiden. Anderzijds mag deze specificatie niet te ver gaan. Zo kunnen we de identificatie op het niveau van de verantwoordelijke ambtenaar in kwestie in principe beschouwen als te verregaand voor het bereiken van het doel van het Kadaster van Verbindingen. Het Kadaster van Verbindingen – een middel om de transparantie van de verwerking van persoonsgegevens naar de burger toe te verhogen – zou dan een inbreuk maken op het recht op privacybescherming van die verantwoordelijke ambtenaar. Wanneer we de rechtspraak van het Europees Hof van de Rechten van de Mens volgen, zouden we er voor kunnen opteren om de identificatiegegevens van de betrokken ambtenaar niet zonder meer weg te laten uit de logs, maar om deze op beveiligde wijze af te schermen van de gebruikers van deze logs. Deze identiteitsgegevens zouden dan enkel vrijgegeven worden aan de bevoegde instanties in het geval van een onrechtmatige verwerking van persoonsgegevens of gegevenskoppeling. De verantwoordelijke ambtenaar wordt dan niet rechtstreeks geïdentificeerd, maar is indien nodig wel identificeerbaar.

BEWAREN VAN LOGS - Logs moeten uiteraard gedurende een bepaalde periode consulteerbaar zijn voor de betrokken partijen. Omdat het loggen zelf ook een verwerking van persoonsgegevens is, mogen deze logs echter niet langer bijgehouden worden dan strikt nodig is voor het bereiken van het doel van deze verwerking. We zagen dat er met betrekking tot deze materie allerlei mogelijke bewaartermijnen voorgesteld worden. Gelet op het doel van het loggen kozen we hier voor een bewaartermijn die gelijkloopt met de verjaringstermijn voor persoonlijke rechtsvorderingen uit artikel 2262bis van het Burgerlijk Wetboek. Logs zouden dan gedurende tien jaar moeten worden bewaard.

DECENTRALISATIE - Het voorgaande onderzoek hebben we vooral getracht het begrip 'Kadaster van Verbindingen' af te bakenen. Daarnaast hebben we ook getracht dit begrip enigszins in te vullen.

Na dit meer theoretisch onderzoek werd er gezocht naar hoe we het Kadaster van Verbindingen juridisch, organisatorisch en technisch moeten organiseren. Allereerst werd er onderzocht op welk niveau het Kadaster georganiseerd zou moeten worden. We besloten hier dat de logs best bij de individuele overheidsdiensten gedecentraliseerd bijgehouden worden. Een gecentraliseerde gegevensopslag zou immers allerlei organisatorische, juridische en technische problemen met zich meebrengen. Een systeem van gedecentraliseerd bewaarde logs zou deze problemen kunnen vermijden. Een belangrijke *caveat* hier is dat we er wel voor moeten zorgen dat de burger het volledige 'end-to-end' audit trail kan traceren. De verschillende overheidsdiensten zullen hun logs dus op elkaar moeten afstemmen. Interoperabiliteit is hier een belangrijk punt bij het verwezenlijken van het centrale portaal dat het Kadaster van Verbindingen zou moeten worden.

ACTOREN - Wat de betrokken actoren betreft onderscheiden we hier allereerst de front office actoren. Zij staan in rechtstreeks contact met de burger en behandelen bijgevolg de aanvraag tot consultatie van de logs. We kunnen de front office actoren bijgevolg aanduiden als de doelsystemen in het audit trail. De bronsystemen zijn dan de individuele overheidsdiensten die hun eigen gedecentraliseerde logs bijhouden, ook wel de back office actoren genoemd. Zij kunnen worden beschouwd als de authentieke bronnen en beschikken over de informatie die de front office actoren nodig hebben voor de verwerking van de aanvraag tot consultatie. Om ervoor te zorgen dat deze actoren voldoende tegenover elkaar geïdentificeerd en geauthentiseerd worden en om ervoor te zorgen dat er niet disproportioneel veel persoonsgegevens tussen beide actoren uitgewisseld worden, is er nog een derde groep actoren: de tussenpersonen. Deze tussenpersonen treden als vertrouwde derde partij op om de communicatie tussen de bron- en doelsystemen vlot te doen verlopen. In de overheidscontext kunnen we de dienstenintegratoren aanduiden als tussenpersonen. Om de samenwerking tussen deze actoren tot een goed einde te brengen, zullen er echter de nodige afspraken gemaakt moeten worden met betrekking tot de taakverdeling en de verdeling van de aansprakelijkheid. Hier merkten we op dat iedere partij haar eigen verantwoordelijkheid draagt binnen het geheel, maar dat de front office actoren een bijkomende verantwoordelijkheid dragen voor de goede werking van het 'end-to-end' gegevensspoor en dat de tussenpersonen – gelet op hun taak als neutrale derde partij – slechts een relatief beperkte aansprakelijkheid op zich mogen krijgen.

FEDERATIE OP BASIS VAN VERTROUWENSKRINGEN - Loutere afspraken zullen echter vaak niet voldoende zijn om de identificatie en authenticatie van de partijen tegenover elkaar voldoende te garanderen. Er zal dan nood zijn aan een systeem dat deze taak op voldoende betrouwbare en beveiligde wijze op zich kan nemen en dat kan zorgen voor een beveiligde gegevensuitwisseling tussen de betrokken actoren. We kunnen dan denken aan het gebruik van de federatie op basis van vertrouwenskringen binnen het hier geplande systeem. Dit systeem kan dan zorgen voor een veilige identificatie en authenticatie – bijvoorbeeld op basis van de e-ID – en regelt dus het gebruikers- en toegangsbeheer voor het audit trail. Ook het eerder aangehaalde verhullen van identiteitsgegevens of afschermen van bepaalde gegevens kan door gebruik van het gefedereerd systeem afgehandeld worden. Tot slot bekeken we een aantal standaarden die men in de praktijk toepast om zulke federatie in te stellen.

HET WETTELIJK KADER - Het gefedereerd systeem kan echter niet verhinderen dat er zich nog een aantal organisatorische problemen zullen voordoen bij het organiseren van het Kadaster van Verbindingen. We zoeken daarom naar een voor deze specifieke problematiek geschikt wettelijk kader dat een aantal van deze organisatorische problemen kan regelen. Er kunnen zich immers conflicten voordoen tussen de verschillende wettelijke bepalingen die op de actoren rusten, alsook tussen de wettelijke bepalingen en de samenwerkingsovereenkomsten tussen de actoren. Anderzijds mag dat kader ook weer geen al te grote afbreuk doen aan de bevoegdheid van de actoren om onderlinge afspraken te maken. Na onderzoek bleek dat er onder de huidige stand van het recht geen wettelijk kader bestaat dat toegepast kan worden op de problematiek van het Kadaster van Verbindingen binnen de overheidscontext. Een wetgevend initiatief zou hier bijgevolg wenselijk zijn. Wat de bevoegde overheid betreft zagen we dat men ervoor moet kunnen zorgen dat elke overheidsdienst verplicht wordt tot medewerking. Een werkelijk 'end-to-end' gegevensspoor kan immers maar tot stand komen indien elke schakel in de keten meewerkt. We duidden daarom de federale overheid aan als principiële wetgever voor deze materie, desnoods door middel van een samenwerkingsakkoord met de regionale overheden. Wat tot slot het beheer van het Kadaster betreft zagen we dat de bestaande actoren al een eerste vorm van controle bieden. De neutraliteit van de tussenpersonen en de bijkomende verantwoordelijkheden van de doelsystemen staan immers voor een deel garant voor de goede werking van het systeem. Gelet op het feit dat het audit trail een verwerking van persoonsgegevens is en op het feit dat de controle door de betrokken partijen vaak onvolledig – en gelet op het principe van de scheiding der machten misschien zelfs onwenselijk – is, kunnen we wel nog denken aan een rol voor de Commissie voor de bescherming van de persoonlijke levenssfeer. Zo zou men het algemeen beheer van de logs onder de hoede van deze centrale Commissie kunnen brengen. De Commissie beschikt immers al over een aantal bevoegdheden voor een *ex post* controle. Bijkomende bevoegdheden kunnen in het wettelijk kader aangeduid worden. Voor het beheer van de centrale gebruikerstoepassing voor het consulteren van de logs – het eigenlijke kadaster – verwijst de Wet op het Rijksregister zelf al naar het sectoraal comité van het Rijksregister.

HET KADASTER IN DE PRAKTIJK - Tot hiertoe ging het voornamelijk over hoe we ons het Kadaster in theorie zouden moeten voorstellen. Daarom wordt er ook nog gekeken naar hoe dit in de praktijk in zijn werk zou moeten gaan. Hier merkten we een probleem op bij de realisatie van het *ex ante* register. Wat de toekomstige machtigingen betreft hoeft men immers eerst een standaardformaat af te spreken om zo deze machtiging – na conversie in een door een informaticasysteem leesbaar formaat – in dat register op te nemen. De vroeger verleende machtigingen zullen echter ook via eenzelfde standaardformaat verwerkt moeten worden. Zoals verder uiteengezet in bijlage 1 bij dit document zal het allereerst een opgave worden om alle verleende en nu nog geldende machtigingen in kaart te brengen. Daarnaast zagen we dat we handmatig de voor het register relevante gegevens uit deze machtigingen zullen moeten distilleren. Voor de machtigingen verleend door het sectoraal comité zal dit geen eenvoudige – maar ook geen volstrekt onmogelijke – opgave worden. De machtigingen bij koninklijk besluit zijn echter maar beperkt in een logisch gestructureerde standaard te vatten. We zijn daarom voorstander van het herzien van deze machtigingen – hoewel moet worden erkend dat ook deze oplossing nog een aantal problemen met zich meebrengt. Door de machtigingen bij koninklijk besluit te herschrijven, zouden ze kunnen worden aangepast aan de huidige realiteit en de nu gangbare opvattingen met betrekking tot het gebruik van het Rijksregisternummer en de toegang tot de gegevens van het Rijksregister. Als tweede praktisch probleem is er de nood aan interoperabiliteit tussen de verschillende overheidsdiensten en de nood om het Kadaster in bestaande systemen te integreren, om op die manier te vermijden dat alle overheidsdiensten hun bestaande infrastructuur moeten aanpassen. Indien men een bestaande toepassing kan uitbreiden tot een centraal platform, vermijdt men bovendien de kosten die gepaard zouden gaan met de creatie van een geheel nieuw platform.

OMVANG VAN HET KADASTER - Tot slot bekeken we de omvang van het Kadaster. Zoals al aangehaald bij het onderzoek naar het wettelijk kader, is er nood aan een centrale gebruikerstoepassing. Het grote gevaar van de gedecentraliseerde gegevensopslag bestaat er immers in dat de burger – door bijvoorbeeld het gebrek aan interoperabiliteit tussen overheidsdiensten of het gebrek aan medewerking van die diensten – niet in staat is om het volledige 'end-to-end' gegevensspoor te reconstrueren. Een centrale gebruikerstoepassing kan de burger de nodige zekerheid bieden en kan toch nog voldoende ruimte laten aan de individuele overheidsdiensten om hun eigen logs te beheren.

TECHNISCH ONDERZOEK - Naast het juridisch en organisatorisch onderzoek werd er ook stilgestaan bij meer technisch georiënteerde problemen. Voor de meeste technisch gerichte vragen hebben we getracht deze te beantwoorden samen met de bespreking van het juridisch en organisatorisch kader. Een bijkomend technisch onderzoek lijkt hier bijgevolg niet noodzakelijk te zijn. In het kader van de meer technische vragen kunnen we hier nog kort verwijzen naar de uitbreiding van het *Online Certificate Status Protocol* (OCSP). Onder deel I van dit project beperkten we ons tot een meer conceptuele omschrijving van dit voorstel. Gelet op het feit dat men zich toch nog enige vragen kan stellen bij deze problematiek werd besloten om dit voorstel nog verder uit te werken. Gezien het nut van het OCSP in het kader van het Rijksregisternummer en de e-ID, wensen we op deze plaats kort te verwijzen naar dit onderzoek.

4.2. PRAKTIJKGERICHTE CONCEPTSTUDIE

VAN THEORIE NAAR PRAKTIJK - In het voorgaande hebben we het steeds gehad over het theoretische concept van het Kadaster van Verbindingen. Deze studie wil zich echter niet alleen richten op louter theoretische beschouwingen. Het is immers het doel van dit project om te komen tot een praktijkgerichte conceptstudie. We herhalen dat het binnen het tijdsbestek van dit project onmogelijk is om tot een volledig uitgewerkt projectplan te komen. We richten ons daarom voornamelijk op praktische aanbevelingen. In wat volgt zullen we daarom trachten een antwoord te bieden op een aantal vragen met betrekking tot de stappen te nemen, de timing, de kostenraming, de middelen en het beheer die gepaard gaan bij de realisatie van dit Kadaster van Verbindingen.

STAPPEN – PUBLICATIE VAN DE LOGS - Aangezien de meeste overheidsdiensten uit allerlei wettelijke verplichtingen vaak al logs zullen bijhouden die melding maken van de transacties die zij uitvoeren met betrekking tot de persoonsgegevens die zij verwerken – hierbij inbegrepen de gegevenskoppelingen die zij uitvoeren door middel van het gebruik van het Rijksregisternummer van de betrokken burger – zou het een interessante eerste stap zijn om zulke logs te publiceren. Op deze manier kan men al enige transparantie bieden in de precieze gegevenskoppelingen die zij dagelijks gemaakt worden. Hierbij moet uiteraard aandacht worden besteed aan het naleven van onder meer de regels met betrekking tot de bescherming van de privacy. Eventuele persoonsgegevens in de logs zullen moeten worden verwijderd of ontoegankelijk gemaakt worden voor wie niet bevoegd is om deze gegevens in te kijken. Deze bestaande logs kunnen vervolgens – eventueel samen met de logs van de overheidsdiensten die op dit moment nog geen dergelijke logs bijhouden – geïntegreerd worden in bestaande toepassingen zoals 'MijnDossier' om de burger een meer gestructureerd beeld te bieden van de gegevenskoppelingen die betrekking hebben op zijn persoonsgegevens. Door gebruik te maken van bestaande logs en toepassingen, kan deze fase snel en zonder bijkomende kost of werklast bereikt worden.

STAPPEN - WETTELIJK KADER - Vervolgens zal men moeten beginnen met het aannemen van een wettelijk kader dat toegepast kan worden op deze figuur. Door de verscheidenheid aan wetgeving – en bij gebrek aan een bestaand kader dat toegepast kan worden op deze figuur – kan een gecoördineerd geheel immers een nuttig initiatief zijn. Zulk wettelijk kader kan een aantal basisvoorwaarden – zoals de inhoud van het Kadaster, het verhullen van identiteitsgegevens, de bewaartermijn en dergelijk – vastleggen. Op deze manier kan men er dan ook voor zorgen – bij voorbeeld door dit kader te realiseren door middel van een samenwerkingsakkoord – dat alle betrokken overheidsdiensten zullen moeten meewerken, wat noodzakelijk is voor de goede werking van het Kadaster. Men kan hier ook al een zekere taakverdeling voor de betrokken actoren voorstellen, hoewel de precieze taakverdeling beter door de actoren zelf geregeld zal worden. Ook de betrokkenheid van de Commissie voor de bescherming van de persoonlijke levenssfeer kan in dit wettelijk kader geregeld worden. Wanneer de wettelijke basis aangenomen is, kunnen de betrokken actoren de nodige onderlinge afspraken maken.

STAPPEN - TECHNISCHE REALISATIE - Wanneer men de juridische basisbegrippen geregeld heeft, kan men beginnen met de realisatie van het technisch kader waarbinnen het Kadaster zal werken. Zoals aangehaald kan men dit concept best initieel realiseren binnen de bestaande infrastructuur. Er wordt binnen de overheidscontext immers al gewerkt met gebruikers- en toegangsbeheer door middel van federaties op basis van vertrouwenskringen. De identificatie en authenticatie van de gebruikers kan dan gebeuren op basis van de e-ID. Voor de realisatie van het Kadaster als centraal portaal waar de burger de logs kan raadplegen kan men kijken naar bestaande overheidsportalen, bijvoorbeeld de toepassing 'MijnDossier' of het portaal van het eHealth project. Voornamelijk voor de *ex post* loggings op het niveau van de individuele overheidsdienst kan waar mogelijk gebruik gemaakt worden van bestaande initiatieven zoals 'MijnDossier'. Belangrijk is dat er hier voldoende aandacht besteed wordt aan het maken van afspraken met betrekking tot het standaardformaat. De logs van de individuele overheidsdiensten zullen immers voldoende interoperabiliteit moeten vertonen.

STAPPEN - EX ANTE REGISTER - Ook voor het *ex ante* register zal men ervoor moeten zorgen dat het afgesproken standaardformaat gehandhaafd wordt. In de eerste plaats zullen de toekomstige machtigingen dan dankzij deze standaard op minstens op quasi-geautomatiseerde wijze opgenomen worden in het register. Vervolgens kan men beginnen met het verwerken van de bestaande machtigingen in het register. Zoals ons onderzoek aantoonde, zal dit een vrij arbeidsintensieve taak worden.

STAPPEN - DAGELIJKSE WERKING - Wanneer men de voorgaande stappen voltooid heeft, kan het Kadaster van Verbindingen van start gaan. Het *ex post* loggen kan beginnen zodra de benodigde technische middelen geïmplementeerd zijn en wanneer een standaardformaat afgesproken is. Het *ex ante* register *ex tunc* kan uiteraard pas na de verwerking van de vroeger verleende machtigingen van start gaan.

TIMING - Indien er binnen de overheid voldoende overeenstemming bestaat voor het oprichten van het Kadaster van Verbindingen, zal de effectieve realisatie ervan op relatief korte termijn kunnen plaatsvinden. De benodigde technische middelen en kennis zijn immers al beschikbaar en worden al op grote schaal door de overheidsdiensten toegepast. Mits kleine aanpassingen aan de bestaande infrastructuur en door de integratie van bestaande initiatieven in deze context, zal de initiële technische realisatie van het Kadaster geen zware werklast met zich meebrengen. Uit deze studie bleken er ook geen ernstige juridische obstakels te zijn die de realisatie van het Kadaster in de weg zouden kunnen staan. Een tussenkomst van de wetgever lijkt ons wel noodzakelijk voor het oprichten van een wettelijk kader waarbinnen het audit trail in de overheidscontext zou werken. Zoals aangehaald kan deze tussenkomst beperkt blijven tot het formuleren van een aantal basisvoorwaarden, waarbij men voldoende ruimte laat aan de betrokken actoren om tot onderlinge overeenkomsten te komen. Het grootste deel van het tijdsbestek voor de realisatie van het Kadaster van Verbindingen zal uitgaan naar het verwerken van de relevante gegevens uit de bestaande machtigingen in het *ex ante* register.[330] Zoals we zagen kan het enige tijd kosten om deze machtigingen in kaart te brengen. Voornamelijk de verwerking van de vroegere machtigingen bij koninklijk besluit kan enige tijd kosten.

MIDDELEN - Zoals aangehaald is de technische infrastructuur die vereist is voor de implementatie van het Kadaster al grotendeels bestaande. Men kan zich daarom beperken tot het aanpassen van de huidige infrastructuur en het integreren van al bestaande initiatieven met betrekking tot het loggen van gegevenskoppelingen, wat voornamelijk tijd en financiën zal vereisen. Bijkomende middelen zullen dus slechts in beperkte mate vereist zijn.

KOSTENRAMING - Gelet op het feit dat de vereiste infrastructuur al grotendeels aanwezig is en er slechts in beperkte mate bijkomende middelen vereist zijn, zullen de kosten voor de realisatie van het Kadaster van Verbindingen grotendeels beperkt kunnen blijven tot de personeelskosten verbonden aan het opzetten van het *ex ante* register, het instellen van het loggen bij de verschillende administraties, en dergelijke. Daarnaast lijkt – doordat het Kadaster grotendeels geautomatiseerd zou moeten werken – een minimum aan voltijds personeel afdoende te zijn om de dagelijkse werking van dit concept te garanderen.

BEHEER - Zoals aangehaald zal het Kadaster tot op zekere hoogte door de betrokken actoren beheerd kunnen worden. De individuele logs per overheidsdienst zullen door diezelfde dienst beheerd worden. De dienstenintegratoren zullen als tussenpersonen instaan voor de communicatie met de front office actoren. Omdat deze laatste actoren een bijkomende verantwoordelijkheid dragen voor de goede werking van het 'end-to-end' audit trail, zullen zij in zekere zin ook dienen als beheerders van het systeem. We zien dus geen nood tot het oprichten van een aparte entiteit voor het beheer van het Kadaster van Verbindingen. We raden echter wel aan om nog de Commissie voor de bescherming van de persoonlijke levenssfeer te betrekken bij het beheer van de logs. Zoals in het onderzoek aangetoond werd, zal de Commissie in ieder geval nauw betrokken worden bij de dagelijkse werking van zulk audit trail. Het lijkt ons daarom aanbevelingswaardig om de centrale privacyautoriteit aan te stellen als de eindbeheerder van het gegevensspoor. Het Kadaster van Verbindingen als centrale gebruikersportaal zal onder het beheer van het sectoraal comité van het Rijksregister komen te staan. Dit volgt immers uit artikel 8 van de Wet op het Rijksregister.

CONCLUSIE - In dit hoofdstuk hebben we proberen aan te tonen dat de praktische realisatie van het Kadaster van Verbindingen voornamelijk enige tijd en politieke overeenstemming zal verei-

[330] Naar de in bijlage 1 gevolgde methode rekenen we een half uur per machtiging door het sectoraal comité, met een geschatte 300 beraadslagingen die verwerkt moeten worden. Voor de machtigingen bij koninklijk besluit rekenen we minstens 1 uur per machtiging. De lijst van Dirk De Bot spreekt over een 120 basismachtigingen, waarvan een groot deel intussen gewijzigd werd. We zullen voor deze berekening enkel de basismachtigingen tellen. Dit brengt ons op een eindtotaal van minimaal 270 manuren. Het totaal aantal werkelijke manuren die nodig zijn voor de verwerking van deze machtigingen zal zeker hoger liggen.

sen. Omdat het Kadaster initieel geïmplementeerd zou kunnen worden binnen de bestaande infrastructuur en applicaties, zal de eerste realisatie ervan geen substantiële investeringen vereisen. Het belangrijkste element bij de realisatie zal bijgevolg de timing zijn. Allereerst zal immers het wettelijk kader aangenomen moeten worden en zullen de betrokken partijen de nodige overeenkomsten sluiten. Dan pas kan men van start gaan met de werkelijke oprichten van het Kadaster, waarbij men eventueel een bestaande toepassing zou kunnen uitbreiden tot een centraal platform. Hierbij vermijdt men de kosten die gepaard gaan met de creatie van een geheel nieuw platform. De *ex post* loggings kunnen vervolgens meteen van start gaan, maar het *ex ante* register zal nog enige verwerking vereisen.

4.3. EINDCONCLUSIE

HET VERALGEMEEND GEBRUIK VAN HET RIJKSREGISTERNUMMER - Onder deel I van dit project hebben we het veralgemeend gebruik van het Rijksregisternummer binnen de overheidscontext onderzocht. We merkten hier bij op dat het gebruik van een nationale enkele unieke identificator zoals het Rijksregisternummer zeker verantwoord kan worden vanuit het standpunt van de privacybescherming. Uit het rechtsvergelijkend onderzoek naar het beleid van een aantal andere Europese landen – en dan in het bijzonder de landen die sectorgebonden identificatoren hanteren – bleek dat transparantie en gebruiksvriendelijkheid twee zeer belangrijke principes zijn voor een succesvol beleid met betrekking tot e-Government, unieke identificatoren en elektronische identiteitskaarten. We merkten echter wel op dat er een belangrijke beleidskeuze gemaakt moet worden. Men kan immers het gebruik van een identificator als het Rijksregisternummer volledig vrij laten – zoals het geval is met de Zweedse *Personnummer* – of men kan het gebruik van dit nummer beperken, bijvoorbeeld door het Belgisch gebruik van voorafgaande machtigingen. Deze beleidskeuze heeft uiteraard zijn gevolgen. Indien we het gebruik van het Rijksregisternummer willen inperken, zal men erover moeten waken dat dit nummer niet nodeloos doorgegeven wordt. Er werd daarom besloten dat de opname van het Rijksregisternummer in het authenticeringscertificaat op de e-ID maar moeilijk verdedigbaar is in het licht van het huidig Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer. We formuleerden een oplossing – de uitbreiding van het Online Certificate Status Protocol – die verder in het project nog meer in detail besproken zal worden.

EFFECTIEVE TRANSPARANTIE - In dit deel van het project zijn we eerst verder gaan nadenken over de eis van transparantie. We haalden aan dat transparantie immers een belangrijk onderdeel is van het Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer, maar dat er een gebrek is aan effectieve transparantie. De principes uit de Richtlijn en de Privacywet die moeten zorgen voor de verhoging van de transparantie van de verwerking, moeten we immers afdoen als onvoldoende. Om tot effectieve transparantie te komen, willen we daarom meer aandacht schenken aan het gebruikersgericht identiteitsbeheer. Indien de burger voldoende op de hoogte gebracht wordt van wat er is gebeurd – of kan gebeuren – met zijn persoonsgegevens en welke gegevenskoppelingen er met betrekking tot die gegevens kunnen plaatsvinden, dan zal de transparantie van de betrokken verwerking aanzienlijk verhogen.

KADASTER VAN VERBINDINGEN - Het Rijksregisternummer is binnen de overheidscontext de ideale manier om gegevenskoppelingen uit te voeren. Omdat het gebruik van het Rijksregisternummer in België beschermd wordt en omdat het nummer zelf een persoonsgegeven is in de zin van de privacywetgeving, is het niet verwonderlijk dat we de nood aan effectieve transparantie bij de verwerking van dit nummer of bij gegevenskoppelingen op basis van dit nummer nog eens extra willen benadrukken. De Wet op het Rijksregister geeft zelf een manier aan om de transparantie van de verwerking te verhogen, namelijk het ‘kadaster van netwerkverbindingen’. Ondanks het feit dat het hier om een belangrijk gegeven gaat, wordt het kadaster nergens verder gedefinieerd of verder uitgewerkt. In dit deel van het project hebben we daarom eerst het concept ‘Kadaster van Verbindingen’ geanalyseerd om het verder te definiëren en in te vullen. Vervolgens hebben we onderzocht hoe we het Kadaster van Verbindingen in de praktijk georganiseerd zou moeten worden.

TRANSPARANTIEVERHOGING - Door middel van de in dit onderzoek voorgestelde principes zou men van het Kadaster van Verbindingen een zeer effectief hulpmiddel kunnen maken om de transparantie van de verwerking van persoonsgegevens en gegevenskoppelingen door middel van het Rijksregisternummer te verhogen. Door bijvoorbeeld de burger inzage te bieden in de logs die door de verschillende overheidsdiensten bijgehouden worden, krijgt de burger immers een nooit eerder geziene graad van inspraak in deze privacygevoelige overheidsprocessen. Het Kadaster is daarom een goede manier om het huidige beleid met betrekking tot het gebruik van het Rijksregisternummer aan te vullen. Door de gegevenskoppelingen door middel van dit identificatienummer effectief transparant te maken, zal het gebruik van een enkele unieke identificator als het Rijksregisternummer immers zonder problemen kunnen voldoen aan de vereisten van de privacybescherming. Deze transparantieverhoging zou voor het Belgisch beleid zelfs het pad kunnen effenen voor een zekere toenadering tot het Zweeds model. Hoewel een openbaarheidsprincipe, zoals dat in Zweden gekend is, een gevolg is van een eeuwenlange evolutie en bijgevolg diep in de cultuur geworteld is, is het niet ondenkbaar dat het Belgisch beleid zou kunnen evolueren naar een systeem waar het nationale identificatienummer vrij gebruikt kan worden mits expliciete en ondubbelzinnige toestemming van de betrokkene. De basisvoorwaarde voor zulke evolutie is uiteraard dat het gebruik van het Rijksregisternummer en de gegevenskoppelingen op basis van dat identificatienummer meer transparant moeten worden. Het Kadaster van Verbindingen dat in dit onderzoek voorgesteld wordt zou zulke transparantie kunnen garanderen.

DEEL III: HET ONLINE CERTIFICATE STATUS PROTOCOL

De tekst van dit deel van het onderzoek kon niet tijdig ingevoegd worden in het eindrapport. De resultaten van het onderzoek naar het Online Certificate Status Protocol zullen daarom opgenomen worden in een latere revisie van dit rapport.

DEEL IV: EINDBESCHOUWING

UNIEKE IDENTIFICATOREN - In dit project hebben we het gebruik van unieke identificatoren onderzocht. Er werd allereerst stilgestaan bij hoe het gebruik van unieke identificatoren zich verhoudt tot de bescherming van de persoonlijke levenssfeer. Daarnaast werd ook de impact onderzocht van het in een Staat gehanteerde systeem van unieke identificatoren op de transparantie, de efficiëntie en de gebruiksvriendelijkheid van de overheidsdiensten. Zoals het historisch onderzoek onder deel I al aangaf, is het gebruik van unieke identificatoren niet meer weg te denken uit de hedendaagse samenleving. De systemen van unieke identificatoren die de Europese lidstaten hanteren, kunnen we onderverdelen in twee groepen: het gebruik van een enkele unieke identificator – zoals het Belgische Rijksregisternummer of het Zweedse *Personnummer* – en het gebruik van meerdere sectorgebonden identificatoren – zoals de *ad hoc* gegenereerde ssPIN in Oostenrijk, de Duitse pseudoniemen of de vaste Portugese sectornummers.

ID-FIX - Unieke identificatoren worden echter niet alleen gebruikt om de burger te identificeren. Zij kunnen gebruikt worden bij het maken van gegevenskoppelingen. Hierbij kunnen overheidsdiensten informatie met betrekking tot de burger – met inbegrip van zijn persoonsgegevens – uitwisselen door gebruik te maken van het betrokken Rijksregisternummer. Het gebruik van een enkele unieke identificator wordt vaak bekritiseerd als een gevaar voor de bescherming van de persoonlijke levenssfeer. Zo vormt bijvoorbeeld in België het veralgemeend gebruik van het Rijksregisternummer in de overheidscontext al jaren een rem op de realisatie van voorstellen en initiatieven op het gebied van de modernisering van de overheidsdiensten. Het is opvallend dat de gegevenskoppelingen die door het gebruik van een unieke identificator tot stand kunnen komen echter niet zo vaak het onderwerp van discussie vormen. Gelet op het feit dat er bij zulke gegevenskoppelingen ook persoonsgegevens doorgegeven worden en gelet op het feit dat het deze gegevenskoppelingen vaak aan transparantie ontbreekt, is het nuttig om ook deze praktijk aan nader onderzoek te onderwerpen. Het ID-FIX project richt zich daarom op zowel het veralgemeend gebruik van het Rijksregisternummer als enige unieke identificator in de overheidssector als op het gebruik van dit nummer bij het maken van gegevenskoppelingen.

1. HET RIJKSREGISTERNUMMER

HET VERALGEMEEND GEBRUIK VAN HET RIJKSREGISTERNUMMER - Onder deel I van dit project hebben we het huidige Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer onderzocht. Bij dit beleid onderscheidden we twee belangrijke punten. Het Rijksregisternummer is allereerst de enige unieke identificator die binnen de overheidssector gebruikt wordt, wat dus in contrast staat met het gebruik van sectorgebonden identificatoren. Er moest daarom eerst onderzocht worden of het gebruik van een enige unieke identificator verdedigd kan worden vanuit het standpunt van de privacybescherming. Hierbij diende er ook gekeken te worden naar andere factoren die bepalend kunnen zijn voor de keuze voor een systeem van een enkele of meerdere identificatoren, zoals de gevolgen van zulke keuze voor de transparantie en de efficiëntie of gebruiksvriendelijkheid van de overheidsdiensten. Een tweede punt dat opvalt bij het Rijksregisternummer is dat het gebruik van dit nummer in principe streng gereguleerd is. Hoewel het gebruik van het Zweedse nationale identificatienummer relatief vrij is, blijkt het gebruik van het Rijksregisternummer onderworpen te zijn aan voorafgaande machtigingen.

UNIEKE IDENTIFICATOREN IN EUROPA - Om te bepalen of het gebruik van een enkele unieke identificator zoals het Rijksregisternummer verdedigd kan worden vanuit het standpunt van de privacybescherming, werd een rechtsvergelijkend onderzoek gevoerd waarbij het Belgisch beleid vergeleken werd met dat van een aantal andere Europese lidstaten. Bij dit onderzoek werd duidelijk dat het Oostenrijks en Duits beleid met betrekking tot sectorgebonden identificatoren toch een aantal problemen inhoudt. Zo is er bij de in deze landen gehanteerde systemen een duidelijke nood aan een verregaande beveiliging van dit systeem. Die beveiliging bleek echter een grote bedreiging te vormen voor de transparantie van het systeem naar de burger toe, alsook voor de gebruiksvriendelijkheid van de overheidsdiensten. Ook het Portugese systeem van vaste sectorgebonden identificatoren leek niet tot meer transparantie of gebruiksvriendelijkheid te leiden. We concludeerden daarom dat het gebruik van een enkele unieke identificator binnen de overheidscontext niet noodzakelijk leidt tot een grotere bedreiging voor de bescherming van de persoonlijke levenssfeer, met inbegrip van de transparantie. Ook blijkt het gebruik van een enkel nationaal identificatienummer voordelen te bieden op het gebied van de efficiëntie en de gebruiksvriendelijkheid van de overheidsdiensten.

VRIJ OF GEGERULEERD GEBRUIK? - Nu uit het voorgaande onderzoek blijkt dat het gebruik van een enkele unieke identificator binnen de overheidscontext zeker verdedigd kan worden vanuit het standpunt van de privacybescherming, de transparantie en de efficiëntie en de gebruiksvriendelijkheid van de overheidsdiensten, kan er onderzocht worden hoe men met zulk nummer dient om te gaan. Zoals eerder aangehaald is het gebruik van het Belgisch Rijksregisternummer in principe strikt gereguleerd. Men mag enkel gebruik maken van dit identificatienummer indien men tot één van de overheden, instellingen of personen behoort die limitatief opgesomd worden in de Wet op het Rijksregister. Daarnaast moet er ook nog een voorafgaande machtiging bekomen worden bij het Sectoraal Comité van het Rijksregister. Het gebruik van het Belgisch Rijksregisternummer is met andere woorden aan strenge voorwaarden onderworpen en is bovendien duidelijk niet bestemd voor een ruim gebruik in de private sector. Het Zweeds beleid met betrekking tot het *Personnummer* is de exacte tegenpool van het Belgisch beleid. Het gebruik van dit nationaal identificatienummer is relatief vrij, zowel voor overheidsdiensten als voor gebruik in de private sector. Dankzij het sterke openbaarheidsprincipe dat de Zweedse samenleving kenmerkt, ervaart de burger geen gebrek aan transparantie door dit vrij gebruik van het identificatienummer.

NAAR EEN VRIJ GEBRUIK? - Uit het onderzoek naar het Zweeds *Personnummer* bleek dat het vrij gebruik van zulk nationaal identificatienummer niet noodzakelijk leidt tot een gebrek aan transparantie of tot een gevaar voor de bescherming van de persoonlijke levenssfeer. Daarnaast dient men ook te onthouden dat eventuele bedenkingen bij het vrij gebruik van zulk identificatienummer ook niet overschat mogen worden. Onderzoek in Zweden en België toonde aan dat een ruime meerderheid van de burgers niet wakker ligt van het gebruik van hun nationaal identificatienummer. Daarnaast kan het vrij gebruik van de nationale identificator ook voordelen met zich meebrengen. Een fonetische opzoeking in een databank zal immers meer persoonsgegevens van meer burgers betrekken bij de taak die men wenst uit te voeren, dan een simpele opzoeking van bepaalde gegevens van een bepaalde persoon door gebruik te maken van zijn Rijksregisternummer. Voor de Belgische situatie is het zeker niet ondenkbaar dat een meer geliberaliseerd gebruik van het Rijksregisternummer tot een verhoging van de efficiëntie van de overheidsdiensten zou kunnen leiden. Bij gebrek aan een sterk openbaarheidsprincipe kunnen er echter wel nog bedenkingen geformuleerd worden met betrekking tot de transparantie indien men het gebruik van dit nummer zou liberaliseren.

HET HUIDIGE BELGISCH BELEID - TRANSPARANTIE - Uit het voorgaande blijkt dat een meer vrij gebruik van het Rijksregisternummer wellicht voordelen met zich mee kan brengen. We merkten hier echter bij op dat er hiertoe eerst gewerkt moet worden aan het verhogen van de transparantie van dit gebruik. Bij gebrek aan een sterk openbaarheidsprincipe zal men er immers over moeten waken dat het vrij gebruik van het Rijksregisternummer – zeker het gebruik ervan door overheidsdiensten – voldoende transparant is. Het vrij gebruik van het Rijksregisternummer in de private sector is – zoals in Zweden – ook denkbaar, maar zal onderworpen zijn aan de expliciete en ondubbelzinnige toestemming van de betrokkene. Uit het hier gevoerde onderzoek blijkt echter dat het huidige Belgisch gebruik van het Rijksregisternummer maar weinig transparant is. De grote hoeveelheid machtigingen tot gebruik van dit identificatienummer vormt een ongestructureerd kluwen waar de burger zich onmogelijk doorheen kan werken. Daarnaast is er ook geen mogelijkheid voor de burger om op gestructureerde wijze zicht te krijgen op welke gegevenskoppelingen er gemaakt worden door het gebruik van zijn Rijksregisternummer. Indien men wil evolueren naar een meer geliberaliseerd gebruik van het Rijksregisternummer, zal er dus eerst gewerkt moeten worden aan transparantieverhogende maatregelen.

HET HUIDIGE BELGISCH BELEID - TEGENSTRIJDIGHEDEN - Daarnaast merken we met betrekking tot het huidige beleid op dat er hier een aantal tegenstrijdigheden aanwezig zijn. Zo staat bijvoorbeeld de sterke aanwezigheid van het Rijksregisternummer op de e-ID haaks op de gereguleerde status van dit nummer. Vooral de aanwezigheid van het identificatienummer in het authentiseringscertificaat op de e-ID kan maar moeilijk verdedigd worden omdat die aanwezigheid hier niet strikt noodzakelijk is. Hoewel het niet het opzet van dit onderzoek is om uitdrukkelijk te pleiten voor het vrij of het gereguleerd gebruik van het Rijksregisternummer, pleiten we er wel voor dat een gemaakte beleidskeuze consequent opgevolgd wordt. Indien men de gereguleerde status van dit identificatienummer wil behouden, lijkt het ons daarom aanbevelingswaardig om enige tegenstrijdigheden in dit beleid weg te werken.

TUSSENTIJDSE CONCLUSIE - Op basis van het onder deel I gevoerde onderzoek kunnen we een tweeledige oplossing voorstellen. In eerste instantie zal het verdere onderzoek gericht zijn op de realisatie van een transparantieverhogende maatregel. Er zal aangetoond worden dat zulke maatregel belangrijk kan zijn voor het huidige gereguleerd gebruik van het Rijksregisternummer, alsook dat zulke maatregel noodzakelijk zal zijn voor de evolutie naar een meer vrij gebruik van dit identificatienummer. We kunnen hier denken aan de realisatie van het Kadaster van Verbindingen. Dit onderzoek werd gevoerd onder deel II van het project. Onder deel III werd een technisch onderzoek gevoerd waarbij aangetoond werd dat het mogelijk is om de huidige tegenstrijdigheden in het Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer weg te werken zonder dat de overheidsdiensten hierbij moeten inboeten aan efficiëntie.

2. HET KADASTER VAN VERBINDINGEN

GEGEVENSKOPPELINGEN - Uit het onderzoek onder deel I bleek dat het gebruik van een enkele unieke identificator binnen de overheidscontext niet noodzakelijk leidt tot een gevaar voor de privacybescherming of tot problemen met betrekking tot de efficiëntie of gebruiksvriendelijkheid van de overheidsdiensten. We haalden hier echter wel aan dat er een probleem is met de praktijk van de gegevenskoppelingen. De overheidsdiensten kunnen immers door middel van het Rijksregisternummer gegevens uitwisselen met elkaar, waarbij er ook persoonsgegevens van de betrokken burger verwerkt worden. Vanuit het standpunt van de privacybescherming kunnen we concluderen dat zulke gegevenskoppelingen voldoende transparant gemaakt moeten worden, zodat de burger op de hoogte gebracht kan worden van wie er over zijn persoonsgegevens beschikt en wat er mee gedaan kan worden. Onder de huidige stand van het recht blijkt zulk overzicht echter niet te bestaan. We concluderen daarom dat de gegevenskoppelingen die op dit moment in België gemaakt worden niet voldoende transparant zijn. Het echte gevaar voor de transparantie – en de bescherming van de persoonlijke levenssfeer in het algemeen – ligt met andere woorden niet bij het gebruik van een enkele unieke identificator, zoals het Rijksregisternummer, maar bij de gegevenskoppelingen die men maakt door middel van dat Rijksregisternummer.

TRANSPARANTIEVERHOGENDE MAATREGEL - In het tweede deel van dit project werd er daarom gezocht naar een manier om de transparantie van zulke gegevenskoppelingen te verhogen. Hiermee zou enerzijds het huidige Belgisch beleid meer transparant kunnen worden, wat gezien de huidige staat van de transparantie met betrekking tot gegevenskoppelingen zeker niet overbodig zou zijn. Anderzijds zou een duidelijke transparantieverhoging een antwoord kunnen bieden op het Zweeds openbaarheidsprincipe. Dit laatste is nodig indien men zou willen overgaan tot een meer geliberaliseerd gebruik van het Rijksregisternummer. Het nut van een transparantieverhogende maatregel laat zich al afleiden uit de huidige regelgeving met betrekking tot de bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens. Uit het onderzoek bleek dat transparantie een zeer belangrijk onderdeel vormt voor de privacybescherming krachtens de Europese Richtlijn. De middelen die de Richtlijn aanreikt om tot voldoende transparantie te komen, blijken in de praktijk echter niet hun doel te bereiken. Effectieve transparantie op het vlak van de verwerking van persoonsgegevens en gegevenskoppelingen blijkt onder de huidige stand van het recht niet aanwezig te zijn. We moeten daarom zoeken naar een maatregel die kan leiden tot zulke effectieve transparantie.

KADASTER VAN VERBINDINGEN - In dit onderzoek hebben we ons gericht op het Kadaster van Verbindingen. Hoewel de aanzet tot dit Kadaster al gevonden kan worden in de Wet op het Rijksregister, is er nooit overgegaan tot de effectieve realisatie van dit concept. Het Kadaster kan omschreven worden als een portaal dat de burger op gestructureerde wijze een overzicht biedt van zowel de gegevenskoppelingen die door het gebruik van zijn Rijksregisternummer kunnen gemaakt worden, als van de gegevenskoppelingen die effectief gemaakt werden. Hiertoe doet het Kadaster beroep op enerzijds een *ex ante* register van de verleende machtigingen en anderzijds op de logs van de gemaakte gegevenskoppelingen. Door de burger op zulke manier duidelijk op de hoogte te brengen van de gegevenskoppelingen die gemaakt werden of gemaakt kunnen worden door het gebruik van zijn Rijksregisternummer, is het Kadaster van Verbindingen een zeer interessante transparantieverhogende maatregel die kan leiden tot effectieve transparantie naar de burger toe bij de verwerking van zijn persoonsgegevens of bij gegevenskoppelingen.

WAT IS HET KADASTER? - In het eerste deel van het onderzoek naar het Kadaster van Verbindingen werd er gefocust op de inhoudelijke en begripsmatige invulling van dit concept. Hiertoe werd eerst een kort rechtsvergelijkend onderzoek gevoerd. Uit dit onderzoek bleek dat het Kadaster van Verbindingen een uniek Belgisch concept zou worden. Hoewel een aantal andere Europese landen wel overgaan tot het loggen van bepaalde verwerkingen en gegevenskoppelingen –

voornamelijk om te voldoen aan een aantal wettelijke bepalingen – en hoewel Portugal in zekere zin een *ex ante* register van verleende machtigingen kent, is er geen enkele andere Europese lidstaat die de gegevens uit deze bronnen op gestructureerde wijze aanbiedt in een centraal portaal dat de transparantie naar de gebruiker toe verhoogt door hem inzicht te verschaffen in de mogelijke of gemaakte gegevenskoppelingen door middel van zijn identificatienummer. Na het rechtsvergelijkend onderzoek werd dieper ingegaan op de inhoudelijke invulling van dit concept. Hier werd besloten dat het Kadaster de burger in de eerste plaats een antwoord moet kunnen bieden op de vraag: “Wie heeft met betrekking tot mijn persoonsgegevens wat gedaan, met welke reden en op welk moment?” Het blijkt echter geen sinecure om deze vraag te beantwoorden. Het loggen zelf is immers te beschouwen als een verwerking van persoonsgegevens en men kan dus niet zonder meer alle relevante gegevens in deze logs opnemen. Men zal er hier dus voldoende over moeten waken dat het loggen zelf kan beantwoorden aan de regels van de privacybescherming. Indien dit niet gebeurt, zal het Kadaster van Verbindingen haar doel als transparantieverhogende maatregel niet kunnen bereiken omdat het gebruik maakt van logs die de regels met betrekking tot de verwerking van persoonsgegevens schenden. Om dit te vermijden werd er in het onderzoek voldoende aandacht besteed aan hoe men bepaalde persoonsgegevens op een correcte wijze kan opnemen in de logs. In het geval van de ambtenaar die de verwerking of de gegevenskoppeling uitvoert in opdracht van de voor de verwerking verantwoordelijke organisatie, pleiten we er bijvoorbeeld voor om deze ambtenaar niet te identificeren, maar om hem identificeerbaar te maken.

HET KADASTER IN DE PRAKTIJK - In een tweede deel van het onderzoek naar het Kadaster van Verbindingen werd er gefocust op een aantal juridische, technische en organisatorische problemen die gepaard gaan met de praktische realisatie van zulk concept. We besloten hier dat het Kadaster wel een centraal platform kan bieden aan de burgers, maar dat het aanbevelingswaardig is om de gegevens waar het Kadaster gebruik van zal maken gedecentraliseerd te bewaren. Hiertoe zou men gebruik kunnen maken van een zogenaamde federatie op basis van vertrouwenskringen. Indien men zulke federatie in het systeem invoert, zou platform de burgers identificeren/authentiseren op basis van hun e-ID vooraleer hen toegang tot de toepassing te verlenen. Het ingebouwde gebruikers- en toegangsbeheer kan er dan voor zorgen dat alleen de daartoe gemachtigde personen bepaalde gegevens – zoals de precieze identiteitsgegevens van de verantwoordelijke ambtenaar – te zien krijgen. Vervolgens bespraken we de betrokken actoren, hun verantwoordelijkheden en het speciale statuut van de tussenpersoon. Uit deze bevindingen bleek al het gebrek aan een wettelijk kader dat toegepast kan worden op de figuur van het Kadaster van Verbindingen. Het lijkt ons daarom aanbevelingswaardig dat een coördinerend wetgevend initiatief een wettelijk kader voor deze figuur zou kunnen instellen dat enerzijds verwijst naar de toepasbare wetgeving en anderzijds een aantal principes – zoals het beheer van de logs en het beheer van het gehele Kadaster – regelt. Omdat er hier in principe nog ruimte zou moeten gelaten worden voor onderlinge afspraken tussen de betrokken partijen, kan het interessant zijn om zulk kader via een samenwerkingsakkoord te regelen. Men kan op die manier alle overheidsdiensten op zowel federaal als deelstatelijk vlak bij dit proces betrekken. Het Kadaster kan immers maar succesvol zijn indien de burger het gehele ‘end-to-end’ gegevensspoor kan reconstrueren. Op een aantal praktische problemen bij de realisatie van het *ex ante* register van verleende machtigingen werd in een bijlage bij dat deel van het onderzoek dieper ingegaan.

CONCLUSIE - Hoewel de aanzet voor het Kadaster al een tijd geleden gegeven werd, is er in de praktijk nog niet veel te merken van dit concept. Hoewel een goed deel van de benodigde infrastructuren, technologieën en kennis voor de realisatie van dit concept al aanwezig is, zijn er toch nog een aantal *caveats* gemoeid bij de uitwerking van dit concept. Men zal erover moeten waken dat de logs waar het Kadaster gebruik van zal maken voldoen aan de voorwaarden van de verwerking van persoonsgegevens. Het Kadaster zal er immers voor moeten zorgen dat de transparantie wordt verhoogd, iets wat enkel kan gebeuren indien het Kadaster niet zelf nog meer persoonsgegevens gaat verwerken. Men zal daarom voldoende basisprincipes moeten aannemen en voldoende waarborgen voor de goede werking van het Kadaster moeten inbouwen. Zo kunnen we denken aan een rol voor de Commissie voor de bescherming van de persoonlijke levenssfeer als onafhankelijk beheerder van de logs, met het sectoraal comité van het Rijksregister als algemeen beheerder van het Kadaster van Verbindingen zelf. Indien de in dit deel van het onderzoek geformuleerde aanbevelingen met betrekking tot de juridische, technische en organisatorische werking van het Kadaster van Verbindingen gevolgd worden, kan het Kadaster een effectieve transparantieverhogende maatregel worden. Hiermee kan zeker het huidige – weinig transparante – Belgisch beleid met betrekking tot gegevenskoppelingen door middel van het gebruik van het Rijksregisternummer aanzienlijk transparanter gemaakt worden. Ook voor toekomstige evoluties zal zulk Kadaster noodzakelijk blijken.

3. HET ONLINE CERTIFICATE STATUS PROTOCOL

TEGENSTRIJDIGHEDEN - Zoals het onderzoek onder deel I van het project aantoonde, zijn er een aantal punten in het huidige Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer die enigszins haaks staan op het gereguleerd gebruik van dit identificatienummer. We gebruikten hiertoe als voorbeeld de aanwezigheid van het Rijksregisternummer op het authentiseringscertificaat op de e-ID. Er werd geconcludeerd dat het Rijksregisternummer hier juridisch gezien niet aanwezig hoeft te zijn. De enige reden voor de aanwezigheid van dit identificatienummer op deze plaats is het vergemakkelijken van een aantal meer technisch gerichte procedures. Indien men het gereguleerd gebruik van het Rijksregisternummer wenst te behouden, is het echter aanbevelingswaardig om zulke keuze consequent door te voeren in het gehele beleid. Tegenstrijdigheden zoals deze dienen uiteraard vermeden te worden.

TECHNISCH ONDERZOEK - In het derde deel van het project werd daarom een technisch onderzoek gevoerd om aan te tonen dat het mogelijk is om het Rijksregisternummer weg te laten uit het authentiseringscertificaat zonder te raken aan de efficiëntie van de overheidsdiensten. Er wordt aangetoond dat het Rijksregisternummer vervangen kan worden door een ander willekeurig nummer, of zelfs volledig geschrapt kan worden uit dit certificaat. Er wordt uitgegaan van twee situaties. Allereerst moet men ervoor zorgen dat de partij die gemachtigd is om het Rijksregisternummer te gebruiken, dit nummer zal ontvangen, ondanks het feit dat dit nummer niet meer aanwezig zal zijn in het certificaat zelf. Daarnaast zal men er ook voor moeten zorgen dat er geverifieerd kan worden of twee certificaten – waarvan men vermoedt dat zij beide tot dezelfde burger behoren – ook werkelijk bij elkaar horen. Het centrale uitgangspunt van het onderzoek is dat ervoor gezorgd moet worden dat bestaande toepassingen met hoogstens minimale aanpassingen blijven werken.

OCSP - UITBREIDING VAN HET ANTWOORD - Om deze doelstelling technisch te realiseren, wordt er een uitbreiding op het *Online Certificate Status Protocol* voorgesteld. In de praktijk zal een gebruiker die de geldigheid van zulk certificaat wenst te verifiëren een ondertekende aanvraag richten aan de OCSP-server van de certificatieautoriteit die het certificaat uitgaf. Deze server geeft dan aan of het certificaat geldig is, of het ongeldig is of dat hij geen uitspraak kan doen over dit bepaalde certificaat. Het hier gevoerde onderzoek wijst uit dat de OCSP-server ook kan controleren of de persoon die de aanvraag ondertekende gemachtigd is om het Rijksregisternummer te gebruiken. Indien dit het geval is, kan de server naast het klassieke antwoord het Rijksregisternummer als bijkomende informatie doorgeven. Dit leidt ertoe dat het Rijksregisternummer nog steeds terecht komt bij de daartoe gemachtigde persoon die de geldigheid van een authentiseringscertificaat wenst te verifiëren, zonder dat dit identificatienummer nog aanwezig is in het certificaat zelf.

OCSP - UITBREIDING VAN DE AANVRAAG - Aan de tweede voorwaarde kan voldaan worden door middel van een uitbreiding van de OCSP-aanvraag. Men kan immers de aanvraag voorzien van een referentie aan het authentiseringscertificaat waarvan vermoed wordt dat het hoort bij dezelfde burger die hoort bij het te controleren authentiseringscertificaat. De OCSP-server kan vervolgens controleren of de aanvraag correct ondertekend werd en of de aanvrager gemachtigd is om zulke link tussen twee certificaten te leggen. Vervolgens zal hij nagaan of beide certificaten inderdaad bij elkaar horen, om dit tot slot bij het OCSP-antwoord mee te geven.

CONCLUSIE - Het onder dit deel gevoerde onderzoek toont aan dat het technisch mogelijk is om het Rijksregisternummer te verwijderen uit het authentiseringscertificaat op de e-ID zonder dat de overheidsdiensten moeten inboeten aan efficiëntie. Uit het onderzoek blijkt dat de voorgestelde uitbreidingen op het *Online Certificate Status Protocol* met slechts minimale aanpassingen bereikt kunnen worden. Daarnaast blijkt dat zulke uitbreidingen geen invloed hebben op de kostprijs van een dergelijke OCSP-verzoek of op de snelheid waaraan zulk verzoek verwerkt kan worden.

4. CONCLUSIE

UITGANGSPUNTEN - Onder deel I van het project werd besloten dat het gebruik van een enkele unieke identificator binnen de overheidscontext – zoals het Rijksregisternummer – zeker verdedigd kan worden vanuit het standpunt van de privacybescherming, de transparantie en de efficiëntie of gebruiksvriendelijkheid van de overheidsdiensten. Er werd echter ook geconcludeerd dat er geen consensus bereikt kan worden in de discussie over de keuze tussen het vrij gebruik van dit identificatienummer of het huidige gereguleerd gebruik ervan. Hierbij kunnen we drie belangrijke opmerkingen formuleren. Allereerst moet er benadrukt worden dat het grote gevaar voor de privacybescherming niet zozeer uitgaat van het gebruik van een enkele unieke identificator op zich, maar van de gegevenskoppelingen die men kan maken door het gebruik van zulk identificatienummer. Er zal daarom voldoende aandacht moeten worden besteed aan hoe men zulke gegevenskoppelingen meer transparant kan maken naar de burger toe. Ten tweede wordt er opgemerkt dat het vrij gebruik van het Zweedse *Personnummer* het gevolg is van het verregaande openbaarheidsprincipe dat de Zweedse samenleving kenmerkt. Bij gebrek aan een dergelijk principe in België zal er ook hier voldoende aandacht moeten worden besteed aan het transparant maken van de gegevenskoppelingen die men maakt door middel van het gebruik van dit identificatienummer, vooraleer men kan overgaan tot een eventuele evolutie naar het Zweeds model. Tot slot merken we op dat het huidige Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer enigszins dubbelzinnig genoemd kan worden. Ongeacht de keuze tussen het vrij of het gereguleerd gebruik moet een gekozen beleid immers consequent toegepast worden.

TRANSPARANTIEVERHOGING - Er werd daarom besloten om in het verdere onderzoek twee pistes te verkennen. Onder deel II werd een praktijkgerichte conceptstudie gevoerd naar het Kadaster van Verbindingen. Dit Kadaster zou een centraal portaal vormen dat de burger inzage biedt in welke gegevenskoppelingen door gebruik te maken van zijn Rijksregisternummer mogelijk zijn of al gemaakt werden. Het Kadaster van Verbindingen kan daarom een transparantieverhogende maatregel genoemd worden. Het is precies zulke transparantieverhoging die nodig is om de huidige situatie met betrekking tot gegevenskoppelingen door gebruik te maken van het Rijksregisternummer meer transparant te maken. Zoals het onderzoek uitwees, is er op dit moment immers maar weinig transparantie te vinden bij het maken van gegevenskoppelingen door middel van het Rijksregisternummer. De bestaande machtigingen tot het gebruik van het Rijksregisternummer zijn in principe publiek toegankelijk, maar vormen zulk ongestructureerd geheel dat de gemiddelde burger hier niet de voor hem relevante informatie in kan terugvinden. Daarnaast zien we dat overheidsdiensten tot op zekere hoogte al logs bijhouden om te voldoen aan een aantal wettelijke verplichtingen. Hoewel zulke logs gebruikt kunnen gebruikt worden om de burger inzicht te verschaffen in wat er precies met zijn persoonsgegevens gebeurt, blijkt zulk initiatief tot op heden nog niet gerealiseerd te zijn. Indien we naar de ratio achter het gereguleerd gebruik van het Rijksregisternummer kijken, zien we dat deze maatregel er voornamelijk gekomen is met het oog op de bescherming van de persoonlijke levenssfeer. Een meer liberaal gebruik van zulk identificatienummer werd toen aanzien als een bedreiging voor de privacy. Gelet op het belang van het transparantieprincipe in de huidige regelgeving met betrekking tot de bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens, kan men het enigszins vreemd vinden dat een maatregel die bedoeld was als privacybeschermend net leidt tot een gebrek aan transparantie. Het Kadaster van Verbindingen zou daarom een goede aanvulling vormen op het huidige beleid met betrekking tot het gereguleerd gebruik van het Rijksregisternummer.

EVOLUTIE - Het Kadaster van Verbindingen kan ons echter ook nog verder leiden. We zagen immers dat het gebrek aan een sterk openbaarheidsprincipe – zoals de Zweedse samenleving dat kent – de belangrijkste reden is waarom het Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer nog niet heeft kunnen evolueren naar een meer geliberaliseerd gebruik van dit identificatienummer. Indien men een transparantieverhogende maatregel zoals het Kadaster van Verbindingen zou kunnen realiseren, concludeerden we al dat dit de transparantie met betrekking tot het gebruik van het Rijksregisternummer en de gegevenskoppelingen die gemaakt worden door middel van dit nummer sterk zou verhogen. Het Kadaster zou bijgevolg voor België kunnen betekenen wat het openbaarheidsprincipe betekent voor de Zweedse samenleving. In zulk geval zou er gepleit kunnen worden voor het liberaliseren van het gebruik van het Rijksregisternummer voor minstens de publieke sector. Het hier gevoerde onderzoek wees immers uit dat het gebruik van een nationale identificator zoals het Rijksregisternummer geen bijzonder gevaar vormt voor de privacybescherming. Ook in de publieke opinie blijken er geen bijzondere bezwaren te zijn tegen het gebruik van dit identificatienummer. We merkten echter op dat de gegevenskoppelingen door gebruik te maken van dit nummer wel een bezwaar kunnen vormen voor de privacybescherming. Indien het Kadaster dit probleem kan oplossen, is er geen juridisch bezwaar meer tegen het vrij gebruik van het Rijksregisternummer in de publieke sector. Daarenboven kan men argumenteren dat zulke liberalisatie de efficiëntie van de overheidsdiensten positief kan beïnvloeden en dat het vrij gebruik van het Rijksregisternummer zelfs positieve gevolgen met zich mee kan brengen voor de privacybescherming. Men kan dan overgaan tot een wetgevend initiatief voor de regeling van het vrij gebruik van het Rijksregisternummer.

AANVULLING OP HET HUIDIG BELEID - In een tweede piste werd dieper ingegaan op de huidige situatie met betrekking tot het gereguleerd gebruik van het Rijksregisternummer. Onder de eerste piste werd al aangehaald dat het Kadaster van Verbindingen als transparantieverhogende maatregel zeker ook nuttig kan zijn voor het huidige beleid. Het gebrek aan transparantie met betrekking tot het maken van gegevenskoppelingen door middel van het gebruik van het Rijksregisternummer staat immers haaks op de status van het gereguleerd gebruik als privacybeschermende maatregel. In het onderzoek naar de tweede piste werd duidelijk dat dit niet de enige contradictie is die teruggevonden kan worden in het huidige beleid. Het gebruik van het Rijksregisternummer op de e-ID – waar dit nummer voor alle betrokken partijen vrij toegankelijk is – staat immers haaks op de beschermde status van dit nummer. In deze piste werd daarom een technisch onderzoek gevoerd dat aantoont dat het mogelijk is om het gebruik van het Rijksregisternummer op de e-ID – en met name het gebruik van dit nummer in het authentiseringscertificaat – enigszins in te perken zonder dat de overheidsdiensten hierbij moeten inboeten aan efficiëntie. Voor deze piste kunnen we daarom concluderen dat het mogelijk is om het gereguleerd gebruik van het Rijksregisternummer te behouden, maar dat men zeker deze tegenstrijdigheden zal moeten wegwerken. Indien men de beleidskeuze voor het gereguleerd gebruik als privacybeschermende maatregel wil behouden, kan men immers niet verantwoorden dat het beschermde identificatienummer op bepaalde plaatsen wel vrij gebruikt kan worden en dat de privacybeschermende maatregel gepaard gaat met een gebrek aan transparantie.

CONCLUSIE - Concluderend kunnen we twee opties voorstellen voor de verdere ontwikkeling van het Belgisch beleid met betrekking tot het gebruik van het Rijksregisternummer en de gegevenskoppelingen die door middel van dit identificatienummer gemaakt kunnen worden. Allereerst is het mogelijk om het gereguleerd gebruik van deze nationale identificator te behouden. Het gebruik van zulke enige unieke identificator is zeker verdedigbaar vanuit het standpunt van de privacybescherming en het gereguleerd gebruik ervan zou inderdaad aanzien kunnen worden als een bijkomende maatregel ter bescherming van de privacy. Hier zijn echter twee belangrijke *caveats* bij te formuleren. Zo zal men een oplossing moeten zoeken voor de huidige tegenstrijdigheden in dat beleid, zoals het gebruik van dit identificatienummer in het authentiseringscertificaat op de e-ID. Vervolgens zal men ook transparantieverhogende maatregelen moeten aannemen, zoals het Kadaster van Verbindingen. Het onderzoek wees immers uit dat het gebrek aan transparantie bij het maken van gegevenskoppelingen door middel van het Rijksregisternummer de status van het gereguleerd gebruik van dit nummer als privacybeschermende maatregel kan ondermijnen. Wanneer het Kadaster van Verbindingen gerealiseerd wordt en de transparantie van het gebruik van het Rijksregisternummer en van de gegevenskoppelingen die gemaakt worden door middel van dit identificatienummer hierdoor sterk verhoogd wordt, kunnen we denken aan een tweede optie. Indien het Belgisch beleid kan evolueren naar een systeem dat steunt op transparantie en openbaarheid, mag men immers niet a priori de evolutie uitsluiten naar een systeem waar het nationale identificatienummer – minstens in de publieke sector – vrij gebruikt kan worden, mits expliciete en ondubbelzinnige toestemming van de betrokkene.

BIBLIOGRAFIE

WETGEVING

België

- Wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten, *B.S.* 17 juli 2007, 38587-38591.
- Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, *B.S*. 29 september 2001, 33070 e.v.
- Wet van 11 april 1994 betreffende de openbaarheid van bestuur, *B.S*. 30 juni 1994, 17662.
- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993.
- Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, *B.S*. 22 februari 1990.
- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.* 21 april 1984.
- K.B. van 5 december 1986 tot regeling van de toegang tot de informatiegegevens en van het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen in hoofde van instellingen die, in het kader van de wetgeving betreffende de ziekte- en invaliditeitsverzekering, opdrachten van algemeen belang vervullen, *B.S.* 19 december 1986, 17351 e.v.
- K.B. van 3 april 1984 betreffende de samenstelling van het identificatienummer van de personen die ingeschreven zijn in het Rijksregister van de natuurlijke personen, *B.S.* 21 april 1984.
- Wetsontwerp van 15 januari 2003 tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl.St.* Kamer 2002-03, nr. 50K2226/001-005; *Parl.St.* Senaat 2002-03, nrs. 2-1494/2 en 2-1494/3.

Duitsland

- Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weitere Vorschriften van 18 juni 2009, *BGBl. I* nr. 33/2009, 1359.
- Bundesdatenschutzgesetz (BDSG), *BGBl. I* 1990 S.2954, laatste amendering 14 augustus 2009, *BGBl. I* S. 2814.
- Gesetz über Personalausweise van 19 december 1950, laatst gewijzigd op 20 juli 2007, *BGBl. I* 1566.

Europese Unie

- Verordening 444/2009 van 28 mei 2009, *Pb.* L 142 van 6 juni 2009.
- Richtlijn 2006/24/EG van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *Pb.* L 105 van 13 april 2006, 54-63.

- Richtlijn 1999/93/EG van 13 december 1999 betreffende een betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *Pb*. L 013 van 19 januari 2000, 12 e.v.
- Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.* L van 23 november 1995, 31-50.

Oostenrijk

- Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz - E-GovG, 27 februari 2004, *BGBl. I* Nr. 10/2004.
- Datenschutzgesetz 2000 (DSG 2000), *BGBl. I* Nr. 165/1999.
- Verordnung des Bundeskanzlers, mit der Tätigkeiten der Stammzahlenregisterbehörde betreffend das Stammzahlenregister nach dem E-Government-Gesetz näher geregelt werden (Stammzahlenregisterverordnung – StZRegV), 2 maart 2005, *BGBl. II* Nr. 57/2005.

Portugal

- Lei Transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relative à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações van 17 juli 2008, nr. 32/2008, *DDR* I-A nr. 137, 4456-4457
- Lei cria o cartão de cidadão e rege a sua emissão e utilização van 5 februari 2007, nr. 7/2007, *DDR* I-A nr. 25, 942.
- Lei da protecçao de dados pessoais van 26 oktober 1998, nr. 67/98, *DDR* I-A nr. 247, 5536-5546.

Verenigd Koninkrijk

- Identity Cards Act, 2006, *c.* 15.
- Data Protection Act 1998, *c.* 29.
- The Identity Cards Act 2006 (National Identity Registration Number) Regulations 2009, S.I. 2009 No. 2574.

Zweden

- Personal Data Act, 29 april 1998, *SFS* 1998:204.
- Freedom of the Press Act, *SFS* 1949:105.

RECHTSPRAAK

- EHRM, *I v. Finland*, 2008.

RECHTSLEER

- ARTIKEL 29 WERKGROEP, “Opinion 4/2007 on the concept of personal data, WP136”, 20 juni 2007, *ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf*.

- BUNDESMINISTERIUM DES INNERN, “E-Government 2.0: Das Programm des Bundes“, 2006, *www.cio.bund.de/cae/servlet/contentblob/63262/publicationFile/4016/egov2_programm_des_bundes_download.pdf*.
- CABINET OFFICE, “Transformational Government Enabled by Technology”, november 2005, *www.cabinetoffice.gov.uk/media/141734/transgov-strategy.pdf.*
- CENTRE DE RECHERCHE PUBLIC GABRIEL LIPPMANN, “Interoperability of eGovernment Systems - The identification number, data sharing and data protection issues, 2005, *www.epractice.eu/files/media/media_508.pdf.*
- Commissie voor de bescherming van de persoonlijke levenssfeer, advies 12/2009 van 29 april 2009, *www.privacycommission.be/nl/docs/Commission/2009/advies_12_2009.pdf*.
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 14/2008 van 2 april 2008, *www.privacycommission.be/nl/docs/Commission/2008/advies_14_2008.pdf.*
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies 26/2003 van 12 juni 2003, *www.privacycommission.be/nl/docs/Commission/2003/advies_26_2003.pdf.*
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, Advies 30/1998 van 25 september 1998, *www.privacycommission.be/nl/docs/Commission/1998/advies_30_1998.pdf*.
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling 03/2009 van 1 juli 2009, *www.privacycommission.be/nl/docs/Commission/2009/aanbeveling_03_2009.pdf.*
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, aanbeveling 01/2008 van 24 september 2008, *www.privacycommission.be/nl/docs/Commission/2008/aanbeveling_01_2008.pdf.*
- DE BOT, D., *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteits-kaart*, Brugge, Vandenbroele, 2005, 469p.
- DEPREST, J., ROBBEN, F., “E-government: The Approach of the Belgian Federal Adminis-tration, 2003, *www.ksz-bcss.fgov.be/documentation/nl/documentation/Pers/2003%20-%20E-government%20paper%20v%201.0.pdf*, 6.
- DUMORTIER, J., ROBBEN, F., “Gebruikers- en toegangsbeheer bij het bestuurlijke elek-tronische gegevensverkeer in België*”*, *Computerrecht*, 2009, nr 2, 52-60.
- DUMORTIER, J., “eID en de paradox van het rijksregisternummer”, *Trends Business ICT*, maart 2005.
- EUSER, “Country Briefs”, *www.euser-eu.org/euser_countrybrief.asp?MenuID=83*.
- FIDIS, “D16.1: Conceptual Framework for Identity Management in eGovernment”, 2009, *fi-dis.net/fileadmin/fidis/deliverables/new_deliverables3/2009_04_16_D16.1_Framework_IDM_in_eGov_Final_2__1_.pdf.*
- FIDIS, “D13.3: Study on ID number policies”, 14 september 2007, *fi-dis.net/fileadmin/fidis/deliverables/fidis-wp13-del13_3_number_policies_final.pdf.*
- FIDIS, “Interoperability of Identities and Identity Management Systems”, *fi-dis.net/resources/deliverables/interoperability.*
- HUYSMANS, X., “Privacy-friendly Identity Management for eGovernment”, 2006, *www.w3.org/2006/07/privacy-ws/papers/25-huysmans-idm-egov*.

- IDABC, “eGovernment Factsheets”, ec.europa.eu/idabc/en/chapter/6016.
- IDABC, “eID Interoperability for PEGS: Update of Country Profiles”, *ec.europa.eu/idabc/en/document/6484.*
- IDABC, “eID Interoperability for PEGS: Analysis and Assessment of similarities and differences Impact on eID interoperability”, 2007, *ec.europa.eu/idabc/servlets/Doc?id=29618*.
- IDEM, “Deliverable 1.2 Conceptual Framework”, *onuitg.*
- IDEM, “Deliverable 1.3 Conceptual Framework Annex I. Glossary of terms (v1.07)”, 2007, *projects.ibbt.be/idem/uploads/media/2007-12-27.idem.glossary.v1.07.pdf.*
- ITAFIT, “Nationale persoonsnummers - Internationale ontwikkelingen: vooronderzoek”, 2002, *www.itafit.nl/download/?doc=natid&type=pdf.*
- LEITOLD, H., “The Austrian Citizen Card, a European Best Practice - Innovation Forum 2009”, 25 maart 2009, *online.tu-graz.ac.at/tug_online/voe_main2.getvolltext?pDocumentNr=107472,* 6.
- MODINIS/IDM, “The Status of Identity Management in European eGovernment Initiatives”, 2006, *www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.5_Identity_Management_Initiative_Report_1_IIR1.pdf.*
- MODINIS/IDM, “National IDM Profiles”, *www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/NationalProfiles*.
- NATIONAL TAX BOARD, “Population Registration in Sweden”, 2007, *www.skatteverket.se/download/18.5cbdbba811c9a768f0c80002830/717b04.pdf*.
- OBSERVATORIUM VAN DE RECHTEN OP HET INTERNET, ‘Advies nr. 3 betreffende denkpistes om het vertrouwen in de elektronische handel te versterken’, 2004, *www.internet-observatory.be/internet_observatory/pdf/advices/advice_nl_003.pdf.*
- OECD, “e-Government Studies: Belgium”, 2008, Paris, OECD Publications, 248p.
- OOSTENRIJKSE FEDERALE KANSELARIJ, “Administration on the Net: The ABC guide of eGovernment in Austria”, juli 2008, *www.digitales.oesterreich.gv.at/DocView.axd?CobId=19394*, 7-10.
- ROBBEN, F., “eGovernment, eHealth en bescherming van de privacy”, 18 april 2008, *www.law.kuleuven.be/icri/frobben/presentations/20080418nl.ppt.*
- ROBBEN, F., “Identity Management in e-Government - 1st MODINIS Workshop”, 2005, www.law.kuleuven.be/icri/frobben/presentations/20050504.ppt.
- ROBBEN, F., “e-Government in the Social Security Sector”, 2005, *www.law.kuleuven.be/icri/frobben/presentations/20050224.ppt.*
- SECTORAAL COMITÉ VAN HET RIJKSREGISTER, “beraadslaging 61/2009” van 7 oktober 2009, *www.privacycommission.be/nl/docs/RR-RN/2009/beraadslaging_RR_061_2009.pdf.*
- SECTORAAL COMITÉ VAN HET RIJKSREGISTER, “Beraadslaging 38/2009” van 17 juni 2009, *www.privacycommission.be/nl/docs/RR-RN/2009/beraadslaging_RR_038_2009.pdf*.
- SECTORAAL COMITÉ VAN HET RIJKSREGISTER, “beraadslaging 12/2008” van 12 maart 2008, *www.privacycommission.be/nl/docs/RR-RN/2008/beraadslaging__RR_012_2009.pdf*.
- SECTORAAL COMITÉ VOOR DE FEDERALE OVERHEID, “Beraadslaging FO nr. 05/2009”, 16 april 2009, *www.privacycommission.be/nl/docs/FO-AF/2009/beraadslaging_FO_005_2009.pdf*.
- STORK, “D2.3. Quality Authenticator Scheme”, 2009, www.*eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577*.

- UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, *E-Government Survey 2008: From E-Government to Connected Governance(ST/ESA/PAD/SER.E/112),* New York, United Nations Publication, 2008, 224.
- VAN ALSENOY, B., DE COCK, D., “Due Processing of Personal Data in eGovernment”, *Datenschutz und Datensicherheit*, 3/2008, 178-183.

BIJLAGE 1: HET REGISTER *EX TUNC*

1. PROBLEEMSTELLING

HET EX ANTE REGISTER - Bij het onderzoek naar hoe we het Kadaster van Verbindingen in de praktijk zouden moeten implementeren, werd duidelijk dat we hier op een aantal praktische problemen kunnen stoten. Zo belooft voornamelijk de praktische implementatie van het *ex ante* register zeer moeilijk of zelfs quasi onmogelijk te worden. Hier zijn twee redenen toe. Allereerst zien we dat alle machtigingen – zowel de vroeger verleende machtigingen als alle toekomstige machtigingen – opgenomen zullen moeten worden in het register. Aangezien we een grote verscheidenheid tussen de verschillende bestaande machtigingen kunnen aantonen, zal het moeilijk worden om al deze machtigingen in een enkele databank te verwerken. De tweede reden voor de moeilijke praktische implementatie van het *ex ante* register is dat de vroeger verleende machtigingen – en dan voornamelijk de machtigingen die dateren van voor de oprichting van het sectoraal comité van het Rijksregister – niet op een duidelijk gestructureerde wijze gepubliceerd zijn. We zullen dus al de vroeger verleende machtigingen handmatig in kaart moeten brengen.

NOOD AAN EEN STANDAARDFORMAAT VOOR TOEKOMSTIGE … - Men zal dus allereerst een akkoord moeten bereiken tot het handhaven van een standaardformaat voor toekomstige machtigingen. Om een *ex ante* register van verleende machtigingen op te richten, zal men immers al de verleende machtigingen moeten opnemen in het register. Wanneer deze machtigingen opgemaakt worden volgens een bepaald standaardformaat, kan men het mogelijk maken dat de voor het register relevante gegevens quasi-automatisch in dat register opgenomen worden. We zullen dan in de eerste plaats moeten kijken naar hoe zulk standaardformaat er zou moeten uitzien. Zoals we al aangaven kunnen we hier voornamelijk denken aan een structuur volgens een opmaaktaal zoals XML.

… EN VROEGER VERLEENDE MACHTIGINGEN - Een bijkomend probleem hier is dat niet enkel de toekomstige machtigingen in het register opgenomen moeten worden, maar ook de vroeger verleende machtigingen. Zoals we zagen werden de eerste machtigingen verleend bij koninklijk besluit, op advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Sinds de wetswijziging van 2003 worden de machtigingen tot het gebruik van het Rijksregister verleend door het sectoraal comité van het Rijksregister. Deze laatste machtigingen volgen een zekere vaste lay-out, maar zijn toch nog niet geschikt om automatisch verwerkt te worden in het *ex ante* register. Zij zullen bijgevolg ook handmatig verwerkt moeten worden. De machtigingen bij koninklijk besluit gaan gebukt onder de meer restrictieve houding die men toen nastreefde. De teksten van deze machtigingen kunnen hierdoor nog het best omschreven worden als volstrekt ongestructureerd en quasi onleesbaar. Ook hier zal een handmatige verwerking aan de orde zijn en is het maar de vraag of deze teksten zich zullen laten verwerken in een geordende structuur.

HET IN KAART BRENGEN VAN DE MACHTIGINGEN - Vooraleer men kan overgaan tot het omzetten van de vroeger verleende machtigingen naar het afgesproken standaardformaat, zal men uiteraard eerst een overzicht moeten hebben van deze machtigingen. Sinds de introductie van het sectoraal comité worden de beraadslagingen van deze instantie online gepubliceerd op de website van de Commissie voor de bescherming van de persoonlijke levenssfeer. Hoewel het hier niet de meeste gebruiksvriendelijke databank betreft, zien we dat de door het sectoraal comité verleende machtigingen in principe wel te vinden zijn. Het in kaart brengen van de vroegere machtigingen bij koninklijk besluit zal echter een grotere uitdaging vormen. Hoewel deze machtigingen allen in het Belgisch Staatsblad gepubliceerd werden, blijkt er nergens een officieel gestructureerd overzicht te bestaan van al deze machtigingen. Bestaande pogingen tot het gestructureerd in kaart brengen van deze machtigingen blijken geen volledig overzicht te kunnen bieden. Het lijkt er dan op dat we deze machtigingen dus handmatig in kaart zullen moeten brengen.

2. STANDAARDFORMAAT

2.1. WELKE STANDAARD VOOR DE MACHTIGINGEN?

EEN STANDAARD VOOR AUTOMATISCHE EN HANDMATIGE VERWERKING - Allereerst zullen we kijken welke standaard het meest geschikt is om de benodigde gegevens uit de machtigingen op geautomatiseerde wijze in het register te laten opnemen. Door het gebruik van zulk standaardformaat zullen de toekomstige machtigingen automatisch – of minstens quasi automatisch – opgenomen worden in het register. De keerzijde van het gebruik van een standaardformaat is dat ook de vroeger verleende machtigingen volgens eenzelfde structuur in het register zullen moeten opgenomen worden. Zoals we al aangaven, zullen vroeger verleende machtigingen op handmatige wijze verwerkt moeten worden. Bij het zoeken naar een standaardformaat voor de geautomatiseerde verwerking van toekomstige machtigingen zal men dus ook rekening moeten houden met de handmatige verwerking van vroeger verleende machtigingen.

EEN GESCHIKTE OPMAAKTAAL - Een ideale werkwijze zou er in bestaan om de toekomstige machtigingen op te stellen volgens een bepaalde structuur die ervoor kan zorgen dat de relevante elementen uit de machtigingen op geautomatiseerde – of minstens op quasi geautomatiseerde – wijze opgenomen worden in het register. We kunnen hier in de eerste plaats denken aan een opmaaktaal zoals XML (*Extensible Markup Language*).[331] Het register zou dan een logisch gestructureerd geheel worden dat zeer eenvoudig aangevuld kan worden. Indien de machtigingen zelf dan op gelijkaardige wijze gestructureerd worden, zullen deze zonder probleem in het register opgenomen kunnen worden.[332] De keuze voor XML als opmaaktaal voor het gestructureerd register is zeer voor de hand liggend. Bestaande applicaties zoals 'MijnDossier' maken immers al gebruik van deze opmaaktaal en ook in de structuur van de e-ID is XML sterk aanwezig. XML werd in deze toepassingen gekozen onder meer omdat het een vrij strikt geregelde opmaaktaal is.[333]

DE RELEVANTE GEGEVENS - Waar het hier allemaal om draait, zijn de gegevens uit de machtigingen die relevant zijn voor het *ex ante* register van de verleende machtigingen. Onder hoofdstuk 2.4.2 gaven we al een overzicht van de gegevens die voor de *ex post* loggings relevant kunnen zijn. Het spreekt voor zich dat we voor het *ex ante* register een gelijkaardige structuur kunnen aanhouden. Belangrijk is dat de logs aan de burger een antwoord bieden op de vraag: Wie kan met

[331] Meer specifiek zou men in dit geval kunnen denken aan de op XML gebaseerde XACML (*eXtensible Access Control Markup Language)*. XACML werd speciaal ontwikkeld met het oog op toegangscontrole.
[332] Deze materie werd al uitgebreid behandeld in DWTC-project I2/AP/110: Standaardisering van een digitaal burgerloket en gegevensuitwisseling in XML.
[333] XML wordt gespecificeerd door het W3C. Deze standaard wordt strikter gehandhaafd dan andere opmaaktalen zoals bijvoorbeeld HTML, *www.w3.org.*

betrekking tot mijn persoonsgegevens welke gegevenskoppelingen verrichten, met welk doel en voor welke tijdsduur? In de eerste plaats zal dus de verantwoordelijke voor de verwerking geïdentificeerd moeten worden. Zoals uit het eerder gevoerde onderzoek blijkt, kan het hier volstaan dat de identificatie gebeurt op het niveau van de organisatie. Als tweede punt zal men moeten aangeven welke verwerking en welke gegevenskoppelingen er kunnen plaatsvinden. In het kader van deze studie zal het gaan om gegevenskoppelingen door middel van het Rijksregisternummer. Vervolgens zullen de omvang van de verwerking, het doel van de verwerking, de voorwaarden voor de verwerking en de duurtijd moeten worden aangeduid. We moeten daarom nagaan hoe we deze gegevens kunnen distilleren uit de verschillende soorten machtigingen.

TOEKOMSTIGE MACHTIGINGEN - Machtigingen die verleend worden na de inwerkingtreding van het *ex ante* register zullen dus volgens een vast patroon gestructureerd moeten worden. De in de vorige paragraaf aangehaalde gegevens die relevant zijn voor het register zullen immers zonder enige moeite doorgestuurd moeten worden aan het register. Het formaat van de machtigingen verleend door het sectoraal comité wijst al op enige standaardisatie. We zullen echter nog zien dat er toch nog een aantal belangrijke onderlinge verschillen zijn tussen verschillende machtigingen. Zulke verschillen maken een geautomatiseerde verwerking van de voor het register relevante gegevens onmogelijk en moeten daarom vermeden worden. Wanneer toekomstige machtigingen zich strikt aan het afgesproken standaardformaat houden, zal de realisatie van het *ex ante* register *ex nunc* zonder noemenswaardige problemen moeten verlopen.

2.2. OPNAME VAN MACHTIGINGEN VERLEEND DOOR HET SECTORAAL COMITÉ

PRAKTIJKVOORBEELD - Nu we een idee hebben van de gegevens die in het *ex ante* register opgenomen zullen moeten worden, kunnen we kijken hoe we deze gegevens kunnen distilleren uit de machtigingen verleend door de het sectoraal comité. We zullen hiertoe een willekeurige beraadslaging van het sectoraal comité van het Rijksregister analyseren.

IDENTIFICATIE - De identificatie van de verantwoordelijke voor de verwerking is bij deze soort machtigingen redelijk voor de hand liggend. Zowel in de aanhef als in het dispositief wordt uitdrukkelijk de verantwoordelijke organisatie waarop de machtiging betrekking heeft aangeduid.[334] Wanneer we bijvoorbeeld naar beraadslaging 61/2009 van het sectoraal comité van het Rijksregister kijken, zien we in het dispositief: "*OM DEZE REDENEN, het Comité machtigt het Agentschap Ondernemen, afdeling Inspectie Economie, …".*[335] De verantwoordelijke voor de verwerking is dan uiteraard de afdeling Inspectie Economie van het Agentschap Ondernemen.

DRAAGWIJDTE VAN DE VERWERKING - Vervolgens geeft men de draagwijdte van de verwerking. Ook dit vinden we beknopt terug in de aanhef en meer uitgebreid in het dispositief. In het voorbeeld van beraadslaging 61/2009 is dit:

---

[334] De aanhef van nieuwe machtigingen begint steeds met de woorden "Betreft: Aanvraag van …". Indien het gaat om een uitbreiding van een eerder verleende machtiging, worden andere woorden gebruikt. In het dispositief begint men met "Om deze redenen, het Comité machtigt …". Ook hier wordt een andere formule gebruikt indien het om een uitbreiding of herziening van een eerder verleende machtiging gaat. Hoewel het dus zeker niet onmogelijk is om de verantwoordelijke voor de verwerking in deze soort machtigingen te identificeren, zien we wel dat deze verschillende formuleringen ertoe leiden dat een geautomatiseerde verwerking van deze machtigingen in het register uitgesloten is.

[335] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 9.

- "*een permanente toegang te hebben tot de informatiegegevens vermeld in artikel 3, eerste lid, 1°, 2° en 5°, WRR;*
- *het identificatienummer van het Rijksregister te gebruiken*".[336]

Net als de identificatie is de draagwijdte van de verwerking zeer duidelijk terug te vinden in het dispositief. Deze gegevens kunnen daarom zonder meer opgenomen worden in het register.

DOEL VAN DE VERWERKING - Na de identificatie en het aangeven van de draagwijdte van de verwerking geeft men – beknopt in de aanhef, meer uitgebreid onder punt A – het doel van de verwerking. In het voorbeeld van beraadslaging 61/2009 wordt er een tweeledig doel voor de verwerking aangehaald. Zo wil men allereerst controle uitoefenen door na te gaan of er daadwerkelijk banen werden gecreëerd en of er geen verschuiving van personeel gebeurde tussen onderling verbonden ondernemingen. Daarnaast streeft men ook administratieve vereenvoudiging na. Het dispositief verwijst naar de doeleinden die onder punt A staan vermeld. Dit leidt er toe dat deze doeleinden niet zo voor de hand liggend aangereikt worden als voorgaande elementen. Voor deze doeleinden moeten we inderdaad de tekst van punt A gaan ontleden, wat een geautomatiseerde verwerking van deze gegevens in het *ex ante* register definitief uitsluit. Ook een handmatige analyse is hier niet zonder gevaren. Men kan immers niet zonder meer de hele tekst onder punt A integraal overnemen. Men zal er dus voor moeten zorgen dat men de precieze doeleinden uit deze tekst weet te halen.

GEGEVENSKOPPELINGEN - Net als de identificatie en de draagwijdte zijn de mogelijke gegevenskoppelingen die kunnen voortvloeien uit deze machtiging vrij duidelijk af te leiden uit de tekst van deze machtigingen. Het sectoraal comité onderzoekt immers steeds of de aanvraag voldoet aan de eis van proportionaliteit van de verwerking en of de voorgestelde verwerking voldoende beveiligd is. Bij het onderzoeken van het proportionaliteitsprincipe wordt er steeds stilgestaan bij de netwerkverbindingen die door middel van het gebruik van het Rijksregisternummer tot stand kunnen komen. In het voorbeeld van beraadslaging 61/2009 blijkt dat er "*er een netwerkverbinding* […] *tot stand* [zal] *komen met de Kruispuntbank van de Sociale Zekerheid voor het bekomen van informatie die beschikbaar is binnen het netwerk van de sociale zekerheid*."[337] Het comité bepaalt daarom dat "*het identificatienummer van het Rijksregister slechts gebruikt kan worden in relaties met derden voor zover dat kadert in de doeleinden waarvoor zij eveneens gemachtigd werden om dit nummer te gebruiken*."[338]

VOORWAARDEN VOOR DE VERWERKING - DISPOSITIEF - De voorwaarden waaraan de verwerking en de gegevenskoppeling moeten voldoen staan volgens het dispositief uiteengezet in de beraadslaging. Dit betekent uiteraard dat we deze voorwaarden doorheen de hele tekst van de machtiging kunnen terugvinden. Dit wil zeggen dat we net als bij het doel van de verwerking het hele document zullen moeten analyseren om die voorwaarden er uit af te kunnen leiden. Soms reikt het dispositief zelf ook al voorwaarden aan. Zo vermeldt het dispositief in beraadslaging 12/2008 dat de machtiging slechts uitwerking zal krijgen "*nadat het Comité op basis van de door de gemachtigden verstrekte stukken en inlichtingen heeft vastgesteld dat een andere consulent inzake informatieveiligheid werd aangesteld die de nodige waarborgen biedt en aan de tekort-*

[336] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 9.
[337] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 8.
[338] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 8.

komingen aangestipt in punt D.2. werd verholpen".[339] Ondanks het feit dat men hier de werking van de machtiging expliciet verbindt aan een opschortende voorwaarde, wordt er verder toch nog verwezen naar andere voorwaarden in de tekst van de beraadslaging. Een handmatige analyse van de gehele tekst is met andere woorden onvermijdelijk. Het dispositief vermeldt wel nog – en dit vinden we in elke machtiging terug – dat de aanvrager van de machtiging een vragenlijst moet invullen. Hoewel het niet naleven van deze verplichting blijkbaar niet de uitwerking van de machtiging opschort, kunnen we het toch wel als een zekere voorwaarde beschouwen. Deze voorwaarde heeft echter geen belang voor het *ex ante* register.

VOORWAARDEN VOOR DE VERWERKING - TEKST - Zoals we al zagen, wordt er in de tekst van de beraadslaging voornamelijk onderzocht of het proportionaliteitsprincipe wel voldoende nageleefd zal worden bij de voorgestelde verwerking en gegevenskoppeling. Daar het naleven van dit principe een wettelijke verplichting is, kunnen we dit niet beschouwen als een voorwaarde opgelegd door het sectoraal comité van het Rijksregister. We zullen dus nog dieper moeten graven om enige voorwaarden af te kunnen leiden uit de tekst. Een eerste voorwaarde die werkelijk van het comité lijkt te komen en niet een loutere bevestiging van bestaande wettelijke verplichtingen lijkt te zijn, is het gegeven dat "*het identificatienummer van het Rijksregister slechts gebruikt kan worden in relaties met derden voor zover dat kadert in de doeleinden waarvoor gemachtigd werd om dit nummer te gebruiken.*"[340]Hoewel het comité hier nadrukkelijk de aandacht op vestigt, zouden we ook dit als een logische gevolgtrekking kunnen beschouwen. Het Rijksregisternummer gebruiken voor doeleinden waarvoor men niet gemachtigd werd om het te gebruiken, schendt vanzelfsprekend de grenzen van de machtiging en dus ook het principiële verbod op het gebruik van het Rijksregisternummer zonder voorafgaande machtiging. Daarnaast zou zulke praktijk verder gaan dan wat strikt nodig is voor het bereiken van het doel van de verwerking. Dit schendt uiteraard de principes van de wetgeving op de verwerking van persoonsgegevens. Ondanks het feit dat het comité de aandacht vestigt op dit gegeven, is ook dit dus maar met moeite te beschouwen als een werkelijke voorwaarde. Een gelijkaardig verschijnsel vinden we terug in het onderzoek naar de beveiliging van de gegevens. Hier wordt vermeldt dat de aanvrager, "*zoals voorgeschreven door artikel 12 WRR, een lijst* [moet] *opstellen waarop de personen vermeld worden die toegang hebben tot de informatiegegevens van het Rijksregister en het identificatienummer ervan gebruiken. Deze lijst zal voortdurend geactualiseerd en ter beschikking van het Comité gehouden worden*."[341] Hoewel men hier een voorwaarde uit zou kunnen afleiden, gaat het dus ook hier slechts om een bevestiging van een wettelijke verplichting. Ook in andere beraadslagingen worden we met hetzelfde probleem geconfronteerd.

VOORWAARDEN VOOR DE VERWERKING - CONCLUSIE - We zien dat de voorwaarden voor de verwerking het moeilijkste element is om in deze teksten terug te vinden. Waar andere elementen vrij duidelijk of na een relatief eenvoudige analyse aangeduid kunnen worden, vereist het zoeken naar de voorwaarden een minutieuze lezing van de tekst. Veelal blijkt wat we zouden kunnen aanduiden als voorwaarden slechts een loutere bevestiging van wettelijke verplichtingen te zijn. Het spreekt voor zich dat zulke bevestiging bijgevolg niet moet worden opgenomen in het *ex ante* register. Daarnaast is er nog een probleem met de voorwaarden zonder opschorting van de

[339] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 12/2008 van 12 maart 2008, *www.privacycommission.be,* 11.
[340] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 8.
[341] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 9.

werking van de machtiging. De burger zal immers uit het register niet kunnen afleiden of aan alle voorwaarden voldaan is. Het lijkt daarom wenselijk om enkel opschortende voorwaarden op te leggen, waarbij het sectoraal comité duidelijk kan aangeven of er voldaan is aan die voorwaarden of niet.

DUURTIJD - Ook dit gegeven kan net als de draagwijdte en de identificatie zonder meer uit het dispositief afgeleid worden. Beraadslaging 61/2009 vermeldt duidelijk dat de machtiging “voor onbepaalde duur” verleend wordt.[342] Het afleiden van de duurtijd uit deze soort machtiging zal dus geen probleem mogen opleveren. In het licht van de zonet besproken problematiek van de opschortende voorwaarde kunnen we ook aanbevelen dat het register niet enkel aangeeft voor hoelang de machtiging verleend is, maar ook vanaf wanneer deze termijn begint te lopen. Op deze manier kan de burger meteen zien of er aan eventuele opschortende voorwaarden voldaan is. De machtiging kan immers maar gelden vanaf er aan zulke voorwaarden voldaan is.

CONCLUSIE - Bij deze soort machtigingen zien we dat het gebruik van een zekere vaste opmaak er toe leidt dat al de voor het register relevante gegevens zonder problemen uit de machtiging afgeleid kunnen worden. De invoer van de benodigde gegevens uit deze machtigingen in het register zal weliswaar handmatig moeten gebeuren, maar dit lijkt in dit stadium geen onoverkomelijk probleem te zijn. Wanneer we dan naar het voorbeeld van beraadslaging 61/2009 van het sectoraal comité van het Rijksregister kijken, kunnen we tot een volgende XML opmaak komen.[343]


```xml
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes" ?>
- <ex_ante_register type="machtiging tot gebruik Rijksregisternummer">
  - <machtiging jaar="2009">
    - <machtiging nr="RN/MA/2009/046">
        <identificatie>Agentschap Ondernemen, afdeling Inspectie Economie</identificatie>
        <draagwijdte>1/ Een permanente toegang hebben tot de informatiegegevens vermeld in
          artikel 3, eerste lid, 1°, 2° en 5°, WRR.
          2/ Het identificatienummer van het Rijksregister gebruiken.</draagwijdte>
        <doel>1/ Nagaan of daadwerkelijk banen werden gecreëerd en of er geen verschuiving van
          personeel gebeurde tussen onderling verbonden ondernemingen.
          2/ Administratieve vereenvoudiging.</doel>
        <gegevenskoppeling>Netwerkverbinding met de Kruispuntbank van de Sociale Zekerheid
          voor het bekomen van informatie die beschikbaar is binnen het netwerk van de sociale
          zekerheid.</gegevenskoppeling>
        <voorwaarden>1/ Het Agentschap Ondernemen afdeling Inspectie Economie moet een
          vragenlijst met betrekking tot de informatieveiligheidstatus waarheidsgetrouw invullen
          en terugbezorgen aan het Comité.
          2/ Het identificatienummer van het Rijksregister kan slechts gebruikt worden in relaties
          met derden voor zover dat kadert in de doeleinden waarvoor gemachtigd werd om dit
          nummer te gebruiken.
          3/ De aanvrager moet, zoals voorgeschreven door artikel 12 WRR, een lijst opstellen
          waarop de personen vermeld worden die toegang hebben tot de informatiegegevens van
          het Rijksregister en het identificatienummer ervan gebruiken. Deze lijst zal voortdurend
          geactualiseerd en ter beschikking van het Comité gehouden worden.</voorwaarden>
        <duurtijd>Onbepaalde duur</duurtijd>
      </machtiging>
    </machtiging>
</ex_ante_register>
```


[342] SECTORAAL COMITÉ VAN HET RIJKSREGISTER, beraadslaging 61/2009 van 7 oktober 2009, *www.privacycommission.be,* 9.

[343] Merk op dat we voor de duidelijkheid enkel de gegevens uit beraadslaging 61/2009 gebruikt hebben. De hier vermelde voorwaarden zijn – zoals besproken – bezwaarlijk werkelijke voorwaarden te noemen, maar werden louter ter illustratie opgenomen.

XML OPMAAK - Uit dit overzicht blijkt hoe men de bestaande machtigingen kan exporteren naar een gestructureerd register dat volgens XML opgemaakt wordt. In de bestaande teksten van de machtigingen kan men de relevante gegevens aanduiden met de bijbehorende XML-tag. Die tags geven dan een XML opmaak zoals hier voorgesteld wordt. Deze opmaak kan vervolgens eenvoudig toegevoegd worden aan een bestaande databank, op voorwaarde dat eenzelfde semantische context gebruikt wordt.

2.3. OPNAME VAN MACHTIGINGEN VERLEEND BIJ KONINKLIJK BESLUIT

PRAKTIJKVOORBEELD - Na de analyse van de machtigingen verleend door het sectoraal comité van het Rijksregister, zullen we nu de machtigingen tot het gebruik van het Rijksregisternummer verleend bij koninklijk besluit analyseren. Zoals we al aangaven, zal duidelijk worden dat het geen sinecure zal zijn om de voor het register benodigde gegevens uit deze soort machtigingen af te leiden. We zullen vervolgens kijken of het mogelijk is om de benodigde gegevens in de voorgestelde XML opmaak onder te brengen. Bij de analyse zullen we gebruik maken van het koninklijk besluit van 5 december 1986 met betrekking tot de ziekte- en invaliditeitsverzekering.[344]

IDENTIFICATIE - De titel van het koninklijk besluit geeft al voor een deel de identiteit van de verantwoordelijke voor deze verwerking en gegevenskoppeling weer. Het gaat hier om de instellingen die in het kader van de ziekte- en invaliditeitsverzekering opdrachten van algemeen nut vervullen. Dit is uiteraard geen voldoende identificatie. We zullen in de tekst zelf moeten zoeken naar een identificatie op het niveau van de betrokken organisaties – of deelorganisaties – zelf. Artikel 1, §1 beschrijft de betrokken organisaties als "*de verbonden en de landsbonden respectievelijk bepaald bij artikel 2, littera's b en c van de wet van 9 augustus 1963 tot instelling en organisatie van een regeling voor verplichte ziekte- en invaliditeitsverzekering".* De bijlage bij de wet somt deze organisaties exhaustief bij naam op. Het lijkt daarom aangewezen deze bijlage te hanteren als de identificatiegegevens voor deze machtiging. Dit zal echter niet voldoende zijn. Artikel 1, §1 bepaalt immers verderop dat deze lijst uitgebreid kan worden. Er wordt verwezen naar een inventaris bijgehouden door het Ministerie van Sociale Voorzorg – de huidige Federale Overheidsdienst Sociale Zekerheid – waarin deze organisaties vermeld worden. We zouden dan in principe naar die inventaris moeten verwijzen, omdat deze de meest recente identificatiegegevens zou moeten bevatten. De lijst uit de bijlage van dit koninklijk besluit mag met andere woorden niet als volledig betrouwbaar beschouwd worden. Deze machtiging handelt echter niet enkel over de zonet aangehaalde instellingen. Artikel 1, §2 gaat over ziekenfondsen, §4 over verplegingsinrichtingen en rust- en verzorgingstehuizen, §5 over tariferingsdiensten en §6 over inrichtingen voor revalidatie en herscholing. Bij elk van deze instellingen hoort een inventaris die bijgehouden wordt door een overheidsdienst. Ook hier zou dus in principe naar die inventarissen verwezen kunnen worden. Tot slot bepaalt artikel 6 dat de verwerkende suborganen of personen aangeduid moeten worden door de verantwoordelijke organisaties die opgesomd werden in artikel 1. Indien we deze gegevens – uiteraard op afgeschermde wijze – wensen op te nemen in het register, zullen we bijgevolg de betrokken organisaties moeten contacteren.

[344] Koninklijk besluit van 5 december 1986 tot regeling van de toegang tot de informatiegegevens en van het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen in hoofde van instellingen die, in het kader van de wetgeving betreffende de ziekte- en invaliditeitsverzekering, opdrachten van algemeen belang vervullen, *B.S.* 19 december 1986, 17351 e.v.

DRAAGWIJDTE VAN DE VERWERKING - Ook hiertoe moeten we kijken naar de afzonderlijke delen van artikel 1 van het koninklijk besluit. Bij elk van de zonet aangehaalde organisaties wordt opgesomd waartoe zij onder welke voorwaarden en met betrekking tot welke personen bevoegd zijn. Algemeen genomen gaat het om de toegang tot de gegevens opgenomen in het Rijksregister – "*informatiegegevens vermeld in artikel 3, eerste lid, 1° tot 9°, en tweede lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen"* – en het gebruik van het Rijksregisternummer. Deze toelating wordt echter beperkt door artikelen 3 tot 8 van het koninklijk besluit. Daarnaast mag men enkel het Rijksregisternummer van hun leden of patiënten gebruiken. We zullen nog zien dat een aantal van de beperkingen uit artikelen 3 tot 8 ondergebracht kan worden bij andere gegevens. Een eerste beperking vinden we in artikel 3 dat bepaalt dat het Rijksregisternummer enkel als een identificatiemiddel gebruikt mag worden. Artikel 4 brengt hier enige nuance in door te bepalen dat het Rijksregisternummer als identificatiemiddel gebruikt mag worden in interne en externe betrekkingen voor de vervulling van bepaalde taken. Het begrip 'externe betrekkingen' wordt vervolgens zorgvuldig gedefinieerd. De vermelding dat bepaalde actoren slechts voor een beperkte periode en voor een beperkt doel over het Rijksregisternummer mogen beschikken, is een beperking op deze nuance. Hoewel artikel 4 enigszins kan doen denken aan de mogelijkheid van gegevenskoppeling, bepaalt artikel 8 dat het Rijksregisternummer in de externe betrekkingen uit artikel 4 enkel als identificatiemiddel gebruikt mag worden. Dan is er nog artikel 7 dat bepaalt dat het Rijksregisternummer in bepaalde gevallen niet louter als identificatiemiddel gebruikt moet worden. In bepaalde gevallen is de vermelding van dit identificatienummer zelfs verplicht.

DOEL VAN DE VERWERKING - Het doel van de verwerking moet in dit koninklijk besluit zeer restrictief geïnterpreteerd worden. Artikel 1 bepaalt immers dat de machtiging uitsluitend geldt voor het uitvoeren van taken die opgelegd zijn door een bepaalde wet, "*alsmede voor het vervullen van de taken welke hun zijn opgelegd door of krachtens een wets- of reglementsbepaling betreffende de sociale zekerheid".* Deze bepaling – die voor al de in artikel 1 opgesomde instelling gelijkaardig is – wordt beperkt gespecificeerd door de doeleinden opgesomd in artikelen 3 tot 8. Wanneer we die artikelen echter analyseren, moeten we echter vaststellen dat het hier niet zozeer gaat om werkelijke doeleinden, dan om beperkingen op de draagwijdte van de machtiging. Het lijkt ons daarom ook aangewezen om deze bepalingen bij de draagwijdte onder te brengen in plaats van deze aan te duiden als doeleinden van de verwerking.

GEGEVENSKOPPELINGEN - Het koninklijk besluit verwijst niet letterlijk naar gegevenskoppelingen of netwerkverbindingen. Dit is uiteraard niet verwonderlijk aangezien de term netwerkverbindingen maar relatief recent aan de wet toegevoegd werd. Artikel 5 lijkt echter het principe van de gegevenskoppeling al aan te halen. Het artikel bepaalt de voorwaarden om de in artikel 1 vermelde organisaties de gegevens uit het Rijksregister mee te delen en om het Rijksregisternummer als identificatiemiddel te gebruiken. Gelijkaardig aan artikel 4 volgt hier een uitgebreide definitie van het begrip 'derden'. Opvallend is dat deze 'derde' maar voor een beperkte periode en voor een beperkt doel mag beschikken over deze gegevens en het Rijksregisternummer. Merk op dat het hier slechts om de voorwaarden tot gegevenskoppeling gaat, en dat er bijgevolg geen overzicht geboden wordt van de precieze gegevenskoppelingen die men kan verwachten.

VOORWAARDEN VOOR DE VERWERKING - Het koninklijk besluit in dit voorbeeld lijkt in principe geen expliciete opschortende voorwaarden te bepalen. In artikel 1 wordt wel meermaals verwezen naar de voorwaarden en de doeleinden gesteld door de artikelen 3 tot 8. Deze artikelen bevatten echter voornamelijk bepalingen in verband met de draagwijdte van de machtiging, het doel van de verwerking en de gegevenskoppelingen. Wat men hier aanduidt als voorwaarden kunnen we daarom ook opvatten als beperkingen en aanvullingen op deze voorgaande bepalingen. Het lijkt ons daarom meer aangewezen om – bij wijze van voorbeeld – de beperkingen bij artikel 4 te classificeren als deel van de gegevens met betrekking tot de draagwijdte van deze machtiging, dan om deze beperkingen apart te beschouwen als voorwaarden voor de verwerking. Wat we eventueel wel kunnen beschouwen als een werkelijke voorwaarde, is bijvoorbeeld de bepaling uit artikel 1, §2 dat de toegang voor de ziekenfondsen slechts kan gebeuren door middel van bemiddeling door de betrokken landsbond of het verbond waarbij het ziekenfonds aangesloten is. Een andere bepaling in dit koninklijk besluit die we als voorwaarde kunnen aanduiden, is het gegeven uit artikel 1, §3 dat het gebruik van het Rijksregisternummer nader geregeld moet worden door middel van onderrichtingen. Uit artikel 9 volgt immers dat de bepalingen uit artikelen 3 tot 8 pas in werking kunnen treden nadat de onderrichtingen bekend gemaakt zijn. Deze onderrichtingen schorten met andere woorden de werking van deze machtiging op en zijn bijgevolg te beschouwen als een opschortende voorwaarde.

DUURTIJD - Dit koninklijk besluit maakt in principe geen melding van enige duurtijd. De enige vermeldingen die betreffende tijdsaanduiding af te leiden zijn uit deze tekst, zijn de inwerkingtreding van bepaalde artikelen en de notie dat de gegevens en het identificatienummer niet langer mogen bijgehouden worden dan nodig voor het bereiken van het doel van de verwerking. Een meer specifieke aanduiding vinden we niet terug.

CONCLUSIE - Nu we ons enigszins een idee kunnen vormen over hoe we de gegevens uit het koninklijk besluit dat we hier als voorbeeld gebruikten moeten onderverdelen in de hier voorgestelde categorieën van de voor het *ex ante* register relevante gegevens, zullen we moeten trachten dit alles samen te vatten in de structuur die we bij de analyse van de machtigingen door het sectoraal comité voorstelden. Zoals we al konden vermoeden, laten de machtigingen bij koninklijk besluit zich echter niet zonder meer omzetten in een bepaalde standaardstructuur. De tekst van deze machtigingen is immers het ongelukkige resultaat van het toenmalige artikel 8 van de Wet op het Rijksregister en de restrictieve houding van de Raadgevende Commissie ter bescherming van de persoonlijke levenssfeer.[345] Wanneer we dit soort machtigingen toch willen onderbrengen in de hier voorgestelde structuur, kunnen we niet anders dan alle beperkingen en constructies in de tekst quasi integraal over te nemen. Dit leidt er dan toe dat de voor opname in het register gestructureerde versie er haast al even onleesbaar zal uitzien als de originele tekst van het koninklijk besluit. Daarnaast merken we ook op dat deze machtigingen door verschillende administraties opgesteld zijn, waarbij elke administratie er uiteraard haar eigen aanpak op na houdt.[346] Dit leidde er toe dat er grote verschillen bestaan tussen deze machtigingen, wat de overzichtelijkheid van de situatie uiteraard niet ten goede komt. Men zou er daarom aan kunnen denken om deze machtigingen te herzien. Op die manier kan men meteen de overbodige machtigingen eruit filteren. Vervolgens kan men de nog relevante machtigingen enigszins aanpassen aan de huidige noden, waarbij deze nieuwe versie van de machtiging onmiddellijk volgens het afgesproken standaardformaat opgesteld kan worden. Zulk initiatief zal echter niet

[345] F. ROBBEN, "De toegang tot het Rijksregister van de natuurlijke personen en het gebruik van het identificatienummer van dat register" in C. PERSYN, D. SIMOENS, J. VAN LANGENDONCK en R. WUYTS (eds.), *Volmachten en sociale zekerheid 1986-87*, Reeks Sociaal Recht nr. 32, Deurne, Kluwer Rechtswetenschappen, 1987, 101-128.

[346] F. ROBBEN, "De toegang tot het Rijksregister van de natuurlijke personen en het gebruik van het identificatienummer van dat register" in C. PERSYN, D. SIMOENS, J. VAN LANGENDONCK en R. WUYTS (eds.), *Volmachten en sociale zekerheid 1986-87*, Reeks Sociaal Recht nr. 32, Deurne, Kluwer Rechtswetenschappen, 1987, 101-128.

zonder meer gerealiseerd kunnen worden. Zo krijgen we al meteen te maken met een probleem met betrekking tot de bevoegdheid van het sectoraal comité van het Rijksregister voor het herwerken van deze koninklijke besluiten. Het sectoraal comité kan aan de begunstigden van de machtigingen bij koninklijk besluit immers niet minder rechten verlenen dan hen toegekend werden krachtens de koninklijke besluiten. Het overnemen van de exacte draagwijdte uit deze machtigingen lijkt echter moeilijk te verzoenen met het doel om door middel van zulke hervorming tot een duidelijke en gestructureerde tekst te komen. Daarnaast zal er ook rekening gehouden moeten worden met het feit dat een volledige herschrijving van de bestaande machtigingen bij koninklijk besluit een aanzienlijke werklast met zich mee zal brengen voor het sectoraal comité van het Rijksregister. Hoewel zulk coördinerend en hervormend initiatief daarom zeker niet gemakkelijk te realiseren zal zijn, moeten we toch besluiten dat een dergelijk initiatief te verkiezen valt boven het krampachtig handhaven van de bestaande machtigingen bij koninklijk besluit. Dit wordt nog duidelijker wanneer we trachten het onderzochte koninklijk besluit te converteren naar de hier gebruikte XML structuur. Met het oog op de burger als doelgroep van dit register, is er besloten de tekst zoveel mogelijk te beperken, met verwijzingen naar de betrokken artikelen uit het koninklijk besluit waar verduidelijking nodig was. De onvolledigheid en onduidelijkheid van dit voorbeeld toont aan dat het quasi onmogelijk zal zijn om deze ingewikkelde machtigingen in een logisch geordende structuur onder te brengen.

```
  <?xml version="1.0" encoding="iso-8859-1" standalone="yes" ?>
- <ex_ante_register type="machtiging tot gebruik Rijksregisternummer">
  - <machtiging jaar="1986">
    - <machtiging nr="KB 1986-12-05/33">
        <identificatie>De verbonden en landsbonden, de ziekenfondsen, de verplegingsinrichtingen,
          de rust-en verzorgingstehuizen, de tariferingsdiensten en de inrichtingen voor
          revalidatie en herscholing, zoals ingeschreven op de inventaris gehouden door de
          bevoegde overheidsdienst. (art. 1)</identificatie>
        <draagwijdte>1/ Toegang tot de informatiegegevens vermeld in artikel 3, eerste lid, 1° tot
          9° en tweede lid, WRR: enkel de verbonden en landsbonden en de ziekenfondsen. (art. 1)
          2/ Gebruik van het identificatienummer van het Rijksregister, beperkt tot hun
          leden/patiënten, en enkel als identificatiemiddel, tenzij in bepaalde gevallen cfr. art. 4:
          alle gemachtigden. (art. 1, art. 3-8)</draagwijdte>
        <doel>Vervullen van taken die, binnen de perken van de toepassing van de wet van 9
          augustus 1963 en van de wet van 23 juni 1894 houdende wijziging van de wet van 3 april
          1851 op de maatschappijen van onderlinge bijstand, tot hun respectieve bevoegdheden
          behoren, alsmede voor het vervullen van de taken die hun zijn opgelegd door of
          krachtens een wets- of reglementsbepaling betreffende de sociale zekerheid. (art. 1, §1,
          eerste lid)</doel>
        <gegevenskoppeling>Zie artikelen 4 en 5 voor voorwaarden voor de
          gegevenskoppeling.</gegevenskoppeling>
        <voorwaarden>1/ De toegang tot het Rijksregister voor de ziekenfondsen is onderworpen
          aan bemiddeling door de betrokken landsbond of verbond. (art. 1, §2, tweede lid)
          2/ Het gebruik van het Rijksregisternummer moet nader geregeld worden door
          onderrichtingen. (art. 1, §3 en art. 9)</voorwaarden>
        <duurtijd>Onbekend</duurtijd>
      </machtiging>
    </machtiging>
  </ex_ante_register>
```

MATRIX VAN HET RIJKSREGISTER - Er kan als oplossing voor dit probleem nog gedacht worden aan een andere mogelijkheid. In recente jaren heeft het Rijksregister de relevante gegevens uit de geldende machtigingen immers geïmplementeerd in een matrixmodel. Deze relevante gegevens worden met andere woorden ingezet in het systeem voor gebruikers- en toegangsbeheer voor toegang tot de gegevens in het Rijksregister. Een dergelijke gegevensbank waar een aantal van de voor het *ex ante* register relevante gegevens uit de machtigingen – zowel de machtigingen bij koninklijk besluit als de machtigingen door het sectoraal comité – op gestructureerde wijze samengebracht worden, kan uiteraard de werklast die gepaard gaat met de realisatie van het *ex ante* register aanzienlijk verminderen. Het zou daarom interessant kunnen zijn om te onderzoeken of een dergelijke matrix opengesteld kan worden om op die manier andere projecten – zoals het Kadaster van Verbindingen – te vergemakkelijken. Aangezien de matrix voor een groot deel bestaat uit gegevens die ook teruggevonden kunnen worden in de publiek toegankelijke machtigingen, lijken hier immers niet onmiddellijk ernstige bezwaren tegen te zijn. We moeten hier echter bij opmerken dat deze toegangsmatrix slechts bestemd is voor intern gebruik binnen het Rijksregister. Daarnaast kan men opmerken dat de wetgever het Kadaster van Verbindingen – en hierbij inbegrepen het gebruikers- en toegangsbeheer van een dergelijke infrastructuur – heeft voorbehouden aan het sectoraal comité van het Rijksregister. Wanneer men het matrixmodel van het Rijksregister wil inschakelen in het Kadaster van Verbindingen, zou men kunnen argumenteren dat er dan sprake is van een overdracht van een taak die wettelijk toegewezen is aan het sectoraal comité van het Rijksregister naar de diensten van het Rijksregister zelf. Deze oplossing kan in zulk geval niet aanvaard worden.

3. MACHTIGINGEN IN KAART BRENGEN

MACHTIGING DOOR HET SECTORAAL COMITÉ - Zoals we al zagen, zal het niet enkel een probleem zijn om de vroeger verleende machtigingen via de omzetting naar een afgesproken standaard op te nemen in een logisch gestructureerd register. Men zal al deze bestaande machtigingen eerst in kaart moeten brengen. Hoewel de machtigingen door het sectoraal comité wel enigszins overzichtelijk gepubliceerd zijn op de website van de Commissie voor de bescherming van de persoonlijke levenssfeer, merken we op dat het toch nog enig werk zal vereisen om al de verleende machtigingen in kaart te brengen. Zo wordt er geen onderscheid gemaakt tussen de beraadslagingen waarna een machtiging verleend werd en de negatieve beraadslagingen. Men zal dus alle beraadslagingen moeten raadplegen om tot een overzicht te komen van het aantal effectief verleende machtigingen. Wanneer we de website van de Commissie consulteren komen we met betrekking tot de beraadslagingen van het sectoraal comité van het Rijksregister tot ongeveer 300 beraadslagingen sinds de oprichting van dit comité.[347] We kunnen hieruit afleiden dat het toch nog enige inspanning zal vergen om de effectief verleende machtigingen door het sectoraal comité in kaart te brengen.

MACHTIGINGEN BIJ KONINKLIJK BESLUIT - In tegenstelling tot de machtigingen door het sectoraal comité zijn de machtigingen bij koninklijk besluit niet op een systematisch geordende wijze gepubliceerd op een website. Net als andere koninklijke besluiten werden deze machtigingen in principe enkel in het Belgisch Staatsblad gepubliceerd, wat het in kaart brengen van die machtigingen zeker niet vereenvoudigt. Het is daarom zeer moeilijk om een enigszins betrouwbaar overzicht te geven van het precieze aantal van dit soort machtigingen er ooit afgekondigd is en hoeveel van die machtigingen vandaag nog gelden. Ook eerdere pogingen tot het in kaart brengen van deze machtigingen zijn grotendeels als onvolledig beschouwen. We denken dan aan een consultatie van de databank Juridat – die ons 150 machtigingen oplevert – en een zeer verdienstelijke poging van Frank Robben – die in een artikel over deze problematiek een vijftigtal machtigingen

[347] Het gaat hier om ongeveer 77 beraadslagingen in 2009, 58 beraadslagingen in 2008, 46 beraadslagingen in 2007, 36 beraadslagingen in 2006, 53 beraadslagingen in 2005 en 36 beraadslagingen in 2004.

aanhaalt.[348] Het wellicht meest volledige overzicht van machtigingen tot het gebruik van het Rijksregisternummer verleend bij koninklijk besluit vinden we terug bij Dirk De Bot. In zijn boek tracht hij een volledig overzicht te bieden van alle machtigingen van deze soort.[349] Indien we dit overzicht als door officiële instanties kunnen laten verifiëren en vervolgens als officiële basis kunnen aanvaarden, zal het in kaart brengen van dit soort machtigingen minder werklast met zich meebrengen dan we oorspronkelijk verwachtten.

CONCLUSIE - We komen hier daarom tot een gelijkaardige conclusie als bij het zoeken naar het standaardformaat. Naar de toekomst toe zal het zeker mogelijk zijn om alle machtigingen op een duidelijk gestructureerde en overzichtelijke wijze te publiceren. De huidige website van de Commissie voor de bescherming van de persoonlijke levenssfeer is daar al een mooie aanzet toe, hoewel we ook hier nog ruimte tot verbetering zien. Wat de machtigingen verleend door het sectoraal comité van het Rijksregister betreft zien we dat het in kaart brengen van de effectief verleende en nu nog geldende machtigingen toch nog enige werklast met zich zal meebrengen. Hoewel het in kaart brengen van de machtigingen bij koninklijk besluit op het eerste zicht een quasi hopeloze taak lijkt, kunnen we ons beroepen op een aantal bestaande overzichten van deze machtigingen. Indien we de lijst van De Bot officieel kunnen laten verifiëren, is deze taak al voltooid. Indien we zulke lijst echter niet als volledig beschouwen, zal een handmatige analyse van elke editie van het Belgisch Staatsblad voor de periode 1984 tot 2004 zich opdringen. Dit zal uiteraard tijd, mankracht en budget vereisen.

4. CONCLUSIE

HET REGISTER EX NUNC … - Zoals we eerder al aangaven zal het geen al te groot probleem vormen om het *ex ante* register *ex nunc* op te richten. De benodigde technologie voor het oprichten van zulk register is immers aanwezig en wordt al gebruikt door verschillende overheidsdiensten in allerlei toepassingen. Ook het voorgestelde standaardformaat via de opmaaktaal XML zal relatief gemakkelijk ingevoerd kunnen worden. XML wordt immers al in een aantal toepassingen – zoals de e-ID – gebruikt. Het *ex ante* register is daarom slechts een nieuwe toepassing van bestaande kennis en het zal daarom met relatief beperkte mankracht, tijd en budget ingevoerd kunnen worden voor het gebruik naar de toekomst toe.

… EN EX TUNC - Het grote probleem bij het oprichten van het *ex ante* register ligt echter niet bij de toekomstige machtigingen, maar bij de vroeger verleende machtigingen. Deze machtigingen zullen immers ook in het register opgenomen moeten worden. Hiertoe zal men allereerst in kaart moeten brengen welke machtigingen er vroeger verleend zijn en welke van die machtigingen nu nog gelden. Bij de huidige machtigingen door het sectoraal comité van het Rijksregister is dit geen onoverbrugbaar probleem. Deze machtigingen worden immers gepubliceerd op de website van de Commissie voor de bescherming van de persoonlijke levenssfeer. Hoewel het enige moeite zal kosten om al de beraadslagingen van het sectoraal comité handmatig te onder-

[348] F. ROBBEN, "De toegang tot het Rijksregister van de natuurlijke personen en het gebruik van het identificatienummer van dat register" in C. PERSYN, D. SIMOENS, J. VAN LANGENDONCK en R. WUYTS (eds.), *Volmachten en sociale zekerheid 1986-87*, Reeks Sociaal Recht nr. 32, Deurne, Kluwer Rechtswetenschappen, 1987, 101-128. Merk op dat deze bijdrage dateert van 1987 en dus slechts melding maakt van de machtigingen die van 1984 tot 1986 afgekondigd werden.

[349] D.DE BOT, *Privacybescherming bij e-Government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 427-463.

zoeken om te kijken of deze effectief tot een machtiging geleid hebben en of die machtiging nog geldt, lijkt dit geen onmogelijke opgave te zijn. Het in kaart brengen van de vroegere machtigingen bij koninklijk besluit kan echter wel nog een quasi onmogelijke taak worden. Bij gebrek aan een officieel exhaustief overzicht van deze machtigingen, hebben we de keuze tussen het aanvaarden van de lijst van Dirk De Bot enerzijds en een handmatige analyse van 20 jaargangen van het Belgisch Staatsblad anderzijds.

HANDMATIGE INVOER - Nadat alle vroeger verleende en nu nog geldende machtigingen in kaart gebracht zijn, zullen deze machtigingen nog opgenomen moeten worden in het register. Omdat deze machtigingen uiteraard niet het af te spreken standaardformaat volgen, zullen zij handmatig in het register ingevoerd moeten worden. Wat betreft de machtigingen verleend door het sectoraal comité van het Rijksregister zien we dat deze wel ingevoerd zullen kunnen worden. Zij volgens immers al een zekere standaardopmaak en het is daarom geen onmogelijke taak om de voor het register relevante gegevens uit deze teksten af te leiden. Dit geldt echter niet voor de vroegere machtigingen bij koninklijk besluit. Deze machtigingen zijn door hun ingewikkelde en onoverzichtelijke teksten niet zonder meer te herleiden tot de individuele gegevens die het register nodig heeft. De handmatige invoer van deze machtigingen zal daarom een zeer tijdrovende en intensieve taak worden, indien we deze taak zelfs als haalbaar zouden beschouwen.