Carolien Coenen
Tweede lic rechten

Seminarie ICT-recht 2005-2006

Authentieke bronnen en privacy

t.a.v. Professor Jos Dumortier

t.a.v. Xavier Huysmans

1 Inleiding

Deze paper beoogt een beter inzicht te geven in het gebruik van authentieke bronnen en de problematiek hier rond. Authentieke bronnen vormen een onontbeerlijk onderdeel van een uitgebalanceerd e-governmentbeleid. Zowel de federale als de Vlaamse invulling van e-government en authentieke bronnen komen aan bod.

Om het begrip "authentieke bronnen" wat minder abstract te maken, worden de twee meest bekende authentieke bronnen (het Rijksregister en de Kruispuntbank Ondernemingen) besproken. Ik bepreek ook kort de Kruispuntbank Sociale zekerheid, die strikt genomen zelf geen authentieke bron is, maar een verwijzingsregister naar andere informatiebronnen. Er zal ook aandacht worden besteed aan de Vlaamse invulling van het begrip "authentieke bronnen".

Het tweede luik van deze paper, zoomt in op de problematiek van de bescherming van persoonsgegevens. Authentieke bronnen bevatten een schat aan informatie over natuurlijke (en rechts-) personen. Wordt er voldoende aandacht besteed aan de bescherming van deze gegevens? Welke maatregelen worden genomen om de vereisten van kwaliteit, integriteit, veiligheid en vertrouwelijkheid te garanderen? Centraal staat de vraagstelling of het gebruik van authentieke bronnen an sich kan bijdragen tot een betere bescherming van persoonsgegevens.

2 Authentieke bronnen en egovernment

2.1 Wat is een authentieke bron?

De site van de Coördinatiecel Vlaams E-government[1] (Corvé) geeft volgende definitie van het begrip "authentieke bron":

Authentieke bronnen zijn hoogwaardige gegevensbronnen, met expliciete garanties wat betreft de kwaliteit van de gegevens en wat betreft het gebruik dat van die gegevens kan gemaakt worden.[2]

Op de site van de Federale overheidsdienst Informatie- en Communicatietechnologie (Fedict) vinden we geen expliciete definitie van het begrip terug. Fedict ziet authentieke bronnen als een belangrijk middel om de eenmalige gegevensinzameling bij burger en bedrijven te

[1] http://www.vlaanderen.be/egovernment.
[2] Definitie van authentieke bronnen op http://www3.vlaanderen.be/e-government/projecten_referentiebestanden.html.

realiseren. Eén instantie is verantwoordelijk voor de correctheid van de gegevens in een authentieke bron. Wanneer derden (bijvoorbeeld andere overheidsdiensten) van deze gegevens gebruik wensen te maken, moeten zij de "authentieke bron" raadplegen.[3]

2.2 Authentieke bronnen als bouwstenen voor e-government

E-government[4] is een fundamenteel nieuwe, geïntegreerde en voortdurend aangepaste manier van dienstverlening waarbij maximaal gebruik gemaakt wordt van de mogelijkheden van de nieuwe Informatie- en Communicatie Technologie[5].

In de federale (en de Vlaamse) visie op e-government staat het voortdurend verbeteren van de dienstverlening aan burgers en bedrijven centraal. Informatie- en communicatietechnologie zijn slechts een middel om deze doelstelling te realiseren. E-government gaat dus verder dan het louter digitaliseren van informatie en deze informatie vervolgens toegankelijk maken op websites. E-government is een structureel hervormingsproces binnen de overheid dat gebaseerd moet worden op een multidisciplinaire aanpak (technisch, juridisch, organisatorisch, ...).

Informatie is voor de overheid een strategische productiefactor om een optimale dienstverlening te bekomen. Om haar dienstverlening zo vlot mogelijk te laten verlopen, heeft de overheid persoons- en andere gegevens van burgers en bedrijven nodig. Deze gegevens kunnen verzameld worden in authentieke bronnen, zoals het Rijksregister en de Kruispuntbank Ondernemingen.

Authentieke bronnen zijn dus een onmisbare bouwsteen voor e-governmenttoepassingen. De filosofie achter het gebruik van authentieke bronnen is tweeledig: enerzijds worden de gegevens van de authentieke bron geacht correct te zijn, anderzijds wil men overbodige verdubbeling van gegevens vermijden door de gegevens slechts één maal op te slaan. Doordat één overheidsdienst instaat voor de correctheid van de gegevens, zijn er ook meer garanties dat er geen fouten in de gegevens sluipen.

Door e-governmenttoepassingen zo veel mogelijk gebruik te laten maken van authentieke bronnen wil men vermijden dat burgers en bedrijven gegevens die al bij een

[3] Uitleg over authentieke bronnen op http://www.fedict.be.
[4] F. ROBBEN en J. DEPREST, "E-government: the approach of the Belgian federal administration", http://www.law.kuleuven.ac.be/icri/frobben/publications/2003%20-%20E-government%20paper%20v%201.0.pdf
[5] Definitie van e-government op http://www.belgium.be.

overheidsinstantie aanwezig zijn, meerdere malen moeten opgeven. Dit alles kadert in het streefdoel naar een efficiëntere en effectievere overheid.

De federale (en ook de Vlaamse) overheid leggen bij de uitbouw van een doelgericht e-governmentbeleid vooral de nadruk op het belang van de integratie van de back-office[6]. Men wil als één virtuele overheid naar buiten treden. De burger wil immers zo snel en efficiënt mogelijk geholpen worden, het interesseert hem niet welke administratie of instantie moet instaan voor het afhandelen van zijn vraag. Vlotte gegevensdeling en -uitwisseling tussen administraties is dus zeer belangrijk.

2.3 Informatie in authentieke bronnen: informatiemodellering[7]

Informatie kan haar potentieel van een strategische productiefactor voor de overheid maar vervullen, als ze op een eenvormige manier gemodelleerd wordt, met hierbij de nodige aandacht voor de kenmerken en de onderlinge relaties van de informatie-elementen. Het informatiemodel sluit best zo nauw mogelijk aan bij de reële wereld. Zo vermijdt men aanpassingen aan het model wanneer bijvoorbeeld juridische begrippen wijzigen door aanpassingen aan de wetgeving.

Bij de modellering moet men ook zo veel mogelijk rekening houden met de voorzienbare gebruiksbehoeften en het temporele aspect van de informatie (termijnen, historiek). Het opgestelde model moet ook gemakkelijk uitbreidbaar zijn. In de toekomst zullen door de uitbreiding van het aantal e-governmenttoepassingen de hoeveelheid en de soorten opgeslagen informatie immers hoogstwaarschijnlijk toenemen, evenals de verschillende manieren waarop van deze informatie gebruikgemaakt wordt.

Het opstellen van een zo goed mogelijk informatiemodel is maar een eerste stap. Dit model moet vervolgens geïmplementeerd worden en gevoed (na validatie van de correctheid) met de nodige informatie. Hierbij moet steeds voor ogen gehouden worden dat informatie door de overheid alleen maar ingezameld mag worden voor **welbepaalde doeleinden** en in de mate dat de informatie **proportioneel is met deze doeleinden**. De opgeslagen informatie moet gemakkelijk consulteerbaar en op een eenvoudige manier (elektronisch) uitwisselbaar zijn.

Het aspect informatiebeveiliging is bij dit alles cruciaal. De veiligheid, de integriteit en de vertrouwelijkheid van de informatie moet worden gewaarborgd aan de hand van een

[6] Zie uiteenzetting “Over e-government” op de federale portaalsite http://www.belgium.be.
[7] F. ROBBEN, “E-government”, http://www.law.kuleuven.ac.be/icri/frobben/publications/2004%20-%20E-government.pdf.

geïntegreerd geheel van structurele, organisatorische, technische, fysische en andere veiligheidsmaatregelen.

2.4 Toepassingen

In dit onderdeel worden kort drie belangrijke bouwstenen van het Belgische e-governmentbeleid besproken: het Rijksregister (RR), de Kruispuntbank Sociale Zekerheid (KSZ) en de Kruispuntbank Ondernemingen (KBO). Zoals eerder aangehaald, zijn het Rijksregister en de KBO authentieke bronnen, terwijl de KSZ een verwijzingsregister is naar andere authentieke bronnen. Bij de bespreking zal ook de nodige aandacht worden besteed aan de voeding van deze gegevensbronnen en de gebruikte unieke identificatienummers die een belangrijk instrument zijn om informatie makkelijker en met hogere waarborgen voor de correctheid uit te wisselen.

2.4.1 Het rijksregister (RR)[8]

Het Rijksregister[9] is een systeem van informatieverwerking dat, overeenkomstig de bepalingen van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, instaat voor de opneming, memorisatie en de mededeling van informatie betreffende de identificatie van natuurlijke personen.

In feite is het Rijksregister een grote databank[10] met daarin 13 verplichte basisidentificatiegegevens[11] en (eventueel) facultatieve informatiegegevens[12] van natuurlijke personen met hoofdverblijfplaats op het Belgische grondgebied en van Belgische onderdanen in het buitenland. De facultatieve gegevens kunnen in het Rijksregister opgenomen worden op vraag van de gemeentebesturen en mogen ook alleen maar door hen opgevraagd worden.

Bij koninklijk besluit van 8 januari 2006[13] werd aangegeven welke informatietypes verbonden zijn aan de 13 verplichte basisidentificatiegegevens zoals bepaald in de Wet Rijksregister. Deze informatietypes verduidelijken wélke informatie bijgehouden moet worden van een natuurlijke persoon. Zo worden onder meer de basisidentificatiegegevens geslacht, hoofdverblijfplaats, administratieve toestand,… verduidelijkt.

[8] http://www.rijksregister.fgov.be.
[9] D. DE BOT, *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, hoofdstuk 6.
[10] Merk op dat in deze tekst Rijksregister in de strikte betekenis gebruikt wordt (het 'bestand' Rijksregister). Rijksregister kan ook slaan op de diensten van het Rijksregister gaan, wat breder is dan louter de gegevensbank.
[11] D. DE BOT, *o.c.*, 110-111.
[12] D. DE BOT, *o.c.*, 116-119.
[13] K.B. 8 januari 2006 tot bepaling van de informatietypes, verbonden met de informatiegegevens bedoeld in artikel 3, eerste lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.* 25 januari 2006.

Het Rijksregister staat dus in voor een geautomatiseerde verwerking die valt onder de bescherming van de Wet Verwerking Persoonsgegevens. In principe wordt de toegang tot de informatiegegevens van het Rijksregister door de Wet Rijksregister niet enkel voorbehouden aan de overheid. Een nauwkeurige lezing van de doeleinden van het Rijksregister[14] laat echter toe te concluderen dat het hier in de praktijk wel op neerkomt.

Deze doeleinden zijn (parafrasering van art. 1, §2 Wet Rijksregister):

- het vergemakkelijken van de uitwisseling van informatiegegevens tussen administraties;
- het mogelijk maken van de automatische bijwerking van de bestanden van de openbare sector wat betreft de algemene gegevens over de burgers;
- het rationaliseren van het gemeentelijke beheer van de bevolkingsregisters;
- het vergemakkelijken van sommige administratieve formaliteiten die geëist worden van de burgers.

2.4.1.1 Voeding van het Rijksregister[15]

Wie zorgt ervoor dat de nodige gegevens in het Rijksregister belanden? Artikel 4 eerste lid Wet Rijksregister leert ons dat de overheden die belast zijn met het houden van de registers waaruit het Rijksregister haar gegevens puurt, de verplichte informatiegegevens en de eventuele wijzigingen ervan ambtshalve meedelen aan het Rijksregister.

Dit betekent dat de gemeenten (voor de bevolkings- en vreemdelingenregisters en het wachtregister) en de diplomatieke zendingen en consulaire posten (voor hun registers) verplicht zijn tot medewerking aan en voeding van het Rijksregister. Gemeenten, diplomatieke zendingen en consulaire posten zijn met andere woorden de gegevensinitiatoren. Zij zijn verantwoordelijk voor de overeenstemming van de meegedeelde informatiegegevens met de akten en documenten die zij in hun bezit hebben (art. 4, tweede lid Wet Rijksregister). De administratie van het Rijksregister is dan de authentieke bron of gegevensbeheerder. De verdere modaliteiten inzake gegevensmededeling worden geregeld in een Koninklijk besluit van 3 april 1984[16].

[14] Artikel 1, §2 Wet Rijksregister.
[15] D. DE BOT, *o.c.*, 107.
[16] K.B. 3 april 1984 betreffende de toegang door sommige openbare overheden tot het Rijksregister van de natuurlijke personen, alsmede betreffende het bijhouden en de controle van de informaties, *B.S.* 21 april 1984.

2.4.1.2 Het Rijksregisternummer

Iedere natuurlijke persoon krijgt bij de eerste inschrijving in het Rijksregister een identificatienummer (artikel 2, tweede lid Wet Rijksregister). Het nummer bestaat uit elf cijfers. De eerste zes cijfers geven de geboortedatum weer (JJMMDD), de drie volgende cijfers dienen om de personen die op dezelfde dag geboren zijn, te identificeren en om het geslacht aan te geven (oneven getal is mannelijk, even vrouwelijk) en de laatste twee cijfers vormen een controlegetal om de geldigheid van het nummer te controleren.[17]

Artikel 1, § 1 Wet Verwerking Persoonsgegevens definieert het begrip "persoonsgegeven" als volgt: "*iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*". Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

Als men de opbouw van het RRN vergelijkt met deze definitie van "persoonsgegeven", moet men concluderen dat het RRN wel degelijk een persoonsgegeven is, omdat het informatie over de titularis bevat. Men denkt erover in de toekomst de geboortedatum en aanduiding van het geslacht uit het RRN weg te laten. Het is echter niet relevant of het nummer zelf al dan niet informatie over de persoon bevat. Het feit op zich dat het nummer toelaat om een welbepaalde natuurlijke persoon te identificeren, maakt dat dit nummer als persoonsgegeven beschouwd moet worden[18].

2.4.2 Kruispuntbank Sociale Zekerheid (KSZ)[19]

De Kruispuntbank Sociale Zekerheid is een instelling die instaat voor de inzameling, opslag en uitwisseling van gegevens met betrekking tot de sociale zekerheid, zoals bepaald bij de wet van Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (Kruispuntbankwet). De Kruispuntbank Sociale Zekerheid is de motor en coördinator van e-government in de sociale sector.

In tegenstelling tot het Rijksregister en de KBO gaat het hier niet om een grote gegevensbank. In de Kruispuntbank worden immers in beginsel geen inhoudelijke gegevens bijgehouden. Zij bevat enkel verwijzingen naar informatie die op een gedecentraliseerde en gedistribueerde

[17] K.B. 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.
[18] D. DE BOT, *o.c.*, 34.
[19] http://ksz-bcss.fgov.be.

wijze wordt bewaard (artikel 6 Kruispuntbankwet). De Kruispuntbank is met andere woorden de spin in een netwerk van gegevensuitwisseling tussen de verschillende actoren van de sociale zekerheid.

Onder coördinatie van de Kruispuntbank van de Sociale Zekerheid hebben de instellingen van sociale zekerheid al heel wat onderlinge relaties grondig herdacht en geautomatiseerd. Via een netwerk kunnen de computers van de instellingen van sociale zekerheid op een beveiligde manier met elkaar gegevens uitwisselen. Een coherent begrippenapparaat[20] doorheen de sociale zekerheid is uitgewerkt om ervoor te zorgen dat gegevens die door één instelling van sociale zekerheid ingezameld worden, gebruikt kunnen worden door alle instellingen van sociale zekerheid die ze nodig hebben.

Aangezien volgens artikel 4 de KSZ gegevens kan bevatten met betrekking tot de identificatie van personen die niet in het Rijksregister opgenomen zijn (deze personen worden geregistreerd onder het identificatienummer van de Sociale Zekerheid), is zij ook onderworpen aan de Wet Verwerking Persoonsgegevens.

In de Kruispuntbankwet zelf werden verschillende artikelen opgenomen om de verwerking en bescherming van de persoonsgegevens te regelen:

⇒ De Kruispuntbank deelt aan de instellingen van sociale zekerheid alleen de sociale gegevens mee die deze instellingen nodig hebben voor de toepassing van de sociale zekerheid (artikel 13 Kruispuntbankwet).

⇒ De mededeling van sociale gegevens van persoonlijke aard door de instellingen van sociale zekerheid geschiedt door bemiddeling van de Kruispuntbank, behalve voor de personen en instellingen opgesomd in artikel 14 Kruispuntbankwet of die een uitdrukkelijke machtiging gekregen hebben om deze gegevens te gebruiken. De Koning kan de voorwaarden bepalen waaronder de machtigingen worden verleend. Deze machtigingen worden schriftelijk gegeven en kunnen een maximale geldigheidsduur bepalen (artikel 14 Kruispuntbankwet).

⇒ Elke mededeling binnen het netwerk, van sociale gegevens van persoonlijke aard, door de Kruispuntbank of de instellingen van sociale zekerheid, vereist een principiële machtiging

[20] Zie ook de uitleg over informatiemodellering onder sectie 2.3 van dit document.

van het sectoraal comité van de sociale, behalve in de door de Koning bepaalde gevallen (artikel 15 Kruispuntbankwet).

⇒ De Kruispuntbank en de instellingen van sociale zekerheid treffen alle maatregelen die nodig zijn om een perfecte bewaring van de persoonsgegevens te verzekeren (artikel 22 Kruispuntbankwet).

⇒ De personen die tussenkomen in de toepassing van de sociale zekerheid mogen enkel de persoonsgegevens inzamelen die ze nodig hebben voor deze toepassing (artikel 23, eerste lid, Kruispuntbankwet).

⇒ Ze mogen slechts beschikken over de verkregen persoonsgegevens gedurende de tijd die nodig is voor de toepassing van de sociale zekerheid; ze moeten maatregelen treffen om het vertrouwelijke karakter van de persoonsgegevens te verzekeren; ze moeten ervoor zorgen dat de persoonsgegevens uitsluitend worden gebruikt voor het uitvoeren van hun wettelijke opdrachten (artikel 23, tweede lid, Kruispuntbankwet).

Bijzonder aan de KSZ is dat zij niet alleen samenwerkt met overheidsinstellingen, maar ook ten dienste staat van private instellingen met een opdracht van algemeen belang, zoals ziekenfondsen of zelfstandigenkassen.

2.4.2.1 Het IdentificatieNummer van de Sociale Zekerheid (INSZ)

De KSZ maakt ook gebruik van een uniek identificatienummer: het IdentificatieNummer van de Sociale Zekerheid. Dit nummer is een unieke identificatiesleutel voor elke natuurlijke persoon die gebruikt wordt in alle domeinen van de sociale zekerheid.

Voor de personen die opgenomen zijn in het Rijksregister is dit nummer het rijksregisternummer. Voor de personen die niet in het Rijksregister opgenomen zijn, is dit het KSZ-nummer[21]. Het KSZ-nummer wordt door de Kruispuntbank toegekend aan elke natuurlijke persoon die in het Bisregister[22] of het Terregister[23] wordt ingeschreven.

[21] K.B. 8 februari 1991 betreffende de samenstelling en de wijze van toekenning van het identificatienummer van de natuurlijke personen die niet ingeschreven zijn in het Rijksregister van de natuurlijke personen, B.S. 19 februari 1991.
[22] Gegevensbank bijgehouden door de Kruispuntbank, die de beschikbare identificatiegegevens bevat over alle natuurlijke personen die niet in het *Rijksregister* zijn ingeschreven, maar waarover wel *minimale identificatiegegevens* beschikbaar zijn.
[23] Gegevensbank bijgehouden door de Kruispuntbank, die de beschikbare identificatiegegevens bevat over alle natuurlijke personen die niet in het Rijksregister zijn ingeschreven en waarover geen minimale identificatiegegevens beschikbaar zijn. De identificatiesleutel en de beschikbare gegevens kunnen enkel worden gebruikt door de instelling die ze heeft ingevoerd.

Het KSZ-nummer bestaat uit elf cijfers. De eerste zes cijfers van dit nummer stellen de geboortedatum voor. De eerste twee cijfers van deze cijfergroep duiden het geboortejaar van de persoon aan. Het derde en het vierde cijfer duiden de geboortemaand aan, verhoogd met 40 indien het geslacht van de persoon is gekend op het ogenblik van de toekenning van het nummer, of verhoogd met 20 indien het geslacht van de persoon niet is gekend. Het vijfde en het zesde cijfer duiden de geboortedag aan.

De volgende drie cijfers worden het reeksnummer genoemd. Dit reeksnummer wordt gevormd door het volgnummer van inschrijving van de persoon. Indien het geslacht van de persoon gekend is op het ogenblik van de toekenning van het nummer, krijgt een vrouwelijke persoon een even en een mannelijke persoon een oneven reeksnummer. De twee laatste cijfers vormen het controlenummer.

Artikel 5 van het Koninklijk Besluit van 8 februari 1991 regelt de samenstelling van het nummer als de geboortedag, de geboortemaand en/of het geboortejaar niet gekend zijn.

2.4.3 Kruispuntbank Ondernemingen (KBO)[24]

De KBO[25] werd op 1 juli 2003 krachtens een wet[26] opgericht als onderdeel van de Federale Overheidsdienst Economie, KMO, Middenstand en Energie.

De Kruispuntbank Ondernemingen is een gegevensbank die alle identificatiegegevens van de ondernemingen[27] bevat. De KBO is belast met het invoeren, het opslaan, het beheren en het ter beschikking stellen van gegevens met betrekking tot de identificatie van ondernemingen. M.a.w. de KBO is voor ondernemingen wat het Rijksregister is voor natuurlijke personen. In tegenstelling tot de Kruispuntbank Sociale Zekerheid, waar de benaming verwijst naar een instelling, heeft de term "Kruispuntbank Ondernemingen" louter en alleen betrekking op de gegevensbank zelf. De Kruispuntbank Ondernemingen is momenteel nog geen echte kruispuntbank voor ondernemingsgegevens zoals de KSZ dat is voor persoonsgegevens, maar het heeft wel de ambitie hiertoe op termijn uit te groeien.

De KBO bevat tien basisidentificatiegegevens die opgesomd worden in artikel 6, §1 Wet KBO. Deze basisidentificatiegegevens kunnen aangevuld worden met andere gegevens die

[24] http://mineco.fgov.be/redir_new.asp?loc=/enterprises/crossroads_bank/home_nl.htm.
[25] D. DE BOT, *o.c.*, hoofdstuk 6.
[26] Wet 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, *B.S.* 5 februari 2003.
[27] Economische of sociale actoren die op Belgisch grondgebied willen ondernemen.

vereist zijn voor de identificatie van ondernemingen dan wel van gemeenschappelijk belang zijn voor meerdere overheidsdiensten (artikel 6, §2 Wet KBO).

De tekst van artikel 6, §2 is echter zo ruim geformuleerd dat dit de mogelijkheid creëert om aanvullend een onbeperkt aantal gegevens in de KBO op te nemen, waardoor een soort register "à la carte" gecreëerd kan worden. Waarborgen om dit tegen te gaan, zijn de vereiste om hiertoe een Koninklijk Besluit uit te vaardigen dat eerst door de Ministerraad is goedgekeurd en een voorafgaand advies van het sectoraal comité van de KBO[28].

2.4.3.1 Voeding van de Kruispuntbank Ondernemingen[29]

Het Koninklijk Besluit van 26 juni 2003[30] ter uitvoering van artikel 7 Wet KBO duidt de gegevensbeheerders en initiatoren aan voor de gegevens die bij de inschrijving in de Kruispuntbank Ondernemingen moeten worden ingevoerd. De gegevensbeheerders zijn verantwoordelijk voor de unieke inzameling van de gegevens, de actualisatie en de juistheid van deze gegevens. Initiatoren zijn de diensten die, onder toezicht van de gegevensbeheerder gemachtigd zijn bepaalde gegevens rechtstreeks in te brengen of te wijzigen in de KBO (artikel 1, 2° K.B. Authentieke bronnen).

De gegevensbeheerders van de KBO zijn onder andere de federale overheidsdienst (FOD) Financiën, de FOD Sociale Zaken (RSZ), de FOD Justitie, de FOD Economie, K.M.O., Middenstand en Energie, de FOD Binnenlandse Zaken, de KSZ, de Nationale Bank van België,… Initiatoren zijn de ondernemingsloketten. Zij zijn verantwoordelijk voor de inschrijving van de handels- en ambachtsondernemingen in de KBO. Sinds de oprichting van de ondernemingloketten worden de verschillende formaliteiten voor het opstarten van handels- en ambachtsondernemingen (bijvoorbeeld inschrijving in de KBO, toegang tot het beroep, aanvraag BTW-identificatie, …) op één enkele plaats gecentraliseerd.

2.4.3.2 Het ondernemingsnummer

Het ondernemingsnummer is ingevoerd sinds 1 juli 2003 en is een uniek identificatienummer, bestaand uit tien cijfers, dat de Kruispuntbank Ondernemingen toekent aan de onderneming. Het ondernemingsnummer wordt voorgesteld als ZNNN.NNN.NNN, waarbij Z 0 of 1 is en N een cijfer van 0 tot 9. Terwijl vroeger elke bestuursinstantie haar eigen identificatienummer

[28] D. DE BOT, *o.c.*, 276-278.
[29] D. DE BOT, *o.c.*, 86-87.
[30] Houdende aanwijzing van de overheden, administraties en diensten die, betreffende bepaalde categorieën van ondernemingen, belast zijn met de eenmalige inzameling en het actualiseren van de gegevens bedoeld in artiekl 6 Wet KBO, *B.S.* 30 juni 2003.

toekende, is het de bedoeling dat er op termijn nog slechts één nummer is, wat de administratieve vereenvoudiging ten goede moet komen.

Het ondernemingsnummer vervangt voortaan het handelsregisternummer, het nummer van het Rijksregister voor Rechtspersonen en het BTW-nummer (het RSZ-werkgeversnummer blijft voorlopig behouden).

De overheid heeft geen volledig nieuw nummer ingevoerd. Zij heeft beslist het BTW-nummer om te vormen tot ondernemingsnummer, door dit nummer vooraf te laten gaan door een index 0.

2.5 Authentieke bronnen in Vlaanderen

Geïnspireerd door het succes van de federale authentieke gegevensbronnen, is sinds kort de Coördinatiecel e-government van de Vlaamse Overheid (Corvé) begonnen aan de uitbouw van eigen authentieke bronnen. Hieronder worden kort twee van deze initiatieven besproken, die beide gebruik maken van basisgegevens uit de KBO en de KSZ.

2.5.1 Verrijkte Kruispuntbank Ondernemingen (VKBO)[31]

De Verrijkte Kruispuntbank Ondernemingen ontstond vanuit een Vlaamse noodzaak aan een unieke referentiebron voor ondernemingsgegevens. Hoewel de federale KBO de enige officiële bron is op het vlak van de basisinformatie over bedrijven, wilde men de gegevens van de KBO uitbreiden met de gegevens aanwezig in Vlaamse gegevensbanken over ondernemingen.

De Verrijkte Kruispuntbank Ondernemingen heeft volgens de Vlaamse e-governmentsite een dubbele doelstelling[32]:

⇒ Centralisatie van Vlaamse diensten en applicaties die met de KBO willen communiceren voor de referentiëring van hun klantenregistratie. Het VKBO-project wil deze massale registratieproblematiek naar het KBO opvangen via één centrale Vlaamse toegang.

⇒ Het verrijken van de essentiële KBO-gegevens met extra informatie over de ondernemingen, om applicaties intelligenter te laten functioneren enerzijds en om een volledigere "ondernemersfoto of -fiche" te kunnen presenteren anderzijds.

[31] Informatie over het VKBO op de Vlaamse e-governmentsite: http://www3.vlaanderen.be/e-government/projecten_refbest_VKBO.html.
[32] Bewerkt citaat van de site http://www3.vlaanderen.be/e-government/projecten_refbest_VKBO.html.

Het datamodel[33] van de VKBO is raadpleegbaar op de Vlaamse e-governmentsite[34].

Op dit moment voorziet de VKBO in 3 wezenlijke dienstverleningen:

1. Webdiensten voor applicaties. De VKBO werkt aan een vast dienstenaanbod dat de grootste informatiebehoeften dekt van de applicaties die werken met en voor ondernemingen.

2. Publicatie van mutaties (gegevenswijzigingen) van ondernemingen. Een volautomatische verdeling van geactualiseerde gegevens is in voorbereiding. Momenteel gebeurt actualisatie op een ad hoc basis.

3. Webtoepassing voor raadpleging van gegevens van ondernemingen. De VKBO–GO is een de grafische gebruikersomgeving om de gegevens te raadplegen. Momenteel is deze toepassing enkel raadpleegbaar voor ambtenaren. Op termijn wil Corvé de burger en onderneming ook toegang verlenen, uiteraard met specifieke machtigingen. Burgers zouden dan enkel de publieke gegevens kunnen consulteren en oppervlakkig kunnen zoeken. Ondernemingen zullen hun gegevens in detail kunnen bekijken, een dossieroverzicht kunnen raadplegen, enz…

2.5.1.1 Ondernemingsnummer als sleutel

In juli 2002 nam de Vlaamse Regering de principiële beslissing[35] om binnen de Vlaamse overheid het federale unieke identificatienummer (d.i. het ondernemingsnummer) van ondernemingen te gebruiken voor haar interne processen.

De Coördinatiecel Vlaams e-government diende bij de Commissie voor de Bescherming van de Persoonlijke levenssfeer een aanvraag in om het identificatienummer van het Rijksregister te mogen gebruiken met het oog op toegang door ambtenaren tot de Verrijkte Kruispuntbank Ondernemingen. Zij kreeg hiervoor op 21 december 2005 de toestemming van de Commissie[36].

[33] Zie ook uiteenzetting over informatiemodellering onder 2.3.
[34] http://www3.vlaanderen.be/e-government/projecten_refbest_VKBO_datamodel.html.
[35] Beslissing van de Vlaamse Regering van 19 juli 2002 (VR/2002/19.07/DOC.0729), te consulteren op http://www3.vlaanderen.be/e-government/documenten/beslissing_Vl_Reg_20190702.pdf.
[36] Beraadslaging RR Nr 52 / 2005 van 21 december 2005 http://www.privacycommission.be/machtigingen/Ber052_2005_RR.pdf.

2.5.2 Van een Verrijkt Personenregister (VPR)[37] naar een Verrijkte Kruispuntbank Personen (VKBP)

De informatie over deze projecten van de Coördinatiecel Vlaams e-government is redelijk summier. De ontwikkeling van het Verrijkt Personenregister staat immers nog in de kinderschoenen. Men wil in eerste instantie ervaring opdoen met het uitwisselen en opslaan van gegevens afkomstig uit de KSZ. Op termijn zou het VPR moeten uitgroeien tot een echte kruispuntbank, de Verrijkte Kruispuntbank Personen, die de basisgegevens van de KSZ aanbiedt, verrijkt met extra informatie afkomstig uit Vlaamse authentieke gegevensbronnen met **rijksregisternummer als unieke sleutel** (cfr. het principe van de VKBO).

Doelstellingen van deze Vlaamse VKBP[38]:

⇒ Het centraliseren van tientallen Vlaamse diensten en applicaties die met de KSZ willen communiceren voor het opvragen van persoonsgegevens. Het VPR-project wil deze massale registratieproblematiek naar de KSZ opvangen door het aansluiten van één centrale Vlaamse toegang.

⇒ Het verrijken van de KSZ gegevens met extra informatie over personen (bijvoorbeeld verrijkte algemene gegevens en Vlaamse dossiergegevens), om applicaties intelligenter te laten functioneren.

2.5.3 Bescherming van de persoonsgegevens in Vlaanderen

Alhoewel de e-governmentsite van de Vlaamse Overheid[39] hier en daar wel melding maakt van de problematiek van de bescherming van persoonsgegevens, blijkt na een grondigere lezing dat de focus van Corvé voornamelijk ligt op het technische aspect van e-government. Dit is begrijpelijk omdat de initiatieven nog zeer pril zijn, maar dit mag geen excuus zijn om de informationele privacy uit het oog te verliezen.

Om meer inzicht te krijgen in de initiatieven van de e-governmentcel en hun visie op de problematiek van het beschermen van persoonsgegevens ben ik gaan praten met Hans Arents, adviseur strategie & technologie van Corvé. Een neerslag van dit gesprek is terug te vinden in bijlage.

[37] Informatie over het VPR op de Vlaamse e-governmentsite: http://www3.vlaanderen.be/e-government/projecten_refbest_VPR.html.
[38] Bewerkt citaat van de site http://www3.vlaanderen.be/e-government/projecten_refbest_VKBP.html.
[39] http://www.vlaanderen.be/e-government

3 Privacy en bescherming van de persoonsgegevens

3.1 Probleemstelling

Om de probleemstelling te illustreren, wordt vertrokken van dit citaat, geplukt van de portaalsite Belgium.be:

"Het principe van de authentieke bron helpt net die privacy te beschermen: doordat er maar één enkele bron is, en dus geen kopieën, kan de bescherming van de gegevens ook optimaal geconcentreerd worden."[40]

Ter verduidelijking van bovenstaand citaat moet vermeld worden dat het aspect van de privacy die in het geding is bij e-governmenttoepassingen de "informationele privacy" is of zoals het in de Wet Verwerking Persoonsgegevens omschreven wordt: "de bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens".

Hieronder zal nagegaan worden in hoe verre bovenstaand citaat met de realiteit overeenstemt. Helpt het gebruik van authentieke bronnen persoonsgegevens beter beschermen of ontstaan er nieuwe problemen? Welke bijkomende waarborgen voor het beschermen van persoonsgegevens worden gegeven/zijn er vereist?

3.2 Wet Verwerking Persoonsgegevens

In België wordt het algemeen wettelijk kader waarmee de overheid rekening moet houden bij de verwerking van persoonsgegevens, gevormd door de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens[41] (Wet Verwerking Persoonsgegevens) die bepaalt dat persoonsgegevens enkel mogen worden gebruikt voor doeleinden die evenredig zijn met de doeleinden waarvoor ze ingezameld werden (**proportionaliteitsbeginsel**). In de bespreking van de belangrijke bouwstenen van e-government is de Wet Verwerking Persoonsgegevens al enkele keren ter sprake gekomen.

De hoekstenen van de wetgeving ter bescherming van persoongegevens wordt gevormd door het **finaliteitsbeginsel**[42] en het **proportionaliteitsbeginsel**. Het finaliteitsbeginsel bevat op zijn beurt twee te onderscheiden regels het **wettigheidsbeginsel** (artikel 4, §1, 2° WVP) dat

[40] http://www.belgium.be/eportal/application?languageParameter=nl&pageid=contentPage&docId=36700.
[41] Informatienota van de privacycommissie over de bescherming van persoonsgegevens in België, http://www.privacycommission.be/publicaties/nota_infor_NL.pdf.
[42] D. DE BOT, *o.c.*, 36-40.

betrekking heeft op de doeleinden van de gegevensverwerking[43], en het **conformiteitsbeginsel** (artikel 4, §1, 3°-5° WVP) dat de gegevens zelf en de kwalitatieve vereisten waaraan deze moeten voldoen vastlegt.

Artikel 5 Wet Verwerking Persoonsgegevens somt enkele gevallen op waarvoor de verwerking van persoonsgegevens is toegelaten, mits naleving van de overige bepalingen van de Wet Verwerking Persoonsgegevens. Voor openbare overheden zullen vooral de nakoming van een wettelijke verplichting (artikel 5 c) en de vervulling van een taak van openbaar of algemeen belang (artikel 5 e) in aanmerking komen, evenals het gerechtvaardigde belang van de verantwoordelijke (artikel 5 f).

Er dient opgemerkt te worden dat de Wet Verwerking Persoonsgegevens bepalingen bevat ten voordele van de overheid die de toepassing van de wet "verzachten". Dit valt te verklaren vanuit de bijzondere taken en opdrachten van de overheid in het maatschappelijk en sociaal leven. De wet mag niet zo streng zijn dat het vervullen van deze taken onmogelijk wordt. Deze versoepelingen kunnen echter leiden tot een gebrek aan transparantie wat betreft de verwerking van de persoonsgegevens van bepaalde personen.[44]

3.3 Commissie voor de bescherming van de persoonlijke levenssfeer[45]

De Commissie voor de bescherming van de persoonlijke levenssfeer werd ingesteld in 1992 als een onafhankelijk toezichtorgaan bevoegd voor de privacybescherming ten overstaan van de verwerking van persoonsgegevens. De Commissie heeft een vrij ruim en algemeen bevoegdheidsgebied; ze is bevoegd voor alle vormen van gegevensverwerking, ongeacht het werkveld waarbinnen deze verwerking plaats vindt en ongeacht de aard ervan: de private sector, de openbare sector, geautomatiseerd of niet.[46]

De Commissie voor de bescherming van de persoonlijke levenssfeer :

- verstrekt adviezen en geeft aanbevelingen aan de bevoegde overheden en/of instanties;
- verleent machtigingen voor de verwerking of de mededeling van persoonsgegevens, aan de bevoegde instanties;
- controleert de wijze waarop de mededeling en verwerking van persoonsgegevens geschiedt;

[43] De gegevens moeten verkregen worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
[44] D. DE BOT, *o.c.*, 46-52.
[45] http://www.privacycommission.be.
[46] http://www.privacycommission.be/de_Commissie/bestuursplan.pdf.

- informeert en verleent bijstand aan de betrokken personen bij de uitoefening van hun rechten en plichten;

om bij te dragen tot de evenwichtige vrijwaring van het grondrecht van elkeen op bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. De Commissie moet ook een register bijhouden waarin alle machtigingen worden vermeld (artikel 12, §1 Wet Rijksregister).

Voor het verwerken van bepaalde persoonsgegevens is een machtiging vereist door het bevoegd sectoraal comité. Er zijn binnen de Commissie voor de bescherming van de persoonlijke levenssfeer vier comités[47]:

- het **sectoraal comité voor de federale overheid**[48] dat in principe zal oordelen over de aanvragen tot machtiging voor de elektronische mededeling van persoonsgegevens door een federale overheidsdienst of een onder de federale overheid ressorterende openbare instelling, andere dan een instelling van de sociale zekerheid;

- het **sectoraal comité van het Rijksregister**[49], dat onder meer belast is met de machtigingsprocedure betreffende de toegang tot de gegevens van het Rijksregister en het gebruik van het Rijksregisternummer.

- het **sectoraal comité voor de Kruispuntbank Ondernemingen**[50], dat onder meer belast is met het verlenen van machtigingen tot toegang tot bepaalde gegevens van de Kruispuntbank Ondernemingen;

- het **sectoraal comité van de Sociale Zekerheid**, dat ondermeer bevoegd is voor het verlenen van machtigingen tot elektronische mededeling van persoonsgegevens binnen het netwerk voor gegevensuitwisseling inzake de sociale zekerheid. Het comité verzekert het toezicht op de toepassing van en de naleving van de vigerende wetgeving.

De drie eerst genoemde sectorale comités bestaat uit zes leden: drie vaste, waaronder de voorzitter, die door de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) worden aangeduid en drie externe leden die door de Kamer van

[47] K.B. 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.
[48] D. DE BOT, *o.c.*, hoofdstuk 9.
[49] D. DE BOT, *o.c.*, hoofdstuk 6, afdeling 11.
[50] D. DE BOT, *o.c.*, hoofdstuk 7, afdeling 10.

Volksvertegenwoordigers worden aangeduid. Het sectoraal comité van de Sociale Zekerheid bestaat uit 5 leden, namelijk 2 leden uit de Commissie persoonlijke levenssfeer, waaronder de voorzitter en 3 externe leden.

Het is niet uitgesloten dat in de toekomst nog bijkomende sectorale comités opgericht worden. De aanwezigheid van verscheidene sectorale comités maakt het voor burgers en bedrijven moeilijker om te weten tot welk sectoraal zij zich moeten richten in geval van klachten of problemen. Het risico bestaat dat het een kluwen wordt voor de burger om te weten welke machtigingen door wie zijn of werden verleend. Eén centraal aanspreekpunt zou in dit opzicht beter zijn.

Gelet op de rolverdeling en de algemene bevoegdheid van de Commissie is een goede samenwerking tussen de sectorale comités en de Commissie van essentieel belang. Dit wordt geregeld in artikel 11 K.B. Sectorale Comités.

3.3.1 Het sectoraal comité voor de federale overheid

Artikel 36 bis WVP handelt over het sectorale comité van de federale overheid. Lid 3 bepaalt het volgende:

"Behalve in de door de Koning bepaalde gevallen, vereist elke elektronische mededeling van persoonsgegevens door een federale overheidsdienst of door een openbare instelling met rechtspersoonlijkheid die onder de federale overheid ressorteert een principiële machtiging van dit sectoraal comité, tenzij de mededeling reeds onderworpen is aan een principiële machtiging van een andere sectoraal comité opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer."

Het is dus mogelijk om bij koninklijk besluit een uitzondering in te voeren op de regel dat voor elke elektronische mededeling van persoonsgegevens een machtiging vereist is. Een koninklijk besluit vereist geen overleg binnen de Ministerraad en/of een advies van het sectoraal comité zelf. Dit houdt in dat de uitvoerende macht, de Regering, zonder al te veel controle zelf kan beslissen in welke gevallen gegevens "zonder meer" kunnen worden uitgewisseld.

3.4 De consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer[51]

De openbare overheden en openbare of private instellingen die toegang tot of mededeling van informatiegegevens van het Rijksregister verkregen hebben, evenals de overheden, instellingen en personen die gemachtigd zijn tot gebruik van het identificatienummer, zijn verplicht om, al dan niet onder hun personeel, een consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer aan te stellen (artikel 10 Rijksregisterwet). De figuur van deze consulent werd waarschijnlijk gebaseerd op de veiligheidsconsulent[52] in de sociale zekerheid[53] die aangesteld wordt krachtens artikel 25 Wet Kruispuntbank Sociale Zekerheid.

De titel van de consulent inzake informatieveiligheid en bescherming geeft al een duidelijk inzicht in de taken die de consulent moet opnemen. Hij vervult een gecombineerde functie: aan de ene kant moet hij instaan voor informatieveiligheid, aan de andere kant is hij ook verantwoordelijk voor de bescherming van de persoonlijke levenssfeer.

De basis voor de verplichte aanstelling van de consulent moet gezocht worden in artikel 16, §4 Wet Verwerking Persoonsgegevens. Dit artikel heeft het over de verplichting tot beveiliging of tot het waarborgen van de veiligheid van de persoonsgegevens. Daartoe moeten de verantwoordelijken voor de verwerking "de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, tegen de wijziging van of de toegang tot persoonsgegevens en tegen iedere andere niet toegelaten verwerking van persoonsgegevens".[54]

3.5 Andere maatregelen

De hierboven toegelichte manieren om persoonsgegevens te beschermen zijn niet exhaustief; In de specifieke wetten en koninklijke besluiten voor het Rijksregister, de KBO en de KSZ zijn bijkomende waarborgen ingebouwd. De naleving van deze bepalingen wordt ook strafrechtelijk afgedwongen.

[51] D. DE BOT, *o.c.*, afdeling 10, 225-238.
[52] Uitleg over de veiligheidsconsulent bij de KSZ, http://ksz-bcss.fgov.be/nl/securite/securite_6.htm.
[53] K.B. 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, *B.S.* 21 augustus 1993.
[54] D. DE BOT, *o.c.*, 228.

Zo worden er verplichtingen opgelegd betreffende het **beroepsgeheim** van de personen die betrokken zijn bij de inzameling, de verwerking of de mededeling van de gegevens. Er wordt ook een zekere vorm van **kwaliteitscontrole** aan deze verantwoordelijken opgelegd. Dit wordt geregeld in artikel 11 Wet Rijksregister, artikel 29 Wet KBO en artikel 22 en 28 Kruispuntbankwet.

De opgelegde normen voor kwaliteitscontrole zijn echter niet altijd even duidelijk geformuleerd. De verplichtingen zijn vaag en in algemene bewoordingen gesteld, wat discussie over de exacte inhoud van deze normen met zich mee kan brengen. Via deze wettelijke bepalingen wordt dus een soort van zelfcontrole opgelegd aan de instanties met toegang tot de authentieke bronnen.

De Wet Verwerking Persoonsgegevens voorziet ook in een **recht van inzage en verbetering**[55] voor elke persoon van wie gegevens worden bijgehouden (artikel 10 en 12 WVP).

3.6 Wordt de privacy voldoende beschermd?

Het valt op dat de Belgische overheid de bescherming van de persoonlijke levenssfeer vooral ziet als een aspect van informatieveiligheid[56]. Deze zienswijze wordt ook geïllustreerd door bovenstaand citaat. De overheid gaat ervan uit dat het op één plaats opslaan van gegevens met een goede technische beveiliging die gebruik maakt van de modernste informaticatechnieken, een garantie is voor een goede bescherming van persoonsgegevens. Hoewel er inderdaad een zekere overlapping tussen technische beveiliging en bescherming van de persoonlijke levenssfeer bestaat, zijn deze twee begrippen echter geen synoniemen.

De problematiek van bescherming van persoonsgegevens (oftewel informationele privacy) is echter ruimer dan louter informatieveiligheid. Het betreft hier de naleving van fundamentele beginselen als **wettigheid, proportionaliteit**[57] en **finaliteit**, inzake de kwaliteit van gegevens, de uitoefening van rechten door de betrokken burgers (recht van inzage, recht op verbetering,…) en enkele administratieve verplichtingen. Dit vereist een andere invalshoek dan bij informatieveiligheid, die in de meeste gevallen zal worden benaderd vanuit een technische invalshoek.[58]

[55] D. DE BOT, *o.c.*, 211-222 (toegepast op het Rijksregister) en 300-302 (toegepast op de KBO).
[56] D. DE BOT, *o.c.*, Informationele privacy versus security, 24-31.
[57] De verwerking van de persoonsgegevens moet evenredig zijn met de beoogde doelstelling of de aanleiding tot de verwerking.
[58] D. DE BOT, *o.c.*, Informationele privacy versus security, 30-31.

Er werd in België op dit moment nog geen globale studie verricht naar de gevolgen van e-government op het vlak van de bescherming van persoonsgegevens. De Commissie voor de bescherming van de levenssfeer heeft hierover nog geen algemeen advies uitgebracht. De Commissie heeft wel al aangegeven in haar advies van 11 februari 2002[59] dat het aangewezen is om de problemen die op het gebied van de fundamentele rechten en vrijheden van de burgers volgen uit het e-governmentbeleid, bij voorkeur door één en hetzelfde orgaan zouden behandeld worden. Zoals hierboven werd uiteengezet (verschillende sectorale comités) is dit op dit moment niet het geval.

Daarnaast is de Commissie geen voorstander van het combineren van de taken van informatieveiligheid en bescherming van de persoonlijke levenssfeer in één persoon (met name de consulent). De Commissie pleit voor een scheiding van deze functies aangezien het hier om zeer uiteenlopende materies gaat, hoewel zij cumul van deze functies in één persoon niet uitsluit. Dit gaat in tegen de visie van de federale overheid die de bescherming van de persoonlijke levenssfeer als een (weliswaar belangrijk) onderdeel van de beveiliging ziet.

Het pleiten voor een geïntegreerde en geautomatiseerde overheid is natuurlijk een zeer nobel streven, maar verregaande integratie brengt ook extra veiligheidsproblemen met zich mee. Corrupte informatie zal zich sneller verspreiden in een genetwerkte omgeving. Informatie die zich over netwerken verplaatst, kan door onbevoegde personen onderschept of zelfs veranderd worden, enzovoort.

In zekere zin is de burger wat betreft de verwerking van zijn persoonsgegevens ook volledig aangewezen op de overheid. De burger heeft immers geen keuze, hij moet zijn persoonlijke gegevens wel doorgeven aan de overheid. Als een burger meent dat een privaat bedrijf zijn privacy met voeten treedt, kan de burger gewoon naar een ander bedrijf stappen voor een product of dienst, dit is echter onmogelijk voor de diensten die de overheid aanbiedt. In die zin is het zeer belangrijk dat de overheid de bepalingen van de Wet Verwerking Persoonsgegevens zeer nauwgezet opvolgt. Men mag hierbij niet uit het oog verliezen dat een overheid zeer veel informatie over haar burgers heeft.

Ook het gebruik van unieke identificatienummers houdt een zeker risico in door de mogelijkheid van het leggen van interconnecties, verbindingen of koppelingen[60]. Door het

[59] Advies nr.07/2002 van 11 februari inzake het wetsontwerp tot oprichting van een Kruispuntbank van Ondernemingen, raadpleegbaar op de website van de Commissie.
[60] D. DE BOT, *o.c.*, Informationele privacy versus security, 58-59.

unieke identificatienummer wordt het eenvoudiger om verbanden te leggen tussen verschillende gegevensbanken en op die manier veel informatie over een bepaalde persoon op één plaats samen te brengen of van op één plaats toegankelijk te maken. Dit kan zonder medeweten van de persoon in kwestie gebeuren. Gegevens kunnen natuurlijk alleen maar gecombineerd worden als men over de nodige machtigingen beschikt om toegang tot deze gegevens te krijgen.

4 Conclusie

Kunnen authentieke bronnen een bijdrage leveren aan de bescherming van persoonsgegevens? Deze vraag verdient een genuanceerd antwoord. Aan de ene kant laat de centralisatie van gegevens in één authentieke bron toe om deze beter te beschermen/beveiligen. Er kunnen ook betere garanties geboden worden voor de integriteit en correctheid van de gegevens. Garanties die moeilijker te bieden zijn indien de gegevens verspreid zitten.

De unieke sleutel die gebruikt wordt, maakt het opzoeken en de verwerking van informatie erg gemakkelijk, maar houdt aan de andere kant ook nadelen in. Via die sleutel wordt het een fluitje van een cent om gegevens van personen met elkaar in verband te brengen en zo een volledig profiel van iemand op te stellen. Handig om de burger beter van dienst te zijn, is de eerste reflex van beleidsmakers en dit is ongetwijfeld zo. Maar dit voordeel brengt ook het nadeel van een “alwetende overheid” met zich mee. Toegegeven, al deze persoonsgegevens zijn momenteel al aanwezig binnen verschillende instanties van de overheid, maar de combinatie ervan brengt nieuwe gevaren met zich mee.

Geen enkele beveiliging is trouwens volmaakt. En dan hoef je niet meteen te denken aan het kraken van informaticasystemen. Wat als een persoon die toegang heeft tot de gegevens in een authentieke bron deze niet gebruikt voor de doeleinden waarvoor zij bestemd waren? Deze persoon kan natuurlijk vervolgd worden, maar de grootte van de schade zal ook samenhangen met de hoeveelheid van gegevens waarover deze malafide persoon kan beschikken.

Authentieke bronnen zijn zonder twijfel één van de belangrijkste (zo niet dé belangrijkste) bouwstenen voor e-government. Hun gebruik brengt echter ook gevaren met zich mee voor de privacy van de burgers van wie de gegevens opgeslagen worden. Het is belangrijk dat men deze gevaren onderkent en authentieke bronnen met de nodige omzichtigheid gebruikt. Er dient over gewaakt te worden de overheid in haar ijver om een optimale dienstverlening te

bieden, de rechten van haar burgers niet uit het oog verliest. Daarom is het aangewezen het aanwezige juridisch kader verder uit te werken en te consolideren om misbruik tegen te gaan.

5 Bibliografie

5.1 Wetgeving

Wet 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen (gecoördineerde versie 2004), *B.S.* 21 april 1984.

Wet 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, *B.S.* 22 februari 1990.

Wet 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 (gecoördineerde versie 2004), *B.S.* 3 september 1991.

Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (gecoördineerde versie juli 2004), *B.S.* 18 maart 1993.

Wet 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, *B.S.* 5 februari 2003.

K.B. 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.

K.B. 3 april 1984 betreffende de toegang door sommige openbare overheden tot het Rijksregister van de natuurlijke personen, alsmede betreffende het bijhouden en de controle van de informaties, *B.S.* 21 april 1984.

K.B. 8 februari 1991 betreffende de samenstelling en de wijze van toekenning van het identificatienummer van de natuurlijke personen die niet ingeschreven zijn in het Rijksregister van de natuurlijke personen, *B.S.* 19 februari 1991.

K.B. 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, *B.S.* 21 augustus 1993.

K.B. 13 februari 2001, ter uitvoering van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 13 maart 2001.

K.B. 26 juni 2003 houdende aanwijzing van de overheden, administraties en diensten die, betreffende bepaalde categorieën van ondernemingen, belast zijn met de eenmalige inzameling en het actualiseren van de gegevens bedoeld in artikel 6 Wet KBO, *B.S.* 30 juni 2003.

K.B. 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.

K.B. 8 januari 2006 tot bepaling van de informatietypes, verbonden met de informatiegegevens bedoeld in artikel 3, eerste lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *B.S.* 25 januari 2006.

5.2 Rechtsleer

DE BOT, D., *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, 468 p.

ROBBEN, F., "E-government", http://www.law.kuleuven.ac.be/icri/frobben/publications/2004%20-%20E-government.pdf.

5.3 Websites

http://www.belgium.be, portaalsite van de Belgische federale overheid.

http://www.rijksregister.fgov.be, site van het Rijksregister.

http://www.ksz.fgov.be, site van de Kruispuntbank van de Sociale Zekerheid.

http://mineco.fgov.be/redir_new.asp?loc=/enterprises/crossroads_bank/home_nl.htm, site van de Kruispuntbank Ondernemingen.

http:/www.law.kuleuven.ac.be/icri/frobben, site van Frank Robben, administrateur-generaal Kruispuntbank van de Sociale Zekerheid.

http://www.privacycommission.be, site van de Commissie voor de bescherming van de persoonlijke levenssfeer.

http://www.vlaanderen.be/e-government, site van de Vlaamse Coördinatiecel e-government.

6 Bijlage: Interview met Hans Arents, adviseur strategie & technologie van de Coördinatiecel Vlaams E-Government

Wat zijn uw ervaringen bij het aanvragen van machtigingen voor het gebruik van persoonsgegevens bij de sectorale comités?

De Coördinatiecel Vlaams E-Government (Corvé) heeft nog niet zoveel ervaring bij het doorlopen van deze procedure. Uit gesprekken met andere afdelingen binnen de Vlaamse Overheid blijkt dat deze de aanvraag voor een machtiging een zware en omslachtige procedure vinden. Soms duurt het een jaar of langer om de goedkeuring van een sectoraal comité te krijgen. Er is echter verbetering in zicht. De privacy commissie heeft zich sterk gemaakt dat de dossiers in de toekomst sneller afgehandeld zullen worden.

Zijn er verschillen binnen de verschillende beleidsniveaus wat betreft de omgang met persoonsgegevens?

Vlaanderen voert in dat opzicht een wat liberalere koers dan Wallonië. In Wallonië bestaat er een grotere gevoeligheid wat betreft het gebruik van persoonsgegevens.

Het valt op dat er in de zuidelijke landen van Europa een grotere gevoeligheid bestaat wat betreft privacy-gerelateerde onderwerpen. Zo is in Frankrijk het gebruik van een uniek identificatienummer bijvoorbeeld bij wet verboden, terwijl men tezelfdertijd in Finland totaal geen graten ziet in het gebruik van een uniek nummer om verschillende persoonsgegevens met elkaar te koppelen.

Dit verschil in gevoeligheid bij de lidstaten wordt meestal toegeschreven aan de bezetting door de Duitsers tijdens Wereldoorlog II die nog voortleeft in het collectief geheugen. Door de Duitsers bezette staten staan huiverachtiger ten opzichte van het gebruik van een uniek identificatienummer. Het unieke identificatienummer in Nederland dat reeds vóór WOII bestond, maakte het voor de Duitsers erg gemakkelijk om joden op te sporen en gevangen te nemen. In België bestond er ook zo'n systeem, maar in ons land hebben de autoriteiten tijdens de bezetting via allerlei vertragingsmanoeuvres belet dat dit systeem effectief werd gebruikt. Op Europees vlak creëren deze verschillen tussen de lidstaten qua visies op privacy vaak problemen. De verschillende opvattingen zijn soms moeilijk te verzoenen.

De manieren waarop men de gegevens beschermt, zijn ook verschillend. In Oostenrijk kiest men bijvoorbeeld voor een sterk technische oplossing om aan de vraag naar bescherming van persoonsgegevens te voldoen. Dit in tegenstelling tot België waar de nadruk eerder ligt op een juridisch-organisatorische bescherming.

Ziet u problemen bij de juridische bescherming van gegevens zoals die in België gehanteerd wordt?

In theorie is de bescherming goed, maar in praktijk gebeurt het soms dat er voor de overheid specifieke uitzonderingen in de privacywetgeving worden opgenomen. Op die manier kan de bestaande wetgeving uitgehold worden. Men moet er ook over waken dat men niet tezelfdertijd rechter en partij is. Zo zijn sommige leden van de sectorale comités ook betrokken bij het opzetten van de infrastructuur voor het bewaren en verwerken van gegevens.

Hoe garandeert Vlaanderen de bescherming van persoonsgegevens?

Vlaanderen moet handelen conform de federale wetgeving. Momenteel is er vooral gegevensuitwisseling met de Kruispuntbank Sociale Zekerheid. Vlaanderen is dus verplicht het in dit kader uitgewerkte veiligheidsmodel (o.a. aanstelling van een veiligheidsconsulent) over te nemen.

In theorie is Vlaanderen een onafhankelijk en gelijkwaardig beleidsniveau, maar in de praktijk is Vlaanderen afhankelijk van de beslissingen van de KSZ. Het is mogelijk dat de prioriteiten van de KSZ en die van de Vlaamse instanties niet gelijklopend zijn. Vlaanderen kan alleen een vraag richten tot de KSZ om een bepaalde toepassing te bouwen. De KSZ hoeft niet in te gaan op deze vraag.

Vragen Vlaamse instanties gegevens op uit het Rijksregister?

Momenteel nog niet. Technisch is het gemakkelijker om de Vlaamse toepassingen te koppelen met de KSZ. De KSZ heeft trouwens ook toegang tot het Rijksregister, waardoor het via een omweg mogelijk is om aan de persoonsgegevens uit het Rijksregister te geraken. Organisatorisch is het ook gemakkelijker om een machtiging te krijgen om gegevens uit de KSZ te gebruiken. Vlaamse instanties zoals bijvoorbeeld de VDAB hebben al toegang tot de KSZ gekregen in het kader van de samenwerking op het vlak van sociale zekerheid.

Hoe gebeurt de informatiemodellering binnen de Vlaamse Overheid?

Momenteel wordt er gewerkt aan een de facto standaard voor de gegevensmodellering. Er werd voor het opstellen van dit model om praktische redenen gekozen voor een top-down benadering. Het zou te veel tijd vergen om met alle belanghebbenden samen te zitten en een consensusmodel overeen te komen.

Kan u wat meer uitleg geven over de Vlaamse authentieke bronnen?

De Verrijkte Kruispuntbank Personen maakt gebruik van de webservices aangeboden door de KSZ en vormt voor de Vlaamse Overheid een soort doorgeefluik voor de basispersoonsgegevens die uit de KSZ gehaald worden. Wat betreft de Verrijkte Kruispuntbank Personen stellen zich twee problemen: enerzijds een beveiligingsprobleem, anderzijds de problematiek van het opstellen van een gestandaardiseerd persoonsgegevensmodel.

De Verrijkte Kruispuntbank Ondernemingen extraheert de gegevens uit de federale Kruispuntbank Ondernemingen. Het aangeleverde datamodel wordt platgeslagen en heropgebouwd in een nieuw datamodel dat geoptimaliseerd is voor raadpleging. Aan dit nieuwe datamodel worden extra gegevens toegevoegd waarover de Vlaamse Overheid beschikt. Het gaat hier niet om authentieke gegevens, maar de bijkomende gegevens die opgenomen worden in de VKBO zijn wel betrouwbaar.

Bovendien biedt de VKBO een aantal extra diensten aan die de gewone KBO niet levert: interactieve raadpleging via een grafische gebruikersinterface en de mogelijkheid om de VKBO te consulteren via webservices.

Instanties als de VDAB zijn vragende partij om de VKBO te gebruiken. De VDAB wil grote delen van de VKBO dupliceren. Hier stelt zich de vraag of dit wenselijk is en of dit zelfs niet in tegenspraak is met de filosofie van authentieke bronnen. Nu, technisch kan men moeilijk anders dan met duplicaten (caches, kopieën) werken. Rechtstreekse consultatie bij de authentieke bron zou immers een zware belasting van zowel het netwerk als van de bron zelf met zich meebrengen. Indien men werkt met duplicaten, moeten wijzigingen aan de oorspronkelijke gegevens zo snel mogelijk doorgegeven worden, zodat het risico op werken met verouderde gegevens beperkt blijft.

Welke rol speelt de coördinatiecel e-government bij dit alles?

Corvé wil een centraal aanspraakpunt zijn voor alles wat met e-government te maken heeft. Via diensten als het VKBP en de VKBO wil de cel e-government back-office diensten met een toegevoegde waarde creëren voor klanten binnen de Vlaamse Overheid (IVA's, EVA's, afdelingen,…).

Een voorbeeld hiervan is het systeem van "mutaties" (dwz. het automatisch doorsturen van wijzigingen in persoonsgegevens) aangeboden door de KSZ. Momenteel is het zo dat deze wijzigingen rechtstreeks doorgestuurd worden door de KSZ. De KSZ moet zelf bijhouden welke gegevens relevant zijn voor welke instantie waarmee ze gekoppeld is. De KSZ stuurt dus alleen maar gefilterde gegevens door. Corvé zou naar een systeem willen evolueren waarbij de KSZ alle voor Vlaanderen relevante wijzigingen doorstuurt en dat binnen de toekomstige VKBP dan zelf bepaald wordt welke wijzigingen doorgestuurd worden naar welke Vlaamse gegevensafnemers.

Dit systeem zou de KSZ ontlasten door gebruik te maken van een verwijzingsysteem dat vergelijkbaar is met de manier waarop domeinnamen op het internet beheerd worden door de Domain Name Servers (een cascade van DNS-servers). De Vlaamse Overheid zou in dat geval zelf een verwijzigingsrepertorium dienen bij te houden. Deze manier van werken is momenteel echter juridisch onmogelijk, omdat persoonsgegevens enkel opgevraagd mogen worden als je een aantoonbaar belang hebt bij het verwerken van die gegevens. De KSZ mag dus niet zomaar álle wijzigingen doorgeven aan de Vlaamse Overheid, en vervolgens aan de Vlaamse Overheid toelaten dat die zelf verder beslist hoe die gegevens mogen gebruikt worden.

Deze beperking maakt het quasi onmogelijk om generieke diensten op te bouwen. De Vlaamse Overheid is dan ook vragende partij om zelf in staat te zijn om machtigingen toe te kennen aan Vlaamse overheidsentiteiten om zo een mutatiefilter te ontwikkelen op maat van de betrokken gegevensafnemer.