Conferentie "Effectieve informatiebeveiliging"
6 en 7 februari 1990
Hilton Hotel te Brussel

DE BEVEILIGING VAN DE SOCIALE KRUISPUNTBANK EN HET GEINTEGREERD INFORMATIENETWERK VAN DE SOCIALE ZEKERHEID

Frank ROBBEN
Adviseur Kabinet van de Eerste Minister
Ondervoorzitter Commissie voor de Informatisering van de Sociale Zekerheid

1. DOELSTELLINGEN EN WERKING VAN HET INFORMATIESYSTEEM VAN DE SOCIALE ZEKERHEID, BEHEERD DOOR DE SOCIALE KRUISPUNTBANK

1.1. Probleemstelling

De sociale zekerheid stelt zich tot doel het voorkomen en schadeloosstellen van menselijke schade ten gevolge van bepaalde sociale ricico's (ziekte, handicap, werkloosheid, ouderdom, armoede, ...). De slechte werking van de sociale zekerheid heeft niet alleen nadelige gevolgen op het individuele, maar evenzeer op het algemeen maatschappelijke vlak (armoede, sociale onrust, bedreiging van de volksgezondheid, ...). Om de noodzakelijke sociale beveiliging te bieden is een nauwkeurige bewaking nodig van de levensrisico's die zich bij de leden van de beschermde groep voltrekken. Een rationeel gegevensbeheer met de nodige garanties inzake de integriteit, de betrouwbaarheid en de beschikbaarheid van de informatie, is dan ook de belangrijkste voorwaarde voor een efficiënte en effectieve werking van de sociale zekerheid en een aangepaste sociale beleidsvoering. Tot nog toe verloopt de gegevensinzameling, -verwerking en -uitwisseling evenwel quasi uitsluitend op papieren wijze en zonder noemenswaardige coördinatie tussen de betrokken instellingen. Dit heeft een aanzienlijke overlast tot gevolg, zowel bij de informatieverstrekkers als bij de sociale zekerheidsinstellingen.

Het belang van een goede functionering van de sociale zekerheid en het daartoe noodzakelijke recht van de gemeenschap op informatie moet evenwel worden afgewogen tegen het recht op privacy van de sociaal verzekerden. Het globale informatiesysteem van de sociale zekerheid moet er ook voor zorgen dat onrechtmatige gegevensbehandelingen maximaal worden verhinderd.

Tenslotte kan ook de historisch gegroeide uitvoeringsorganisatie van de Belgische sociale zekerheid, die een weerspiegeling is van de maatschappelijke ordening, uit naam van de rationalisering niet fundamenteel door elkaar worden gegooid. De computer mag inderdaad niet worden ingezet als machtsinstrument om structuren te veranderen of bevoegdheden te verleggen. Dergelijke beslissingen vergen een fundamenteel debat ten gronde, en mogen niet door

de technologie worden opgedrongen.

Uit de beschreven probleemstelling blijkt dat diverse aspecten van de problematiek van de informatieveiligheid wezensbestanddelen uitmaken van het geïntegreerd informatiesysteem dat de werking van de sociale zekerheid moet ondersteunen. Zowel de confidentialiteit van de informatie als de integriteit, de betrouwbaarheid en vlotte beschikbaarheid ervan dienen gegarandeerd.

1.2. De werking van het informatiesysteem beheerd door de sociale kruispuntbank

Begin 1986 werd door de toenmalige Minister van Sociale Zaken, J.L. Dehaene een informatiseringsplan voor de sociale zekerheid afgekondigd, waarvan de uitvoering onverkort wordt verdergezet door zijn opvolger, Ph. Busquin. De kern van dit plan bestaat in de oprichting van een elektronisch sternetwerk voor gegevensuitwisseling tussen de ruim 2000 instellingen van sociale zekerheid. Centraal knooppunt van dit netwerk is de sociale kruispuntbank, die wettelijk wordt opgericht medio 1990 en vermoedelijk operationeel zal zijn tegen september 1990.

De sociale kruispuntbank slaat in principe geen inhoudelijke gegevens op centrale wijze op, maar beschikt enkel over een wie-wat-waar-repertorium waarin per persoon wordt aangegeven welke soorten gegevens in welke sociale zekerheidsinstellingen of-sectoren worden bewaard. Of in het wie-wat-waar-repertorium van de kruispuntbank wordt verwezen naar de sector in het algemeen dan wel rechtstreeks naar de betrokken instelling, hangt af van het feit of instellingen uit de betrokken sector al dan niet zelf een wie-wat-waar-repertorium (laten) bijhouden met verwijzingen tot op het niveau van de instellingen. Uit de rechtstreekse verwijzing in het repertorium van de sociale kruispuntbank naar de instelling zou immers in bepaalde gevallen op zich reeds belangrijke inhoudelijke informatie kunnen worden afgeleid, zoals het lidmaatschap van een mutualiteit of van een vakbond. Vandaar dat in de takken waarin private, meewerkende instellingen opdrachten uitvoeren, kan worden geopteerd voor een tweetraps-

systeem waarbij de kruispuntbank enkel de referentie naar de tak of het stelsel bezit en de parastatale die de tak beheert of de betrokken meewerkende instellingen in onderlinge samenwerking op hun beurt een sectorieel repertorium bijhouden met verdere doorverwijzingen tot op het niveau van de instellingen. De keuze voor deze mogelijkheid leidt ertoe dat de knooppunten van het netwerk beheerd door de sociale kruispuntbank op hun beurt een kruispuntfunctie uitoefenen m.b.t. de betrokken tak of stelsel.

De inhoudelijke gegevens worden op basis van een functionele bevoegdheidsverdeling tussen de diverse sociale zekerheids-instellingen op gedistribueerde en gedecentraliseerde wijze bewaard. De bedoeling bestaat erin elk gegeven in zijn authentieke vorm slechts op één plaats in het net te bewaren. Grosso modo zullen de identificatiegegevens worden bewaard in het rijksregister, de loon- en arbeidstijdinformatie bij de inningsinstellingen en de overige gegevens bij de instelling die ze in eerste instantie nodig heeft voor de uitvoering van haar opdrachten. Binnen het netwerk worden de verantwoordelijkheden aldus duidelijk verdeeld, waarbij elke betrokken instelling haar autonomie bewaart.

Wanneer een sociale zekerheidsinstelling een inlichting betreffende een bepaalde persoon nodig heeft en nog niet bezit, dient ze zich in principe, desgevallend via de instelling die het specifieke repertorium m.b.t. de betrokken tak bijhoudt, eerst tot de sociale kruispuntbank te wenden. Wanneer haar een vraag om informatie wordt gesteld, voert de sociale kruispuntbank eerst een controle uit op de rechtmatigheid van de vraag aan de hand van het lager beschreven gegevensmodel van de sociale zekerheid. Mag de gevraagde informatie verstrekt worden, wordt via een consultatie van de wie-wat-waar-gegevensbank nagegaan of het gegeven reeds in het net beschikbaar is, en waar het desgevallend kan worden opgevraagd. Indien de benodigde informatie aanwezig blijkt te zijn, haalt de kruispuntbank ze automatisch op bij de bewarende instelling, die verplicht is deze informatie (elektronisch) te verstrekken, en maakt ze over aan de opvragende instantie. Slechts indien de gegevens niet in het net voorhanden blijken te zijn, is de belanghebbende instelling gemachtigd de

sociaal verzekerde of andere personen, die de betrokken inlichtingen kunnen verstrekken (vb. de werkgever), te ondervragen. Ter actualisatie van de wie-wat-waar-gegevensbank dient de gegevensinzamelende instelling dan wel het resultaat van de ondervraging aan de kruispuntbank, desgevallend via het specifieke repertorium m.b.t. de betrokken tak of stelsel, over te maken. De sociale kruispuntbank zal het meegedeelde resultaat dan automatisch doorzenden naar de instelling die met de opslag van de gegevens is belast.

Voor de identificatiegegevens zal bovendien gezorgd worden voor een automatische mededeling, via een elektronisch brievenbussensysteem, van gegevenswijzigingen aan de belanghebbende instellingen.

Om de uitwisseling van gegevens binnen het geschetste samenwerkingsmodel met de grootst mogelijke juistheidswaarborg te laten verlopen, wordt gebruik gemaakt van een unieke, onveranderlijke identificatiesleutel per persoon doorheen de hele sociale zekerheid.

De afspraken omtrent wie welke gegevens bijhoudt en welke gegevensuitwisselingen geoorloofd zijn, worden op geïntegreerde wijze omschreven in een gegevensmodel van de sociale zekerheid.

2. DE BEVEILIGING VAN HET GESCHETSTE INFORMATIESYSTEEM

2.1. Basisprincipes die ten grondslag liggen van de uitgewerkte veiligheidsmaatregelen

De veiligheid van het informatiesysteem bestaat uit de preventie van schade die kan worden toegebracht aan de goede werking van de sociale zekerheid enerzijds en aan de persoonlijke levenssfeer van de sociale verzekerden anderzijds.

Primaire preventie gaat voor secundaire en tertiaire preventie, omdat de eerste het optreden van schade vermijdt, terwijl de tweede de reeds aangerichte schade herstelt en de derde slechts verhindert dat de schade nog erger wordt. Toch zijn de drie

vormen van preventie nodig, omdat niet alle schade kan vermeden worden, ook niet bij het beste veiligheidsbeleid.

De inspanningen gericht op de informatieveiligheid moeten gericht zijn op het bereiken van een redelijk evenwicht tussen het behalen van de winst- en het vermijden van de verlieskansen, die uit de vernieuwing voortvloeien. Absolute veiligheid mag niet voorgesteld worden als een na te streven ideaal. Anders dreigt elke vernieuwing in de kiem te worden gesmoord.

De beveiliging van het informatiesysteem is geen technisch product dat door deskundigen in het systeem kan worden ingebouwd, maar volgt uit de zorgzame uitvoering van de dagelijkse opdracht van iedere persoon die bij de werking ervan betrokken is. De sociale organisatie van de beveiliging is de conditio sine qua non van gelijk welk veiligheidssysteem. Zelfs de beste technologische hulpmiddelen kunnen nooit de sociale controle vervangen.

Een informatiesysteem is zo veilig als de veiligheid van zijn zwakste schakel. Een homogeen geheel van maatregelen is nodig, zoniet zijn de inspanningen zinloos.

Het voorstellen van een omnivalente modeloplossing inzake informatieveiligheid is onmogelijk. Een onderscheid dient te worden gemaakt tussen de algemene doelstellingen, die globaal kunnen worden vastgelegd, en de manier waarop deze doelstellingen worden gerealiseerd. Bij de keuze van de manier waarop de doelstellingen worden gerealiseerd dient voldoende ruimte te worden gelaten om optimaal in te spelen op de concrete behoeften en risico's van elke instelling. Responsabilisering van de betrokkenen via het opleggen van gecontroleerde zelfregulering werkt in dit kader efficiënter dan overnormering van bovenuit.

De beste preventie, met name de primaire, vernietigt de bewijzen van haar efficiëntie. Zij laat immers de schade niet ontstaan. Dit veroorzaakt mettertijd een valse indruk van nutteloosheid, gevolgd door verslapping van de aandacht en van de inspanning. Daarom is een volgehouden motivatie onontbeerlijk.

2.2. Uitwerking van de principes

2.2.1. Informatiebeveiligende effecten van de structuur van het netwerk

De structuur van het netwerk en het uitgetekende samenwerkingsmodel maakt een preventieve controle op de rechtmatigheid van elke elektronische gegevensuitwisseling mogelijk evenals een centrale, computerondersteunde opsporing van bepaalde misbruiken. Alle rechtstreekse elektronische verbindingen die de sociale zekerheidsinstellingen met mekaar of met derden hebben, moeten immers in principe via de sociale kruispuntbank verlopen. Binnen het netwerk wordt een systeem van controles uitgebouwd, gebaseerd op informatie omtrent de uitvoerder van een transactie, het tijdstip van een transactie, de gebruikte toegangsweg en het type van de transactie. Het controlesysteem wordt trapsgewijze opgebouwd op basis van gecoördineerde afspraken tussen alle betrokken instellingen, die elk een deel van de controleverantwoordelijkheid toebedeeld krijgen. Het centraal loggen en controleren van alle transacties zou niet alleen technisch moeilijk realiseerbaar zijn, maar bovendien op zijn beurt leiden tot een ongewenste centrale opslag van uitgebreide persoonsinformatie.

Via het netwerk kunnen slechts de types van transacties worden uitgevoerd die voorafgaandelijk te zijn toegestaan door een onafhankelijk Toezichtscomité (zie lager) en met hun kenmerken beschreven zijn in het gegevensmodel van de sociale zekerheid.

De optie voor een gedistribueerde gegevensopslag volgens de beschreven functionele bevoegdheidsverdeling tussen de sociale zekerheidsinstellingen, beperkt tenslotte de redundantie en de beschikbaarheidsgraad van de informatie en verlaagt daardoor de kans op fouten en misbruiken. Bovendien is de inbraak in één computer onvoldoende om alle sociale gegevens betreffende een bepaald persoon te kunnen accederen.

2.2.2. Organisatorische maatregelen

Bij de sociale kruispuntbank wordt vooreerst een onafhankelijk, door het Parlement benoemd Toezichtscomité ingesteld. Verscheidene bepalingen uit de wet streven ernaar de onafhankelijkheid van de leden van het Toezichtscomité, en in het bijzonder van zijn voorzitter, optimaal te waarborgen. Het Toezichtscomité is in het algemeen belast met het toezicht op de naleving van de bepalingen van de wet op de sociale kruispuntbank, in het bijzonder de gegevensbeschermende bepalingen, door de sociale kruispuntbank, de sociale zekerheidsinstellingen en, in het algemeen, alle personen die voor de toepassing van de sociale zekerheid omgaan met gegevens van persoonlijke aard. Het Toezichtscomité kan in dit verband helpen bij de oplossing van geschillen en aanbevelingen formuleren, zonder afbreuk te doen aan de gewone bevoegdheden van de hoven en rechtbanken.

Het Toezichtscomité handelt op eigen initiatief of op verzoek. Behoudens uitdrukkelijke toestemming van de betrokkene mag de naam van een aanklager niet bekend worden gemaakt.

Het Toezichtscomité houdt een gegevensmodel bij waarin op geïntegreerde wijze de afspraken worden omschreven omtrent wie welke gegevens bewaart, met welke frequentie ze dienen te worden geactualiseerd, en welke gegevensuitwisselingen geoorloofd zijn. Dit model is te allen tijde raadpleegbaar door het publiek.

De leden van het Toezichtscomité beschikken, individueel of collegiaal, over ruime onderzoeksmogelijkheden. Ze kunnen bovendien bij hun activiteiten beroep doen op sociale inspecteurs met uitgebreide controlebevoegdheden. De voorzitter bezit de mogelijkheid om geschillen, die het Toezichtscomité niet kan oplossen of waarvoor de betrokkenen geen bevredigende oplossing voorstellen, aanhangig te maken bij de arbeidsgerechten.

Elk jaar stelt het Toezichtscomité een omstandig activiteitenverslag op ten behoeve van het Parlement, de Regering en het Beheerscomité van de sociale kruispuntbank, dat door iedere belanghebbende persoon kan worden geraadpleegd of verkregen.

In de wet wordt bijzondere aandacht besteed aan de verhouding en de bevoegdheidsafbakening tussen het Toezichtscomité specifiek bevoegd voor de sociale zekerheid en de algemene Commissie voor de bescherming van de persoonlijke levenssfeer. De bedoeling van één en ander bestaat erin een efficiënte controle op de naleving van de gegevensbeschermende maatregelen binnen de sociale zekerheid door materiedeskundigen te verzoenen met een uniforme toepassing van de algemene beginselen inzake de bescherming van de persoonlijke levenssfeer doorheen alle maatschappelijke sectoren.

Naast de oprichting van een onafhankelijk en extern controleorgaan, werd in elke instelling van sociale zekerheid een interne veiligheidsfunctionaris aangesteld met een adviserende, motiverende en controlerende functie inzake informatieveiligheid. De interne veiligheidsfunctionaris rapporteert rechtstreeks aan het dagelijks bestuur en helpt dit bij de uitwerking van het informatiebeveiligingsbeleid. Hierbij dient hij zich te richten naar de reglementaire bepalingen die door of in uitvoering van de wet inzake gegevensbescherming worden uitgevaardigd. Bij koninklijk besluit kunnen overigens normen worden uitgevaardigd inzake de technische werking van het netwerk en de informatieveiligheid. Overigens ondergaan de veiligheidsfunctionarissen in dit verband een permanente vorming georganiseerd door het Toezichtscomité.

De interne veiligheidsfunctionaris fungeert als omnipracticus inzake informatieveiligheid in zijn instelling. Voor specifieke deelproblemen kan hij terugvallen op een algemene dienst inzake informatieveiligheid die op kostendelende basis tussen de sociale zekerheidsinstellingen wordt uitgebouwd en wordt bemand door specialisten m.b.t. de onderscheiden aspecten van de problematiek van de informatieveiligheid.

2.2.3. Wettelijke verplichtingen van de gegevensverwerkende instanties en rechten van de geregistreerden

Naast de beschreven organisatorische maatregelen, voorziet de wet

in een belangrijk aantal bepalingen ten gronde inzake gegevensbescherming. Het betreft evenwel eerder kadervoorschriften die de verplichting opleggen tot het nemen van maatregelen om bepaalde doeleinden te bereiken dan materiële bepalingen waaruit inhoudelijk rechtstreeks kan worden afgeleid wat mag en niet mag. De schikkingen in uitvoering van de kaderbepalingen kunnen dan optimaal worden afgestemd op de concrete behoeften en risico's van de verwerkingsomgeving. Dit is in de eerste plaats de taak van de interne veiligheidsfunctionaris, die één en ander zal vastleggen in een specifieke veiligheidscode voor zijn instelling.

De regeling is van toepassing op alle informatie die betrekking heeft op een identificeerbaar persoon en die wordt aangewend voor sociale zekerheidsdoeleinden, ongeacht de gebruikte drager (papier, magneetbanden of -schijven, ...).

De personen die tussenkomen bij de toepassing van de sociale zekerheid mogen enkel de gegevens inzamelen die ze nodig hebben voor de toepassing van de sociale zekerheid. Ze mogen de verkregen informatie slechts bewaren en gebruiken gedurende de tijd die is vereist voor de uitvoering van hun wettelijke verplichtingen en ze enkel in dat raam aanwenden. Ze moeten alles in het werk stellen om de goede bewaring van de persoonsgegevens te verzekeren en het vertrouwelijk karakter ervan te waarborgen. Onjuiste, onvolledige en onnauwkeurige informatie moet worden verbeterd en overbodige en onrechtmatig verkregen gegevens dienen te worden gewist. De sociale kruispuntbank staat in voor de mededeling van de verbeteringen en de uitwissingen aan de overige belanghebbende sociale zekerheidsinstellingen.

De gebondenheid door het beroepsgeheim van elke persoon die tussenkomt bij de inzameling, verwerking of uitwisseling van persoonsgegevens in het kader van de sociale zekerheid wordt bovendien uitdrukkelijk bevestigd.

Specifieke bijkomende regelen gelden bij de omgang met medische persoonsgegegevens. Het bewaren en bewerken van medische persoonsgegevens dient te geschieden onder het toezicht van een

verantwoordelijk geneesheer, die bij naam de personen aanwijst die de betrokken informatie mogen opslaan, raadplegen, wijzigen, verwerken of vernietigen. Per persoon wordt in een daartoe bestemd register de inhoud en de draagwijdte van de verstrekte machtiging vermeld. Indien medische persoonsgegevens worden bewaard in geautomatiseerde bestanden, dient de toegang plaats te vinden aan de hand van individuele toegangs- en bevoegdheidscodes. Eenmaal gearchiveerd, dienen de op elektronische dragers beschikbare medische persoonsgegevens op niet rechtstreeks toegankelijke dragers te worden bewaard.

De sociale zekerheidsinstellingen zijn ertoe gehouden uit eigen beweging en in een goed verstaanbare vorm aan de sociaal verzekerden de persoonsgegevens mee te delen waarop ze zich hebben gebaseerd voor het beoordelen van de eventuele rechten van de betrokkenen. Dergelijke mededeling dient uiterlijk te geschieden tezamen met de kennisgeving van de beslissing over het recht dat aan de hand van de betrokken informatie werd geëvalueerd en dient te worden herhaald bij elke nieuwe beoordeling van dat recht. Daarnaast kunnen de sociaal verzekerden op eigen initiatief hun recht op informatie laten gelden onder de voorwaarden en volgens de modaliteiten die zullen worden vastgelegd bij koninklijk besluit. Voorzover daartoe aanleiding bestaat, beschikken de sociaal verzekerden over de mogelijkheid om de verbetering, het gebruiksverbod of de uitwissing van de gegevens te eisen.

De wet bevat uitgebreide strafsancties bij de schending van de bepalingen gericht op het waarborgen van een efficiënte gegevensbescherming en een afdoende informatieverstrekking aan de sociale verzekerden, in geval van verhindering van de controle op de naleving van deze bepalingen en in geval van computercriminaliteit.

Vermeldenswaard is tenslotte de bepaling die voorziet in de mogelijkheid van de aanduiding, door de Koning, van een persoon belast met (het bevelen van) de vernietiging van de gegevensbanken waarin persoonsgegevens voor de sociale zekerheidsdoeleinden worden bewaard in geval van oorlog of bezetting van het grondge-

bied door de vijand. Bij dergelijke vernietiging dient er evenwel zoveel mogelijk voor te worden gezorgd dat de toepassing van de wetgeving inzake sociale zekerheid niet in het gedrang wordt gebracht.

2.2.4. Check-list van beveiligingsmaatregelen uitgewerkt door de werkgroep van veiligheidsfunctionarissen

De werkgroep van interne veiligheidsfunctionarissen in samenwerking met de gemeenschappelijke cel van veiligheidsspecialisten werkt aan een basisdocument met suggesties over de wijze waarop de toepassing van de beschreven principes inzake gegevensbescherming technisch en organisatorisch naar behoren kunnen worden geconcretiseerd. De daarin vermelde maatregelen hebben o.a. betrekking op:

- het uitwerken van duidelijke bevoegdheidsafbakeningen (scheiding van functies);
- fysische beveiliging en toegangsbeheersing;
- logische toegangsbeveiliging, op basis van een combinatie van kennis en bezit;
- transactielogging en -controle;
- netwerkbeveiliging;
- back-up en herstelprocedures, waarbij optimaal wordt ingespeeld op de mogelijkheden tot wederzijdse hulp van de instellingen die deel uitmaken van het netwerk;
- de opstelling van rampenplannen;
- bescherming van de programma's en gegevensbestanden, o.a. door selectieve gegevensversluiering en stricte wijzigingsprocedures;
- interne veiligheidscontrole;
- veiligheidsplanning en -budgettering.

Het basisdocument zal de interne veiligheidsfunctionarissen helpen bij het uitwerken van een specifieke code inzake informatieveiligheid voor hun instelling. Deze code zal dan ter beoordeling worden voorgelegd aan het Toezichtscomité.

3. BESLUIT

Binnen het globale informatiesysteem van de sociale zekerheid nemen de maatregelen inzake informatieveiligheid een cruciale rol in. De nadruk wordt hierbij gelegd op preventie en een ver doorgedreven responsabilisering van alle betrokken instanties.

Er wordt geopteerd voor een systeem van gedistribueerde gegevensbehandeling en een stapsgewijze verfijning van de gegevensbeschermende maatregelen via het stimuleren van zelfregulerende initiatieven. Wel worden de betrokken instanties optimaal begeleid bij het uitwerken van de nodige maatregelen, die overigens aan een permanente controle worden onderworpen. Op deze wijze wordt de efficiëntie van de veiligheidsmaatregelen verhoogd, maar wordt er tegelijk voor gezorgd dat er zo weinig mogelijk onnodig storende invloed van uitgaat op een rationeel gegevensbeheer.

De structurele en organisatorische schikkingen worden in het geheel van maatregelen als veel efficiënter beschouwd dan de technische maatregelen, die enkel ondersteunend kunnen werken.

Een specifiek extern controleorgaan met verregaande bevoegdheden staat in voor de preventieve en repressieve controle op de naleving van de gegevensbeschermende verplichtingen en houdt een geïntegreerd overzicht bij van alle toegelaten gegevensbehandelingen.