Mag het een bitje minder zijn?

Over Privacy Enhancing Technologies (PET) en de juridische basis van hun gebruik

Drs. J.J. Borking

Dit artikel gaat in op de rol van artikel 13 van de Wet bescherming persoonsgegevens (Wbp) en geeft antwoord op de vraag hoe specifieke toepassingen van de informatie- en communicatietechnologie ten dienste van de privacybescherming, die bekendstaan onder de naam Privacy Enhancing Technologies (PET), een belangrijke bijdrage kunnen leveren aan de rechtmatige verwerking van persoonsgegevens.

Inleiding

De toepassing van de informatie- en communicatietechnologie (ICT) om informationele privacy te beschermen is wijd en zijd bekend geworden als Privacy Enhancing Technologies (PET). PET wordt gedefinieerd als een samenhangend geheel van ICT-maatregelen dat de persoonlijke levenssfeer (conform de Wbp) beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem. PET heeft inmiddels in de landen met een privacywetgeving een belangrijke plaats ingenomen in het praktische en theoretische repertoire om privacy te beschermen. Vandaar dat het van belang is om hier het licht over PET te laten schijnen en uiteen te zetten welke rol PET verwacht wordt te gaan spelen in het preventief beschermen van privacy.

Basisniveau en beginselen van privacybescherming

Het van kracht geworden zijn van de Wet bescherming persoonsgegevens (Wbp) op 1 september 2001 heeft gevolgen voor alle organisaties. Deze wet heeft betrekking op zowel geautomatiseerde als niet-geautomatiseerde gegevensverwerking. Dit houdt in dat verantwoordelijken[1] voor gegevensverwerkingen ervoor moeten zorgen dat adequate invulling aan de Wbp wordt gegeven. Dit vereist een doelgerichte aanpak van de voorzieningen die in het kader van deze wet moeten worden getroffen. Eerder genomen maatregelen en procedures voor het beheer, de beveiliging en de verwerking zullen wellicht moeten worden heroverwogen en getoetst aan de doelstellingen van de Wbp.
De Wbp schrijft voor de rechtmatige verwerking van persoonsgegevens en het zorgvuldig omgaan met persoonsgegevens een aantal dwingende normen voor. Het gaat globaal om de volgende daarvan afgeleide voorwaarden:

1. *Melden van de verwerking*
   De verwerking van persoonsgegevens moet vooraf worden gemeld bij het College Bescherming Persoonsgegevens (CBP) (de opvolger van de Registratiekamer) of een privacyfunctionaris, tenzij de verwerking daarvan is vrijgesteld[2].
2. *Transparantie van de verwerking*
   De betrokkene moet kunnen overzien door wie en voor welk doel zijn persoonsgegevens worden verwerkt[3].
3. *Doelbinding voor de verwerking*
   Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn[4].
4. *Rechtmatige grondslag voor de verwerking*
   De verwerking van persoonsgegevens moet berusten op een in de Wbp genoemde grondslag, zoals toestemming, overeenkomst, wettelijke plicht en gerechtvaardigd belang. Voor bijzondere gegevens, zoals over gezondheid, gelden striktere normen[5].
5. *Kwaliteit van de gegevens*
   De persoonsgegevens moeten zoveel mogelijk juist en nauwkeurig zijn en toereikend, terzake dienend en niet bovenmatig gelet op de doeleinden waarvoor ze worden verzameld of vervolgens verwerkt[6].
6. *Rechten van de betrokkenen*
   De betrokkenen hebben rechten op kennisneming, verbetering, verwijdering en afscherming van hun gegevens alsmede het recht om bezwaar te maken of verzet aan te tekenen[7].
7. *Beveiliging tegen verlies en onrechtmatige verwerking van persoonsgegevens*
   Passende maatregelen van technische en organisatorische aard vormen het noodzakelijke sluitstuk van een rechtmatige verwerking tegen verlies of enige vorm van onrechtmatige verwerking[8].
8. *Verwerking van persoonsgegevens door een bewerker*
   Als de verwerking wordt uitbesteed aan een bewerker, moet worden verzekerd dat deze zich houdt aan de aanwijzingen van de verantwoordelijke, doorgaans vastgelegd in een overeenkomst of andere rechtshandeling, zodat er een verbintenis ontstaat tussen bewerker en verantwoordelijke[9].
9. *Gegevensverkeer met landen buiten de EU*
   Het verkeer van persoonsgegevens naar een land buiten de EU is in principe alleen toegestaan als dat land een toereikend niveau van bescherming heeft[10].

In het antwoord over de Wbp dat de minister van Justitie aan de Eerste Kamer gaf, wordt gesteld dat de tegenwoordige informatie- en communicatietechnologieën, bekend onder de term Privacy Enhancing Technologies (PET), een belangrijk hulpmiddel kunnen zijn om een behoorlijke en zorgvuldige omgang met persoonsgegevens te waarborgen en de werking van de privacybeginselen te realiseren[11].

De in de Wbp geformuleerde eisen dienen op een doeltreffende manier in de organisatie te worden geïmplementeerd om de informationele privacyrechten van de burger op adequate wijze te ondersteunen. Het is daarom van belang een adequaat stelsel van algemene verwerkingsmaatregelen en -procedures (die op grond van de bewaking van bedrijfsprocessen toch al aanwezig moeten zijn) in samenhang met de specifieke beschermingsmaatregelen voor de verwerking van persoonsgegevens te realiseren[12]. Wil men tot een evenwichtig verwerkingsbeleid voor persoonsgegevens komen en dit implementeren en onderhouden, dan zal dat een belangrijke plaats in de managementcyclus moeten innemen.

Wettelijke basis voor PET

Artikel 17 van de EG Richtlijn 95/46 en het daarop gebaseerde artikel 13 van de Wbp[13] vormen de grondslag van de inzet van Privacy Enhancing Technologies. Artikel 13 luidt:

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.[14]

Dit artikel schrijft dus voor dat de verantwoordelijke voor de verwerking van persoonsgegevens passende technische maatregelen[15] neemt om persoonsgegevens te beveiligen:
- tegen verlies;
- tegen enige vorm van onrechtmatige verwerking.

Bovendien geldt voor persoonsgegevens conform dit artikel dat de maatregelen dienen te voorkomen:
- onnodige verzameling;
- onnodige verdere verwerking.

Deze maatregelen worden gewogen aan de hand van de criteria:
- stand der techniek;
- kosten;
- risico's van zowel de verwerking als de aard en omvang van de gegevens.

Daar waar technische maatregelen niet voldoende of niet haalbaar zijn, kunnen organisatorische maatregelen worden genomen of kunnen organisatorische maatregelen de technische ondersteunen in een samenhangend pakket van maatregelen.

Wanneer als onderdeel van een evenwichtig verwerkingsbeleid de keuze bestaat tussen een organisatorische en een technische voorziening, geeft het CBP de voorkeur aan de laatste. Technische maatregelen zijn doorgaans doeltreffender, omdat het moeilijker is aan het effect ervan te ontkomen.[16]

Technische maatregelen zijn doorgaans doeltreffender, omdat het moeilijker is aan het effect ervan te ontkomen.

Bij de behandeling van de Wbp in de Eerste Kamer antwoordde de minister van Justitie aan de Eerste Kamer *'dat de tegenwoordige informatietechnologische mogelijkheden om persoonsgegevens te misbruiken noodzaken om te zien naar aanvullende mogelijkheden om een behoorlijke en zorgvuldige omgang met persoonsgegevens te waarborgen. Hierbij kan gedacht worden aan gedeeltelijke of algehele anonimisering, bijvoorbeeld door persoonsgegevens te ontdoen van identificerende kenmerken of door ze af te schermen voor bepaalde toepassingen of gebruikers, of het gebruik tot bepaalde doeleinden te beperken.*
In deze lijn is bij amendement 22 van de Tweede Kamer artikel 13 van het wetsvoorstel aangevuld in die zin dat de voorgeschreven beveiligingsmaatregelen er mede op moeten zijn gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Daarmee is de wettelijke basis gegeven voor de toepassing van Privacy Enhancing Technology (PET). Dit soort regels sluit aan bij de zich ontwikkelende informatietechnologie.'[17]

Daar komt bij dat de Tweede Kamer motie nummer 31 van het lid Nicolaï (VVD) heeft aangenomen, waarin de regering wordt opgeroepen in haar eigen informatiesystemen ook dergelijke technologieën toe te passen. Dat de regering deze motie ook daadwerkelijk wil uitvoeren, blijkt uit de Memorie van Toelichting van het Ministerie van Binnenlandse Zaken voor het begrotingsjaar 2001. In het budget voor de uitvoering van de nota 'Contract met de Toekomst' zal jaarlijks een bedrag van 25 miljoen gulden worden uitgetrokken om de rol van de overheid als aanjager en gebruiker van technologische innovatie (met name PET) reële inhoud te geven[18]. Zonder een dergelijke verplichting door de overheid zou een PET-bepaling in de wet weinig kans maken gerealiseerd te worden!

De Registratiekamer heeft in een brief van 13 januari 1999 aan de Tweede Kamer erop gewezen dat *'dit met zich meebrengt dat de verantwoordelijke dan ook passende maatregelen zal moeten nemen tegen het verzamelen, vastleggen en bewaren van persoonsgegevens in strijd met de voorwaarden die daaraan elders in de Wbp worden gesteld. In het bijzonder betekent dit dat het verzamelen en verwerken van persoonsgegevens zonder toereikende grondslag als bedoeld in artikel 8 Wbp zal moeten worden tegengegaan. Artikel 13 Wbp zet de verantwoordelijke ertoe aan de juridische normen van de*

Wbp te vertalen in de feitelijke inrichting van de verwerking van persoonsgegevens en daarmee ook rekening te houden bij het ontwerp en verdere ontwikkeling van informatiesystemen.'

Klassieke beveiligingsmaatregelen niet voldoende

Wanneer organisaties wordt gevraagd welke maatregelen zij hebben getroffen om de privacy te beschermen, wijzen zij er steevast op dat zij zich hebben ingespannen om de persoonsgegevens te beveiligen. Hoewel het gebruik van beveiligingsmaatregelen om ongeautoriseerde toegang tot persoonsgegevens te voorkomen een belangrijke component van privacybescherming is, is een dergelijke beveiliging als zodanig niet toereikend om de privacy adequaat te beschermen. De gegevens over de personen zijn in bijna alle gevallen onversleuteld opgeslagen en de bescherming van de privacy is daarmee afhankelijk van het correct functioneren en uitvoeren van de beveiligingsmaatregelen. Een beter alternatief is een stelsel van technologische maatregelen waarmee de privacy van het individu direct bij het verzamelen wordt afgeschermd. Het gaat dan om technologische maatregelen die ervoor zorgen dat er geen enkel gegeven wordt gegenereerd en vastgelegd of ertoe bijdragen dat het gebruik en de opslag van identificerende gegevens tot een minimum kunnen worden beperkt, of zelfs achterwege kunnen blijven.

Gezien het wettelijk voorgeschreven basisniveau van privacybescherming zal duidelijk zijn dat – wil privacy in technologisch opzicht adequaat beschermd worden – er dus meer moet gebeuren dan alleen maar informatiebeveiliging, namelijk het inzetten van PET. De EG Richtlijn 95/46 en daarop gebaseerde nationale wetgevingen hebben dan ook gevolgen voor systeemontwikkelaars.

Het PET-rapport en de definitie van PET

Internet maakt duidelijk dat de in de negentiende eeuw in een agrarische samenleving ontwikkelde rechtsbeginselen gebaseerd op plaats, tijd en territorium moeilijk zijn te handhaven. Internet en andere internationale computernetwerken trekken zich niets aan van het nationale territorium, terwijl actor, actie en gevolg van deze actie niet meer aan één plaats gebonden zijn[19]. Sterker nog, de actor is vaak niet te achterhalen. Rechtshandhaving, met name voor het strafrecht, kan niet overal en zeker niet snel worden gerealiseerd. Belastinginning binnen *e-commerce* vereist de inzet van nog niet ontwikkelde *intelligent software agents*, die als douaneambtenaar op de elektronische snelweg zouden moeten worden ingezet.
Daar komt nog bij dat de doorbraak van ICT en internet en de mondialisering (globalisering) ervoor zorgen dat er in toenemende mate een discrepantie ontstaat tussen de maatschappelijke, economische en technische levensduur van ICT-producten en -diensten (negen tot twaalf maanden, binnen internet ruim drie tot zeven maanden) enerzijds en wetgevende producten (een nieuwe wet kost gemiddeld tien jaar, te rekenen van de conceptie tot het van kracht worden) anderzijds. De kans neemt daardoor toe dat de wetgever en de rechter in toenemende mate achter de feiten aanhollen.

Het is mijn persoonlijke overtuiging dat het recht alléén niet in staat is de privacy van de burger te beschermen, omdat het recht en de handhaving daarvan met name binnen de virtuele wereld reactief en te langzaam zijn, slechts per geval (vaak het topje van een ijsberg) kunnen worden ingeroepen en binnen de virtuele wereld rechtsinbreuken vrijwel niet te achterhalen zijn. Preventie dient langs andere wegen te worden gerealiseerd door in plaats van voornamelijk achteraf te reageren door rechtsregels ex post toe te passen op situaties die uit de hand zijn gelopen, proactief te worden door onder andere de (technische) aandacht te richten op informatieverwerkende processen met de ambitie om aan het begin van die processen te bewerkstelligen dat van het begin af aan automatisch de privacy van de burger of consument binnen een informatiesysteem gewaarborgd is.

Het inzetten van PET heeft de belofte in zich dat daardoor de snelle ontwikkeling van de ICT kan worden bijgehouden. De vraag is evenwel of de wettelijke vereisten van de Wbp in technische specificaties voor informatiesystemen kunnen worden vertaald, zonder de functionaliteit van het informatiesysteem te beperken. Tijdens transacties is het gebruikelijk dat binnen informatiesystemen de identiteit van het individu via de verschillende verwerkingsprocessen wordt gevolgd.
De restricties die privacywetgeving aan de inrichting van informatiesystemen en de verwerking van persoonsgegevens evenwel kan opleggen, zijn aanzienlijk. Een eenvoudig voorbeeld van een dergelijke restrictie is dat een systeem dat een niet te omzeilen veld 'geboortedatum' bevat, niet is toegestaan als een juridische privacyanalyse van het bedrijfsproces aantoont dat het vastleggen van de geboortedata van alle in dit systeem opgenomen personen excessief is.

In 1994 brak bij de Registratiekamer het inzicht door dat systeemontwerp ervoor kan zorgen dat de gebruikers van informatiesystemen zich houden aan de wet en dat de privacy van de burger goed beschermd kan worden door het aantal identificerende gegevens te verminderen. In augustus 1995 verscheen de op dit inzicht gebaseerde publicatie *Privacy Enhancing Technologies: The Path to Anonymity*, die in nauwe samenwerking met TNO/FEL te Den Haag en de Information and Privacy Commissioner van de Canadese provincie Ontario te Toronto geschreven was.

In het rapport stellen de onderzoekers twee centrale vragen, namelijk:

- Welke voorwaarden moeten in acht worden genomen wanneer een informatiesysteem wordt gebouwd om te bewerkstelligen dat het informatiesysteem effectief en efficiënt kan worden gebruikt zonder de identiteit van de gebruiker, consument of burger te openbaren, en onrechtmatige verwerking van persoonsgegevens te voorkomen?
- Welke vormen van informatie- en communicatietechnologie dragen bij tot het bereiken van dit doel?

De beantwoording van deze vragen leidde tot de kernvraag of identiteit noodzakelijk is voor alle verwerkingsprocessen binnen een informatiesysteem. In het rapport wordt aangetoond dat het vaak niet nodig is de identiteit van de gebruiker, consument of burger te weten. Er zijn evenwel situaties waarin – soms om wettelijke redenen – de identiteit wel bekend moet zijn, bijvoorbeeld bij het betalen voor het gebruik van een bepaalde dienstverlening of bij het openen van een bankrekening.

Om een en ander technisch te realiseren wordt binnen het informatiesysteem gebruikgemaakt van een systeemelement, de 'Identity Protector' of Identiteitsbeschermer genaamd, dat de identiteit van de betrokkene (degene van wie de gegevens worden verwerkt) converteert in één of meer pseudo-identiteiten of volledige anonimiteit.

Door het plaatsen van de identiteitsbeschermer ontstaan twee soorten domeinen binnen het informatiesysteem: één domein waar de identiteit van de betrokkene bekend of toegankelijk is (het identiteitsdomein) en één of meer domeinen waar dit niet het geval is (het pseudo-identiteitsdomein).

Het doel van het pseudo-identiteitsdomein is enerzijds ervoor te zorgen dat de betrokkene niet kan worden getraceerd aan de hand van eerder verkregen persoonsgegevens en anderzijds dat de persoonsgegevens niet kunnen worden gevonden aan de hand van de verkregen identiteit.

In informatiesystemen kan de identiteitsbeschermer op verschillende manieren gestalte krijgen, zoals:
* een aparte functie geïmplementeerd in het informatiesysteem;
* een apart informatiesysteem dat onder toezicht staat van de consument (bijvoorbeeld de smartcard bij biometrische identificatie);
* een informatiesysteem dat onder toezicht staat van een door de dienstverlener en de consument vertrouwde partij (Trusted Third Party of TTP)[20].

Het gebruik van een Identity Protector maakt het dus mogelijk preventief binnen het informatiesysteem in te grijpen in de identificeerbaarheid van de betrokkene. Technieken die hierbij kunnen worden gebruikt, zijn onder meer digitale handtekeningen, blinde digitale handtekeningen, digitale pseudoniemen, MIX-netwerken en Trusted Third Parties.

De conclusies van het rapport *Privacy Enhancing Technologies*, de inmiddels gedurende vijf jaar opgedane ervaringen van de Registratiekamer en de voortgaande research leiden tot de volgende definitie van PET:

Privacy Enhancing Technologies (PET) zijn een samenhangend geheel van ICT-maatregelen dat de persoonlijke levenssfeer (conform de EG Richtlijn 95/46 en Wbp) beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem.

PET-strategieën

Bij het inzetten van PET om de privacy te beschermen kan de verantwoordelijke voor verschillende strategieën kiezen:
1. of hij richt zich op het voorkomen of verminderen van identificeerbaarheid;
2. of hij zet conform de Wbp in op het voorkomen van het onrechtmatig verwerken van persoonsgegevens;
3. of hij gebruikt andere technologieën die de privacybescherming ondersteunen;
4. dan wel hij combineert deze strategieën.

Daarnaast zal de verantwoordelijke vaak ook organisatorische maatregelen nemen.

Voorkomen van identificatie en het criterium van onevenredige inspanning

Wat de eerste strategie betreft het volgende:
PET heeft gevolgen voor persoonsgegevens binnen informatiesystemen. Om dit vast te stellen moet eerst duidelijk zijn wat persoonsgegevens zijn. Onder persoonsgegevens verstaat de wet:
elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Of er sprake is van een persoonsgegeven hangt dus af van een aantal elementen, waarvan in het kader van deze strategie vooral het element 'identificeerbaar' van belang is. Volgens artikel 2 van de EG Richtlijn 95/46 kan een natuurlijk persoon direct of indirect identificeerbaar zijn. Direct identificeerbaar is men aan de hand van NAW-gegevens, een persoonsnummer, een pseudo-identiteit die in brede kring bekend is, een biometrisch kenmerk zoals een vingerscan, enz.
Indirect identificeerbaar is men aan de hand van andere unieke kenmerken of attributen of een combinatie van beide, waaruit voldoende informatie is af te leiden voor de identificatie. Zo kan met behulp van de cd-foongids uit de postcode en het huisnummer de naam van de bewoner van een huis worden achterhaald.

Het gebruik van een Identity Protector maakt het mogelijk preventief binnen het informatiesysteem in te grijpen in de identificeerbaarheid van de betrokkene.

Met PET kunnen de direct identificerende gegevens binnen een informatiesysteem worden geanonimiseerd. Wanneer de gegevens ook van indirect identificerende kenmerken zijn ontdaan, is er sprake van een situatie waarbij geen persoonsgegevens meer aanwezig zijn en de beschermende bepalingen van de Richtlijn en de Wbp niet meer van toepassing zijn.

Niet-identificeerbaarheid wordt ook aangenomen als de hoeveelheid en de aard van de indirect identificerende gegevens dusdanig zijn dat alleen door een onevenredige inspanning tot identificatie van het individu kan worden

gekomen, dan wel dat hiervoor de medewerking van derden buiten de macht en zeggenschap van de verantwoordelijke noodzakelijk is.[21]
Of er sprake is van onevenredige inspanning hangt aan de ene kant af van de aard van de gegevens en de grootte van de populatie, en aan de andere kant van de middelen (tijd en geld) die men bereid is te spenderen om tot identificering te kunnen komen.

Waarborgen tegen onnodige verwerking van persoonsgegevens

PET kan worden toegepast bij het beveiligen tegen de verschillende vormen van onrechtmatige verwerking van persoonsgegevens. Daarmee kan worden voorkomen dat persoonsgegevens onnodig verzameld, vastgelegd, bewaard, in- of extern verstrekt of samengebracht of in verband gebracht (koppelen) worden.

Door het inzetten van PET bij deze vormen van verwerken van identificerende gegevens kan de verantwoordelijke (degene die verantwoordelijk is voor een goed privacybeleid) ervoor kiezen zijn informatiesysteem zo in te richten met identiteits- en pseudo-identiteitsdomeinen, dat minder of geen persoonsgegevens worden verwerkt (bijvoorbeeld bij het verzamelen of vastleggen) en/of dat afhankelijk van de privileges binnen het informatiesysteem aan verschillende gebruikers al dan niet geanonimiseerde gegevens worden verstrekt of *mutatis mutandis* toegang daartoe wordt gegeven. Bijvoorbeeld voor wetenschappelijk onderzoek en statistiek verkrijgt men niet-identificerende gegevens, terwijl in een ziekenhuis op basis van functionele autorisatie en de relatie tussen zorgverlener en patiënt wel identificerende gegevens worden verstrekt.

PET kan bij het toetsen van de verwerking van gegevens aan het privacybeginsel van rechtmatige grondslag voor de gegevensverwerking een belangrijke rol vervullen, namelijk in die gevallen waarin de toets zo uitvalt dat bepaalde gegevens niet verwerkt mogen worden of als er niet meer dan strikt noodzakelijke gegevens verwerkt mogen worden. Als de doelbinding normatief is vastgesteld en PET in het kader van rechtmatige grondslag wordt toegepast, kan PET bovendien als spin-off een bijdrage leveren aan het handhaven van die doelbinding.

Last but not least kan PET uitstekend worden ingezet in het kader van de informatiebeveiliging. Dit is conform de toelichting bij artikel 13 van de Wbp, waarin erop wordt gewezen dat dit artikel zich uitstrekt over alle onderdelen van het proces van gegevensverwerking[22].

Of in redelijkheid mag worden gevergd dat PET wordt ingezet, hangt af van de wegingsfactoren die op de situatie betrekking hebben. De Registratiekamer heeft in een brief van 13 januari 1999 duidelijk gemaakt dat de inzet van deze technische middelen mede afhankelijk is van de maatstaven die artikel 13 Wbp aanlegt. Een passend beveiligingsniveau als bedoeld in artikel 13 zal in steeds meer gevallen, naarmate de doelmatigheid wordt vergroot en de realisering daarvan door PET mogelijk is, zonder inzet van PET niet meer mogelijk zijn.

Voorbeelden van PET

Landelijk Alcohol en Drugs Informatiesysteem (LADIS)

Probleemstelling
In opdracht van de minister van VWS is er een beleidsondersteunend informatiesysteem ontwikkeld voor het bewaken van de hulpverlening in het kader van alcohol- en drugverslaving. Hierbij is het noodzakelijk de behandelgegevens van alle zorgverlenende instellingen op cliëntniveau te verzamelen en vervolgens te aggregeren waarbij de cliënt anoniem wordt gevolgd.

De PET-oplossing
In elk van de deelnemende instellingen wordt aan de hand van de identiteitsgegevens van de cliënt een cliëntcode vastgesteld bestaande uit de eerste drie letters van de familienaam, de geboortedatum en de geslachtscode. Deze code wordt vervolgens met behulp van een 'one-way-hashing' algoritme versleuteld. Aan de zo verkregen code worden de benodigde behandelgegevens toegevoegd. Deze gegevensset wordt verstuurd naar de LADIS-organisatie. Daar wordt de versleutelde cliëntcode nogmaals versleuteld met een vergelijkbaar algoritme. Aan deze uiteindelijke cliëntcode wordt de gegevensset toegevoegd. Hierna worden de behandelgegevens, zoals deze uit de instelling zijn verkregen, vernietigd.

Door de toegepaste techniek van de dubbele versleuteling en vernietiging van eerder verkregen behandelgegevens is het bij de LADIS-organisatie onmogelijk om, zelfs als de identiteit van de cliënt beschikbaar is, de behandelgegevens van deze cliënt te selecteren. Het gebruik van een 'one-way-hashing' algoritme garandeert dat het niet mogelijk is de oorspronkelijke cliëntcode uit de dubbel versleutelde code te verkrijgen.

Aangezien in elk van de instellingen dezelfde versleuteling wordt toegepast, is er wel de garantie dat de gegevens van een cliënt die in meerdere instellingen behandeld werd, in het landelijke systeem worden gekoppeld.

Anoniem elektronisch betalen

Probleemstelling
Bij het betalen met chartaal geld is de anonimiteit van de klant gegarandeerd. Voor het betalen met giraal geld bestaan thans twee systemen. De pinbetaling, waarbij on line wordt gecontroleerd of de klant kredietwaardig is. Anonimiteit hierbij behoort niet tot de mogelijkheden. Bij het betalen met een elektronische beurs (de Chipknip of Chipper) moet dezelfde anonimiteit worden gegarandeerd als bij het betalen met chartaal geld.

De PET-oplossing
Door de banken is hiervoor een systeem ontwikkeld waarbij voor de winkelier de identiteit van de klant onbekend is en blijft, terwijl de betaling voor bank,

winkelier en klant gegarandeerd is. Bij het opwaarderen van de e-beurs wordt op basis van het systeem van een pinbetaling geld van de klant gestort in een speciaal daartoe ingerichte bankrekening, tegelijkertijd wordt het saldo op de Chipknip opgewaardeerd. Bij het betalen met de e-beurs wordt het geld vanaf de speciale bankrekening overgemaakt naar die van de winkelier en de e-beurs wordt gedebiteerd.

Het creëren van verschillende domeinen waarin personen deels bekend en deels anoniem zijn behoort ook tot de mogelijkheden van PET. Uitsluitend geautoriseerde gebruikers zijn in staat gegevens in pseudo-identiteitsdomeinen identificeerbaar te maken. Voorbeelden hiervan zijn Teradata van NCR en anonymizer.com op internet. De eerste praktische implementatie (uit 1997) van de Identity Protector betrof de Privacy Incorporated Database® [23] bij de ziekenhuisinformatiesystemen van ICL/SIAC (thans McKessonHBOC).

Ziekenhuisinformatiesysteem met PET

Probleemstelling
Als reactie op een door de Registratiekamer uitgevoerde privacyaudit werd de leverancier van het gebruikte ziekenhuisinformatiesysteem verzocht de theoretische beschrijving van de Identity Protector in concrete technische maatregelen te vertalen en in ziekenhuisinformatiesystemen (inclusief het elektronisch patiëntendossier).

De PET-oplossing
De gegevens van de patiënten in de database werden gesplitst in twee groepen. De eerste groep omvat de direct tot de patiënt herleidbare gegevens als naam, adres, geboortedatum, verzekering, enz. (identiteitsdomein). In de tweede groep werden alle diagnostische en behandelgegevens verzameld (pseudo-identiteitsdomein).

In beide domeinen worden de patiënten geïdentificeerd door een patiëntnummer, echter deze zijn ongelijk aan elkaar. Dit betekent dat er op het niveau van de database geen relatie kan worden gelegd tussen de gegevens in de twee domeinen. Het resultaat hiervan is dat een gebruiker die niet langs een geautoriseerde weg toegang tot deze database heeft weten te krijgen, geen samenhangende verzameling van gegevens aantreft.

Bij het ontwerpen van de systematiek van de patiëntnummers is in het eerste domein gekozen voor een systeem van volgnummers. Het patiëntnummer in het tweede domein wordt verkregen door encryptie van dit volgnummer. Het gebruikte encryptieprotocol maakt het ook mogelijk het oorspronkelijke patiëntnummer te decrypten. De encryptie/decryptie vindt plaats binnen de toepassingssoftware. Het protocol maakt gebruik van een encryptiesleutel. Deze sleutel wordt pas verstrekt, bij voorkeur door een TTP, nadat de identiteit van de gebruiker van de toepassing is vastgesteld. Voor wetenschappelijk onderzoek worden meerdere pseudodomeinen gemaakt.

Andere privacyondersteunende technologieën

Er zijn vele andere technologieën die kunnen bijdragen tot een betere privacybescherming, wanneer de hiervoor besproken PET-strategieën niet effectief kunnen worden ingezet. Dit is heel duidelijk het geval bij de volgende van de privacybeginselen afgeleide voorwaarden voor de gegevensverwerking:
- transparantie;
- kwaliteit;
- rechten van de betrokkenen;
- beveiliging.

Enkele voorbeelden van het inzetten van technologieën ter bevordering van privacy zijn:
- Transparantie wordt bevorderd door het gebruik van P3P (een technologie om het privacybeleid van websites te toetsen), maar dit hangt met name af van de *default setting*. Deze dient zo te zijn dat niet automatisch alle ingevoerde gegevens worden geopenbaard. Microsoft gaat P3P in versie 6 van de Internet Explorer opnemen. Dit zal ertoe leiden dat bedrijven een privacy policy voor hun website zullen moeten hebben.
- Een statistisch-taalkundige analysetoepassing binnen een adressensysteem kan de juistheid van de gegevens vrijwel honderd procent maken en daarmee de kwaliteit van de gegevens verbeteren.
- De rechten van betrokkenen kunnen beter worden bewaakt door feedback en controle. Deze ontwerpbeginselen zorgen ervoor dat informatiesystemen op elk gewenst moment terugkoppelen naar het individu over datgene wat hij/zij aan persoonsgegevens aan het informatiesysteem heeft afgestaan, met als reactiemogelijkheid de inzage, aanvulling, wijziging en verwijdering van persoonsgegevens.
- Logging (het vastleggen in een elektronisch logboek van handelingen binnen een informatiesysteem) is een uitstekend beveiligingsmiddel. Bij het verzamelen en vastleggen kan de herkomst van de gegevens automatisch worden gelogd. Bij opvraging, raadpleging, wijziging of verstrekking (intern of extern) kan eveneens automatische logging plaatsvinden. Dergelijke loggingen dienen dan uitsluitend door de systeembeheerder te worden verwijderd, waarbij van een dergelijke verwijdering een log wordt gemaakt waarover de verantwoordelijke zich dan zal moeten verantwoorden.
- Voor toegangscontrole geldt hetzelfde. Bij het afschermen, raadplegen, wijzigen, uitwissen en vernietigen van gegevens kan automatische toegangscontrole als beveiligingsmiddel worden ingezet.
- Automatisch wissen van gegevens kan eveneens worden ingezet. Bewaartermijnen kunnen softwarematig worden vastgelegd en bij het verstrijken van de bewaartermijn worden de gegevens automatisch gewist.

Voor de verwerking door een bewerker en het gegevensverkeer buiten de EU kunnen eveneens technische maatregelen worden getroffen teneinde onrechtmatige handelingen in de zin van de Wbp tegen te gaan.

Gestapelde technologieën

Wanneer slechts één van de in de Wbp vastgelegde privacy-basisnormen technologisch wordt nagekomen, is die technologie op zichzelf niet voldoende om optimale privacybescherming te realiseren. Bijvoorbeeld: een statistisch-taalkundige analysetoepassing binnen een adressensysteem kan de juistheid van de gegevens vrijwel honderd procent maken, maar is op zichzelf niet in staat privacybescherming te garanderen.

Het gebruik van een aantal op elkaar gestapelde technische maatregelen tegelijk binnen het informatiesysteem kan wel leiden tot een bevredigende privacyveilige omgeving, mits deze functionaliteit in het informatiesysteem ook daadwerkelijk wordt gebruikt. Bijvoorbeeld door de statistisch-taalkundige analyse te combineren met gespreide opslag, protocollering van de herkomst, het gebruik en de verstrekking van gegevens, logging, enz.

Marktontwikkelingen

In de praktijk blijkt dat inmiddels op veel plaatsen PET-systemen worden ontwikkeld (Research Universiteit van Dresden, ICSI Berkeley-CA, TNO/FEL) of commercieel op de markt worden gebracht, waarbij gebruik wordt gemaakt van een Identity Protector of Identiteitsbeschermer of daarmee vergelijkbare technieken.
Het arsenaal aan PET-middelen binnen de netwerken wordt ook steeds groter, waardoor de niet-identificeerbaarheid van zowel de gebruiker als de aanbieder en de niet-waarneembaarheid van het netwerk, de server, de query, enz. kunnen worden gerealiseerd.

Geschat wordt dat binnen Nederland minder dan één promille van de informatiesystemen op dit ogenblik van PET gebruikmaakt. Het van kracht worden van de Wbp, de uitvoering van de eerder vermelde motie-Nicolaï, de toenemende autonome vraag naar betere beveiliging van informatie en de bescherming van de informationele privacy zullen daarin de komende jaren ongetwijfeld verandering brengen.

De grote kansen voor PET-systemen liggen bij het ontwerpen en implementeren van nieuwe informatiesystemen.

Kansen en grenzen van PET

Naarmate er meer meetbare en kwantificeerbare ervaringscijfers komen waaruit blijkt dat PET efficiency-voordelen tot gevolg heeft voor het gegevensverwerkingsbeleid, bijvoorbeeld door versimpeling van procedures, het afschaffen van maatregelen of het versterken van de beveiligingssituatie, zullen de kansen van PET toenemen.

Het toepassen van PET in oude, reeds lang bestaande informatiesystemen zal doorgaans niet haalbaar zijn. Het 'openknippen' van bestaande informatiesystemen en het daarna toevoegen van een Identity Protector is erg kostbaar omdat door de vele releases en patches de 'spaghetti' vaak niet te ontwarren is.

De grote kansen voor PET-systemen liggen bij het ontwerpen en implementeren van nieuwe informatiesystemen. Daarbij moet rekening worden gehouden met het feit dat het maatschappelijk gezien vaak niet mogelijk zal zijn volledige anonimiteit c.q. niet-identificeerbaarheid toe te passen. Uit ervaringsgegevens blijkt dat als informatiebeveiliging direct bij het ontwerp van het informatiesysteem wordt meegenomen en binnen het security-ontwerp met PET rekening wordt gehouden, de extra kosten beperkt blijven tot ongeveer één procent van de totale bouwkosten van het informatiesysteem.

Informatiesystemen waarbij de verantwoordelijke kiest voor een combinatie van PET-strategieën en andere privacybevorderende technologieën zullen naar verwachting het meest worden toegepast.

Als geen technologische maatregelen toepasbaar zijn

Als objectief gemeten noch PET, noch andere technische maatregelen kunnen worden gerealiseerd, dienen er procedurele (organisatorische) maatregelen te worden ingezet. Hoewel met de huidige ICT-toepassingen theoretisch in elk informatiesysteem ten minste één van de privacybeginselen kan worden verwerkelijkt, is dat soms zo prohibitief kostbaar in verhouding tot het te beschermen belang, dat het invoeren van dergelijke technische maatregelen niet kan worden gevergd.

PET-scan

In het algemeen geldt dat de samenleving als geheel steeds complexer wordt. Daarom ontstaat in toenemende mate behoefte aan snel en eenduidig inzicht in de kwaliteit van producten en diensten. Dergelijke kwaliteitsuitingen worden doorgaans gedaan via een door een deskundige en onafhankelijke derde afgegeven certificaat. Zo'n certificaat kan een belangrijke rol spelen in de beantwoording van de vraag of in een informatiesysteem op adequate wijze PET is toegepast. Om zo'n certificaat af te geven dient er een PET-scan te hebben plaatsgevonden volgens een van tevoren vaststaand certificatieschema. Zo'n certificaat geeft aan dat het betreffende informatiesysteem zodanig is gebouwd, dat met redelijke zekerheid kan worden gesteld dat met behulp van PET de beoogde bescherming van persoonsgegevens plaatsvindt. Op dit moment wordt in samenwerking met onze collega's in Kiel en Toronto door ons gezamenlijk in het PETTEP (Privacy Enhancing Technologies Testing Project) gewerkt aan het ontwikkelen van een testsysteem om PET-toepassingen op hun effectiviteit te meten. Vermoedelijk zullen rond 2003 de eerste resultaten beschikbaar zijn.

De normatieve kant van PET

Het voorgaande brengt met zich mee dat het inbouwen van PET in systemen niet alleen een technische opgave is, maar ook een normatieve. Voordat PET 'inside'[24] informatiesystemen zit, moet duidelijk zijn welke eisen de nationale privacywetgeving aan een informatiesysteem stelt. Technologen en juristen zullen normen moeten vertalen in harde technische systeemspecificaties. Zolang niet duidelijk is aan welke normen verwerkingen in een specifiek geval moeten voldoen, zal de term 'PET-inside' zonder betekenis zijn. Omgekeerd kan door middel van een PET-scan of privacyaudit worden getoetst of systeemeisen en -toepassingen voldoen aan de Wbp. Gebeurt dat niet, dan zal van een effectieve privacybescherming geen sprake kunnen zijn.

Conclusie

De ontwikkelingen in de ICT bieden steeds meer mogelijkheden om gegevens over personen te verzamelen, op te slaan, te bewerken en te verspreiden. De kans op inbreuk op de privacy van de consument en burger neemt hierdoor toe. Diezelfde ICT biedt echter ook oplossingen om de bescherming van de privacy van de gebruiker, consument en burger vorm te geven. PET is een uitstekend en veelbelovend hulpmiddel om met name de privacy-basisnorm 'rechtmatige grondslag voor gegevensverwerking' te realiseren. Uiteraard blijven aandacht en research noodzakelijk en zullen er voortdurend inspanningen moeten worden verricht om PET-toepassingen in informatiesystemen te stimuleren, zoals thans in het door de Europese Unie gesubsidieerde Privacy Incorporated Software Agent (PISA)[25] -project gebeurt. Bovendien zal via privacyauditing of specifieke PET-scans moeten worden gecontroleerd of met PET uitgeruste systemen werkelijk voldoen aan de Wbp. Certificering in het kader van een privacyaudit kan hieraan bijdragen en de noodzakelijke zekerheid bieden aan de burger en consument wat betreft zijn of haar privacybescherming binnen e-commerce en e-government.

Noten

1) Hier wordt ex art. 1d Wbp onder verstaan: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Ex art. 14 Wbp geldt bij verwerking van persoonsgegevens door een bewerker dat deze zelfstandig kan worden aangesproken op zijn wettelijke verplichtingen. Zie voor toelichting: *Privacy in Bedrijf*, AWVN, FME-CWM, VNO-NCW, Den Haag, 2000, blz. 10.
2) Zie art. 24, 27 t/m 32 en 43 Wbp.
3) Zie art. 33, 34, 41, 43, 44 Wbp.
4) Zie art. 7, 9, 10 Wbp.
5) Zie art. 6, 8, 16 t/m 23 Wbp.
6) Zie art. 6, 10, 11 Wbp.
7) Zie art. 5, 35 t/m 42 Wbp.
8) Zie art. 6, 12, 13 Wbp.
9) Zie art. 14 Wbp
10) Zie art. 76 en 77 Wbp.
11) Zie Memorie van Antwoord Eerste Kamer betreffende de Wbp no. 25 892 # 92c, Jaar 1999-2000, blz. 16.
12) Zo zal privacybescherming in de regel een aanvullend stelsel van maatregelen en procedures zijn boven op de normaliter al vereiste verwerkings- en beveiligingsmaatregelen.
13) In art. 17 van de richtlijn 95/46/EC staat dat datacontrollers, 'appropriate technical and organisational measures' dienen te nemen 'to protect personal data, especially in network transmissions'. Overweging 46 stelt uitdrukkelijk dat dergelijke maatregelen moeten worden genomen 'both at the time of the design of the processing system and at the time of the processing itself'. In de Duitse wetgeving is in §3 Abs. 4 van het Teledienstedatenschutzgesetz en in §12 Abs. 5 van het Mediendienste-Staatsvertrag een specifieke bepaling opgenomen die aanspoort tot gegevensreductie en gegevensvermindering. Zie voor meer informatie: L. Gundermann, *Das Teledienstedatenschutzgesetz – ein virtuelles Gesetz*, in: H. Bäumler (Hrsg.), E-Privacy, Datenschutz im Internet, Braunschweig/Wiesbaden, 2000, blz. 58-68. In de federale privacywet van Duitsland, de BDSG, is in art. 3 eveneens een dataverminderings- en vermijdingsbepaling opgenomen.
14) Bij de behandeling in de Tweede Kamer is door middel van amendement 22 van de Tweede-Kamerleden Scheltema-De Nie en Wagenaar de laatste zin van art. 13 van de Wbp toegevoegd.
15) PET biedt niet alleen de mogelijkheid passende technische maatregelen te nemen, maar ook een structurele oplossing voor het juist toepassen van de Wbp.
16) Zie Advies Beveiliging Persoonsgegevens van de Registratiekamer, Den Haag 1994, blz. 11.
17) Zie Memorie van Antwoord Eerste Kamer betreffende de Wbp, blz. 16.
18) Zie Kamerstukken 27400 VII, no. 2 en Kamerstukken 26 643, 26 387 no. 15 Jaar 2000-2001.
19) W. Derksen, *Hoe de Nationale Staat Blijft, Tegen de ICT-Verdrukking In*, in: K. Versteegh, Rijksdienst 21, Hersenkrakers voor het Openbaar Bestuur in de Nieuwe Eeuw, Alphen aan den Rijn 1999, blz. 16-17.
20) Er zijn TTP-diensten voor enerzijds authenticiteit en integriteit en anderzijds vertrouwelijkheid. Zie J.A.G. Versmissen, *Sleutels van vertrouwen, TTP, digitale certificaten en privacy – de juridische randvoorwaarden verkend*, Achtergrondstudies en Verkenningen no. 22, Den Haag, maart 2001.
21) Overweging 26 van de EG Richtlijn 95/46.
22) Een aantal van de thans bekende en gerealiseerde PET's kan worden beschouwd als maatregelen die buiten een privacybeschermende werking ook een werking hebben op algemene informatiebeveiliging. Het toepassen van PET leidt derhalve tot een 'Privacy Enhanced Corporate Security'.
23) Het patent van de Privacy Incorporated Database® staat op naam van ICL.
24) De term is 'geleend' van de reclame: Intel Inside.
25) J.J. Borking, *Privacy Incorporated Software Agent (PISA): Proposal for Building a Privacy Guardian for the Electronic Age*, in: H. Federrath (Ed.), Designing Privacy Enhancing Technologies, Design Issues in Anonymity and Unobservability, Berlin 2001, blz. 130-140.

Drs. J.J. Borking
is vice-voorzitter van het College Bescherming Persoonsgegevens (CBP).