Privacyrecht is Code

Over het gebruik van Privacy Enhancing Technologies

Πανταπασι δη, ην δ’ εγω, οι τοιουτοι ουκ αν αλλο τι νομιζοιεν το
αλη ε ητα των σκευαστων σκια .

In alle opzichten, zei ik, zullen zulke mensen wel niets anders als de werkelijkheid
beschouwen dan de schaduwen van de voorwerpen.

Plato – Politeia : 515 c

PRIVACYRECHT IS CODE

Over het gebruik van privacy enhancing technologies

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van de rector magnificus prof. mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 9 juni 2010
klokke 15:00 uur

door

Johannes Josephus Franciscus Maria Borking

geboren te Breda in 1945

Promotiecommissie

Promotor: prof. mr. H. Franken

Overige leden:

prof. dr. H.J. van den Herik (Universiteit Leiden en Universiteit van Tilburg)

prof. mr. A.H.J. Schmidt

prof. dr. J.B.F. Mulder (Universiteit van Antwerpen, België)

prof. mr. J.M.A. Berkvens (Radboud Universiteit Nijmegen)

prof. mr. J.E.J. Prins (Universiteit van Tilburg)

dr. mr. C.N.J. de Vey Mestdagh (Rijksuniversiteit Groningen)

Voorwoord

Door mijn werk als bedrijfsjurist bij Rank Xerox kwam ik vanaf 1974 in aanraking met geavanceerde ict-toepassingen waarover de onderzoekers van Xerox PARC in Palo Alto (CA) juridische vragen stelden. De antwoorden daarop waren van invloed op het in productie nemen van de ontworpen machines en informatiesystemen. Om echter relevante juridische kanttekeningen te kunnen plaatsen was kennis van informatica vereist. Kennis die ik niet bezat en die ik mij zo snel mogelijk eigen moest maken om met de Xerox-onderzoekers te kunnen communiceren. De informaticakennis kwam mij vervolgens goed van pas toen in 1984 de discussie over de bescherming van computerprogrammatuur losbarstte en later weer toen ik medebestuurder werd van de Registratiekamer en haar opvolgster het College bescherming persoonsgegevens.

Dit boek bestrijkt een periode van vijftien jaar onderzoek naar de inzet van ict om de privacy van de burger en zijn persoonsgegevens te beschermen en daardoor het vertrouwen in de correcte verwerking van zijn persoonsgegevens te vergroten. Vanaf het begin ben ik actief betrokken geweest bij dit onderzoek. In eerste instantie richtte het onderzoek zich op het voorkomen van privacyinbreuken door middel van anonimisering en pseudonimisering. Later breidde het onderzoek zich uit naar het toepassen van technieken om informatiesystemen zo in te richten, dat verwerking van persoonsgegevens uitsluitend conform de wet- en regelgeving en/of het privacybeleid van de organisatie kon plaatsvinden.

De titel van dit proefschrift, 'Privacyrecht is code', is geïnspireerd door Lessigs stelling 'code is law'. Hij schrijft in zijn boek *Code and Other Laws of Cyberspace*:

"In real space, we recognize how laws regulate through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different code regulates- how the software and hardware (i.e. the 'code' of cyberspace) that make cyberspace what it is regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's law".

'Code is Law' is een onwenselijke en ondemocratische ontwikkeling. Vanuit een democratisch perspectief zou het wenselijk zijn dat ook het omgekeerde het geval is en dat 'Law is Code' geldt. Het woord Code verwijst naar de subtitel 'Over het gebruik van privacy enhancing technologies' (PET). Met PET, een informatietechnologie toepassing, kunnen de rechtsbeginselen met betrekking tot de gegevensbescherming in de programmacode of zelfs in objectcode (machinetaal)

worden geïntegreerd in informatiesystemen. PET kan voorkomen dat ‘code is law’ werkelijk bestaat.

Om de burger c.q. consument en zijn informationele privacy goed te kunnen beschermen is PET van belang. PET worden ondanks hun privacy beschermende mogelijkheden slechts op zeer beperkte schaal toegepast. Ik bleef me maar afvragen waarom PET niet massaal in informatiesystemen worden ingebouwd, terwijl het aantal privacyincidenten hand over hand toeneemt. Het is belangrijk de redenen hiervoor te achterhalen, omdat met dit inzicht PET effectiever kunnen worden ingezet.

Zonder de veelvuldige en intensieve discussies met onderzoekers van het EU Joint Research Center in Ispra, de National Research Council Canada (Conseil national de recherches Canada) in Ottawa, TNO in Delft, Den Haag en Rijswijk, IBM in Zürich en HP in Bristol, zou ik de toepassingen om de privacy te beschermen die ik in dit boek bespreek, niet op papier hebben gezet. Ik dank al deze mensen zeer voor hun herhaalde uitleg van uiteenlopende theorieën en ideeën. Professor Piet Ribbers en Alea Fairchild van de Universiteit van Tilburg en de Vrije Universiteit van Brussel dank ik voor hun stimulerende enthousiasme en ideeën tijdens het economisch onderzoek naar de motieven van bedrijven om privacybeschermende maatregelen toe te passen. In het bijzonder bedank ik Frank van Vliet voor het kritisch lezen van de informatica inhoud en Peter van Schelven voor zijn juridische opmerkingen. De belangrijkste rol bij de totstandkoming van dit boek heeft echter mijn promotor Hans Franken gespeeld. Als hij niet herhaaldelijk bij mij erop had aangedrongen dit boek te schrijven, dan was het er nooit van gekomen.

Ik bedank mijn vrouw Pauline voor haar liefde, geduld en steun bij het schrijven van dit boek.

Wassenaar, 1 december 2009

Inhoudsopgave

Lijst van gebruikte afkortingen

A

ALE:	Annual Loss Expectancy
AMI:	Ambient Intelligence
APPEL:	A P3P Preference Exchange Language
AOL:	America Online
APEC:	Asia-Pacific Economic Cooperation
APK:	Algemene Periodieke Keuring
APS:	Agent Practices Statement
ARO:	Annual Rate of Occurrence

B

B2B:	Business to Business;
B2C:	Business to Consumers
BSI:	British Standards Institute
BSN:	Burger Service Nummer

C

CBP:	College bescherming persoonsgegevens
C.CR:	Wet Computercriminaliteit
CCTV:	Closed Circuit Television
CEN:	Comité Européen de Normalisation
CEO:	Chief Executive Officer
CFO:	Chief Financial Officer
CMMi:	Capability Maturity Model
CNIL:	Commission nationale de l'Informatique et des Libertés
COBIT:	Control Objectives for Information and related Technology
COM:	Commission (European-)
CRM:	Customer relation Management
CSCW:	Computer Supported Cooperative Work
CVA:	Cerebro Vasculair Accident
CWA:	CEN Workshop Agreement

D

DC:	Digital Cash
DDoS:	Distributed Denial of Service
DIN:	Deutsches Institut für Normung
DOI:	Diffusion of Innovation
DNS:	Domain Name System
DPA:	Data Protection Authority
DPD:	Directive on the Protection of Individuals with regard to the Processing of Personal data and on the Free Movement of such Data 95/46/EC
DPEC:	Directive on Privacy and Electronic Communications 2002/58/EC
DS:	Data Subject
DSL:	Digital Subscriber Line

E

EEA:	European Economic Area
ECHR:	European Convention for the Protection of Human Rights and Fundamental Freedoms
EC:	European Community
ECJ:	European Court of Justice
EDP:	Electronic Data Processing
EDPS:	European Data Protection Supervisor
EKD:	Elektronisch Kind Dossier
EPAL:	Enterprise Privacy Authorization Language.
EPML:	Event-Driven Process Chain Markup Language
EPTA:	European Parliamentary Technology Assessment
ERA:	Expected Revenue Accrual
EU:	European Union
ETSI:	European Telecommunications Standards Institute
EU:	Europese Unie
EVRM:	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden

F

FBI:	Federal Bureau of Investigation
FTC:	Federal Trade Commission
FIPA:	Foundation for Intelligent Physical Agents

G

GBA:	Gemeentelijke basisadministratie
GAEA:	Government of Alberta Enterprise Architecture
GIS:	Geographic Information Systems

GPS:	Global Positioning Systems
GSM:	Global System for Mobile communications
H	
HCI:	Human Computer Interfaces
HIV:	Human Immunodeficiency Virus
HLT:	human language technology
HMS:	Home Media Spaces
HRM:	Human Resources Management
HTTP:	Hypertext Transfer Protocol
HTTPS:	Hypertext Transfer Protocol Secure
I	
IAM:	Identity and Access Management
ICC:	International Chamber of Commerce
ICIF:	International Contactless Technologies Forum
ict:	Informatie en Communicatietechnologie
ID:	Identiteits Domein
IDP:	Identity Protector
IEC:	International Electrotechnical Commission
IEEE:	Institute of Electrical and Electronics Engineers
IET:	Information Extraction Technology
IRR:	Internal Rate of Return
IM:	Identity Management
IMS:	Identiteitsbeheer (Management) Systeem
IMEI:	International Mobile Equipment Identity
IMSI:	International Mobile Subscriber Identity
INK:	Instituut Nederlandse Kwaliteit
IP:	Internet Protocol
IPSE:	Initiative for Privacy Standardization in Europe
I-RIS:	Internet Registratie systeem
I.S.:	Informatie Systeem
ISA:	Intelligente Software Agent
ISACA:	Information Systems Audit and Control Association
ISO:	International Organization for Standardization
ISP:	Internet Service Provider
ISS:	Information Society Service
ITGI:	IT Governance Institute
ITIL	(Information Technology Infrastructure Library)
ITSEC:	Information Technology Security Evaluation Criteria

J

JITCA:	Just-In-Time-Click-Through Agreements
JTC:	Joint Technical Committee (ISO)

K

KDD:	Knowledge Discovery in Databases

L

LNS:	Local Name Server

M

MAS:	Multi Agent System
MvT:	Memorie van toelichting

N

NFC:	Near Field Communication
NGO:	Non-Governmental Organization
NIC:	Network Interface Card/Controller
NMI:	Nederlands Mediation Instituut
NPV:	Net Present Value
NTIS:	Nederlands Trauma Informatie Systeem

O

OECD:	Organization for Economic Co-operation and Development
OM:	Openbaar ministerie
OMS:	Obligation Management System
OV:	Ov-chipkaart, betaalmiddel voor het openbaar vervoer
OWL:	Web Ontology Language

P

P2P:	Peer to Peer (netwerk)
P3P:	Platform for Privacy Preferences
P4P:	Personalization for Privacy
PBA:	Privacybedreigingsanalyse
PBRS:	Patiënt Barcode Registratie Systeem
PC:	Personal Computer
PDA:	Personal Digital Assistant
PDT:	Privacy Diagnostic Tool
PET:	Privacy-Enhancing Technologies (ook wel afgekort als PETs)
PIA:	Privacy impact analyse

PID:	Pseudo Identiteits Domein
PII:	Personal Identifiable Information
PIM:	Privacy & Identity Management
PISA:	Privacy Incorporated Software Agent
PMS:	Privacy Management Systeem
PNR:	Passenger Name Record, is een record in het bestand van een Computerreserveringssysteem (CRS)
PRIME:	Privacy and Identity Management for Europe, EU research project Contract No. 507591(2004-2008)
PRITAC:	Privacy Technology Assessment Committee
PRIVIS:	Privacy- Veilig Informatiesysteem

R

RAPID:	Roadmap for Advanced Research in Privacy and Identity Management EU research project, Project Nummer: IST-2001-38310,
RPC:	Recurring Privacy Costs
RRC:	Reputation Recoverage Costs
RDF:	Resource Description Framework
RDFS:	Subclass of RDF
RDBMS:	Relationele Database Management Systeem
RDQL:	RDF Data Query Language
RFID:	Radiofrequentie-identificatiechip
RFG:	Regionaal Geneeskundig Functionaris
RGK:	Registratiekamer
ROI:	Return On Investment
ROIPI:	Return On Investment of Privacy Investments
ROSI:	Return On Security Investment

S

SAML:	Security Assertion Markup Language
SC 27/WG 5:	Sub Committee 27/ Workgroup 5 (ISO)
SCT:	Social Cognitive Theory
SEPA:	Single Euro Payments Area
SIM:	Subscriber Identity Module
SLE:	Single Loss Exposure
SPAN:	Spanning time Ontology
SNAP:	Snapshot Ontology
SOX:	Sarbanes-Oxley Act
SRA:	Amerikaanse Society of Risk Analysis
SWAMI:	Safeguards in a World of Ambient Intelligence
SWAPPEL:	Semantic Web APPEL

SWIFT:	Society for Worldwide Interbank Financial Telecommunication
SWOT:	Strengths, Weaknesses, Opportunities, and Threats
T	
TAM:	Technological Acceptance Model
TCP:	Transmission Control Protocol
TIPHON:	Telecommunications and Internet Protocol Harmonization over Networks
TNO:	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek
TTP:	Trusted Third Party
TISPAN:	Telecoms & Internet coverged Services & Protocols for Advanced Networks
TRA:	Theory of Reasoned Action
U	
UICN:	Uniek Identificerend Ongeval Nummer
USP:	Unique Selling Point
USVISIT:	United States Visitor and Immigrant Status Indicator Technology
UTAUT:	Unified Theory of Acceptance and Use of Technology
UTIS:	Utrechts Trauma Informatie Systeem
V	
ViTTS:	Victim Tracking and Tracing System
VoIP:	Voice over Internet Protocol
W	
W3C:	World Wide Web-Consortium
Wbp:	Wet bescherming persoonsgegevens
WP29:	Article 29 Data Protection Working Party
WSTL:	Web Services Trust Language
Z	
ZBO:	Zelfstandige Bestuursorgaan

1. Inleiding en probleemstelling

"[Our aim] is to encourage the application of scientific methods to the study of the legal system. As biology is to living organisms, astronomy to the stars, or economics to the price system, so should legal studies be to the legal system."
R. Posner, 'An Afterword', *Journal of Legal Studies* (1972) Vol. 1, p. 437.

In 1854 stierven in Londen in één week meer dan 500 mensen aan cholera binnen een straal van 250 meter rond het kruispunt Cambridge Street en Broad Street. Niemand begreep hoe en waarom deze vreselijke infectie zich verspreidde. John Snow, een 41 jaar oude huisarts, meende dat hij de bron van de besmetting gevonden had. Door de adressen van de overleden cholerapatiënten op de plattegrond van Londen aan te kruisen, ontdekte hij dat bijna alle slachtoffers rond de waterpomp van Broad Street woonden. Snow vroeg de plaatselijke overheid de pomp van zijn zwengel te ontdoen, hetgeen gebeurde. Binnen een paar dagen was de cholera-epidemie voorbij.[1] Het zou echter nog tientallen jaren duren voordat medici erachter kwamen hoe zij cholera-epidemieën effectief en structureel konden bestrijden. Vandaag de dag komt de ziekte praktisch niet meer voor in de westerse wereld. Dit is te danken aan de aanleg van riolen, kwaliteitscontrole van het water door het waterleidingbedrijf, preventieve vaccinatie en de bewustwording van het belang van hygiëne met name tijdens de opvoeding van kinderen.

Is er een parallel te trekken tussen de aanpak van cholerabestrijding en de preventie en bestrijding van privacyinbreuken? Als we de metafoor doortrekken en privacyinbreuken als een akelige ziekte beschouwen die de grondrechten ondermijnt en daardoor het individu en de samenleving aantast, dan zijn er twee manieren waarop we deze ziekte zouden kunnen aanpakken. Wanneer de arts (de behandelaar van de klacht over een privacyinbreuk bij het College bescherming persoonsgegevens (CBP)) de ziekteverschijnselen (de privacyinbreuk) via klachten van de patiënt (de burger) constateert, kan hij geneesmiddelen voorschrijven (relevante bepalingen in de wet of uit de jurisprudentie toepassen). De ziekte (de privacyinbreuk) die al schade aan de patiënt (de burger) heeft toegebracht kan dan bij die specifieke patiënt verdwijnen, maar steekt mogelijk elders weer de kop op. De inmiddels uitgebreide jurisprudentie van de Registratiekamer en haar opvolger

1 Jaret, 1991, p. 116-140.

het CBP over de toepassing en interpretatie van de Wet Persoonsregistraties en haar opvolger de Wet bescherming persoonsgegevens kan in dit geval vergeleken worden met een receptenboek of een handboek met 999 ziektebeelden.[2] Door nieuwe rechtsregels en nieuwe interpretaties van die rechtsregels kan de patiënt (de burger) steeds beter geholpen worden. Om de ziekte echt uit te roeien en te bestrijden, moeten wij structurele en preventieve maatregelen nemen (bijvoorbeeld vaccins ontwikkelen).

1.1. Omgevingsanalyse

De samenleving staat niet stil. Dagelijks voltrekken zich allerlei demografische, economische, sociale, technologische, politieke of juridische gebeurtenissen. Onze maatschappelijke omgeving verandert snel en leidt tot nieuwe vraagstukken. De omgevingsanalyse in dit hoofdstuk brengt negen factoren in kaart die van invloed zijn op de privacybescherming. De omgevingsanalyse wordt hier gemaakt om tot een probleemstelling en een zestal onderzoeksvragen te komen.[3]

1.1.1. Toenemende gegevensverwerking

In postindustriële landen, zoals de Verenigde Staten, Canada, Australië en Japan en de landen van de Europese Unie, zijn informatie- en communicatiesysteemtoepassingen in gebruik die op een steeds verfijndere manier gegevens over personen verzamelen, opslaan, uitwisselen, (her)gebruiken, identificeren en monitoren. Voorbeelden hiervan, naast het internet, zijn videocameratoezicht, chipkaarten, radiofrequentie-identificatiechips (RFIDs) en dienstverlening gebaseerd op het lokaliseren van gebruikers van mobiele telefoons.[4] Bovendien verschijnen geavanceerde ict-toepassingen op de markt die een veelvoud aan 'real time'-gegevens van gebruikers doorgeven aan omringende communicatiesystemen, interactieve digitale televisie en zelfs aan genetische identificatiesystemen, die via internet met elkaar in verbinding staan. Het internet is inmiddels een informatie-infrastructuur die onze hele planeet omspant en bestaat uit wereldwijd vertakte netwerken met daarin miljarden gegevensverwerkende systemen. Onafhankelijk van plaats en tijd verbindt het internet gebruikers met andere partijen waar de gebruikers vaak niet meer over weten dan de IP-adressen[5] en de beschikbare informatie op webpagina's.

---

2 Crouwers-Verbrugge, Van Eck & Schreuders, 1997.
3 Borking & Vriethoff, 1995, p. 32.
4 Banisar, 2006, p. 21-31.
5 Een IP-adres, waarin IP staat voor Internet Protocol, is een adres waarmee een NIC (*network interface card* of *controller*), of in het Nederlands 'netwerkkaart', van een host op het internet eenduidig geadresseerd kan worden binnen het TCP/IP-model (de standaard van 'het' internet).

1.1.2. Aanjagers

Het zijn vooral commerciële belangen en verbeterde openbare dienstverlening die ervoor zorgen dat persoonsgegevens in toenemende mate worden vergaard en bewerkt. Dankzij de informatie- en communicatietechnologie (ict) kunnen zowel organisaties als particuliere personen vrijwel onbeperkt tegen betaalbare kosten gedragingen van burgers in profielen vastleggen en grondig analyseren. Steeds meer informatiesystemen zijn in staat om onafhankelijk van het besturingssysteem via internet of andere netwerken verbindingen met databases te leggen en automatisch en onbelemmerd (persoons)gegevens uit te wisselen. Het gebruik van geavanceerde analyse- en marketinggereedschappen, zoals *data warehousing* en *data mining*, voor het in kaart brengen van het gedrag van internetgebruikers neemt snel toe.[6] Hiermee is het mogelijk om vaak, zonder dat de internetgebruiker zich daarvan bewust is, steeds betere psychogrammen (profielen die psychisch gedrag zichtbaar maken) van de consument en burger te maken. Reid concludeert:

> "Too much information about too many people is being collected and exchanged simply because it is technically possible to do so. Some business models seem to depend on amassing information about consumers to be resold to third parties when the focus should be on best practices and best technologies that can protect privacy and build trust".[7]

1.1.3. Risico van identiteitsdiefstal

Hoe meer persoonlijke informatie beschikbaar is, des te groter wordt het risico van identiteitsdiefstal[8] door kwaadwillige personen, die persoonsgegevens van burgers zonder hun toestemming zich toe-eigenen en gebruiken.[9] De malafide gebruiker kan met de gestolen informatie de indruk wekken dat hij de persoon is van wie hij de informatie heeft gestolen en vervolgens kan hij de gestolen persoonsgegevens voor fraude en andere onwettige activiteiten gebruiken. Door verlies of diefstal van een mobiele telefoon, een personal digital assistant (PDA) of een laptopcomputer neemt het gevaar van identiteitsdiefstal aanmerkelijk toe.[10]

1.1.4. Toezichtsamenleving

In de discussie over privacybescherming is ook het beschermen van de nationale veiligheid een steeds belangrijkere factor geworden. Het cliché dat '9/11' de

---

6 Borking, Artz & Van Almelo, 1998.
7 Reid, 2000.
8 Nationale ombudsman rapportnummer: 2008/232 21 oktober 2008. Door fraude met zijn identiteit stond een man (R. Kowsoleea) dertien jaar onterecht geregistreerd als harddrugscrimineel in informatiesystemen van de overheid.
9 Van Schijndel, 2007, p. 31-33.
10 Friedewald, Vildjiounaite & Wright, 2006, p. 127.

wereld heeft veranderd, is met name waar als het gaat om het verzamelen, analyseren, verwerken en bewaren van persoonsgegevens bestemd voor de wetshandhavers. Door de communicatiemiddelen te gebruiken die voorhanden zijn, kunnen verkeersgegevens gecombineerd met persoonsgegevens ongemerkt doorgegeven en verwerkt worden voor zowel marketingdoeleinden als opsporingsanalyse aan respectievelijk de bedrijven en de politie.

De Britse Information Commissioner (de zusterorganisatie van het CBP die toeziet op de naleving van de privacybescherming) wijst er in 'A Report on the Surveillance Society' op dat de publieke en private sfeer inmiddels op veel manieren worden bewaakt.[11] Videocamera's registreren de burger te pas en te onpas; camera's herkennen nummerborden en gezichten automatisch, elektronische enkelbanden controleren of veroordeelden in hun proeftijd zich aan de regels voor reclassering houden; zonder legitimatie kan de burger geen uitkeringen of gezondheidszorg krijgen; in de chip van het paspoort zijn biometrische identiteitskenmerken opgenomen gekoppeld aan een databank met persoonsgegevens; als de burger buiten het Schengengebied[12] reist, controleert de grenspolitie zijn identiteit en als hij naar de Verenigde Staten reist niet alleen zijn reisbestemming, verblijfsadres, eetgewoonten en godsdienst maar ook nog veertig andere kenmerken.[13] Inlichtingendiensten kunnen bovendien telefoons aftappen en e-mailcorrespondentie of internetgebruik screenen op verdachte sleutelwoorden en ideeën. Overheid en bedrijfsleven hebben een doelbewuste, routinematige, systematische en doelgerichte interesse in onze persoonsgegevens. Zij controleren en beheren deze gegevens om hun doelstellingen te realiseren. De burger ontkomt er niet aan. Rechtshandhavers en nationale veiligheidsdiensten oefenen grote druk uit op de wetgever om communicatiegegevens te onderscheppen of om toegang tot verkeersgegevens te krijgen zonder dat zij iemand in het bijzonder verdenken.[14]

De Amerikaanse wetgeving verplicht de Society for Worldwide Interbank Financial Telecommunication (SWIFT) de verwerkte bankgegevens van Europese burgers door te geven aan de inlichtingendiensten (CIA en FBI) van de Verenigde Staten.[15] In 2007 hebben de EU-landen een nadere overeenkomst met de Verenigde Staten gesloten, waardoor het is toegestaan bankgegevens van Europese burgers in het kader van terrorismebestrijding in de VS te bekijken en

11 Ball, e.a., 2006.

12 Het Schengengebied bestaat uit de landen België, Denemarken, Duitsland, Finland, Frankrijk, Griekenland, Italië, IJsland, Luxemburg, Nederland, Noorwegen, Oostenrijk, Portugal, Spanje en Zweden. Vanaf 21 december 2007: Estland, Letland, Litouwen, Malta, Hongarije, Polen, Tsjechië, Slowakije en Slovenië. Vanaf 12 december 2008: Zwitserland.

13 ECJ 30 mei 2006 zaken C-317/04 en C-318/04; BNC-fiche 22112, 317, 4 (BNC staat voor Beoordeling Nieuwe Commissie voorstellen door de Nederlandse regering).

14 Diffie & Landau, 2008, p. 33-39.

15 European Data Protection Supervisor betreffende SWIFT, Brussel 2007: www.edps.europa.eu/EDPSWEB/edps/site/mySite/op/edit/lang/en/pid/38. www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/25. Détraigne & Escoffier, 2009 p. 94.

maximaal vijf jaar te bewaren. Het White paper van het PRIME-consortium[16] wijst erop dat deze vorm van gegevensverzameling op zichzelf in het licht van haar doelstelling niet in strijd hoeft te zijn met de wet. Bij gebrek aan voldoende controle door de toezichthouders voor de bescherming van de persoonlijke levenssfeer kan dit echter leiden tot gevaren voor onze democratie. Dit is het geval wanneer er professionele 'verblinding' (*function creep*) optreedt, er te weinig openheid is over wat er met de verzamelde persoonsgegevens precies gebeurt en er steeds meer gegevens worden verzameld.

1.1.5. Profilering

Binnen de wereld van de beveiliging zijn gegevensprofielen niets bijzonders, maar wat er met die profielen gebeurt, onttrekt zich aan onze waarneming. Hoe nobel de intenties ook mogen zijn, wanneer de Staat ongebreidelde gegevens verzamelt ter bescherming van de nationale veiligheid kan dit leiden tot niet-gerechtvaardigde en uiteindelijk niet rechtens toelaatbare 'zwarte lijsten'. Dit gebeurt overigens niet alleen in totalitaire regimes, maar ook in vrije democratische samenlevingen. Zo is bijvoorbeeld bekend dat de Amerikaanse senator Ted Kennedy op de 'no-fly list' stond en meerdere malen in de Verenigde Staten de toegang tot het vliegtuig om onduidelijke redenen is geweigerd.[17] Dit is slechts het topje van de ijsberg.

1.1.6. Steeds meer privacyproblemen

Door allerlei nieuwe technische ontwikkelingen, bijvoorbeeld 'cloud computing', neemt de aandacht voor de bescherming van de persoonlijke levenssfeer toe. Deskundigen geven steeds meer adviezen over het beschermen van de privacy bij het gebruik van ict-systemen, maar burgers of consumenten laten zich nauwelijks horen. Daardoor blijft hun mening onderbelicht. Soms worden er wel privacy-vragen gesteld bij de introductie van ict-toepassingen die mensen verplichten een computer, mobiele telefoon of smart card te gebruiken om toegang te kunnen krijgen tot openbare dienstverlening of gezondheidszorg.[18] Lips & Nouwt merken op dat:

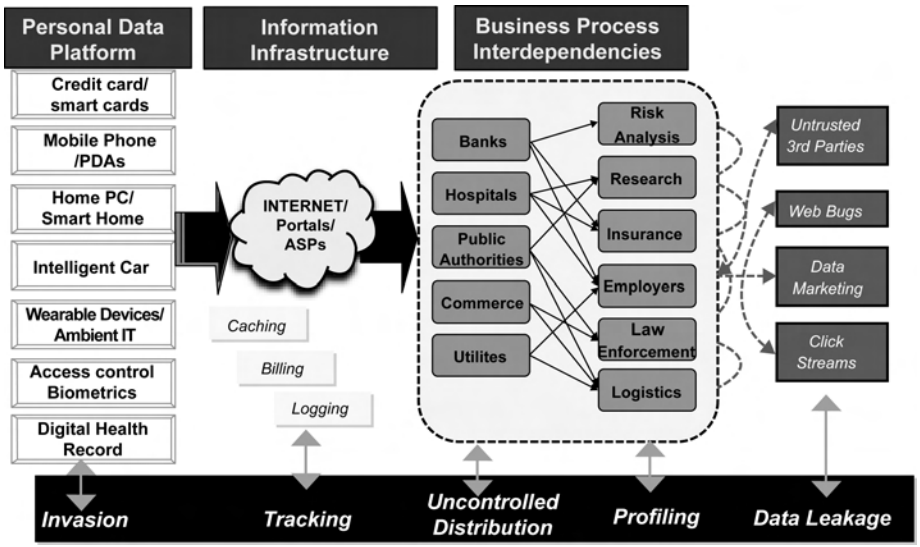
> "a distinction can be made between younger and older people. Usually, older people tend to be much more concerned about their privacy, as they are not familiar with (using) the technology, in contrast to younger people. Younger people seem to know better what to expect and which conditions to look for in making use of new technologies. In general, besides age, other

16 PRIME 2005, p. 3, EU research project PRIME (Privacy and Identity Management in Europe) project Contract No. 507591(2004-2008).
17 Kehaulari Goo, 2004, p. A01.
18 Lips, e.a., 2003, p. 4.

sociological variables like gender, race, education, and income, may indicate differences in the privacy experience of people regarding ict-applications as well".[19]

Onderstaand figuur 1.1 geeft aan dat er binnen onze moderne samenleving geen gebied meer bestaat waar zich geen privacyproblemen voordoen. Figuur 1.1 bevat vier horizontale kolommen. De eerste betreft de toepassingen waar persoonsgegevens worden verwerkt en waar inbreuken in de privacysfeer kunnen plaatsvinden. De tweede kolom betreft de infrastructuur waar langs persoonsgegevens worden verspreid (publieke en private netwerken, internet). Binnen deze infrastructuur wordt het mogelijk persoonsgegevens en de daarbij behorende personen te volgen. De derde kolom gaat over de bedrijfsprocessen waar de gegevens worden verwerkt en geeft de onderlinge verbanden tussen de bedrijfsprocessen aan waardoor het gevaar van ongecontroleerde distributie van persoonsgegevens en profilering ontstaat. De vierde kolom maakt de mogelijkheden van het lekken van gegevens zichtbaar onder andere via click streams en web bugs. Deze problemen worden ook nog eens versterkt door de veelvoudige opslag van dezelfde gegevens.[20]

Figuur 1.1: Potentiële privacy problemen, EU Research Project RAPID 2002.[21]



19 Lips, e.a., 2003, p. 4-5.
20 De Consumentenbond rapporteerde in 2001 al dat van de gemiddelde Nederlander op ongeveer 900 plaatsen in naar schatting 70.000 bestanden digitale gegevens zijn geregistreerd.
21 Project Titel: RAPID – Roadmap for Advanced Research in Privacy and Identity Management Brussels 2001-2002, Project Nummer: IST-2001-38310.

Privacykwesties kunnen de gemoederen danig te verhitten. Dyson schrijft: "Privacy is a public Rorschach test: say the word aloud, and you can start any number of passionate discussions. One person worries about governmental abuse of power; another blushes about his drug use and sexual history; a third vents outrage about how corporations collect private data to target their ads or how insurance companies dig through personal medical records to deny coverage to certain people."[22]

Ook in Nederland blijven wij niet achter. In 2007 speelde de kwestie over de invoering van het Burger Service Nummer (BSN).[23] Het BSN is een algemeen persoonsnummer dat als uniek identificerend gegeven dient voor personen in overheids- en bedrijfsadministraties. De invoering ervan riep weerstand op omdat de privacyrisico's niet voldoende zouden zijn afgedekt.[24] Maar ook bij de voorgenomen landelijke invoering van het elektronisch patiëntendossier,[25] de ov-chipkaart, de bodyscans op Schiphol of de kilometerheffing zorgt de bescherming van persoonsgegevens voor veel commotie.[26]

1.1.7. Vertrouwen

Het is de intentie om de dienstverlening aan de burger en consument in de nabije toekomst nog sneller en efficiënter te laten zijn. De op de individuele consument gerichte commerciële marketing (de zgn. een-op-eenmarketing) van goederen en diensten en de 'éénloketgedachte' van de landelijke, provinciale en gemeentelijke overheden kan echter alleen maar succesvol zijn als er een hoge graad van vertrouwen bestaat tussen de overheid en de aanbieders van commerciële diensten enerzijds en de burger en consumenten anderzijds. Vertrouwen zorgt ervoor dat mensen kunnen communiceren en samenwerken en steunt in onze tastbare wereld dikwijls op non-verbale lichaamstaal. In de virtuele wereld ontbreken echter zulke 'tastbare' signalen. Dit houdt in dat als wij op het internet surfen, wij geen terugkoppeling krijgen om ons gedrag aan te passen. Zonder terugkoppeling kunnen wij gedrag vertonen waaruit mogelijk kwetsbare informatie over ons is af te leiden.

Détraigne en Escoffier rapporteren dat informatiesystemen wantrouwen oproepen vanwege hun ondoorzichtigheid:

> "(…) en matière de nouvelles technologies, nous nous trouvons souvent dans la situation de Joseph K., le héro du Procès de F. Kafka, qui se retrouve un jour au centre d'un procès sans savoir qui sont ses accusateurs, quel est l'objet de la plainte ni quelles sont les charges retenues contre

22 Dyson, 2008, p. 26.
23 Mom, 2007, p. 8-11.
24 CBP 2005, advies Z 2005-1198; Advies Z 2005-0807.
25 Meer dan 500.000 Nederlanders maakten bezwaar tegen het elektronische patiëntendossier (2008).
26 Jacobs, 2009: "OV Card uses Mifare Classic chip, with proprietary weak crypto (48 bits); Completely broken in 2008; This Card is an 'open wallet' without data protection".

> lui: l'opacité des systèmes d'information conduit ainsi à une méfiance générale des individus, qu'accompagne une tendance générale au conformisme et au mimétisme social".[27]

Ondernemingen erkennen dat vooral bij het elektronisch zakendoen vertrouwen een onontbeerlijk element is. Elektronisch zakendoen biedt duidelijke voordelen ten opzichte van ouderwets zakendoen waar partijen fysiek aanwezig zijn. Zo is het niet aan plaats en tijd gebonden, is het sneller en biedt het veel grotere keuzemogelijkheden. Toch zijn gebruikers vaak omzichtig omdat zij de gevolgen van gegevensinzameling door ondernemingen niet kunnen overzien. Het is bijvoorbeeld bekend dat veel EU-burgers bang zijn om hun creditcard voor online transacties te gebruiken, niet zozeer vanwege persoonlijk ondervonden problemen, als wel vanwege berichtgeving in de media over misbruik van creditcardgegevens. Zelfs al zijn burgers echter wel op hun hoede bij creditcardtransacties, dan nog beseffen zij niet (precies) weten wat er met hun online verstrekte persoonsgegevens kan gebeuren.

In onze informatiemaatschappij is vertrouwen de kritische succesfactor voor de groei van de economie.[28] Om een digitale interactie en transactie aan te gaan moet er voldoende vertrouwen zijn. Vertrouwen is een relationele eigenschap en is geen meetbare systeemeigenschap. In de digitale wereld hangt vertrouwen van veel zaken af. Zo is het belangrijk van tevoren in te schatten of derden waarmee gecommuniceerd en handel gedreven wordt betrouwbaar zijn. Een dergelijke inschatting hangt af van de reputatie die partijen hebben en van de aanbevelingen die betrouwbare derden (bijvoorbeeld banken) geven over de partijen waarmee zij communiceren en handel drijven. Bovendien is het voor het vertrouwen belangrijk dat het individu te allen tijde weet wat het informatiesysteem doet met de verwerking, verspreiding en het gebruik van de gegevens die hij heeft verstrekt. Dit vertrouwen kan toenemen als derden controles uitvoeren (door bijvoorbeeld electronic dataprocessing (EDP) accountants) en dergelijke controles openbaar maken. Evenzeer belangrijk voor dit vertrouwen zijn de eigenschappen en de robuustheid van het informatiesysteem, het verwerkingsproces, de toegepaste applicaties, de betrouwbaarheid van de privacybedreigingsanalyses en de toegepaste beveiliging. Wanneer geaccrediteerde derden certificaten verstrekken die de privacyveiligheid van het systeem garanderen, zoals EuroPrise bijvoorbeeld doet[29], komt dat de transparantie ten goede. Daarmee krijgen betrokkenen ook meer vertrouwen in het desbetreffende systeem of proces dat hun gegevens verwerkt.[30]

---

27 Détraigne & Escoffier, 2009, p. 67.

28 De kredietcrisis die in de zomer van 2007 was ontstaan door *subprime* hypotheken is daar een sprekend bewijs van. Er was overigens niet uitsluitend sprake van een *krediet*crisis in de zin van een beperkte beschikbaarheid van liquiditeiten en (langer lopend) kapitaal, doch op een aantal momenten ook van een algehele vertrouwenscrisis in de financiële sector.

29 Het EU gesubsidieerde EuroPrise research project begon op 10 juni 2007 en is 28 februari 2009 geëindigd. www.european-privacy-seal.eu/about-europrise/fact-sheet.

30 Van Rooy & Bus, 2009, p. 1.

Wetten die de persoonsgegevens beschermen spelen eveneens een uiterst belangrijke rol bij het hebben en behouden van vertrouwen in het elektronisch verkeer. De rechtsorde kan daardoor worden gehandhaafd c.q. afgedwongen en burgers en consumenten kunnen mogelijke schade verhalen en conflicten beslechten.

1.1.8. Risicobewustzijn

Zoals hiervoor al aangegeven, zijn burgers zich nauwelijks bewust van de vele privacyrisico's, laat staan dat zij weten hoe deze risico's te voorkomen zijn.[31] Dit gebrek aan inzicht in de registerende, waarnemende, tracerende en 'etiket opplakkende' mogelijkheden van systemen geldt niet alleen voor internetgebruik, maar ook voor andere ict-toepassingen, zoals bijvoorbeeld videotoezicht en 'contactloze' chipkaarttechnologie. De burger realiseert zich niet welke gegevens deze soms 'verborgen' ict-toepassingen kunnen verzamelen en uitwisselen. Daar komt nog bij dat het voor iemand zonder specifieke kennis vrijwel onmogelijk is om na te gaan welke informatie over hem wanneer, waarom en waar is opgeslagen. Zonder duidelijke visuele of auditieve waarschuwing kan hij niet weten of hij heimelijk door de overheid of het bedrijfsleven in de gaten wordt gehouden, bijvoorbeeld via 'cookies' en elektronische spionnen op zijn harde schijf. Ook merkt hij het niet wanneer organisaties interactieve middelen inzetten om psychografische gegevens over hem te verzamelen.

1.1.9. Ambient Intelligence

De komst van Ambient Intelligence (AMI) omgevingen, die voor de aanwezigheid van mensen gevoelig en ontvankelijk zijn, ook wel aangeduid als 'ubiquitous computing environment', brengt een geheel nieuwe situatie met zich mee. Onze persoonlijke ruimte (een onzichtbaar veld dat ieder mens omringt en voelbaar wordt als andere mensen te dichtbij komen) staat steeds meer onder druk door indringende technologieën.[32] In de nabije toekomst zal de mens zowel in zijn privéruimte (huis, kantoor) als in de publieke ruimte omgeven zijn met en drager zijn van zeer kleine sensoren met een 'ingebouwde' intelligentie (geavanceerde RFIDs) die volledig geïntegreerd ('embedded') zijn in zijn leefomgeving. Dergelijke sensoren zouden bijvoorbeeld in een 'smartphone' kunnen worden ingebouwd. Deze sensoren die aan ict-netwerken gekoppeld zijn en in de toekomst nanomicroscopisch klein zullen zijn, zullen voortdurend van de drager en zijn omgeving gegevens verzamelen en verspreiden.

Een van de kenmerken van AMI is dat het de gebruiker en zijn gedragingen 'leert kennen', zichzelf 'leert aan te passen' aan de wensen en behoeften van de gebruiker en contextgevoelig is. Deze sensoren zullen binnen tien jaar in aantal

---

31 www.pewinternet.org.
32 Van den Berg, 2008, p. 49-54.

exponentieel toenemen.[33] Albrecht citeert Lin, vice-president van het bedrijf China Public Security Technology, die RFIDs beschrijft als "a way for government to control the population in the future".[34]

Het ziet ernaar uit dat er rond 2020 een life recorder[35] (een draagbare RFID of implanteerbare chip) beschikbaar zal zijn die alles vastlegt wat een mens via zijn lichaam in zijn leven meemaakt,[36] terwijl tegelijkertijd persoonsgegevens via ontelbare netwerken aan elkaar zullen zijn gekoppeld. Nu al zijn voor alle cellen die zich in ons lichaam bevinden IP-adressen gereserveerd, waardoor intelligente machines de cellen straks afzonderlijk kunnen aanspreken. In 'the Internet of Things' zouden de verschillende privacylagen (fysiek, ruimtelijk en informationeel) hierdoor ineen kunnen storten.[37]

Persoonsgegevens van gebruikers die door AMI-sensoren zijn geregistreerd kunnen onbeperkt aan meer apparaten worden doorgegeven dan gebruikers zelf weten en wensen. Het is echter nog volkomen onduidelijk hoe wij deze stroom van persoonsgegevens moeten beveiligen tegen privacyinbreuken. Vooral de mogelijkheden om het individu ongewild te profileren en zijn persoonsgegevens te onderscheppen is zorgelijk.

1.1.10. Resultaten van de omgevingsanalyse

Ofschoon de ict onze moderne samenleving zonder twijfel vele voordelen heeft gebracht, blijkt dat burgers zich steeds meer zorgen maken dat de overheid en het bedrijfsleven hun persoonsgegevens zouden kunnen misbruiken. De verwerking, verspreiding en opslag van persoonsgegevens neemt sterk toe. De ontwikkeling van onze gedigitaliseerde samenleving maakt heimelijk toezicht mogelijk. Identiteitsdiefstal neemt wereldwijd epidemische vormen aan. Het vertrouwen van de burger wordt steeds meer op de proef gesteld. Volgens de Eurobarometer[38] van 17 april 2009, maken in de Europese Unie (EU) steeds meer mensen zich zorgen om hun privacy. 82% van de Europese internet gebruikers hebben weinig vertrouwen in het beschermen van persoonsgegevens op het Web en 68% twijfelen aan de bescherming van persoonsgegevens binnen de EU. Het inzicht en risicobewustzijn van de burgers in de privacy bedreigingen blijkt laag te zijn. De voor de deur staande AMI omgeving zal zonder adequate technische privacybescherming leiden tot een veelvuldig ongewenste binnendringing in de persoonlijke ruimte en de privacybescherming volledig kunnen ondermijnen.

---

33 Wayt Gibbs, 2005, p. 26.
34 Albrecht, 2008, p. 51.
35 Picard, 2006: Interview met B. Schneier: "A 'life recorder' is a reasonable thing to carry? That's something that you'll wear on your lapel that'll audio-record everything that happens to you. That's probably only five or six years away. Nobody will mug you because you have your life recorder as evidence."
36 Tot welke levensbedreigende situaties een life recorder kan leiden, is te zien in de film *Final Cut* (2004).
37 Kerr, 2007, p. 4.
38 http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

1.2. Probleemstelling en zes onderzoeksvragen

De titel van dit proefschrift 'Privacyrecht is code' is geïnspireerd door Lessigs stelling 'Code is Law'. Hij schrijft in zijn boek *Code and Other Laws of Cyberspace*:

> "In real space, we recognize how laws regulate-through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different code regulates- how the software and hardware (i.e. the 'code' of cyberspace) that make cyberspace what it is regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's 'law'."[39]

Franken schrijft daarover:

> "De programmeur staat nog dichter bij de individuele netburger. Hij stelt technische protocollen en netwerkarchitecturen vast. Hij bepaalt daarmee de weg waarlangs je kan lopen en de manier waarop deuren worden geopend of gesloten blijven. Sterker nog: hij/zij bepaalt daarmee wat wel of niet mogelijk is, of beter gezegd: wat wel of niet *mag* en *moet*."[40]

Schmidt ziet terecht een ernstige bedreiging in het reguleren van het gedrag van mensen met behulp van informatiesystemen:

> "want dan is het immers wenselijk dat die systemen zodanig in elkaar zijn gezet dat de regels die zij verwezenlijken gelegitimeerd zijn. Dat is niet makkelijk vast te stellen voor een eenvoudige ingenieur (…) voor het normeren van menselijk gedrag via informatiesystemen is juridische kennis nodig. En dat houdt weer in dat er juristen beschikbaar moeten zijn om *legitieme* normatieve modellen te maken die door informatici kunnen worden vertaald naar informatiesystemen".[41]

'Code is Law' is een onwenselijke en ondemocratische ontwikkeling. Hoe dwingend in de praktijk de objectcode voor de gebruikers van informatiesystemen ook is, objectcode kan niet gelijk gesteld worden met het Recht. Objectcode is en mag niet het equivalent van een juridische norm zijn. Het Recht komt tot stand als gevolg van het van kracht worden van wetgeving, gewoonte of door middel van jurisprudentie en niet door dat een systeemontwerper bepaalde programmacode, al dan niet 'hardwired' in een informatiesysteem implementeert.[42] Vanuit een democratisch perspectief zou het dan ook wenselijk zijn dat het omgekeerde het geval is en 'Law is code' geldt.[43] Het woord 'is' in 'Law is code' moet niet absoluut worden gezien, maar als een 'hulpwerkwoord' dat verwijst naar de

---

39 Lessig, 1999, p. 6; Reidenberg, 1998, p. 553-593 omschrijft "'Code is Law' als de 'Lex Informatica'".
40 Franken, 2001, p. 7.
41 Schmidt, 2004, p. 15-16.
42 Koelewijn, 2009, p. 204-205.
43 Lessig, 1999, (A) p. 546: "We must make a choice about life in cyberspace. (…) The code of cyberspace (…) can be made to constitute values that resonate with our tradition."

mogelijkheid om bij de bescherming van onze privacy van informatie en communicatietechnologie gebruik te maken.

De doelstelling van dit onderzoek is na te gaan of het technologisch haalbaar is, onder meer door toepassing van privacy enhancing technologies (PET), om de rechtsbeginselen met betrekking tot de gegevensbescherming in het ontwerp van de architectuur van informatiesystemen op te nemen en zo bij de verwerking van persoonsgegevens die rechtsbeginselen in de programmacode of zelfs in object-code (machinetaal) te integreren.

De bescherming van persoonsgegevens wordt geregeld in een aantal wetten, die ik hier met de verzamelnaam 'privacywetgeving' aanduid. De Europese Unie heeft in een reeks Richtlijnen vastgelegd hoe persoonsgegevens van burgers online en offline moeten worden beschermd.

Uit de resultaten van de omgevingsanalyse in 1.1.10 blijkt onder meer dat burgers en consumenten zich er zorgen over maken dat de overheid en het bedrijfsleven hun persoonlijke informatie mogelijk misbruiken. Zij zijn niet in staat na te gaan wat er met hun persoonsgegevens gebeurt en aan wie die worden verstrekt. Het ligt voor de hand dat zij controle willen hebben en houden over het gebruik van hun persoonsgegevens. Het is echter in de praktijk voor burgers en consumenten zeer moeilijk gebleken om hun rechten op het gebied van de bescherming van persoonsgegevens te handhaven. Daardoor neemt hun vertrouwen in de verwerking van hun persoonsgegevens door de overheid en het bedrijfsleven af.

Het CBP heeft dan ook in 2007 gemeend dat het noodzakelijk was een koerswijziging in gang te zetten om de naleving van privacy als collectief belang krachtiger af te dwingen.

Kohnstamm, de huidige voorzitter van het CPB, verwoordde het als volgt: "De bescherming van de persoonlijke levenssfeer overstijgt het belang van het individu, van gezin of samenlevingsverband. Die bescherming dient uiteindelijk bovenal de samenleving als geheel. De grenzen die de wetgever niet voor niets heeft getrokken, dienen dan ook daadwerkelijk gerespecteerd te worden. De prioriteit van de toezichthouder is verlegd naar het doen van onderzoek en handhavend optreden bij ernstige overtredingen met een structureel karakter en grote gevolgen voor vele burgers of groepen van burgers."[44]

Tijdens een door de Europese Commissie georganiseerde Data Protection Conference in mei 2009 verduidelijkte hij dat: "DPAs need to be selective in order to be effective: thus shift focus from ex ante to ex post".[45] Om evenwel de bescherming van persoonsgegevens niet tot een papieren tijger te laten verworden en burgers controle over de verwerking van hun persoonsgegevens te laten behouden, is het echter noodzakelijk de rechtsregels met adequate technologische

44 CBP, 2007, p. 6,11.
45 Kohnstamm, 2009, p. 5.

maatregelen ex ante te ondersteunen. De toepassing van Privacy Enhancing Technologies (PET) is zo'n ex-ante maatregel. In principe kan dezelfde ict-technologie die voor gegevensverwerking wordt gebruikt ook voor gegevensbescherming worden ingezet. De EU-commissie schreef in haar eerste evaluatierapport over de werking van de persoonsgegevens beschermende Richtlijn 95/46/EC dat "(…) the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection (…)".[46]

Krisch verdedigde tijdens de eerder genoemde Data Protection Conference dat het noodzaak is "to improve possibilities for individual data(self) protection".[47] Informatietechnologie kan daarbij van dienst zijn. Door de intensieve koppeling van geautomatiseerde gegevensverwerking en telecommunicatie zijn de privacy van persoonsgegevens en die van persoonlijke communicatie steeds meer met elkaar verbonden geraakt. Deze twee vormen van privacy tezamen wordt aangeduid met 'informationele privacy'. In dit boek gaat het om deze informationele privacy. Dit onderzoek houdt zich dus niet bezig met de lichamelijke privacy in relatie tot bijvoorbeeld bloed- en DNA-testen of verplichte sterilisatie, noch met de privacy die het persoonlijk gedrag betreft, bijvoorbeeld seksuele geaardheid.

De probleemstelling in dit proefschrift is:

> *"Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker?"*[48]

Deze probleemstelling impliceert dat de huidige wet- en regelgeving op het gebied van de bescherming van persoonsgegevens door informatiesystemen kan worden ondersteund en gehandhaafd. Om de vereiste privacybescherming in de programma code in te kunnen bouwen, zijn voorafgaand aan de ontwerpfase privacybedreiginganalyses en risicoanalyses noodzakelijk, waarbij niet alleen een beveiligingstechnische maar ook een juridische afweging plaatsvindt.[49]

De probleemstelling leidt tot zes onderzoeksvragen (OV):

OV 1: Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacywet- en regelgeving worden afgeleid?

---

46 COM, 2003, 265.
47 Krisch, 2009, p. 8.
48 De definitie van het begrip verantwoordelijke en bewerker wordt gegeven in Wbp artikel 1, onder d respectievelijk e, en wordt in hoofdstuk 2.7 en 2.5.11 behandeld.
49 Schmidt, 2004, p. 15-16.

De basis beginselen voor de bescherming van persoonlijke informatie zijn uitgewerkt in privacyrealisatiebeginselen. De beginselen hebben tot doel de mogelijkheid voor het individu te scheppen om controle te hebben en te houden over zijn persoonsgegevens ongeacht de technologische omgeving. De privacy-realisatiebeginselen liggen aan de basis van de Europese wet- en regelgeving. Ontwerpers van informatiesystemen dienen hiermee rekening te houden. Met uitzondering van de Richtlijn 2006/24/EG zijn de bepalingen in de Europese Richtlijnen 95/46/EG en 2002/58/EG in de wetgeving van alle EU-lidstaten getransponeerd. De Data Retentie Richtlijn 2006/24/EG zal bij transpositie in het nationale recht van de lidstaten consequenties inhouden voor de architectuur van informatiesystemen. Nationaal recht van de EU-lidstaten zal in dit onderzoek niet worden geanalyseerd, te meer daar de informatie- en communicatietechnologie zich onafhankelijk van nationale wettelijke stelsels ontwikkelt en wereldwijd kan worden toegepast.

OV 2: Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding?

Dankzij de technologische vooruitgang kan de overheid surveillancemiddelen inzetten die veel verder reiken dan het afluisteren van telefoongesprekken. Sinds '9/11' is deze ontwikkeling onmiskenbaar gaande. De overheid en rechtshandhavers krijgen steeds meer bevoegdheden voor de rechtshandhaving en zetten steeds vaker geavanceerde ict-systemen in die ertoe kunnen leiden dat de privacybescherming erodeert. De burger kan zich daartegen niet adequaat verweren. Als het intensieve toezicht van de overheid en bedrijfsleven tot erosie van onze privacy leidt, kan dezelfde ict technologie, die surveillance mogelijk maakt, ook ingezet worden als remedie tegen disproportioneel toezicht?

OV 3: Met welke privacybedreigingen en privacyrisico's moeten de burger en de ontwerper van systemen rekening houden?

Uit de omgevingsanalyse blijkt dat burgers en consumenten nauwelijks op de hoogte zijn van de risico's die zij lopen als zij hun persoonsgegevens voor verwerking verstrekken. Om een zorgvuldig en behoorlijk gebruik van persoonsgegevens te garanderen, is het noodzakelijk om de privacybedreiging of privacyrisico's te analyseren. De aanpak hiervan dient zo te zijn dat een juiste interpretatie van rechtsregels ertoe leidt dat de bouwers van informatiesystemen de noodzakelijke maatregelen kunnen implementeren die de gesignaleerde privacyrisico's moeten voorkomen. Er zijn nochtans geen gestandaardiseerde methoden voor het uitvoeren van privacybedreiging – en privacyrisicoanalyses voor informatiesystemen. De uitkomst van de analyses moet leiden tot adequate maatregelen om de bedreigingen en risico's te beperken.

OV 4: Wat houdt het concept Privacy Enhancing Technologies (PET) in?

Als in de hierboven vermelde analyses privacyrisico's en – bedreigingen worden geconstateerd, dan moeten hiervoor structurele oplossingen worden gevonden. Organisatorische oplossingen blijken doorgaans niet afdoende te zijn en nopen tot een (aanvullende) technische oplossing om de informationele privacy te beschermen. Veel technologische oplossingen beveiligen wel gegevens maar zorgen er tegelijkertijd voor dat het individu minder te zeggen heeft over het gebruik van zijn persoonsgegevens. Om preventief privacy te beschermen dient in de architectuur van informatiesystemen voorzieningen te worden getroffen. PET kan hiervoor mogelijk een oplossing bieden. Bij de beantwoording van deze onderzoeksvraag komen ook encryptie, anonimisering, 'rule-based' privacy- managementsystemen en persoonsgegevensbeschermende ontologieën aan de orde.

OV 5: Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen?

De resultaten die voortvloeien uit de beantwoording van onderzoeksvragen 3 en 4 over de privacybedreigingen en privacyrisico's en over *Privacy Enhancing Technologies* kunnen worden toegepast in het ontwerp van informatiesystemen. Bovendien wordt onderzocht of door de resultaten van onderzoeksvraag 1 op privacyveilige architecturen en privacyveilige systemen toe te passen, de rechtsbeginselen die zijn vastgelegd in de EG-richtlijnen 95/46/EG, 2002/58/EG en 2006/24/EG over de bescherming en het opslaan van persoonsgegevens kunnen worden gemigreerd naar objectcode.[50] Daartoe zullen vier informatiesystemen, waarvan door de eigenaars wordt beweerd dat zij privacyveilig zijn, worden onderzocht.

OV 6: Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?

Reacties en commentaren van belanghebbenden op privacygevoelige identiteitsrijke projecten zoals bijvoorbeeld het elektronische patiëntendossier, de ov-chipkaart, het opnemen van biometrische kenmerken in paspoorten, geven aan dat de overheid en het bedrijfsleven in haar gegevensverwerking PET niet structureel toepast. Zij vertrouwen eerder op klassieke organisatorische en technische informatiebeveiligingsmaatregelen. Het blijkt moeilijk organisaties te overtuigen hun bedrijfsprocessen zo in te richten dat persoonsgegevens worden getransformeerd tot gegevens waaruit de identiteit niet direct herleidbaar is en identificerende gegevens worden losgekoppeld van overige persoonsgegevens.

---

50 Objectcode of een objectbestand is in de informatica een mogelijke representatie die een compiler (een computerprogramma dat een invoer vertaalt in een bepaalde uitvoer) heeft gegenereerd na het vertalen van een broncode bestand (de broncode (ook wel brontekst) van een computerprogramma is de code die door de programmeur in een formele programmeertaal is geschreven).

1.3. Onderzoeksmethode

Om de onderzoeksvragen te beantwoorden zal het onderzoek op verschillende manieren worden uitgevoerd:

1. Vanuit het vakgebied van de rechtsgeleerdheid, informatica en economie zullen geanalyseerd worden: a de literatuur op het gebied van de bescherming van persoonsgegevens en privacy; b de conceptuele modellen op het gebied van beveiliging, PET, architectuur en c de adoptie van innovatieve technologieën.
2. Als onderzoeksmethode zullen er verschillende casestudies, zoals onder meer beschreven door Yin,[51] worden uitgevoerd over privacyveilige systemen en de organisatorische en economische hindernissen en de belemmeringen om op grote schaal PET te implementeren.
3. Door middel van interviews met experts uit de verschillende disciplines zullen de bevindingen uit de casestudies worden getoetst aan conceptuele modellen. De interviews zullen worden uitgevoerd conform de *Chatham House Rule.* Deze regel bepaalt hoe moet worden omgegaan met de vertrouwelijkheid van de bron van informatie die tijdens een interview of vergadering wordt verkregen.[52] Sommige interviews zullen worden opgenomen op audiotapes en vervolgens in een transcript worden uitgewerkt. Het protocol van de vragen die tijdens de interviews zijn gesteld, staat achter de lijst van aanbevelingen achter in dit boek.

1.4. Leeswijzer

De hierboven in hoofdstuk 1 geformuleerde probleemstelling en zes onderzoeksvragen zullen in dit boek als volgt behandeld worden. In hoofdstuk 2 komt onderzoeksvraag 1 aan de orde en worden de begrippen ‘privacy’, ‘persoonlijke ruimte’ en ‘identiteit’ kort verkend. Daarna volgt een beschrijving van het positieve recht, de in de EG-richtlijnen vastgelegde beginselen die van toepassing zijn op de bescherming van persoonsgegevens. De Data Retentie Richtlijn 2006/24/EG wordt eveneens in hoofdstuk 2 behandeld. In hoofdstuk 3 wordt onderzoeksvraag 2 behandeld en komt de toezichtsamenleving aan de orde. Hierbij worden de maatschappelijke ontwikkelingen en technologieën geanalyseerd die de overheid en het bedrijfsleven inzetten om terrorisme, misdaad en fraude te bestrijden.

---

51 Yin, 2003. Een casestudie kan gezien worden als een empirisch onderzoek waarin een bepaald verschijnsel wordt bestudeerd dat gelijktijdig met het onderzoek in haar eigen omgeving beschouwd kan worden.

52 De regel luidt: “When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.” www.chathamhouse.org.uk/about/chathamhouserule/.

Nadat de juridische omgeving in kaart is gebracht, wordt in hoofdstuk 4 een antwoord op onderzoeksvraag 3 gegeven. Verschillende vormen van de privacy-bedreigingsanalyse, impactanalyse en risicoanalyse komen aan de orde. Daarmee worden de bedreigingen en risico's voor het individu en de gegevensverwerkende organisaties duidelijk. De resultaten van dergelijke analyses kunnen voor bouwers van informatiesystemen als input dienen bij het ontwerp van architecturen. Hierin kunnen zij technologieën en maatregelen implementeren die 1 de gesignaleerde privacyrisico's en –bedreigingen moeten voorkomen en 2 het vertrouwen van de burger en consument in informatiesystemen, waaraan zij hun persoonsgegevens hebben toevertrouwd, vergroten. Hoofdstuk 5 beantwoordt de vierde onderzoeks-vraag. Dit hoofdstuk verkent de inhoud en reikwijdte van het concept 'privacy enhancing technologies' (PET), gaat na hoe PET kan bijdragen aan de bescher-ming van persoonsgegevens in informatiesystemen, welke rol er is weggelegd voor de 'Identity Protector' en langs welke weg de privacyrealisatiebeginselen in programmacode kunnen worden omgezet. In dit hoofdstuk komen de gereed-schappen om persoonsgegevens te beschermen aan de orde, zoals encryptie,'rule-based'-privacymanagementsystemen en privacyontologieën. Hoofdstuk 6 behan-delt onderzoeksvraag 5 aan de hand van vier modellen van privacyveilige informatiesystemen die met succes gerealiseerd zijn in verschillende sectoren van de samenleving. Hoofdstuk 7 beantwoordt de zesde onderzoeksvraag en gaat na waarom PET nauwelijks wordt toegepast. Organisatorische en economische belemmeringen bij de adoptie van PET zullen worden geanalyseerd, onder meer aan de hand van casestudies. Uit onderzoek is gebleken dat het toepassen van PET in informatiesystemen een economische rechtvaardiging vereist. In dit hoofdstuk zullen een aantal financiële formules worden toegelicht, die meer inzicht kunnen geven in de financiële haalbaarheid van de PET-investering. Slotbeschouwingen in hoofdstuk 8 sluiten deze studie af. Dit hoofdstuk resulteert in een antwoord op de in hoofdstuk 1 geformuleerde probleemstelling en de zes onderzoeksvragen en komt met tien aanbevelingen. Direct na hoofdstuk 8 volgt de samenvatting zowel in het Nederlands als Engels.

2. Privacy, een veelzijdig vraagstuk

> "Il est clair que la vérité que je cherche n'est pas en lui, mais en moi. Il l'y a éveillée, mais ne la connaît pas, et ne peut que répéter indéfiniment, avec de moins en moins de force, ce même témoignage que je ne sais pas interpréter et que je veux au moins pouvoir lui redemander et retrouver intact, à ma disposition, tout à l'heure, pour un éclaircissement décisive."
> M. Proust, À la recherche du temps perdu, Du côté de chez Swann: Combray 1, Paris 1999, p. 45.

In dit hoofdstuk wordt een antwoord geven op de eerste onderzoeksvraag (OV 1): *Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacywet- en regelgeving worden afgeleid?*

Het antwoord op deze vraag komt terug in hoofdstuk 6 waar de privacyveilige architecturen aan de orde komen.

Alvorens de EU privacy richtlijnen te analyseren worden de sleutelbegrippen 'privacy', 'persoonlijke ruimte', 'identiteit' en 'persoonsgegevens' verkend en de algemene beginselen die ten grondslag liggen aan de privacybescherming met hun uitwerking in de privacyrealisatiebeginselen in kaart gebracht. Paragraaf 2.1 bevat een aantal opmerkingen over de complexiteit van het begrip privacy en de inperking van dit onderzoek tot informationele privacy. Paragraaf 2.2 verkent de begrippen privacy, persoonlijke ruimte, identiteit en persoonsgegevens.

Paragraaf 2.3 behandelt de vijf universele kenmerken die aan informationele privacy ten grondslag liggen. In de paragrafen 2.4, 2.5 en 2.6 volgt de uitwerking van de vier universele kenmerken in de privacyrealisatiebeginselen, zoals onder meer vastgelegd in de EU Richtlijnen 95/46 en 2002/58.

Paragraaf 2.7 bespreekt de positie van de verantwoordelijke. Paragraaf 2.8 betreft het gegevensverkeer met landen buiten de EU en paragraaf 2.9 behandelt de dataretentierichtlijn 2006/24/EG en de problemen die deze richtlijn niet oplost.

In 2.10 worden enige kritische kanttekeningen bij de privacyrichtlijnen geplaatst. 2.11 gaat in op de pogingen tot standaardisatie van de privacyrealisatiebeginselen. De paragrafen 2.12 en 2.13 wijzen op de invloed van de persoonlijke privacyvoorkeuren en de wettelijke bepalingen op het ontwerp van informatiesystemen en de daaruit af te leiden juridische specificaties (requirements).

Daarmee wordt de eerste onderzoeksvraag beantwoord. 2.14 sluit het hoofdstuk met een samenvatting af.

2.1. Enige observaties

Privacy is een grondrecht en een belangrijke maatschappelijke norm. Het versterkt de menselijke waardigheid en ondersteunt andere grondrechten zoals recht van vereniging en vergadering, godsdienst en levensovertuiging en de vrijheid van meningsuiting. Privacy wordt beschouwd als een van de belangrijkste grondrechten van het informatie tijdperk. Van alle grondrechten is privacy misschien het meest problematische begrip om te definiëren, omdat volgens Nieuwenhuis over privacy geen consensus bestaat over de karakterisering, reikwijdte en afbakening.[1] Solove stelt[2] *privacy is a concept in disarray*, want niemand kan precies omschrijven waar het voor staat. Privacy is een te vaag begrip om als leidraad te dienen bij de rechtspraak in de Verenigde Staten of bij het maken van wetten. Volgens Solove kunnen abstracte uitspraken over het belang van privacy, zich niet staande houden tegenover concreet geformuleerde tegengestelde belangen.[3] Solove probeert privacy als maatschappelijk verschijnsel te benaderen. In de door hem ontwikkelde taxonomie zijn op een gestructureerde wijze de verschillende opvattingen over privacy weergegeven. Daarnaast zijn de maatschappelijk herkenbare privacy inbreuken en de maatschappelijke activiteiten die invloed uitoefenen op de bescherming van privacy door hem geïdentificeerd. In paragraaf 4.7 zal ik hierop nader ingaan.

Nieuwenhuis[4] onderscheidt twee manieren om het recht van privacy te benaderen. In de eerste plaats als een recht om het individu te beschermen tegen inbreuken in zijn privéleven en om persoonsgegevens onder voorwaarden te mogen verwerken (in het Franse recht aangeduid met "le secret de la vie privée"). In de tweede plaats als een recht dat er voor zorgt dat het individu de mogelijkheid heeft om in vrijheid te handelen (in het Franse recht aan geduid als "la liberté de la vie privée"). Privacybescherming en gegevensbescherming worden in vrijwel alle literatuur door elkaar gebruikt. Bij privacybescherming gaat het om een 'negatief' geformuleerd recht om zonder toestemming niet iemands privésfeer binnen te dringen. Bij gegevensbescherming gaat het om een 'positief' geformuleerd recht als een systeem van 'checks and balances' om 'fair play' in de informatie samenleving te bevorderen. Gegevensbescherming en informationele privacy overlappen elkaar in belangrijke mate.

In dit boek gaat het primair om informationele privacy.[5] De privacybescherming van persoonlijke informatie en van persoonlijke (tele)communicatie zijn steeds meer met elkaar verbonden geraakt. De oorzaak hiervan ligt in steeds intensievere koppeling van geautomatiseerde gegevensverwerking met telecommunicatie. De

1 Nieuwenhuis, 2001, p. 11.
2 Solove, 2006, p. 477.
3 Solove, 2006 (A), p. 1
4 Nieuwenhuis, 2001, p. 41.
5 Etzioni, 1999, p. 15.

privacy van de persoonlijke informatie en van de persoonlijke (tele)communicatie tezamen wordt aangeduid met 'informationele privacy'. De informationele privacy omvat permanente, variabele en andere persoonlijke informatie die van het individu afkomstig is. Het gaat om alle persoonsgegevens, ook als deze niet rechtstreeks uit de privésfeer afkomstig zijn. Deze vorm van privacy staat of valt met het vermogen van het individu om autonoom controle uit te oefenen over de onthulling en de verspreiding van zijn persoonsgegevens.[6] Om die controle te kunnen uitoefenen gelden regels voor de verzameling, verwerking en verspreiding van persoonsgegevens. Als begrip manifesteert informele privacy zich niet eerder dan in de zeventig jaren van de vorige eeuw.[7] Door de explosieve ontwikkeling van de informatie- en communicatietechnologie krijgt het een duidelijke mondiale erkenning in de Guidelines on the Protection of Privacy and Transborder Flows of Personal Data van 23 september 1980 van de Organization for Economic Co-operation and Development (OECD), waarover in paragraaf 2.4.1 meer.

2.2. Verkenning van het begrip informationele privacy

Het recht op privacy wordt verdeeld in vier groepen: 1 Het recht op ruimtelijke privacy. 2 Het recht op relationele privacy. 3 Het recht op lichamelijke integriteit. 4 Het recht op informationele privacy. Dit laatste heeft betrekking op de verwerking van persoonsgegevens. In dit boek gaat het voornamelijk om informationele privacy. Maar zoals hieronder zal blijken zijn er ook andere indelingen te maken. In paragraaf 2.2.1 wordt privacy omschreven. In paragraaf 2.2.2 gaat het over persoonlijke ruimte en identiteit. In paragraaf 2.2.3 wordt het begrip persoonsgegevens behandeld.

2.2.1. Omschrijving

Brandeis zette privacy op de agenda van de moderne mensheid, toen hij in zijn klassiek geworden artikel in 1890 privacy omschreef als: "the right to be left alone" en meer specifiek als: "(…)the principle (…) of an inviolate personality".[8] Hij wees er met name op dat privacy van essentieel belang is voor de bescherming van de persoonlijkheid, de onafhankelijkheid, de waardigheid en integriteit van het individu.[9] Brandeis vestigde in zijn beschouwing voor de eerste keer de aandacht op inbreuken in iemands persoonlijke levenssfeer ten gevolge van de uitvinding van de in massaproductie gefabriceerde fotocamera.[10] Hij verschoof

6 Vedder, 1998, p. 115-120.
7 De eerste wetten op het gebied van de gegevensbescherming werden in de Duitse deelstaat Hessen (1970) en in Zweden (1973) ingevoerd. In Nederland werd het recht op privacy (eerbiediging van de persoonlijke levenssfeer) sinds 1983 vastgelegd in artikel 10 van de Grondwet.
8 Warren & Brandeis, 1890, p. 193-220.
9 Freedman, 1987, p. 2.
10 Kodak brengt in 1888 een fotocamera op de markt met de slogan 'you press the button, we do the rest.' www.kodak.com/…/kodakHistory/eastmanTheMan.shtml.

hiermee de aandacht van lichamelijke en ruimtelijke privacy naar de informationele privacy, hoewel op dat moment die term nog niet werd gebruikt. Later in 1928, toen Brandeis rechter bij het U.S. Supreme Court was, extrapoleerde hij in Olmstead v. United States,[11] dat technologische vooruitgang het de overheid mogelijk zou maken surveillancemiddelen in te zetten, die veel verder zouden reiken dan het afluisteren van telefoongesprekken. Justice Bandeis stelde daarom dat de bescherming die het Fourth Amendment[12] biedt, zo geïnterpreteerd moet worden dat "the right to be left alone" blijft gelden ongeacht wat voor (nog onbekende) technologie door de overheid zou kunnen worden ingezet.

Pas in 1967 komt informationele privacy echt in de belangstelling. Westin definieert dan privacy[13] als: "the claim of individuals (…) to determine for themselves when, how and to what extent information about them is communicated to others" en als een middel "(…) for achieving individual goals of self realization".[14] In aanvulling op Brandeis' opvatting is privacy niet alleen het recht om met rust gelaten te worden en anoniem te blijven, maar ook het recht om bepaalde op het persoonlijke leven betrekking hebbende feiten geheim te houden en zelf in alle vrijheid te beslissen wat men over zichzelf aan anderen wil meedelen. In Duitsland is in 1983 de formulering over privacy van Brandeis door het Bundesverfassungs gericht aangevuld met het "Grundrecht auf informationelle Selbstbestimmung".[15]

Rothfeder schrijft in zijn boek 'Privacy for Sale' dat: "in the newly developing 'information democracy' the thirst for privacy is going to the very core of human existence.(…) The feeling of not being able to make your own free choices, but being at the mercy of direct marketeers, credit bureaus, which collect, examine, match, collate, and sell data of individuals without their consent, will have in the end detrimental consequences for society. People will feel like being in custody, unable to control the information about themselves. (…) They will become passive sensing not being any longer a participant in the world around them. People will stop being productive citizens".[16]

Bij de hierboven vermelde omschrijvingen van het begrip privacy horen dus twee onderscheidende kenmerken, namelijk het recht om met rust gelaten te worden en het recht om zelf te bepalen wat men over zichzelf wil publiek maken. Zoals al eerder gesteld is het, gezien de complexiteit van het begrip privacy, moeilijk, zo niet onmogelijk, een algemeen aanvaarde definitie van privacy te geven. De Calcutt Committee[17] stelde in 1990, dat: "nowhere have we found a wholly

11 277 U.S. 438, 466, 472-74, 478 (1928) (Brandeis, J., dissenting).
12 Het Fourth Amendment van de Amerikaanse Grondwet is onderdeel van de Bill of Rights. In Katz v. United States, 389 U.S. 347 (1967), oordeelde het Supreme Court dat dit amendment ook betrekking had op "reasonable expectation of privacy" van het individu.
13 Westin, 1967, p. 7.
14 Westin, 1967, p. 39.
15 Urteil von 15 Dezember 1983, BVerfGE 65,1 ff(43).
16 Rothfeder 1992, p. 30, 210.
17 Calcutt, 1990, p. 7.

satisfactory definition of privacy". Zestien jaar later rapporteert EPIC: "Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information".[18]

Clarke wijst erop dat privacy verschillende dimensies heeft:

1. De lichamelijke privacy. Het gaat hier om de integriteit van het lichaam van het individu. Problemen die hierbij kunnen optreden zijn bijvoorbeeld: verplichte immunisatie, bloedtransfusie zonder toestemming, verplicht afstaan van lichaamsvloeistoffen, haar en huid, en verplichte sterilisatie.
2. De privacy met betrekking tot het persoonlijk gedrag. Dit betreft alle aspecten van gedrag, maar vooral intieme, seksuele gedragingen, zowel in privé en in openbare ruimten. Hij noemt het ook wel 'media privacy'.
3. De privacy van de persoonlijke communicatie. Voor individuen is het belangrijk dat zij met gebruikmaking van allerlei media met elkaar kunnen communiceren, zonder dat hun communicatie in de gaten wordt gehouden door andere personen of organisaties. Hij duidt deze vorm van privacy ook aan als 'interception privacy'.
4. De privacy ten aanzien van persoonlijke informatie. Individuen claimen dat gegevens over henzelf niet automatisch beschikbaar zouden moeten zijn voor andere individuen en organisaties, en dat, zelfs al zouden anderen over dergelijke gegevens beschikken, het individu zelf in staat moet zijn een behoorlijke mate van controle over die data en het gebruik daarvan te kunnen uitoefenen. Dit wordt vaak als 'data privacy' of 'informationele privacy' aangeduid.[19]

Clarke's opsomming is niet volledig. Hij vermeldt bijvoorbeeld niets over de ruimtelijke privacy, als afscherming van het eigen territorium. Nieuwenhuis wijst erop dat bij de beschrijving van privacy nu eens een gedraging, dan weer een plaats centraal staat, en elders ligt de nadruk op bescherming of afscherming.[20] Een sluitende beschrijving is kennelijk niet te geven. Wanneer er zich zo'n fluïde situatie rond een zo belangrijk grondrecht voordoet dan is het aan de rechter om het begrip nader inhoud te geven. Dat is dan ook meerdere malen gebeurd door de European Commission of Human Rights en de European Court of Human Rights. Zij hebben zich gebogen over de inhoud en uitleg van artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de fundamentele

18 EPIC, 2006.
19 Clarke, 2006.
20 Nieuwenhuis, 2001, p. 33.

vrijheden (EVRM)[21] en met name over het vergaren en registeren van gegevens, het inzagerecht, de vernietiging van gegevens en wat onder gevoelige gegevens moet worden verstaan. Artikel 8 EVRM is evenwel niet van toepassing op de private sector en dat gaf mede de aanzet tot specifieke Europese wetgeving.[22]

Als men voor wat betreft de bescherming van informationele privacy naar de wereldkaart kijkt, dan zijn er vele verschillen vast te stellen. Er zijn landen met een hoge graad van privacybescherming; landen die privacy maar gedeeltelijk en beperkt beschermen en er zijn vele landen waar privacybescherming nog steeds "terra incognita" is. Het betreft hier ongeveer 100 staten voornamelijk in Afrika en Azië.[23] Grofweg zou hieruit afgeleid kunnen worden dat informationele privacy vooral een kwestie is in de Westerse en op het Westen georiënteerde wereld. De mondialisering met zijn elektronische communicatiediensten schreeuwt evenwel om een wereldwijd geldende privacyregime. De vraag is nochtans of de mensheid met zijn veelvoud aan rechtssystemen de komende vijftien jaar in staat zal zijn wereldwijd geldende wetgeving op het gebied van de bescherming van persoonsgegevens te verwezenlijken?[24] Cottier zegt hierover, dat dit enerzijds afhangt van de politieke, juridische, economische en culturele obstakels en anderzijds van de druk van cyberspace om in onze Global Society wereldwijd economische systemen te integreren.[25] Mijn verwachting is dat door het gebruik van internet en de verspreiding van persoonsgegevens tot in alle gaten en uithoeken van de wereld, het belang van een wereldwijd regime voor de privacybescherming zo sterk zal toenemen, dat er een oplossing gevonden zal moeten worden.

2.2.2. Identiteit en persoonlijke ruimte

Informationele privacy vooronderstelt dat een individu een identiteit[26] heeft. Varella schrijft dat het hebben van een identiteit de bron van zingeving is en ons in staat stelt ervaringen in het leven op te doen.[27]

Het hebben van een identiteit vereist zelfkennis om in staat te zijn een onderscheid te maken tussen zichzelf en de ander. Door het hebben van een identiteit krijgt de mens een in zichzelf besloten eenheid. Dit leidt tot de

---

21 De tekst van het Verdrag is gewijzigd in een reeks Protocollen. Alle bepalingen die een wijziging hadden ondergaan of waren toegevoegd door deze Protocollen zijn vervangen door Protocol Nr. 11 (ETS Nr. 155), met ingang van 1 november 1998, de inwerkingsdatum. www.echr.coe.int/NR/rdonlyres/655FDBCF-1D46-4B36-9DAB-99F4CB59863C/0/Dutch Néerlandais.pdf.

22 De Hert & Gutwirth, Brussels 2007.

23 Cottier, 2005, p. 15.

24 David, 2002: David maakt een fundamenteel onderscheid tussen vier rechtssystemen: Het Romeins/Frans/Duitse rechtssysteem; Het Angelsaksische rechtssysteem (*common law*), het religieus rechtssysteem (Talmud, Sharia), het socialistisch rechtssysteem (Marxistisch-leninistische doctrine). Glenn, 2000 onderscheidt er zeven, die zijn ontstaan het primitieve "*chthonic*" (met de grond verbonden) rechtssysteem, dat het allereerst in de mensheid ontstond, los van enige traditie en met als kenmerk mondeling overdracht.

25 Cottier, 2005, p. 16.

26 Prins, 2007, p. 849 maakt een onderscheid van vijf vormen van identiteit.

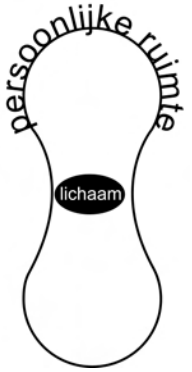
27 Varella, 1998, p. 16.

belangrijkste kernwaarde in het morele en politieke leven, namelijk de vrijheid om zichzelf te zijn en te leren begrijpen wie men is. Mensen blijken de psychologische behoefte te hebben om (enige) controle te kunnen uitoefenen over de manier waarop zij (als identiteit) door hun omgeving worden gezien.[28] Menselijke waarden, zoals de beslotenheid van de persoonlijke levenssfeer, kunnen felle emoties bij mensen oproepen, zoals angst wanneer het respect ervoor verslapt, verdriet als het verdwijnt, blijheid als het in ere wordt hersteld en schuldgevoel als de waarde door hen zelf niet wordt nageleefd.[29]

Identiteit gaat niet alleen het individu aan, maar is een belangrijke zaak voor de gemeenschap. Castells[30] onderschrijft het belang van de identiteit voor het individu. Het stelt de mens in staat andere mensen in een betekenisvol kader te plaatsen. Door het hebben van een identiteit kan de mens zich als herkenbaar persoon binnen de tijd/ruimtedimensie handhaven. De samenleving kan een dergelijke identiteit legaliseren en dat leidt tot het ontstaan van een beschaafde samenleving.[31] Identiteit leidt voorts tot de vorming van gemeenschappen[32] die zichzelf organiseren om weerstand te kunnen bieden tegen onderdrukking. Uiteindelijk bereiken dergelijke gemeenschappen over een lange periode van hun bestaan een evenwicht tussen individuele rechten (grondrechten) en sociale verantwoordelijkheden.

Het proxemics onderzoek (het vakgebied op het snijvlak van sociologie, culturele studies en psychologie, dat onderzoek doet naar manieren waarop in verschillende culturen omgegaan wordt met ‘sociale ruimte’ en ‘persoonlijke ruimte’ en de verhouding daartussen) heeft proefondervindelijk vastgesteld dat de persoonlijke ruimte van de mens een onzichtbare beschermhuls is, ongeveer in de vorm van een zandloper, die zich om hem heen bevindt.

Figuur 2.1: persoonlijke ruimte, Van den Berg, 2008 p. 51.



28 Ortony, Clore & Collins, 1988.
29 Frijda, 1988, p. 368-369.
30 Castells, 2004, p. 6, 7, 184.
31 Castells, 2004, p. 8 “this generates a civil society”; p. 420.
32 Etzioni, 1996, p. 7.

De persoonlijke ruimte is al heel lang een aanvaard verschijnsel en heeft in vele culturen geleid tot de erkenning van lichamelijke en ruimtelijke privacy.[33]

In Ambient Intelligence, elektronische omgevingen die voor de aanwezigheid van mensen gevoelig en ontvankelijk zijn (AMI), ook wel aangeduid als 'ubiquitous computing environment'[34] is het menselijk lichaam de kern waar omheen door toepassing van kunstmatige intelligente sensortechnologie een tweede persoonlijke ruimte tot stand komt. Deze ruimte komt voor een deel overeen met de 'wolk' van persoonsgegevens van een individu die nu al zijn opgeslagen in databanken. Binnen de AMI zorgt de koppeling van de sensoren met de fysieke aanwezigheid van het lichaam van de mens voor de verwerkelijking van zijn persoonlijke voorkeuren. AMI kan er bijvoorbeeld voor zorgen dat bij het betreden van een ruimte, deze wordt voorzien van bij de persoon behorende persoonlijke accenten. Even gemakkelijk kan in de AMI omgeving de gezondheidstoestand in de gaten gehouden worden en een medicijn worden toegediend. Er ontstaat wel een probleem, als twee mensen dezelfde ruimte betreden. Wiens persoonlijke voorkeuren zullen dan prevaleren? Van den Berg vraagt zich dan ook af of dit zou kunnen betekenen dat het mogelijk wordt de persoonlijke ruimte van een ander te 'koloniseren'?[35] AMI kan ook worden ingezet om mensen voortdurend in de gaten te houden.

Jung wijst erop dat identiteit wordt opgebouwd door een proces van individuatie.[36] Door psychoanalyse is vastgesteld, dat de diepere ontdekking van de identiteit van het individu plaatsvindt door zichzelf innerlijk te onderzoeken. Jung,[37] voortbouwend op het werk van Freud, heeft ontdekt dat het individu naast het Ego ook een Zelf heeft. Dit Zelf is het totaal van het Ego en het (persoonlijk) onderbewuste. Het is veel omvangrijker dan het Ego.[38] Het Ego is het ik-veld van het bewustzijn. Het Ego is de voorwaarde voor de identiteit en continuïteit in het beleven van het bewuste zijn van het individu. De onderbewuste lagen waarin zich de traumata, de conflicten en de verdringingen kunnen bevinden, hebben invloed op het handelen in het ik-veld van het bewustzijn.[39] De psychische totaliteit van het individu zorgt voor het hebben van een eigen identiteit, die zich in de wereld om hem heen reflecteert.

Het hebben van een door de samenleving gerespecteerde identiteit en het daarbij behorende privacygebied, beschermt onze maatschappelijke uitgangspositie van anonimiteit ten opzichte van derden die niet tot onze intieme kring van mensen behoren. Buiten de sfeer van de intimiteit zal het individu alleen onder al dan niet strikte voorwaarden geheimen over zichzelf en persoonsgegevens met anderen

33 Westin, 2005.
34 Bellotti & Sellen, 1993.
35 Van den Berg, 2008, p. 54-61.
36 Jung, 1984. Individuatie is de weg die de mens moet afleggen om zijn volledig Zelf te kennen door volledige integratie van alle bewuste en onbewuste processen en psychische elementen en complexen waardoor ego, schaduw, anima/animus en de diep in het onderbewustzijn liggende delen van het Zelf worden geïntegreerd.
37 Jung, 1951.
38 Jung, Toronto 1939 vertaald in Bewust en Onbewust door De Vries-Elk, 1989, p. 20-35.
39 Assagioli, 1965.

delen. Wij weten allemaal dat ieder individu van tijd tot tijd de behoefte heeft, gewild of ten gevolge van omstandigheden, 'afgesneden' te willen zijn van zijn gebruikelijke metgezellen of omgeving.[40] Deze behoefte heeft tot gevolg dat het individu de toegang tot zijn eigen sfeer van onafhankelijkheid ontzegt aan de Staat, private organisaties en andere individuen.

Een vergelijkbare situatie doet zich voor bij dieren. Uit bestudering van het territoriuminstinct van dieren is gebleken dat ernstige inbreuken op het territorium van een dier leidt tot het in het in gevaar brengen van het voortbestaan van dat dier en wanneer dat op grote schaal gebeurt, dan leidt dat tot het uitroeien van die bepaalde diersoort.[41]

Privacy heeft betrekking op persoonlijke controle, de inhoud en integriteit van de identiteit, en de vrijheid van keuze. Privacy gaat over jezelf kennen en jezelf zijn. Een door het individu als pijnlijk ervaren inbreuk op zijn informationele privacy of misbruik van zijn identiteit zal leiden tot zelfdisciplinerend,[42] conformistisch of zelfs saboterend gedrag van dit individu.[43] Het individu zal daardoor niet meer in vrijheid kunnen handelen en niet meer zichzelf kunnen zijn. Van Schijndel stelt in zijn scriptie over identiteitsdiefstal dat conform Locke's theorie (weergegeven in zijn 'An Essay Concerning Human Understanding')[44] de identiteit in het bewustzijn besloten ligt, "omdat wij onszelf herkennen in onze gedachten en daden, zijn wij wie wij zijn". Interessant is dat hij meent dat "de enorme proliferatie van administraties er toe heeft geleid dat zich een extern bewustzijn heeft ontwikkeld (…) daar wordt minutieus geregistreerd wat we doen en laten". In de daarbij behorende noot schrijft hij "In administraties zijn geen gedachten opgeslagen. Dat is simpelweg (nog) niet mogelijk".[45]

Over bewustzijn bestaan veel verschillende opvattingen. De algemene deler is dat bewustzijn een subjectieve reflectie van het individu is op indrukken uit de buitenwereld (weten wat je ziet, hoort of voelt en daarover kunnen vertellen) of op eigen mentale processen (weten wat er in je omgaat en daarover kunnen vertellen). Het 'extern bewustzijn' zoals Van Schijndel dat beschrijft is een representatie van het individu vastgelegd in persoonsgegevens. Bij herkenning van de extern opgeslagen persoonsgegevens door het individu dat deze gegevens heeft verstrekt of gegenereerd, vindt in het individu zelf de activering van zijn bewustzijn plaats. Een extern bewustzijn dat bestaat uit één of meerdere verzamelingen van persoonsgegevens los van het individu lijkt mij bij geavanceerde kunstmatige intelligentie alleen mogelijk als bijvoorbeeld robots de mogelijkheid tot

40 Andweg & Van der Tak, 1975, p. 157.
41 Van Dongen, 1975, p. 13.
42 Koelewijn 2009, p. 15, p. 202.
43 Hulsman & Ippel, 1994, p. 15.
44 Russell, 1967, p. 589. Dit belangrijke filosofisch werk werd in 1690 gepubliceerd. In dit werk zet hij zijn theorie over kennis uiteen gebaseerd op empirie. In An Essay Concerning Human Understanding' boek 2 chapter I, section 2: "Let us then suppose the mind to be, as we say, white paper. Void of all characters, without any ideas: how comes it to be furnished? (…) To this I answer in one word, from experience; In that all our knowledge is founded, and from that it ultimately derives itself".
45 Van Schijndel, 2007, p. 15.

zelfreflexie zouden hebben.[46] De toerekening van persoonsgegevens aan een persoon door een derde (menselijk of elektronisch) kan niet als extern bewustzijn worden gekwalificeerd. Wel kan een onderzoeker van een set persoonsgegevens bij een diepgaande psychologische analyse (psychogrammen, profielen die psychisch gedrag zichtbaar maken) veel over de persoonlijkheid van het individu ontdekken en daarvan gebruik maken.[47]

De verschillende bewustzijnstoestanden van een individu genereren verschillende niveaus van persoonsgegevens en dat heeft consequenties voor het niveau van privacybescherming. De gegevens van de diepere lagen van het (onder)bewustzijn van het individu kunnen omschreven worden als data die het individu slechts binnen de bescherming van de intimiteit zou willen delen met die individuen die het tot zijn of haar intimiteitsfeer toelaat. Er zijn ook persoonsgegevens dat het individu met niemand wil delen en data waarvan het individu zelf zich (nog) niet bewust is. Een inbreuk van de privacy op dit niveau zal als uiterst pijnlijk worden ervaren. Ik noem deze data de IK BEN persoonsgegevens. De gegevens over het in de buitenwereld gekende Ego noem ik de DAT BEN IK persoonsgegevens. Dat zijn gegevens waar het individu ook mee gekend en bekend wil zijn. Die gegevens ben ik bereid makkelijker (onder voorwaarden) af te staan aan derden. Om gegevens over een persoon (persoonsgegevens) aan iemand toe te rekenen, moet het individu over een juridische identiteit beschikken. Een dergelijke identiteit wordt aan een individu in de Westerse samenleving toegekend wanneer het individu wordt ingeschreven in het register van de burgerlijke stand van de stad waar de geboorte van het individu heeft plaatsgevonden of door middel van een gerechtelijke uitspraak over het toekennen of veranderen van iemands naam of, wanneer er geen civiel register bestaat, in een register van een godsdienstige organisatie of daarmee te vergelijken organisatie.

2.2.3. Persoonsgegevens

Zoals hierboven gesteld leidt identiteit tot persoonsgegevens. Dit begrip kan worden gedefinieerd als een verzameling van alle data die kunnen worden gerelateerd aan een individu. Dus zowel de ‘IK BEN’ data, als de ‘DAT BEN IK’ data vallen hieronder. Het betreft feitelijke gegevens, zoals lichamelijke gegevens, gedragsgegevens, psychische, sociale en financiële gegevens en elk ander gegeven dat als een attribuut kan worden gezien van het desbetreffende individu. De informatie over een persoon behoeft nochtans niet waar of bewezen te zijn. Persoonsgegevens kunnen direct of indirect tot identificatie leiden. De

46 Illustratief is bijvoorbeeld de sciencefictionfilm A.I. Artificial intelligence van Spielberg (2001) met David, een robotjongen (mecha), die is uitgerust met het vermogen lief te hebben.
47 In hoofdstuk 3 paragraaf 4.1 wordt hierop ingegaan.

kwalificatie dat er sprake is van persoonsgegevens kan ook afhankelijk zijn van de context waarbinnen informatie wordt gebruikt. Door het gebruik kunnen gegevens aan een persoon gerelateerd worden. Persoonsgegevens kunnen ter beveiliging in informatiesystemen in verschillende niveaus van toenemende identificeerbaarheid gesplitst worden, zoals beschreven in paragraaf 6.9.1 over het PISA-project.[48]

In de Europese Richtlijn 95/46/EG wordt in artikel 2(a) een definitie gegeven van het begrip persoonsgegevens als: "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit". Het gaat om welke informatie dan ook met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (Betrokkene). Natuurlijke personen betreffen slechts levende individuen en niet overleden of rechtspersonen.

Niet-identificeerbaarheid van gegevens wordt aangenomen als de hoeveelheid en aard van de indirect identificerende gegevens zodanig is, dat de identificatie slechts mogelijk is wanneer er sprake is van een disproportionele inspanning (een juridisch open begrip) om de identificatie te bewerkstelligen.[49] Of er sprake is van een disproportionele inspanning hangt enerzijds af van de aard van de gegevens en de grootte van de populatie[50] en anderzijds van de middelen aan tijd en geld die men bereid is te besteden om een persoon te identificeren.

Veel data kunnen dus persoonsgegevens zijn of worden. Bijvoorbeeld: internet identificeerders zoals een IP-adres, sessie logindata en de lijst van door een internetgebruiker bezochte websites worden ook als persoonsgegevens gekwalificeerd.[51] Een subcategorie persoonsgegevens zijn de gevoelige gegevens waaraan artikel 8(1) van de Richtlijn 95/46/EG refereert. Het gaat hier om persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook gegevens die de gezondheid of het seksuele leven betreffen. Artikel 8(5) bevat een speciale categorie persoonsgegevens die betrekking hebben op overtredingen, strafrechtelijke veroordelingen of getroffen veiligheidsmaatregelen. Voor de verwerking van deze gegevens gelden restrictieve voorwaarden.

---

48 Privacy Incorporated Software agent (PISA) EU research project IST - 2000 – 26038 (1-1-2000 – 31-12-2003).

49 Overweging 26 van de EU Richtlijn 95/46/EG en overweging 20 van de Richtlijn 2002/58/EG.

50 Het woord 'populatie' heeft betrekking op een statistische analyse context en kan worden gedefinieerd als enige set van gegevens met gemeenschappelijke waarneembare karakteristieken. Hoe kleiner de populatie, hoe sneller de identiteit van het individu kan worden ontdekt.

51 EU Article 29 Data Protection Working Party, Opinion WP 37: Privacy on the Internet – An integrated EU Approach to On-line Data Protection. Dit document gepubliceerd in 2000, is beschikbaar op: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm.

De EU Article 29 Data Protection Working Party[52] (WP29) heeft in haar 'Opinion on the concept of personal data'[53], uitvoerig commentaar geleverd op het begrip en de definiëring van persoonsgegevens in de Richtlijn 95/46/EG. Zij geeft daarbij aan dat "The scope of the data protection rules should not be overstretched, but unduly restricting the interpretation of the concept of personal data should also be avoided".[54] De EU-Commissie schrijft dat de definitie die in de Richtlijn in artikel 2(a) is gebruikt, de bedoeling van de Europese wetgever weerspiegelt om een zo breed mogelijke omschrijving te geven over het begrip persoonsgegevens. Bij het indienen van de tekst verklaarde de EU-Commissie dat "as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual".[55] In het geamendeerde voorstel schreef de EU-Commissie dat "the amended proposal meets Parliament's wish that the definition of 'personal data' should be as general as possible, so as to include all information concerning an identifiable individual".[56] De Raad van Ministers van de Europese lidstaten was het met deze opvatting eens.[57]

Opinie WP136[58] onderscheidt op pagina 6 vier bouwstenen:
1. "enige informatie";
2. "betrekking hebbend op";
3. "een geïdentificeerd of identificeerbaar";
4. "natuurlijk persoon".

Met betrekking tot het eerste bouwsteen: "enige informatie" stelt deze Opinie op pagina 7: "The concept of personal data includes information kept in any form, e.g., on paper, in the form of information stored in a computer memory by means of binary code, or in analogue form on a videotape, for instance. In particular, sound and image data qualify as personal data (…), insofar as they may represent information on an individual".

De Opinie WP 136 merkt over de betekenis van 'natuurlijk persoon' op bladzijde 21 op, dat de Richtlijn (95/46/EG) universeel van toepassing is op alle natuurlijke personen en niet is beperkt tot ingezetenen van de EU of ingezetenen in bepaald land.

WP29 stelt betreffende overleden personen op pagina 22: "Information relating to dead individuals is therefore in principle not to be considered as personal data subject to the rules of the Directive, as the dead are no longer natural persons in

52 De Working Party is opgericht ex artikel 29 van de Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviserend orgaan over gegevensbescherming en privacy. De taken zijn beschreven in Artikel 30 of de Richtlijn 95/46/EG en Artikel 15 van de Richtlijn 2002/58/EG.
53 Opinion No. 4/2007, # 01248/07/EN-WP 136.
54 Opinion No. 4/2007, # 01248/07/EN-WP 136, p. 5.
55 COM (90) 314 final, 13-9-1990, p. 19 (commentaar op artikel 2).
56 COM (92) 422 final, 28-10-1992, p. 10 (commentaar op artikel 2).
57 Common position (EC) No 1/95, aanvaard door de Raad op 20 februari 1995, OJ NO C 93 van 13-4-1995, p. 20.
58 WP 136 (Opinion No. 4/2007 on the concept of personal data).

civil law". Nochtans, kunnen de gegevens van overledenen in bepaalde gevallen nog indirect beschermingswaardig zijn.

Het Europese Hof (ECJ) bevestigt de ruime opvatting over persoonsgegevens in de zaak C-101/2001 van 6 november 2003 (Lindqvist). Lindqvist maakte een website waarop zij persoonsgegevens van haarzelf en mensen uit haar geloofsgemeente plaatste. Lindqvist werd in Zweden veroordeeld voor onrechtmatige verwerking van persoonsgegevens. Volgens het Europese Hof van Justitie bevatten de bepalingen van de Europese Richtlijn 95/46 als zodanig geen beperkingen die in strijd zijn met de vrijheid van meningsuiting. Deze zaak is in dit kader van belang in verband met de ruime begripsopvatting over persoonsgegevens, zoals blijkt uit overwegingen 24 en 27: "The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies".

> "Referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data […] within the meaning of […] Directive 95/46/EC."[59]

De door WP29 gegeven definities over anonieme en pseudonieme gegevens, spelen een belangrijke rol bij het ontwerpen van privacyveilige informatiesystemen. Deze definities luiden:

> "'Anonymous data' in the sense of the Directive can be defined as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual. 'Anonymised data' would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible.
>
> Pseudonymisation is the process of disguising identities. […] Pseudonymisation can be done in a retraceable way by using correspondence lists for identities and their pseudonyms or by using two-way cryptography algorithms for pseudonymisation. Disguising identities can also be done in a way that no reidentification is possible, e.g. by one-way cryptography, which creates in general anonymised data."[60]

In hoofdstuk 5 en 6 kom ik op anonimiteit en pseudonimiteit terug. WP29 behandelt in verschillende Opinies vele soorten gegevens die als persoonsgegevens kunnen

---

59 http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en.

60 Opinion WP 136 – Opinion 4/2007 on the concept of personal data, p 18 (pseudonimiteit) en p. 21. (anonimiteit) http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/.

worden aangemerkt, zoals IP-adressen (Opinion WP148), medische gegevens (Opinion WP131) en genetische gegevens (Opinion WP91).[61]

Poullet stelt dat de Ambient Intelligence (AMI) omgeving nieuwe categorieën van persoonsgegevens zal genereren, die uitbreiding van de definitie van persoonsgegevens in de derde generatie privacywetgeving zal noodzaken.[62] Voor alle duidelijkheid: de eerste generatie startte met de EVRM; privacy als recht om gevoelige gegevens, huis, gezin en familierelaties te beschermen tegenover de buitenwereld. De tweede generatie loopt van de Raad van Europa Convention N° 108 (1981) tot Charter on fundamental rights van de Europese Unie (2000). Hierin wordt de bescherming tot alle persoonsgegevens met 3 beginselen verbreed: legitimiteit van de verwerking, recht op transparante verwerking voor de betrokkene en de rol van de Toezichthouder (DPA) om het evenwicht tussen de betrokkene en de verantwoordelijke te bewaren.

Hustinx is geen voorstander van een hernieuwde discussie over de reikwijdte van de wettelijke begrippen.[63] Dit omdat hij voorstander is van een brede werkingssfeer en ook omdat de discussies over de reikwijdte van de begrippen volgens hem leiden tot dogmatische en praktische problemen. Daarbij ziet hij zo'n discussie als een 'signaal van zwakte': "[Het] is de weg terug, want daarmee bouw je een enorm dogmatisch en praktisch probleem aan de voordeur. Elke keer weer discussies over de vraag is dit nu wel of niet een persoonsgegeven. Ik ben een groot voorstander van een brede werkingssfeer die je dan wel verstandig en flexibel moet toepassen. Door nu aan de richtlijn te morrelen geef je internationaal een signaal van zwakte af en ontstaat er wederom een discussie van jaren met de bijbehorende implementatietrajecten."[64]

2.3. Algemene beginselen betreffende persoonlijke informatie

In het kader van het PISA-project[65] en door de Information and Privacy Commissioner of Ontario (IPC) (Canada)[66] is onderzocht welke internationale afspraken er over de toepassing van privacybeginselen bestaan. Zowel de PISA-onderzoekers als de IPC concluderen dat de Westerse wereld vier fundamentele privacybeginselen onderschrijft. "These principles are called 'global' to indicate their general acceptance by at least the democratic countries, although such

61 Zie de Lijst van geraadpleegde documenten van de Article 29 Working Party achterin dit boek.
62 Poullet, Brussel 2009, p. 4.
63 Zwenne, e.a., Leiden 2007, p. 64.
64 Hustinx, 2004, p. 270-272.
65 PISA (Privacy Incorporated Software Agent) EU research project IST - 2000 – 26038 (1-1-2000 – 31-12-2003).
66 Toronto, 2006.

countries are not necessary actively pursuing a full national deployment of the principles".[67]

Deze universeel geaccepteerde privacybeginselen zijn technologie- en situatieonafhankelijk en vormen het fundament voor de regelgeving die persoonsgegevens beschermen. Het gevolg van deze algemeen aanvaarde beginselen is dat het de ontwikkeling en toepassing van privacybeschermende technologieën wereldwijd mogelijk maakt. Technologen kunnen bij de ontwikkeling van privacyveilige informatiesystemen[68] uitgaan van deze universele waarden en zijn daardoor niet genoodzaakt om per land een aangepast informatiesysteem te bouwen. De beginselen geven de internationale consensus op het gebied van de bescherming van persoonlijke informatie weer en zullen in dit boek worden gebruikt voor een methodologische benadering van het probleem van het geautomatiseerd beschermen van persoonsgegevens. Vanuit het individu bezien kunnen wat betreft het recht op informationele privacy vijf universele beginselen onderscheiden worden.

2.3.1. Het beginsel van het bestaan van identiteit

Een mens (de betrokkene op wie een persoonsgegeven betrekking heeft) bezit een fysieke, ruimtelijke, sociale, en mentale identiteit. Prins onderscheidt naast de eigen identiteit een juridische, administratieve, culturele, en religieuze identiteit.[69] De verzameling van alle informatie (de 'IK BEN' data en 'DAT BEN IK' data) over de verschillende vormen van identiteit wordt als persoonlijke informatie beschouwd en is mondeling of schriftelijk (elektronisch) overdraagbaar aan anderen. Het hebben van een identiteit zorgt er voor dat het individu weet en voelt dat hij iemand is.

2.3.2. Het beginsel van het niet vrijgeven van persoonlijke informatie

Een mens heeft de keuzevrijheid om zijn persoonlijke informatie geheel of gedeeltelijk te delen met anderen en met organisaties.[70] Dit betekent dat er sprake dient te zijn van een toestemmingsvereiste van het individu. Het individu kan niet tegen zijn wil gedwongen worden zijn persoonlijke informatie prijs te geven. Dit recht kan evenwel door (inter)/(supra)nationale wetgeving beperkt worden.

---

67 Borking, e.a., Brussels 2001, p. 9.

68 Mulder, 1990, p. 28-38. Informatiesystemen zijn bedoeld om aan mensen informatie te verschaffen voor het besturen, plannen, uitvoeren en controleren van doelgerichte activiteiten. De volgende typen worden onderscheiden: transactiegerichte informatiesystemen, kantoorinformatiesystemen, kennis- en expertsystemen, strategische informatiesystemen, documentaire informatiesystemen, geprogrammeerde beslissingssystemen en beslissingsondersteunende systemen.

69 Prins, 2007, p. 849.

70 Borking, 1984, p. 91.

2.3.3. Het beginsel van gecontroleerde verspreiding

Een mens heeft het recht naar eigen inzicht beperkingen te verbinden aan het gebruik, de verwerking, bekendmaking en opslag van zijn persoonlijke informatie, die hij met anderen heeft gedeeld. Anderen kunnen niet zonder zijn toestemming zijn persoonlijke informatie verwerken. Ook dit recht kan evenwel door (inter)/(supra)nationale wetgeving beperkt worden.

2.3.4. Het beginsel van vertrouwelijkheid en beveiliging

Personen en organisaties die persoonlijke informatie of persoonsgegevens verzamelen, verwerken, doorgeven en opslaan dienen zich te houden aan de door het identificeerbare individu en de door de rechtsnormen opgelegde beperkingen. De opgelegde beperkingen van het individu impliceren dat de verspreiding en overbrenging van de persoonsgegevens van de één naar de ander onder dezelfde voorwaarden en beperkingen dienen plaats te vinden als geldend voor de personen en organisaties die in eerste instantie de persoonsgegevens hebben verzameld, verwerkt en opgeslagen.

2.3.5. Het beginsel van terugkoppeling

Privacy heeft vanuit het psychologisch[71] perspectief gezien betrekking op enerzijds het niet binnendringen in iemands levenssfeer (iemand met rust laten en als individu gevrijwaard zijn van een niet door hem toegestane inmenging in zijn persoonlijke leven) en anderzijds betrekking op het zichzelf buitensluiten (alleen willen zijn) en het hebben van de keuze vrijheid een eigen leven te (kunnen) leiden. Belotti & Sellen stellen dat individuen controle en terugkoppeling over persoonsgegevens dienen te hebben. Informatiesystemen dienen zo ingericht te zijn dat ze "empowering people to stipulate what information they project and who can get hold of it".[72]

Deze beginselen leiden tot een geheel van gedragsregels geldend tussen het individu en de omgeving rondom het individu wat betreft de manier waarop met zijn persoonlijke informatie wordt omgegaan. Het probleem waar het individu voortdurend tegen aanloopt betreft de verificatiemogelijkheid van het individu met betrekking tot de verspreiding en het gebruik van zijn persoonlijke informatie. De behoefte aan controle en verificatie van het individu is direct gerelateerd aan zijn gevoel van het vertrouwen in de ander. Overkleeft wijst erop dat zelfs al is de gegevensverwerking observeerbaar, dit nog niet inhoudt dat de controle op de verwerkingsprocessen geen moeilijkheden met zich meebrengt. Met name twee eigenschappen van informatie veroorzaken nog al wat moeilijkheden indien men

71 Regan, 1995.
72 Belloti & Sellen, 1993, p. 3.

wil bewijzen dat er onrechtmatige informatie overdracht heeft plaatsgevonden. Overkleeft schrijft: "Deze eigenschappen zijn:
- Het overnemen van informatie tast de oorspronkelijke informatie niet aan. Aan deze zin is bijvoorbeeld niet te zien of u hem zojuist gelezen hebt.
- Informatie, eenmaal ontvangen, laat weinig of geen zichtbaar residu achter. Aan u is niet te zien, dat u zojuist deze zin hebt gelezen. De aanwezigheid van informatie is slechts indirect, uit acties van een systeem of uit de persoon aanwijsbaar. Bovendien is vaak uit deze acties niet exact te bepalen op basis van welke informatie zij genomen zijn".[73]

In paragraaf 4.5 komt het terugkoppelingsbeginsel als een van de mogelijkheden van beveiliging van persoonsgegevens aan de orde. In paragraaf 5.11.2 is dit beginsel vertaald in kleefbeleid (*sticky policies*) dat in gegevensbeheerssystemen ervoor kan zorgen dat conform de privacyvoorkeur van het individu de persoonsgegevens worden verwerkt.

2.4. De juridische uitwerking van de universele beginselen

De vijf universele privacybeginselen zijn uitgewerkt in wet- en regelgeving over de bescherming en verwerking van persoonsgegevens.[74] Deze uitwerking leidt tot een aantal privacyrealisatiebeginselen, waarbij afhankelijk van het rechtssysteem de uitwerking en reikwijdte van de universele privacybeginselen verschillend kan uitvallen. De privacyrealisatiebeginselen hebben ten doel het individu in staat te stellen om controle uit te oefenen over zijn persoonsgegevens ongeacht de technologische omgeving. Daarmee wordt zijn vertrouwen in de verwerking vergroot. De privacyrealisatiebeginselen bieden aan derden de mogelijkheid te toetsen of de bescherming van de persoonlijke informatie en daarmee de informationele privacy voldoende is gewaarborgd. Bovendien kan vanuit deze realisatiebeginselen het spiegelbeeld worden afgeleid, namelijk de te vervullen verplichtingen door degenen die de persoonlijke informatie verzamelen, verwerken en verspreiden. Deze beginselen kunnen, zoals in hoofdstuk 6 zal worden aangetoond, in informatiesystemen in de gegevensverwerkingsprocessen worden ingebouwd. De privacyrealisatiebeginselen liggen dan ook aan de basis van de Europese wet- en regelgeving betreffende de bescherming van persoonsgegevens.

2.4.1. Europese wet- en regelgeving

De rol van de nationale- en Europese overheden wat betreft de privacybescherming is tweezijdig en ambigu. Overheden dienen het respect voor de privacyrechten van het individu te verzekeren en anderzijds dienen zij ook de nationale en

73 Overkleeft, 1975, p. 192.
74 Borking & Raab, 2001, p. 2.

publieke veiligheid te waarborgen. Het vinden van een evenwicht tussen beide rollen is een van de kernproblemen in de ontwikkeling van een regelgevend kader op dit gebied. Een belangrijke randvoorwaarde voor het beschermen van de persoonlijke levenssfeer is het autonome respect voor de rechtsorde, dat wil zeggen dat dit respect voor de 'rule of law' de arbitraire en discretionaire bevoegdheden van de overheden inperkt. Wat betreft de bescherming van privacy zijn de overheden dan ook verplicht de internationale verdragen op dit gebied te respecteren en ernaar te handelen.[75]

Het grondrecht op privacybescherming, ook wel aangeduid als het grondrecht met betrekking tot respect voor de persoonlijke levenssfeer, is opgenomen in de European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) van 1950. Artikel 8 is de Europese basis voor privacybescherming en stelt uitdrukkelijk vast, dat de overheid het privé-, gezins- en familieleven, de woning en de correspondentie dient te respecteren, met de beperking: "unless interference is required by the law, national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health, of morals or the protection of rights and freedoms of others".

Hieruit kan geconcludeerd worden dat privacybescherming geen absoluut recht is en dus beperkingen kent in de relatie tussen overheid en burger. Omdat het geen absoluut recht is, dient er bij het toepassen van het recht op privacy altijd een belangenafweging plaats te vinden. Bij de toepassing van de in de hoofdstuk 4 te bespreken privacybedreigingsanalyse en de keuzes bij het ontwerp van privacyveilige informatiesystemen dient een dergelijke afweging dan ook plaats te vinden.

Naast de verticale werking (verhouding tussen overheid en burgers) van het privacyrecht bestaat er ook een horizontale werking. Het betreft dan de verhouding tussen burgers onderling. Dit is van belang omdat inmiddels goedkope ict-toepassingen het voor burgers mogelijk maken om bij andere burgers 'naar binnen' te kijken. Verheij stelt: "het is een historisch gegeven dat bedreigingen van grondrechten niet alleen kunnen uitgaan van de overheid, maar ook van particulieren. Het risico hierop bestaat met name bij een gezags- of afhankelijkheidsrelatie. Het bieden van weerstand tegen dergelijke bedreigingen vormt van oudsher één van de doelstellingen van grond- en mensenrechten".[76]

Het EVRM, tot stand gekomen binnen de Raad van Europa, leidde tot de oprichting van het Europese Hof voor de Rechten van de Mens dat de naleving overziet. Dit hof heeft artikel 8 met betrekking tot de in dit artikel genoemde aandachtsgebieden dikwijls extensief en wat betreft de restricties nauw geïnterpreteerd. Het hof vonniste in 1976 dat het privéleven in artikel 8 niet alleen betekent het recht op privacy, maar ook als een recht op de ontwikkeling en

75 Dumortier & Goemans, 2004, p. 191-212.
76 Verheij, 1992, p. 61.

zelfontplooiing van iemands eigen persoonlijkheid.[77] Bovendien beschouwt het Europese Hof het verzamelen, verwerken en/of opslaan van persoonsgegevens in veel gevallen als een inbreuk op het privéleven ('as an invasion into the private life sphere'). Nieuwenhuis stelt vast dat de inhoud van artikel 8 EVRM dynamisch[78] en ruim is uitgelegd. Het recht op privacy beschermt enerzijds een bepaalde handelingsvrijheid en geeft anderzijds een recht tot afscherming.[79] Ondanks artikel 8 EVRM kwam er toch Europese wetgeving om de bescherming van persoonsgegevens nader te regelen. De redenen daarvoor waren: 1 artikel 8 EVRM is niet op de particuliere sector van toepassing; 2 het recht op het privéleven omvat niet noodzakelijkerwijs alle persoonsgegevens waardoor het niet zeker was of alle gegevens wel afdoende beschermd zouden worden; 3 het recht tot inzage van de eigen gegevens werd niet afgedekt door de omschrijving van het begrip 'het recht op privéleven' in artikel 8.[80]

Twee internationale vormen van wet- en regelgeving hebben in het begin van de tachtiger jaren van de vorige eeuw een grote rol gespeeld bij het verder uitkristalliseren van het begrip informationele privacy. Dat zijn de Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[81] van de Raad van Europa (Convention 108) (1981) en de Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[82] van de Organisatie voor Economische Samenwerking en Ontwikkeling (1980). Het Explanatory Report van Convention 108[83] vermeldt hoe vanaf 1968 in de Parliamentary Assembly en het Committee of Ministers werd gepleit voor een sterke gegevensbescherming in de lidstaten van de Raad van Europa. In 1980 waren er zeven landen die wetgeving op het gebied van gegevensbescherming in het leven hadden geroepen en andere landen binnen Europa wilden dit voorbeeld volgen. De procedurele aanpak verschilde, maar er was een grote mate van overeenstemming over de doelstelling en de algemene beginselen. Het echte pijnpunt was de toenemende zorg over het grensoverschrijdende data verkeer.[84] Enerzijds waren de beleidsmakers bezorgd over het feit dat de nationale bescherming van de persoonsgegevens kon worden ontdoken door data te exporteren naar 'data havens' waar geen of minder bescherming gold. Anderzijds vreesden de beleidsmakers dat

---

77 X vs. Iceland, 5 European Commission of Human Rights 86.87 (1976): "(…) the right to establish relationships with other human beings, especially in the emotional field, for the development and fulfilment of one's own personality(…)"; Goldhaber, 2007, p. 22.
78 Nieuwenhuis, 2001, p. 114 dynamisch :'zodat reikwijdte en gewicht niet eens en voor altijd vaststaan'.
79 Dit blijkt onder meer uit de zaken: ECHRights, 26 March 1987 (case Leander vs. Sweden) application no. 9248/81; Gaskin vs. U.K., ECHR 7 juli1989 case no. 2/1988/146/200; Johansen vs. Norway ECHR 7 August 1996, ECHR 1996-III www.echr.coe.int/echr/Homepage_EN.
80 De Hert & Gutwirth, 2007, p. 2.
81 http://conventions.coe.int/Treaty/EN/Treaties/108.
82 www.oecd.org/dsti/sti/it/secur/prod/pRIV-EN.
83 Council of Europe (CoE), Explanatory Report to Convention 108. p. 8. Strasbourg 1981.
84 Borking, 1984, p. 97: de Noorse wetgeving vereiste een speciale exportvergunning voor gegevens die naar het buitenland moesten worden verzonden. In Oostenrijk diende elke bedrijf dat deed aan grensoverschrijdend dataverkeer dit ter goedkeuring voor te leggen aan de commissie belast met gegevensbescherming.

dergelijke wetgeving het internationaal gegevens- en handelsverkeer en de 'free international flow of information' zou kunnen belemmeren.[85] Teneinde de nationale wet en regelgeving te versterken en het probleem van het grensoverschrijdende data verkeer op te lossen, instrueerde in 1976 het Committee of Ministers het Committee of Experts on Data Processing om een Verdrag te ontwerpen. Het uiteindelijk gekozen model baseerde zich niet uitsluitend op het beginsel van reciprociteit tussen staten, maar op de aanvaarding van een standaard set van beginselen. Daarnaast zouden er ook speciale regels komen op het gebied van het grensoverschrijdende data verkeer en wederzijdse bijstand.[86]

De gemeenschappelijke kernbeginselen werden gedistilleerd uit eerdere resoluties van het Committee of Ministers en uit wetgeving van de lidstaten. Die beginselen waren de thans bekende regels met betrekking tot de kwaliteit van gegevens, zoals bijvoorbeeld de eerlijke en rechtmatige verzameling en verwerking van gegevens, gevoelige gegevens, beveiliging, en de rechten van het individu. Derogerende rechten werden gemodelleerd aan de hand van artikel 8 van het EVRM en regels werden opgenomen die een verbod of een beperking van het exporteren van gegevens over de grenzen van de lidstaten bevatten op grond van privacybescherming. Het bijzondere van het verdrag is dat ook niet-Europese lidstaten tot dit verdrag konden toetreden, maar het heeft niet geleid tot toetreding van de Verenigde Staten. De Convention 108 werd in de tachtiger en vroege negentiger jaren van de vorige eeuw de belangrijkste stimulans voor gegevensbescherming in geheel Europa.[87]

Tegelijkertijd met het concipiërende werk dat in de Raad van Europa plaatsvond, besprak men in de Organisation for Economic Co-operation and Development (OECD) dezelfde gegevensbescherming problemen. Bij de OECD was evenwel de insteek een andere, namelijk de primaire angst dat de verspreiding van de nationale gegevensbeschermende wetgeving het grensoverschrijdende data verkeer zou kunnen frustreren met ernstige gevolgen voor de wereldeconomie. De Verklarende Memoranda bij het Convention 108 en de OECD Richtlijnen maken duidelijk dat de twee groepen die aan de Convention 108 en de OECD aanbeveling werkten, dat in nauwe samenwerking deden. Het zal dan ook geen verbazing wekken dat de twee teksten in velerlei opzicht op elkaar lijken. Maar zoals gezegd, de OECD had bewust een andere benadering van bepaalde kwesties, waarschijnlijk omdat er een grotere niet-Europese vertegenwoordiging onder haar leden was. Het onderscheidende verschil van de OECD-benadering was dat zij zich niet zo zeer concentreerde op de geautomatiseerde verwerking van persoonsgegevens, maar eerder op het in kaart brengen en behandelen van de gevaren voor de privacy en de individuele grondrechten die inherent zijn aan het gebruik van persoonsgegevens. Desalniettemin, ondanks het verschil in de benadering,

85 Borking, 1984, p. 97.
86 Borking, 1984, p. 98.
87 Aldhouse, 2005, p. 12.

waren de kernbeginselen vrijwel gelijkluidend. Dus ook in de OECD Guidelines zijn er regels betreffende eerlijke en rechtmatige verzameling van persoonsgegevens, hun juistheid en de doeleinden van de verzameling. Data moeten actueel blijven en mogen niet worden gebruikt voor niet van tevoren bepaalde doeleinden. Bovendien moeten ze beveiligd worden en voor het individu toegankelijk worden gemaakt. Verder zijn er nog regels ten aanzien van de nationale invoering en internationale samenwerking.

Zoals gezegd liggen de privacy beginselen die opgenomen zijn in de OECD Guidelines en de Convention 108 aan de basis van de verdere Europese en internationale wet- en regelgeving. Halverwege de negentiger jaren is binnen de Europese Economische Gemeenschap (later Europese Unie) de privacyrichtlijn 95/46/EG op 24 oktober 1995 van kracht. De Richtlijn (DPD) van het Europees Parlement en de Raad betreft de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens. Op de lidstaten rust de verplichting dat zij uiterlijk op 24 oktober 1998 hun nationale wetgeving op het gebied van bescherming van persoonsgegevens moeten hebben geharmoniseerd met de Richtlijn. De burgers dienen dan eenzelfde bescherming als beoogd in de Richtlijn te hebben. De harmonisatie duurde overigens wel een stuk langer. Zo werd in Nederland pas in 2001 de wetgeving, die door de Richtlijn voorgeschreven was, ingevoerd.[88]

De Richtlijn heeft twee belangrijke doelstellingen, namelijk dat de privacyrechten van het individu EU-breed een equivalente bescherming genieten en dat de persoonsgegevens vrijelijk binnen de Gemeenschappelijke Markt van de EU kunnen worden verwerkt en elektronisch verzonden. De Richtlijn zorgt voor een juridisch generiek raamwerk. Om effectief te werken moet de inhoud van de Richtlijn worden gecomplementeerd met aanvullende implementatiemiddelen. In de Richtlijn zijn naast de rechten van het individu ook de verplichtingen van de verantwoordelijken voor de verwerking van de gegevens geregeld. De onafhankelijke toezichthoudende autoriteiten, de data protection authorities (DPA), controleren op naleving. In 1997 volgt de Richtlijn 97/66/EG, die in 2002 wordt vervangen door de e-Privacy Richtlijn 2002/58/EC (Directive on Privacy and Electronic Communications) (DPEC).[89] Deze Richtlijn vertaalt de beginselen van de DPD voor de telecommunicatiesector, waarbij de toepaste telecommunicatietechnologie niet van belang is. Toch kwamen ook hier vragen. Valt VoIP (Voice over Internet Protocol) over private netwerken[90] nu wel onder deze Richtlijn? Te meer omdat de DPEC refereert aan "available electronic communications services in public communications networks in the Community". Extra aandacht krijgt in deze Richtlijn: beveiliging, confidentialiteit, verkeersgegevens, gespecificeerde rekeningen, calling line identification, spam en bepaalde technische kenmerken en standaardisatie. In 2006 ziet ten gevolge van de 'war on terror' de Data Retentie

88 Millard, 2005, p. 79-82.
89 Richtlijn 2002/58/EG behoort tot een groep van 5 Richtlijnen die de hele telecommunicatiemarkt bestrijken.
90 Een dergelijke *Peer to Peer* (P2P) dienstverlening komt steeds meer voor.

Richtlijn 2006/24/EG[91] (DRD) het licht, waarin in afwijking van het bepaalde in 2002/58/EG het bewaren van verkeersgegevens ten behoeve van de opsporing van (potentiële) terroristen en misdadigers nader wordt geregeld.

De dispariteit tussen de privacywetgeving van de Europese Unie en de Verenigde Staten leidt na lange onderhandelingen tussen beide partijen ertoe dat tussen de EU en de VS op 26 juli 2000 de Safe Harbor Agreement wordt gesloten. Deze heeft tot doel het in artikel 25 van de Richtlijn 95/46/EG vereiste niveau van bescherming van persoonsgegevens te garanderen. Een dergelijke afspraak was nodig, omdat uit een in opdracht van de EU-Commissie uitgevoerd onderzoek was gebleken dat de Amerikaanse privacywetgeving in vergelijking met de Richtlijn 95/46/EG grote gaten vertoonde en derhalve niet de vereiste adequate bescherming bood.[92] De bepalingen in de DPD en DPEC zijn nader verklaard in vele door de Article 29 Working Party opgestelde werkdocumenten en aanbevelingen en zogenaamde Opinions. Een lijst van de relevante Opinions in het kader van dit proefschrift is achterin dit boek opgenomen.

Het begrip 'Article 29' slaat op artikel 29 van de DPD, waarin een onafhankelijke adviserende 'groep' is voorzien om, hetzij op eigen initiatief, hetzij op verzoek van een vertegenwoordiger van de nationale toezichthoudende autoriteiten (DPA), hetzij op verzoek van de Commissie met betrekking tot de kwesties rond de verwerking en bescherming van persoonsgegevens te adviseren. In deze Working Party hebben zitting een vertegenwoordiger van het toezichthoudend orgaan (DPA) in iedere lidstaat, een vertegenwoordiger van de European Data Protection Supervisor (EDPS), de voor de communautaire instellingen en organen opgerichte autoriteit op het gebied van de bescherming van persoonsgegevens en een vertegenwoordiger van de Commissie. Sinds 1997 heeft de Werkgroep meer dan 160 documenten aangenomen.[93]

Als aanvulling op de DPD, DPEC zijn er door de Europese wetgever een aantal specifieke wettelijke bepalingen aangenomen, die een aanvulling zijn op de DPD. Een voorbeeld hiervan is Artikel 8 van de Elektronische Handtekeningen Richtlijn (1999/93/EG).[94] Artikel 8 bepaalt: "1. (…) certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC. 2. (…) a certification-service-provider (…) may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject. 3. Without prejudice to the legal effect given to pseudonyms under

91 PbEG, 13 April 2006, L 105 p. 54.

92 Schwarz & Reidenberg, 1996, Testimony of Joel R. Reidenberg before the Subcommittee on Commerce, Trade and Consumer Protection, Committee on Energy and Commerce, United States House of Representatives; Hearing on the EU Data Protection Directive: Implications for the U.S. Privacy Debate March 8, 2001.

93 Alle documenten zijn beschikbaar via: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

94 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML.

national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name."

Het sprak vanzelf dat de Europese Commissie zichzelf en haar instellingen ook verbond aan de getrouwe uitvoering van de DPD. Het gevolg van deze intentie is Regulation (EC) No 45/2001.[95]

In de artikelen 7 t/m 14 van de Guidelines on the Protection of Privacy and Transborder Flows of Personal Data van de OECD[96] als in de artikelen 5,6 en 8 van de Convention 108 van de Raad van Europa[97] wordt een opsomming van de privacyrealisatiebeginselen voor gegevensbescherming gegeven. Deze beginselen zijn ter bevordering en het effectief uitoefenen van de privacybescherming geïncorporeerd en verder uitgebreid in de Richtlijn 95/46/EG (DPD).

Er kunnen elf privacyrealisatiebeginselen worden onderscheiden en in de Richtlijn 2002/58/EG (DPEC) zijn daaraan nog vier extra vereisten toegevoegd, die vanuit het individu kunnen worden gezien als verdere aanvulling op de specifieke uitoefeningsrechten van het individu met betrekking tot zijn persoonsgegevens.

Omdat het Europese Hof in Luxemburg in 1996 had uitgemaakt dat de oprichtingsverdragen van de Europese Gemeenschap het voor de Europese gemeenschap niet mogelijk maakten om tot European Convention on Human Rights toe te treden,[98] werd tijdens de Europese Raad van 3 en 4 juni 1999 in Keulen besloten een Charter of Fundamental Rights op te stellen. In dit Charter van 7 december 2000 erkennen de Europese Raad, de Europese Commissie en het Europese Parlement uitdrukkelijk: "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".[99]

De erkenning leverde dit Handvest niet de status van EU gemeenschapsrecht op. Het gevolg hiervan is, dat rechtsgedingen niet uitsluitend op grond van strijdigheid met dit Handvest kunnen worden gevoerd. Daarom was het noodzakelijk om het Handvest onderdeel te maken van de Europese Grondwet van 2004. Deze Grondwet kon nochtans na de referendumnederlagen in Frankrijk en Nederland niet worden geratificeerd. Vervolgens werd gepoogd het enigszins gewijzigde Handvest onderdeel te laten zijn van het Verdrag van Lissabon van

---

95 Regulation (EC)45/2001on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1-22.
96 www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.
97 http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
98 WP 29, Opinion 2/94 "Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms" van 28 maart 1996.
99 http://ec.europa.**eu**/justice_home/unit/charte/index_en.html.

2007. Ierland verwierp in een referendum evenwel dit Verdrag, waardoor het Verdrag niet van kracht kon worden. Het Verdrag, dat de werking van de Unie van 27 landen moet organiseren, is op Ierland na ondertussen door alle lidstaten via hun parlement geratificeerd. De Ieren hebben inmiddels op 2 oktober 2009 vóór goedkeuring van het Verdrag van Lissabon gestemd. Als laatste heeft de President van Tsjechië het Verdrag van Lissabon op 3 november 2009 ondertekend.

Gezien de wereldwijde consensus over de universele privacybeginselen is het niet verwonderlijk dat de Fair Information Practices and Principles,[100] de Safe Harbor Agreement en de APEC (Asia-Pacific Economic Cooperation) Privacy Principles dezelfde privacyrealisatiebeginselen vermelden. Evenwel zijn in het APEC voorstel van 2004 niet alle in Europa aanvaarde privacyrealisatiebeginselen opgenomen.[101] De in paragraaf 2.3 vermelde universele privacybeginselen worden wel erkend in alle verdragen, wet- of regelgeving of voorstelteksten op het gebied van de bescherming van persoonsgegevens.

2.5. Uitwerking van privacyrealisatiebeginselen

Er kunnen elf privacyrealisatiebeginselen worden onderscheiden en in de Richtlijn 2002/58/EG (DPEC) zijn daaraan nog vier extra vereisten toegevoegd, die vanuit het individu kunnen worden gezien als verdere aanvulling op de specifieke uitoefeningsrechten van het individu met betrekking tot zijn persoonsgegevens. Hieronder worden deze beginselen individueel geanalyseerd.

2.5.1. Melding van de verwerking van persoonsgegevens

Om de vraag van het individu naar het wat, wie, waar, waarom en wanneer van zijn persoonsgegevens te kunnen beantwoorden, moet de verwerking (in de ruime definitie van de Richtlijn)[102] van persoonsgegevens idealiter van tevoren door de verantwoordelijke[103] aan het individu worden gemeld.[104] In de praktijk blijkt dit vrijwel niet haalbaar. Daarom is in de wet- en regelgeving vastgelegd dat de verantwoordelijke van tevoren de verwerking van persoonsgegevens dient aan te melden bij de nationale commissie voor de bescherming van de persoonlijke levenssfeer (Data Protection Authority, DPA) van een lidstaat van de Europese Unie[105] waar de verwerking plaatsvindt. Deze verplichting is vastgelegd in

100 The Fair Information Practices zijn: 1. Accountability; 2. Identifying purposes; 3. Consent; 4. Limiting link ability; 5. Limiting collection; 6. Limiting use, disclosure and retention; 7. Data quality; 8. Safeguards; 9. Openness; 10. Individual access; 11. Challenging compliance. Beschikbaar via www.ftc.gov/reports/privacy3/fairinfo.shtm.
101 Rotenberg, 2006, p. 13-14.
102 Artikel 2b van 95/46/EG.
103 In hoofdstuk 2.7 wordt het begrip verantwoordelijke behandeld.
104 Leerentveld & Van Blarkom, 2000, p. 26-28.
105 In Nederland het College bescherming persoonsgegevens in Den Haag.

Overweging 25 en de artikelen 18,19 en 20 van 95/46/EG. De aanmelding kan ook gedaan worden bij een functionaris gegevensbescherming (privacy officer) wanneer die in de organisatie is aangesteld. Nationale wetgeving kan bepalen dat bepaalde persoonsgegevens zijn vrijgesteld van aanmelding.[106] De aanmelding dient volgens Opinion WP 8 Notification van de Article 29 Working Party als volgt te gebeuren: "the data controllers, in order to notify, must assess and describe their processing operations, define in advance what data are to be used and for which purpose. In order to perform adequately these functions and contribute to the transparency of data processing the given information must not be general but specific".

Opinion WP 8 Notification vermeldt over de bedoeling van de aanmelding: "The overall aim of notification (…)it should serve as the basis for selective monitoring of the legitimacy of processing operations by the supervisory authority."[107]

Het gevolg van de melding door de verantwoordelijke aan de nationale toezichthouder (DPA) is, dat er door de DPA een voorafgaand onderzoek ex artikel 20 van de Richtlijn 95/46/EG[108] kan plaatsvinden. De aanmeldingen worden in een centraal register bijgehouden waar aan iedereen na verzoek inlichtingen kunnen worden verstrekt over de aangemelde verwerkingen. Dit realisatiebeginsel kan onder het Openness Principle van de OECD Guidelines worden gerangschikt. In de Safe Harbor Agreement is dit geregeld in de bepalingen die de Notice en Onward Transfer regarderen. Deze bepalingen zijn ook aan het principe van openheid gerelateerd. Een privacy policy die op een website is geplaatst, is een, zij het niet altijd afdoend middel,[109] om aan het transparantiebeginsel gevolg te geven.

2.5.2. Transparantie of Openheid

Het universeel principe van vertrouwelijk en beveiligd gebruik brengt met zich mee, dat aan de betrokkene, het individu waarvan de persoonsgegevens worden verwerkt, bekend moet zijn wie zijn persoonsgegevens verwerkt, om welke redenen, met welk doel en welke procedures en technologie worden gebruikt.[110] Het maakt hierbij niet uit of de gegevens rechtstreeks of langs een andere weg zijn

106 In Nederland is dit geregeld in het Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp), *Staatsblad* 2001-250.

107 WP 29 Opinion WP 8 p. 3. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp8_en.pdf.

108 PbEG nr. L 281 van 23-11-1995, p. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

WP 29 Opinion 106 on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union (2005): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf.

109 WP 29 heeft dit duidelijk gemaakt. Zie www.europa.eu.int/commm/internal market/en/dataprot/wpdoc.

110 WP 29, Opinion WP 37, Privacy on the Internet, an Integrated EU Approach to On-line Data Protection, Brussels, 2000.

verkregen. In de DPD is dit vereiste op veel plaatsen vastgelegd.[111] In de OECD Guidelines kan het beginsel van transparantie ook gelezen worden in het Individual Participation Principle. In de Safe Harbor Agreement is het transparantiebeginsel vastgelegd in de artikelen die zich met toegang en keuze bezighouden. In de Fair Information Principles wordt de openheid bevorderd door het recht van Access, Inspection, Review en Amendment. Een specifiek probleem betreft de transparantie van websites. Op de websites wordt vaak informatie in 'privacy statements' verstrekt over hoe de eigenaar van de website met persoonsgegevens omgaat. Het is dan van belang of de privacy mededeling voldoende en duidelijke informatie geeft, met name over het gebruik van cookies en de verwerking van IP-adressen. In hoofdstuk 6 wordt ingegaan op 'cookies' en 'IP-adressen'.

Een 'carte blanche' mededeling als: "By clicking on the xyz button, you are agreeing to the provisions of our privacy policy" is niet voldoende om de instemming van de bezoeker met het privacy beleid van de eigenaar van de website aan te nemen. Een dergelijke mededeling dient vervangen te worden door: "Please read our privacy policy before clicking on button xyz". Op sommige websites worden 'highlight notices' (zeer algemene mededelingen over het privacy beleid) gebruikt. Daarover zegt de 'Opinion 100 on more harmonized information' op pagina 8: "The Working Party (…) endorses the principle that a fair processing notice does not need to be contained in a single document. Instead – so long as the sum total meets legal requirements – there could be up to three layers of information provided to individuals."[112]

2.5.3. Toestemming

De universele privacy beginselen betreffende het niet vrijgeven van persoonlijke informatie en de gecontroleerde verspreiding, impliceert dat een vrije, ondubbelzinnige en specifieke toestemming van het individu is vereist voor de verzameling, het gebruik, de verwerking, de openbaarmaking en de verspreiding van zijn persoonlijke informatie. Het toestemmingsvereiste is geregeld in Artikel 7 van 95/46/EG. Artikel 13 van 95/46/EG bevat uitzonderingen en beperkingen hierop. De toestemming kan op een later moment weer worden ingetrokken. Als er geen sprake is van een vrije wilsuiting, dan is iedere gegeven toestemming ongeldig, dus nietig en/of vernietigbaar. Omdat de toestemming gegeven moet zijn met betrekking tot een specifiek verwerkingsdoel en specifieke data, is een generiek gegeven toestemming niet geldig. De toestemming moet in beginsel iedere keer gegeven worden. Hoe gevoeliger de persoonlijke gegevens (IK BEN data), hoe zwaarder het vereiste van toestemming. Dat blijkt uit artikel 8 van 95/46/EG. In de

111 Overweging 25 en de artikelen 6(1) (a), 10 a, b, c, f, 11 sub 1 a, b, c, 11 sub 2, 13 sub 1 a, c, d, e, f, g, 13 sub 2 van 95/46/EG en 5(3) van de Richtlijn 2002/58/EG.

112 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

OECD Guidelines is het toestemmingsvereiste het gevolg van het Collection Limitation beginsel.

De Article 29 Working Party heeft in een aantal Opinions het toestemmingsvereiste verder uitgewerkt. Bijvoorbeeld in Opinion WP 114 Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC[113] bij het elektronisch verzenden van persoonsgegevens naar landen buiten de EU en EEA; in WP 160 – Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) betreffende de toestemming van minderjarigen[114] en wat betreft het toestemmingsvereiste in de context van arbeidsverhoudingen in WP 48 – Opinion 8/2001 on the processing of personal data in the employment context.[115]

Wat betreft het toestemmingsvereiste bij de telecommunicatiediensten vermeldt Overweging 17 van Richtlijn 2002/58/EG: "In deze richtlijn dient 'toestemming van een gebruiker of abonnee', ongeacht of deze laatste een natuurlijke of rechtspersoon is, dezelfde betekenis te hebben als 'toestemming van de betrokkene' zoals gedefinieerd en nader bepaald in Richtlijn 95/46/EG. Toestemming kan worden gegeven op elke wijze die de gebruiker in staat stelt vrijelijk een specifieke en geïnformeerde indicatie te geven omtrent zijn wensen, onder andere door bij een bezoek aan een internet website op een vakje te klikken".

2.5.4. Rechtmatige verwerking van persoonsgegevens

De rechtmatige verwerking van persoonsgegevens is geregeld in het tweede hoofdstuk van de Richtlijn 95/46/EG, in de artikelen 6, 7, 8 en de Overwegingen 30-32.

De verzameling, verwerking en verspreiding van persoonlijke informatie (persoonsgegevens) mag slechts plaatsvinden op basis van toestemming van het individu en dient eerlijk en rechtmatig te zijn en zich te beperken tot het opgegeven doel van de verwerking. Van een rechtmatige verwerking van persoonsgegevens is ex artikel 7 van de DPD sprake in de volgende gevallen:

a. De betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend.
b. De verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene.
c. De verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is.
d. De verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene.
e. De verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan

113 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf, p. 10-12.
114 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf.
115 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48_en.pdf.

de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, drager is opgedragen.

f. De verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van artikel 1, lid 1, van deze richtlijn, niet prevaleren.[116]

De in artikel 7 gebruikte begrippen hebben geleid tot uitvoerig commentaar van de Article 29 Working Party in verschillende Opinions. Zonder uitputtend te willen zijn volgen hieronder een aantal interessante uitspraken. Wat betreft de verwerking op grond van een wettelijke verplichting merkt de Article 29 Working Party in haar Opinion WP 158 – Working Document 1/2009 on pre-trial discovery for cross border civil litigation[117] over wettelijke verplichtingen die het gevolg zijn van wetten in landen buiten de EU of EEA op: "An obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate."[118] Voor specifieke en gevoelige (bijzondere) gegevens, zoals bijvoorbeeld medische gegevens, godsdienst, filosofische overtuiging, ras, strafrechtelijke persoonsgegevens, politieke opvattingen, seksuele geaardheid, lidmaatschap van een vakbond, gegevens over antisociaal gedrag e.d., gelden striktere voorwaarden, zoals het vereiste van uitdrukkelijke toestemming of er kan zelfs een wettelijk verbod gelden.

De Article 29 Working Party geeft in haar Opinion WP 131 – Working Document on the processing of personal data relating to health in electronic health records (EHR), op pagina 9 het commentaar dat: "In contrast to the provisions of Article 7 of the Directive, consent in the case of sensitive personal data […] must be explicit. Opt-out solutions will not meet the requirement of being 'explicit'. In accordance with the general definition that consent presupposes a declaration of intent, explicitness must relate, in particular, to the sensitivity of the data. The data subject must be aware that he is renouncing special protection. Written consent is, however, not required".[119]

Wat als verwerking ter vrijwaring van een vitaal belang van de betrokkene moet worden verstaan stelt de Article 29 Working Party op pagina 9 in haar Opinion WP 131 – Working Document on the processing of personal data relating to health in electronic health records (EHR): "The processing of sensitive personal data can be justified if it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.

116 Artikel 7, sub f opent de mogelijkheid tot een flexibele interpretatie.
117 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.
118 Kuner, 2007, p. 244.
119 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.

The processing must relate to essential individual interests of the data subject or of another person and it must – in the medical context – be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions.

Accordingly, this exception could be applied only to a small number of cases of treatment and could not be used at all to justify processing personal medical data for purposes other than treatment of the data subject such as, for example, to carry out general medical research that will not yield results until some time in the future."[120]

In de Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data van de Raad van Europa (28-1-1981) is dit beginsel vermeld in artikel 5 en in de OECD Guidelines in het Collection Limitation beginsel.

2.5.5. Finaliteit en Doelbinding[121]

Dit beginsel betreft de verzameling van data. Persoonsgegevens mogen slechts worden verzameld voor vooraf bepaalde specifieke, expliciete en gerechtvaardigde doeleinden en niet verder verwerkt worden op een manier die niet strookt met die doeleinden. Met andere woorden, als er geen vooraf bepaalde gerechtvaardigde doeleinden aanwezig zijn om de persoonsgegevens te verwerken, dan mogen die gegevens niet verzameld en verwerkt worden en moet de persoonlijke informatie en de identiteit van het desbetreffende individu anoniem blijven. Onder dit beginsel valt ook het bewaren van persoonsgegevens. De termijn daarvan mag niet langer zijn dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor deze gegevens zijn verzameld en verwerkt.[122] Ook dit beginsel heeft veel tongen losgemaakt. De Article 29 Working Party heeft zich hier ook niet onbetuigd gelaten. Over proportionaliteit (artikel 6 (1) (c)) was haar commentaar:

"In WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes: […] processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Combined, these […] rules are sometimes referred to as the 'proportionality principle'."[123]

In WP 55 – Working document on the surveillance of electronic communications in the workplace: "This principle requires that personal data including those involved in monitoring must be adequate, relevant and not excessive with regard

120 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.
121 Artikel 6.1. b en e van 95/46/EG; bij gebrek aan legitimiteit zie ook artikel 7 van die richtlijn.
122 Leerentveld & Van Blarkom, 2000, p. 31.
123 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf, p. 9.

to achieving the purpose specified. The company policy in this area should be tailor made according to the type and the degree of risk, which the particular company faces.

The proportionality principle therefore rules out blanket monitoring of individual e-mails and Internet use of all staff other than where necessary for the purpose of ensuring the security of the system where the objective identified can be achieved in a less intrusive way the employer should consider this option (for example, he/she should avoid systems that monitor automatically and continuously)."

Het hierboven besproken beginsel is ook terug te vinden in het Purpose Specification beginsel in de OECD Guidelines. Ook op dit realisatiebeginsel zijn uitzonderingen, waarop ik later terugkom.

2.5.6. Gegevensminimalisering

Dit realisatiebeginsel is gebaseerd op Artikel 6(1)c en e van 95/46/EG en Artikel 6 en 14(3) van 2002/58/EG en zorgt er voor om de verzameling, verwerking en verspreiding van persoonlijke informatie binnen de perken te houden. Het vereist dat de verzameling van persoonlijke informatie tot een strikt minimum moet worden beperkt. Er mag niet meer worden verzameld en verwerkt dan strikt noodzakelijk is voor de realisering van het doel waarvoor de persoonsgegevens zijn bestemd. Het concept gegevensbeperking en minimalisering wordt niet uitdrukkelijk vermeld in Richtlijn 95/46/EG, maar het kan uit artikel 6 (b), (c), (e) en artikel 7 (b) – (f) worden gelezen uit de woorden: "(…)toereikend, ter zake dienend en niet bovenmatig" en "(…) verwerking van persoonsgegevens slechts mag geschieden (…)". Het is nauw verwant aan het principe van proportionaliteit, maar reikt verder dan proportionaliteit door het idee van gegevensminimalisatie in te zetten om hardware en software op een zodanige manier te ontwerpen dat zo min mogelijk persoonsgegevens worden verwerkt.

Dit beginsel houdt ook in, dat de identificatie van het individu niet langer mag duren dan overeenkomstig de doeleinden van de verwerking noodzakelijk is.

Dit principe heeft grote gevolgen voor het ontwerp en de inrichting van informatiesystemen, waarbij de identificatie, observering en traceerbaarheid van het desbetreffende individu zoveel mogelijk wordt beperkt, zoals ik zal onderbouwen in hoofdstuk 5 en 6. Een bijkomend voordeel is dat gegevens die niet zijn vastgelegd ook niet beschermd of beveiligd behoeven te worden. Bovendien daalt de kans op vervuiling van persoonsgegevens door gegevensminimalisering.

Voorbeelden van gegevensminimalisering zijn:

1. Wanneer een gebruiker van een informatiesysteem wel persoonsgegevens nodig heeft, maar niet noodzakelijk de identificerende gegevens, dan kan een aantal identificerende gegevens worden verwijderd. Een andere oplossing is om een deel van de gegevens van een veld te verwijderen, bijvoorbeeld de laatste drie cijfers van de postcode, waardoor het unieke adres onbekend blijft,

maar de ontvanger van de persoonlijke informatie wel een indicatie heeft van de buurt.

1. Wanneer wel de complete gegevensverzameling noodzakelijk is, maar niet de exacte waarde van een veld, kan volstaan worden met het categoriseren van de gegevens. Wil een gebruiker bijvoorbeeld weten of een persoon meerderjarig is, dan geeft de applicatie niet de leeftijd of de geboortedatum, maar alleen de mogelijkheid van ja of nee op de vraag: bent u 18 jaar of ouder? Door ja of nee te laten kiezen als antwoord, weet de steller van de vraag niet de exacte leeftijd van de persoon in kwestie, wel dat hij voldoet aan de criteria als voor de aangeboden dienst meerderjarigheid vereist is. Wanneer de gebruiker niet de exacte waarde van een veld hoeft te weten, kan ook de bandbreedte van de vastgelegde gegevens worden vergroot. Bij de leeftijd kan bijvoorbeeld een willekeurig getal worden opgeteld.[124]

Een aantal gecombineerde minimaliseringstechnieken lijkt op het volledig anoniem verwerken van gegevens, maar dit is echter niet het geval. Anonimisering en pseudonimisering zullen in hoofdstuk 5 en 6 worden besproken.

Niet alleen in Nederland in artikel 13 Wbp,[125] maar ook in andere lidstaten van de Europese Unie wordt gegevensminimalisering bevorderd. In Duitsland wordt in artikel 3 (7) van de Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung[126] gesproken over de depersonalisering van persoonsgegevens waardoor deze niet meer toegerekend kunnen worden aan een geïdentificeerd of identificeerbaar individu. In de Teledienstedatenschutzgesetz[127] gaat de wetgeving veel verder en worden de rechtsregels directe aanwijzingen voor de ontwerpers van de architectuur.

Zo wordt in artikel 4 (3) bepaald dat de aanbieder van diensten door middel van technische en organisatorische voorzieningen er voor moet zorgen, dat de gebruiker de mogelijkheid geboden wordt om anoniem de teledienst te kunnen gebruiken en overeenkomstig Artikel 4 (6) onder een pseudoniem daarvoor moet kunnen betalen. In artikel 4 (4) wordt gescheiden verwerking voorgeschreven (die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden können) en mogen profielen van gebruikers worden gemaakt, mits voorzien van een pseudoniem. Bij *retrieval* van de gepseudonimiseerde profielen mogen de data niet worden gecombineerd met de data die gerelateerd zijn aan de houder van die data. “Nutzerprofile nach § 6 Abs. 3 nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden können”.

---

124 Koorn e.a, 2004, p. 28.
125 Zie paragraaf 4.6 en paragraaf 5.1.
126 Wet van 20 december 1990 (BGBl.I 1990 S.2954), geamendeerd bij de wet van 14 september 1994 (BGBl. I S. 2325).
127 Wet van 22 juli 1997 (BGBl. I, S. 1870), laatstelijk veranderd in verband met wijziging van artikel 3 van Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG) van 14 december 2001 (BGBl. I, S. 3721).

In Slowakije wordt gegevensminimalisatie door middel van pseudonimisering en anonimisering in artikel 6(3)b van de Wet op de bescherming van persoonsgegevens[128] als geoorloofde middelen van bescherming genoemd en in Spaanse privacy wet wordt in artikel 11 (6) bepaald, dat wanneer een depersonalisatieprocedure is toegepast, de voorafgaande leden (over het geven van toestemming voor het verder verspreiden van persoonsgegevens) niet van toepassing zijn.

De Commissie van de Europese Unie bevordert gegevensminimalisatie en constateert dat:[129] "This legislation lays down several substantive provisions imposing obligations on data controllers and recognizing rights of data subjects. It also prescribes sanctions and appropriate remedies in cases of breach and establishes enforcement mechanisms to make them effective. This system may prove insufficient when personal data is disseminated worldwide through ICT networks and the processing of data crosses several jurisdictions, often outside the EU, (…) A further step to pursue the aim of the legal framework, whose objective is to **minimize the processing of personal data** and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs – that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult."

Met 'this system' wordt bedoeld de Richtlijnen 95/46/EG, 2002/58/EG en de Verordening (EC) 45/2001, betreffende de verwerking van persoonsgegevens door de communautaire instellingen en organen.[130]

2.5.7. Verzet

Dit realisatiebeginsel is terug te voeren op het in 2.3.3 besproken beginsel van gecontroleerde verspreiding. Verzet is geregeld in artikel 14b van 95/46/EG en voor geautomatiseerde besluiten zie Artikel 15.1 van 95/46/EG. De Richtlijn 95/46/EG kent aan het individu het recht toe om bezwaar te maken tegen de verzameling en verwerking van zijn persoonsgegevens in verband met persoonlijke omstandigheden (relatief verzet) en bij direct marketing (absoluut verzet). Van alle in dit hoofdstuk vermelde wet- en regelgeving, kent alleen de DPD zo'n duidelijk verzetsrecht voor het desbetreffende individu. Deze Richtlijn beschermt de betrokkene vooral bij direct marketing door een opt-in handeling van het individu te vereisen. Komt die niet, dan mogen de verkregen data niet worden gebruikt. Mocht de verzameling via een website plaats vinden dan mag een 'just-in-time-click-through agreement' worden aangewend voor het vastleggen van de toestemming voor het gebruik binnen het opgegeven doel van de

128 Wet nr. 52/1998 Coll. Op 1 September 2002 treedt deze wet in werking door middel van de Wet nr. 428/2002 Coll.

129 Communication From The Commission To The European Parliament And The Council On Promoting Data Protection By Privacy Enhancing Technologies (PETs), COM (2007) 228 Final, Brussels, 2.5.2007.

130 OJ L 8 van 12-1-2001, p. 1.

direct marketing.[131] Het individu heeft eveneens de mogelijkheid verzet aan te tekenen tegen het feit dat hij onderworpen is aan een besluit, waaraan voor hem rechtsgevolgen zijn verbonden. Het gaat dan om een besluit dat het gevolg is van een geautomatiseerde beslissing (bijvoorbeeld door data mining), die aspecten van zijn persoonlijk leven betreffen.

Wat betreft het recht tot verzet bij direct marketing ziet het er naar uit dat artikel 13(4) in Richtlijn 2002/58/EG zal worden gewijzigd. Dit en andere wijzigingsvoorstellen zijn in behandeling bij het Europese Parlement.[132]

De wijzigingstekst luidt: "In any event, the practice of sending electronic mail for the purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or in contravention of Article 6 of Directive 2000/31/EC (richtlijn inzake elektronische handel),[133] or without a valid address to which the recipient may send a request that such communications cease, or encouraging recipients to visit websites that contravene Article 6 of Directive 2000/31/EC, shall be prohibited". Er is ook een nieuw lid 6 van artikel 13 voorgesteld met de tekst: "Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article."[134]

2.5.8. Kwaliteit van gegevens

Dit vereiste geregeld in Artikel 6 (d), zie ook artikel 15 van 95/46/EG, houdt in dat de verwerking van persoonsgegevens moet voldoen aan kwaliteitsnormen. Kwaliteit betekent dat persoonsgegevens correct, accuraat, toereikend, ter zake dienend en niet bovenmatig in relatie tot de doeleinden waarvoor de data wordt verzameld en vervolgens wordt verwerkt. Bovendien dient er met de volgende zaken rekening gehouden te worden: 1 bewaartermijnen; 2 het gebruik van diacrieten (bijzondere tekens); 3 periodieke opschoning; 4 nformeren over het iverstrekken van gecorrigeerde gegevens aan derden aan wie die gegevens zijn

131 Van Blarkom, Borking & Olk, 2003, p. 256.
132 Kuner, 2007, p. 308.
133 PbEG 2000, L 178/1.
134 Article 29 Working Party WP 159 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf.

verstrekt; 5 eindcontrole bij geautomatiseerde beslissingen en 6 juistheids-, volledigheids- en autorisatiecontroles bij ingevoerde gegevens.

2.5.9. Rechten van het Individu

Conform het bepaalde in Artikel 12 van 95/46/EG worden de informatierechten van het individu geregeld in de artikelen 10 en 11 en in artikel 14b (verzet). Personen over wie gegevens worden verzameld, verwerkt of opgeslagen, hebben het recht om hun persoonsgegevens in te zien, te verbeteren, aan te vullen, te verwijderen of af te schermen. Uit het bepaalde in artikel 10 en 11 van de DPD volgt dat er een onderscheid kan worden gemaakt tussen informatierechten en –plichten wanneer de gegevens van het individu direct worden verkregen en wanneer de gegevens over het individu niet zijn verkregen van hemzelf. Essentieel is informatie over de identiteit van de verantwoordelijke (zie paragraaf 2.7) en het doel van de gegevensverwerking. Daarnaast de ontvanger van de persoonsgegevens bekend te zijn en dient duidelijk te zijn op welke wijze de betrokkene toegang heeft tot zijn gegevens en hoe hij deze kan rectificeren.

Holvast merkt hierover op dat: “als onderdeel van het inzagerecht heeft de betrokkene het recht te allen tijde op zijn verzoek van de logica op de hoogte te worden gesteld indien gebruik wordt gemaakt van bijzondere computerprogrammatuur. De bekendmaking van de logica, zo stelt de Europese Richtlijn,[135] mag geen afbreuk doen aan het zakengeheim of aan het intellectuele eigendom en met name aan het auteursrecht dat de software beschermt. Dit mag er echter niet toe leiden dat alle informatie wordt geweigerd.”[136] De verplichtingen die voortvloeien uit Richtlijn DPEC, te weten artikel 4, beveiliging, artikel 5 vertrouwelijkheid van de communicatie, artikel 6 de verkeersgegevens, artikel 9 de locatiegegevens en artikel 13 de ongewenste communicatie (Spam), kunnen ook gezien worden als rechten die aan het individu toekomen. In Opinion WP 105 – Working document on data protection issues related to RFID technology van de Article 29 Working Party – wordt veel aandacht besteed aan de rechten van het individu. De verantwoordelijke dient de volgende informatie te verstrekken: “Pursuant to Article 10 of the data protection Directive data controllers processing information through RFID technology must provide the following information to data subjects: identity of the controller, the purposes of the processing as well as, among others, information on the recipients of the data and the existence of a right of access (…) In addition, depending on the specific use of RFID, the data controller will also have to inform individuals about: (v) how to discard, disable or remove tags from the products, thus preventing them from disclosing further information and (vi) how to exercise the right of access to information.”[137]

---

135 Richtlijn 95/46/EG, PbEG, L 281/31-50, Overweging 41.
136 Holvast, 2002, p. 7.
137 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf, p.10.

Afhankelijk van de toepassing van de RFID dient door de verantwoordelijke aanvullende informatie aan het individu worden gegeven. De Opinion 105 wijst er ook op dat artikel 12 van de DPD het individu de mogelijkheid geeft om de nauwkeurigheid van de gegevens te controleren en zich ervan te vergewissen dat zijn persoonsgegevens regelmatig worden bijgehouden, zodat zijn gegevens een juist beeld over hem verschaffen. Het recht van inzage, verbetering, aanvulling en verwijdering van het individu geldt dan ook onverkort voor de verwerking van persoonsgegevens door middel van RFID-technologie.[138]

2.5.10. Beveiliging

Beveiliging van persoonsgegevens is geregeld in Artikel 17 van 95/46/EG en artikel 4 van 2002/58/EG. Het universele principe van vertrouwelijk en beveiligd gebruik vereist het treffen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Het is een van de hoekstenen van de Richtlijn 95/46/EG om de informationele privacy van het individu te verwezenlijken. De getroffen maatregelen moeten geschikt en proportioneel zijn in relatie tot de gevoeligheid van de persoonsgegevens en de verwerking en de aard van de mogelijke privacyrisico's. Bovendien dient het de betrokkene te behoeden voor misbruik of ongeautoriseerde verspreiding en openbaarmaking. De maatregelen zijn er ook op gericht om onnodige verzameling en verwerking van persoonsgegevens te voorkomen. Bij de beoordeling of de getroffen maatregelen toereikend zijn, wordt gelet op de stand der techniek, de implementatiekosten, de risico's zowel van de verwerking als de aard en omvang van de verwerkte persoonsgegevens.[139]

Hoewel de realisatiebeginselen, die in de privacyrichtlijnen zijn vermeld, de algemene maatregelen duidelijk maken die genomen moeten worden om de informationele privacy te beschermen, is dit onvoldoende om de inbreukgevaren af te dekken. De inbreukgevaren moeten zijn onderzocht en in kaart moeten zijn gebracht voordat een informatiesysteem is gebouwd. Een privacy impact- of bedreigingsanalyse[140] is onvermijdelijk. De privacy impact- en bedreigingsanalyse en de beveiliging zullen uitgebreid in hoofdstuk 4 aan de orde komen.

De Privacy Commissioners hebben al in 1999 verklaard dat de ontwikkelaars van informatiesystemen de implicaties van het gebruik van het systeem voor de privacy van individuen in beschouwing moeten nemen en daarmee rekening moeten houden in een vroeg stadium van het systeemontwerp.[141] De Article 29 Working Party stelt in haar Opinion WP 55 Working document on the surveillance

---

138 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf, p. 12.
139 Leerentveld & Van Blarkom, 2000, p. 39.
140 Borking, 2003, p. 215-222.
141 The International Working Group on Data Protection in Telecommunications. *Common Position Adopted on Selected Emerging Global Issues.* Berlin, 29 April 1999: www.pcpd.org.hk/english/infocentre/files/garstka-paper.doc.

of electronic communications in the workplace, dat de beveiliging rekening moet houden met het proportionaliteitsbeginsel. "The proportionality principle therefore rules out blanket monitoring of individual e-mails and Internet use of all staff other than where necessary for the purpose of ensuring the security of the system where the objective identified can be achieved in a less intrusive way the employer should consider this option (for example, he/she should avoid systems that monitor automatically and continuously)."

De 'rule of law' impliceert dat overheden verplicht zijn hun bestanden te beveiligen en dat slechts bij uitzondering die beveiliging mag worden opgeheven, bijvoorbeeld in de gevallen genoemd in artikel 8 lid 2 van het Europees Verdrag voor de Rechten van de Mens.[142] De enorme groei van wetgeving ter bestrijding van misdaad en terrorisme met maatregelen die de beveiliging van gegevens opheffen, hebben tot gevolg dat het veelvuldig raadplegen van persoonsgegevens door een relatief grote groep van geautoriseerden de beveiliging van persoonsgegevens verzwakt en het vertrouwen in de privacyrespecterende overheid onder druk zet. Over de surveillance door de overheid zal in hoofdstuk 3 een analyse volgen.

De (lopende) voorstellen met betrekking tot de herziening van de Richtlijn 2002/58/EG hebben ook consequenties voor artikel 4 (beveiliging) van die Richtlijn. De tekst wordt uitgebreid met een nieuw lid en luidt:

> "Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:
> – ensure that personal data can be accessed only by authorised personnel for legally authorized purposes;
> – protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and
> – ensure the implementation of a security policy with respect to the processing of personal data.
>
> Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve."

In een nieuw artikel 4 lid 3 zal de aanbieder van telecommunicatiediensten verplicht worden om beveiligingsincidenten te melden aan de autoriteiten en de abonnee. Tijdens de eerste lezing van het voorstel tot wijziging van de Richtlijn 2002/58/EG (e-Privacy Richtlijn) in september 2008 voegden leden van het Europese Parlement aan de tekst toe: "Providers shall annually notify affected

142 "(…) in the interest of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protector of health or morals, or for the protector of the right and freedoms of others".

users of all breaches of security that have lead to the accidental or unlawful destruction, loss or alteration or the unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available communications services in the Community. National regulatory authorities shall also monitor whether companies have complied with their notification obligations under this article and impose appropriate sanctions, including publication, as appropriate, in the event of a failure to do so."[143]

De European Data Protection Supervisor (EDPS)[144] en de Article 29 Working Party[145] zijn voorstander van het feit dat de melding van de 'security breach' niet alleen geldt voor de 'electronic communication services and networks' (De telecommunicatiebedrijven en de ISPs), maar ook voor 'information society services'.[146] Het moet dan gaan om 'harm to the consumer' waarvan EDPS stelt, dat "the breach is reasonably likely to cause adverse effects to individuals".

De melding van de security breach heeft als belangrijk voordeel, zo blijkt uit een onderzoek van de School of Law van de University of California-Berkeley, dat het een stimulus geeft om geavanceerde technische beveiligingsmaatregelen te nemen zoals encryptie, en het leidt tot empirische gegevens over privacyinbreuken.[147] Door de melding van privacyincidenten zullen de cijfers over de veroorzaakte schade betrouwbaarder worden, waardoor privacyrisico's in het vervolg beter kunnen worden ingeschat door de voor de gegevensverwerking verantwoordelijken. In hoofdstuk 4 behandel ik de technische inschatting van privacyrisico's en in hoofdstuk 7 kom ik op de financiële kant van de privacyrisico's terug.

2.5.11. Verwerking door de bewerker

De bewerker moet van de verantwoordelijke (zie paragraaf 2.7) worden onderscheiden. De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. De bewerker die persoonsgegevens namens de verantwoordelijke behandelt vervult slechts een hulpfunctie met betrekking tot de verwerking van persoonsgegevens. In tegenstelling tot verantwoordelijken hoeven bewerkers niet aan de overgrote meerderheid van vereisten van de Richtlijn 95/46/EG te voldoen.

---

143 www.europarl.europa.eu/sides/get Doc.do?pubRef_//EP//TEXT + TA + P6_TA_2008_0452 + 0 + Doc + xml + Vo//En & Language_ En.

144 EDPS, second opinion on the review of Directive 2002/58/EC, Brussels 2009.

145 WP 29, Opinion 1/2009 on the proposal amending Directive 2002/58/EC on privacy and electronic communications, Brussels 2009.

146 De definitie van een information society service (ISS) in Richtlijn 98/46/EC is: "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". Daarmee dekt deze definitie vrijwel alle 'online services'.

147 Van Quathem, 2009, p. 4.

Zij moeten met inachtneming van de risico's de geëigende technische en organisatorische maatregelen ten uitvoer leggen zodat een adequate beveiliging van de gegevens is gewaarborgd. Als de verwerking van de persoonsgegevens (deels) is uitbesteed aan een bewerker, dan mag die slechts handelen in opdracht en voor rekening en risico van de verantwoordelijke. Zijn werkzaamheden dienen te zijn vastgelegd in een schriftelijke overeenkomst. In de overeenkomst dient tenminste te worden gestipuleerd, dat:

1. De bewerker slechts in opdracht van de verantwoordelijke de gegevens zal verwerken.
2. De beveiligingsverplichtingen nakomt die op de verantwoordelijke rusten ongeacht het land (binnen of buiten de Europese Unie) waar de verwerking plaatsvindt. Dit laatste is van groot belang bij outsourcing van de verwerking buiten de EU.

De Europese standaardenorganisatie CEN heeft een "Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)" opgesteld, omdat gebleken is dat verantwoordelijken niet op de hoogte bleken te zijn van de wettelijke vereisten.[148]

2.6. De vier vereisten van Richtlijn 2002/58/EG

Artikel 2 van de Richtlijn 2002/58/EG (de e-privacy richtlijn) (DPEC)[149] luidt: "Tenzij anders is bepaald, zijn de definities van Richtlijn 95/46/ EG (…) van toepassing". Als aanvulling op de rechten van het individu vastgelegd in de DPD zijn vier extra vereisten als aanvulling op de rechten van het individu in de DPEC opgenomen. Deze vereisten zijn van toepassing op:

1. het vertrouwelijk karakter van de communicatie (2.6.1);
2. verkeersgegevens (2.6.2);
3. locatiegegevens anders dan verkeersgegevens (2.6.3);
4. ongewenste communicatie (spam) (2.6.4).

2.6.1. Het vertrouwelijk karakter van de communicatie

Op grond van artikel 5 lid 1 en 2 van de Richtlijn 2002/58/EG moeten de lidstaten er voor in staan, dat de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten vertrouwelijk is en vergelijkbaar met de al eeuwenoude geheimhouding van briefwisseling. Met name wordt verboden het

148 http://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15292-00-2005-May.pdf.
149 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (*e*Privacy Directive).

afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen, indien de betrokkene daarin niet heeft toegestemd, tenzij dat bij wet is toegestaan ten behoeve van de nationale veiligheid, verdediging, openbare veiligheid en ten behoeve van het voorkomen, onderzoeken, ontdekken en vervolgen van misdrijven of om het niet toegestane gebruik van het communicatiesysteem te onderscheppen. Dit laat onverlet de technische opslag voor het overbrengen van informatie. De wijzigingsvoorstellen voor de Richtlijn houden een nieuw artikel 5 lid 3 in waarin de verplichting is opgenomen dat de gebruiker wordt ingelicht over cookies en andere in de computerterminal opgeslagen informatie en dat hij zijn toestemming heeft gegeven. De voorgestelde tekst luidt: "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his/her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

2.6.2. Verkeersgegevens

Verkeersgegevens (elk gegeven dat wordt verwerkt met betrekking tot het transport van de communicatiesignalen) met betrekking tot de communicatie van het individu worden beschouwd als persoonsgegevens. Vandaar dat in artikel 6 van de Richtlijn 2002/58/EG (DPEC) wordt voorgeschreven, dat verkeersgegevens van abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst, moeten worden gewist of anoniem gemaakt, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie. Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en elektronische betalingen, mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.

Artikel 3 van Richtlijn 2006/24/EG[150] (Data Retentie Richtlijn DRD) vereist nochtans dat voor rechtshandhaving (onder andere) verkeersgegevens voor een langere periode wordt bewaard, dan in artikel 6 van de DPEC is toegestaan. In paragraaf 2.10 zal nader op de DRD worden ingegaan. Omdat volgens Opinion 148 van de Article 29 Working Party zoekmachines niet onder de definitie van de

150 OJL 105, 13-4-2006, p. 54.

openbare elektronische communicatiedienst in de DRD vallen, is de DRD niet van toepassing op bedrijven die zoekmachines aanbieden.[151]

2.6.3. Locatiegegevens anders dan verkeersgegevens

Locatiegegevens zijn gegevens die worden verwerkt in een elektronisch communicatienetwerk om de geografische positie aan te geven waar het apparaat dat voor communicatie wordt gebruikt, zich bevindt. Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische communicatienetwerken of telecommunicatiediensten verwerkt kunnen worden, mag dit uitsluitend wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde, aldus artikel 9 van de Richtlijn. Ook deze gegevens zijn dus persoonsgegevens. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.

Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

2.6.4. Ongewenste Communicatie (Spam)

Artikel 13 maakt duidelijk dat het gebruik van automatische oproepsystemen zonder menselijke tussenkomst (automatische oproepapparaten), fax of e-mail met het oog op direct marketing alleen kan worden toegestaan met betrekking tot abonnees (de persoonsgegevens genererende individuen) die daarin vooraf (opt-in) hebben toegestemd. Dit artikel is niet alleen van toepassing op elektronische communicatiediensten, maar op elke dienstverlening die gekwalificeerd kan worden als spam. Als uitzondering op deze algemene regel blijft het voor handelaren mogelijk om e-mail naar hun eigen klanten, waarvan zij het e-mailadres hebben verkregen, te sturen in het kader van direct marketing voor dezelfde diensten en goederen die zij al bij hun klanten hebben afgezet. Dit onder de voorwaarde, dat die klanten duidelijk en expliciet de gelegenheid wordt geboden kosteloos en op gemakkelijke wijze bezwaar te maken tegen het gebruik van het e-mailadres bij

151 WP 29, Opinion 1/2008 on data protection issues related to search engines, beschikbaar via http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp148_en.pdf.

het verzamelen ervan en, ingeval de klant zich in eerste instantie niet tegen dat gebruik heeft verzet, bij elke nieuwe boodschap. In het vierde lid van artikel 13 wordt uitdrukkelijk bepaald dat het in ieder geval is verboden elektronische post met het oog op direct marketing te verzenden waarbij de identiteit van de afzender namens wie de communicatie plaatsvindt wordt gemaskeerd of verborgen of zonder dat een geldig adres wordt vermeld waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten. Andere vormen van ongewenste communicatie bijvoorbeeld door middel van sms ten behoeve van de direct marketing zijn onderworpen aan een opt-in- of opt-outregime zulks ter bepaling door de lidstaten.

2.7. De verantwoordelijke

Bij de uitoefening van de privacyrealisatiebeginselen speelt de verantwoordelijke een cruciale rol. Artikel 2(d) van de richtlijn 95/46/EG omschrijft de voor de verwerking verantwoordelijke, "als de natuurlijke- of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij nationale of communautaire wettelijke of bestuursrechtelijke bepalingen, kan in het nationale of communautaire recht worden bepaald wie de voor de verwerking verantwoordelijke is of volgens welke criteria deze wordt aangewezen".

Deze definitie is van belang voor het vaststellen wie welke verplichting draagt en wie aansprakelijk is bij onrechtmatige verwerking van persoonsgegevens. Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele inhoud van het begrip.[152] De meeste verplichtingen die in de Richtlijn 95/46/EG zijn vastgelegd, zijn bedoeld voor de verantwoordelijke. De definitie van de verantwoordelijke maakt het mogelijk dat er meer dan een verantwoordelijke is met betrekking tot de verwerking van persoonsgegevens. Als verschillende eenheden zich presenteren als medeverantwoordelijken, dan houdt dat in dat zij gezamenlijk verantwoordelijk zijn voor het voldoen aan de vereisten van de Richtlijn 95/46/EG. De verplichtingen van de verantwoordelijke worden geregeld in onder andere de artikelen 10,11,12 en 14 van de Richtlijn 95/46/EG. De verantwoordelijke moet ex artikel 16 van de Richtlijn ervoor zorgen dat de vereiste informatie aan de betrokkene in duidelijke en begrijpelijke taal geschiedt en voldoende informatie bevat om het individu zijn rechten te kunnen laten uitoefenen om toegang tot eigen gegevens te

152 MvT 25 892, II, nr. 3, p. 55; idem nr. 3, p. 16. In de publieke sector geldt het krachtens het geldende staats- en bestuursrecht bevoegde bestuursorgaan als de verantwoordelijke (MvT, II, nr. 3, p. 57).

krijgen, te kunnen rectificeren, bezwaar te maken met name wanneer de persoonsgegevens worden gebruikt voor direct marketing doeleinden. Voorts is de verantwoordelijke aansprakelijk voor de rechtmatigheid en vertrouwelijkheid van de verwerking van de persoonsgegevens, de beveiliging van de verwerking en de melding aan de toezichthouder conform de artikelen 17, 18 en 19 van de Richtlijn 95/46/EG. Artikel 23 regelt de aansprakelijkheid van de verantwoordelijke.

Tijdens de 31e International conference of data protection and privacy commissioners in Madrid is op 6 november 2009 een resolutie aangenomen waarin wordt aangedrongen de verantwoordelijke aansprakelijk te stellen als hij adequate organisatorische en technische maatregelen heeft achterwege gelaten om de verwerking van persoonsgegevens privacyveilig te laten plaatsvinden.[153] Daardoor zal de druk op de verantwoordelijke om een privacyimpact- of bedreigingsanalyse te laten uitvoeren voor dat de verwerking van persoonsgegevens plaatsvinden, toenemen.

2.8. Gegevensverkeer met landen buiten de Europese Unie

In beginsel, is de verzending van persoonsgegevens naar een land buiten de Europese Unie (EU) alleen toegestaan als dat land een vergelijkbare (adequate) bescherming biedt zoals die geldt binnen de EU, zo bepaald artikel 25 van 95/46/EG. Het verkeer van persoonsgegevens is vrij binnen de 25 lidstaten van de EU en de drie landen van de European Economic Area (EEA), Noorwegen, Liechtenstein en IJsland. De Europese Commissie kan door middel van een officiële beslissing vaststellen of een land buiten de EU en EEA een adequaat niveau van bescherming van persoonsgegevens biedt. Het gevolg van zo'n beslissing is dat daardoor persoonsgegevens van de EU en EEA landen zonder dat verantwoordelijken extra beveiligingsmaatregelen te hoeven nemen, verzonden mogen worden naar dat land.

De Commissie heeft tot nu toe een dergelijke positieve beslissing genomen over Andorra, Argentinië, Canada, Bailiwick of Guernsey, The Isle of Man, Jersey, en Israel, Zwitserland, het US Safe Harborsysteem en over de verzending van gegevens van passagiers van vliegtuigen, de zogenaamde Passenger Name Record (PNR) aan het Bureau of Customs and Border Protection van het Department of Homeland Security van de Verenigde Staten.

Op 30 mei 2006 vonniste het Europese Hof van Justitie in Luxemburg in de gezamenlijke zaken C-317/04 en C318/04 (European Parliament vs. Council) echter dat de beslissing van de Commissie over de adequate bescherming van de PNR door het Department of Homeland Security van de Verenigde Staten niet valt binnen de reikwijdte van de Richtlijn 95/46/EG en dat derhalve het hof de beslissing hierover vernietigde. Het resultaat van deze beslissing was dat de passagiersgegevens niet

153 www.privacyconference2009.org/privacyconf2009/program/index-iden-idweb.html.

meer na 30 september 2006 naar de Verenigde Staten mochten worden verzonden. Op 4 oktober werd opnieuw een tijdelijke overeenkomst tussen de EU en USA gesloten waarbij voorlopig verzending naar en gebruik van PNR door het Department of Homeland Security werd toegestaan.[154] In juli 2007 is er een nieuwe definitieve overeenkomst tussen de EU en de USA gesloten over de verzending van PNR van vliegtuigen aan Department of Homeland Security.

Artikel 25 gaf ook aanleiding tot interpretatieproblemen. In het vonnis van 6 november 2003 van het Europese Hof van Justitie in de zaak C-101/2001 (Lindqvist) oordeelt het hof in de 24e overweging: "[…] there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country".

Overeenkomstig Artikel 26 (2) van Richtlijn 95/46/EG kan een Lidstaat een elektronische doorgifte of een reeks van doorgiften van persoonsgegevens aan een land toestaan dat geen passende bescherming in de zin van Artikel 25 (2) kan bieden. De voorwaarde is dan wel dat de verantwoordelijke contractueel zich verplicht zelf te zorgen voor de adequate bescherming van de persoonsgegevens. De Europese Commissie heeft een aantal standaardclausules opgesteld die de doorgifte van persoonsgegevens mogelijk maakt. Tot dusver, keurde de EU Commissie twee verschillende sets van standaard contractuele clausules voor 'controller-to-controller transfers' en een set aanvullende standaard contractuele clausules voor 'controller-to-processor transfers' goed.[155]

2.9. De Data Retentie Richtlijn 2006/24/EG

Hiervoor is aangegeven dat het recht op privacy geen absoluut recht is en dat de overheid onder strikte voorwaarden hierop inbreuk kan maken. Specifieke wetgeving is hiervoor noodzakelijk. Opsporingsdiensten hadden in het verleden in het kader van de fraude-, misdaad- en terrorismebestrijding aangegeven, dat de verkeersgegevens niet (altijd) lang genoeg opgeslagen en/of niet (volledig) beschikbaar waren. Zij vroegen om verdergaande bevoegdheden. Door de druk vanuit de opsporingsdiensten heerste er bij de elektronische communicatiedienstenindustrie grote onduidelijkheid over wat er nu wel en niet bewaard moest worden en voor

154 SEC (2006) 1276 – 410-2006. Er moet per passagier op 34 vragen antwoord gegeven worden. Er zijn onderhandelingen tussen de EU en VS gaande die onder meer het aantal vragen terugbrengt van 34 naar negentien.

155 Commission Decision C (2004) 5271 Commission approves new standard clauses for data transfers to non-EU countries (7.1.2005). Zie voor de rapportage hierover: Commission Staff Working Document SEC (2006) 95, beschikbaar via http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

WP 29 Opinion 161 - Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp161_en.pdf.

hoelang. Bovendien was voor hen een complicerende factor de vraag welk rechtsstelsel er gold wanneer sprake was van internationale dienstverlening. Aan de andere kant van het spectrum nam de weerstand van de activistische privacybeschermers, die elke vorm van traceerbaarheid onacceptabel vonden, toe.[156] Het werd tijd voor de Europese wetgever dat er wat ging gebeuren.

De 'war on terror' en de lobby van de opsporingsdiensten zorgde voor de uiteindelijke totstandkoming van de Richtlijn 2006/24/EG (DRD).[157] De Richtlijn betreft de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of – communicatienetwerken. En passant vond ook een wijziging van Richtlijn 2002/58/EG plaats om de harmonisatie van de wetgeving van de lidstaten op dit gebied mogelijk te maken. Volgens de negende overweging van de Richtlijn is een van de dwingende redenen voor de DRD gelegen in het feit, dat gebleken is dat de bewaring van gegevens[158] een noodzakelijk en doeltreffend onderzoeksinstrument is voor de wetshandhaving in verschillende lidstaten, met name bij ernstige aangelegenheden zoals georganiseerde misdaad en terrorisme. Daarom stelt de DRD dat gedurende een bepaalde periode en onder specifieke voorwaarden de bewaarde gegevens beschikbaar dienen te zijn voor de wetshandhavingsautoriteiten. Artikel 3 van de DRD stelt onder meer de retentieverplichting van de verkeersgegevens vast. Dit artikel schuift dus artikel 6 van de Richtlijn 2002/58/EG terzijde.

Artikel 1 legt aanbieders van elektronische communicatie diensten of openbaar communicatienetwerken verplichtingen op betreffende het bewaren van bepaalde gegevens die door hen gegenereerd of verwerkt worden. Dit maakt het mogelijk dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.[159] De bewaarde gegevens kunnen ex artikel 5 zowel op rechtspersonen als natuurlijke personen betrekking hebben en betreffen:

a. gegevens die nodig zijn om de bron van een communicatie te traceren en te identificeren;
b. gegevens die nodig zijn om de bestemming van een communicatie te identificeren;
c. gegevens die nodig zijn om de datum, het tijdstip en de duur van een communicatie te bepalen;
d. gegevens die nodig zijn om het type communicatie te bepalen, onder andere de International Mobile Subscriber Identity (IMSI) en de International Mobile Equipment Identity (IMEI) van de oproepende deelnemer;
e. gegevens die nodig zijn om de communicatieapparatuur of de vermoedelijke communicatieapparatuur van de gebruikers te identificeren;

156 Beirens, 2006.
157 OJ L 105, 13-4-2006, p. 54.
158 Het betreft niet gegevens die de inhoud van de gecommuniceerde informatie betreffen, maar verkeers- en locatiegegevens, en de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren.
159 Artikel 1(1) 2006/24/EG (DRD).

f. gegevens die nodig zijn om de locatie van mobiele communicatieapparatuur te bepalen;

Volgens artikel 6 DRD dienen de hierboven genoemde categorieën gegevens gedurende ten minste zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie te worden bewaard. De lidstaten moeten uiterlijk op 15 september 2007 aan deze richtlijn voldoen.

Elke lidstaat kan de toepassing van DRD op de bewaring van gegevens in verband met internettoegang, internettelefonie en e-mailverkeer ex artikel 15 (3) DRD uitstellen voor een periode van ten hoogste 18 maanden, te rekenen vanaf 15 maart 2009.

De te bewaren gegevens betreffen niet de inhoud van het gesprek, maar het gaat om de signalen die tijdens de verbinding worden gegenereerd, gebruikt en vastgelegd en informatie verschaffen over de gebruiker, het apparaat en de geografische plaats en met wie gecommuniceerd wordt. De inhoud van het gesprek kan na rechterlijke toestemming via een tap vastgelegd en later geanalyseerd worden.[160]

De telecommunicatie-industrie en elektronische dienstverleners waren, gezien de hoge kosten van het bewaren van alle hierboven genoemde gegevens, op zijn zachtst gezegd niet erg blij met deze DRD. Zij vrezen dat 98% van alle vastgelegde gegevens spam zullen betreffen en dat door het vastleggen van de verkeersgegevens gebruikers minder of geen vertrouwen in de aangeboden diensten zouden kunnen gaan hebben. Bovendien stellen zij dat bij gebrek aan voldoende menskracht en middelen het analyseren van de opgeslagen gegevens nooit 100% nauwkeurig en volledig zou kunnen gebeuren. De onnauwkeurigheid, die hiervan het gevolg zou zijn, zou kunnen leiden tot steeds meer slachtoffers. Onschuldige burgers zullen, hoewel zij ogenschijnlijk aan de profielen van de opsporingsdiensten voldoen, ten onrechte de status van verdachte krijgen met alle gevolgen van dien.

Franken schrijft dat de maatregelen die het gevolg zijn van Richtlijn 2006/24/EG: "niet meer is dan holle retoriek. Spierballentaal van een schijnbaar krachtige overheid om de burger gerust te stellen, terwijl de maatregel niet alleen een volgens het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) ontoelaatbare inbreuk op de bescherming van de persoonlijke levenssfeer van de burger betekent, maar ook hoge kosten voor de Europese consument met zich meebrengt en buitengewoon makkelijk door iedere kwaadwillende kan worden ontlopen".[161]

Inmiddels heeft het Europese Hof van Justitie het eerste vonnis over de DRD uitgesproken. Het betreft de Zaak C-301/06 Ireland vs. Parliament and Council. Ierland stemde tegen de DRD. Ierland legde het Europese Hof van Justitie de vraag voor, of de Richtlijn 2006/24/EG niet zou moeten worden geannuleerd op grond van het feit dat Richtlijn 2006/24 niet op artikel 95 van het EG Verdrag kon worden

160 Vedder, 2007, p. 29-30.
161 Franken, Zoeken naar een druppel in de oceaan, in Donkers e.a., p. 93.

gebaseerd, aangezien de omschrijving "misdrijven op te sporen" van de DRD niet het functioneren van de interne markt betrof. Het primaire doel van de DRD was immers om misdrijven op te sporen en te berechten. Het hof besloot dat een aanzienlijk deel van de inhoud van Richtlijn 2006/24/EG voornamelijk gericht was op activiteiten van dienstverleners in de relevante sector van de interne markt. In overweging 84 en 85 oordeelt het hof: "It follows that the substantive content of Directive 2006/24 is directed essentially at the activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty. In light of that substantive content, Directive 2006/24 relates predominantly to the functioning of the internal market."

Derhalve is Richtlijn 2006/24/EG niet in strijd met artikel 95 van het EG Verdrag en het hof oordeelde in overweging 93: "(…) Directive 2006/24 had to be adopted on the basis of Article 95 EC". Het beroep van Ierland werd dienovereenkomstig verworpen en het hof veroordeelde Ierland in de kosten.[162]

2.9.1. Een zestal niet opgeloste problemen

Met de DRD zijn echter niet alle problemen voor de opsporingsdiensten opgelost. Ik signaleer er vijf:

1. Bij de virtuele aanbieders, Skype, webmail aanbieders, bedrijfse-mail, msn-verkeer, twitteren, internetcafés, en hotels is onduidelijk wie de gegevens bewaart en/of er zelfs een verplichting tot bewaren voor hen bestaat.
2. De DRD heeft ook niet de zorgen van de privacyvoorvechters weggenomen.
3. De bewaartermijn en de kostenvergoeding is variabel.
4. Het gebrek aan duidelijke grenzen voor de toegang tot de gegevens is een punt van zorg. De Article 29 Working Party heeft zich steeds op het standpunt gesteld dat de invoering van een bewaarplicht voor historische verkeersgegevens van alle burgers een zeer ingrijpende maatregel is waarvan de noodzaak onweerlegbaar dient te worden aangetoond.[163] Bovendien dient er openheid te komen over het gebruik van de opgeslagen gegevens, door de overheid te verplichten statistieken te publiceren waaruit het aantal bevragingen door de inlichtingendiensten blijkt.

Naar het oordeel van de Article 29 Working Party in haar Opinion WP 148 on data protection issues related to search engines is de DRD evenwel niet op aanbieders van zoekmachines van toepassing, want "Article 5(2) of the Data Retention Directive specifically states, that 'No data revealing the content of the communication may be retained pursuant to this Directive'" en "Search queries themselves would be considered content rather than traffic data and the Directive would therefore not justify their retention."

---

162 ECJ 10 February 2009 beschikbaar via http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-301/06.

163 CBP, 2007, p. 2.

Zoekvragen worden dus gekwalificeerd als inhoud, en niet als verkeersgegevens. Dat betekent voor de opspoorders dat er veel minder informatie kan worden gebruikt om subversieve activiteiten op te sporen. Voor Google heeft de opvatting van de Article 29 Working Party gevolgen voor haar bewaartermijnen van de zoekvragen van gebruikers. De Article 29 Working Party had kritiek geuit op het onbeperkt bewaren van de zoekgeschiedenis van gebruikers en verzocht om de bewaartermijnen aan te passen. Google maakte vervolgens in de zomer 2007 bekend dat zij de maximale bewaartermijn van de Data Retentie Richtlijn als uitgangspunt zou nemen. De tot personen herleidbare zoekgeschiedenis zou slechts achttien maanden worden bewaard. Na achttien maanden zouden de gegevens worden geanonimiseerd. De Article 29 Working Party stelde vervolgens dat de bewaartermijn van tot personen herleidbare zoekgeschiedenis slechts maximaal zes maanden mocht zijn, waarna de aanbieder ervoor moet zorgen dat de gegevens op een zodanige wijze worden geanonimiseerd, dat herleiding tot de persoon onmogelijk wordt.[164] Terecht stelde de Opinion WP 148 uitdrukkelijk dat: "Consequently, any reference to the Data Retention Directive in connection with the storage of server logs generated through the offering of a search engine service is not justified".[165] In hoofdstuk 6 zal ik bij de bespreking van de metazoekmachine Ixquick op deze problematiek verder ingaan.

5. De bewaarplicht voor communicatiegegevens is dan wel in werking getreden, maar juiste toepassing van de wet is nog ver weg. De Opta breekt zich naar eigen zeggen "het hoofd op de afbakening van de wet in de praktijk".[166] Met name de grote hoeveelheid opgeslagen gegevens die geanalyseerd moeten worden om bruikbare informatie te verkrijgen, lijkt onbeheersbaar. Stampfel, Ganster & Ilger becijferden dat als een internetserviceprovider van 500.000 gebruikers voor de duur van zes maanden internet gerelateerde data moet opslaan, dat dit dan ruim 9 gigabytes schijfruimte kost, voor e-mails is dat 624 gigabytes en voor internet-telefonie 73 gigabytes.[167] De Nederlandse markt heeft ruim vijf miljoen huishoudens die een internetverbinding hebben. Klooster, Verdonk & Associates becijferden in 2006 dat bij een bewaartijd van één jaar tenminste 365 terabytes opslagruimte nodig is,[168] dat wil zeggen de informatie in 220 Leidse universiteitsbibliotheken bij elkaar. Wordt zo de mogelijk waardevolle informatie door de grote hoeveelheid verzamelde data dan niet onbereikbare exformatie?

Van de zijde van de Information & Privacy Commissioner van het Verenigd Koninkrijk kwam scherpe kritiek over de neiging van de opsporingsdiensten alles maar te willen verzamelen en bewaren. In september 2006 publiceerde hij een studie over het huidige toezicht in de samenleving met zijn toenemend aantal

164 De Vries, 2008, p. 2.
165 WP 29, Opinion WP 148 on data protection issues related to search engines, Brussel 2008, p. 12.
166 www.sconline.nl 23 oktober 2009.
167 Stampfel, Gansterer & Ilger, 2006.
168 Verdonk, Klooster & Associates 2006.

videocamera's en de vele geavanceerde opsporingssystemen.[169] Hij is het met de experts[170] eens dat de explosieve toename van deze technische middelen een disproportioneel inbreukmakende effect op de privacy van het individu kan hebben. In hoofdstuk 3 komt dit rapport aan de orde.

Artikel 14 van de Richtlijn voorziet in een evaluatie: "No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public."

In de tweede motie-Franken constateert de Eerste Kamer bij de behandeling van de bewaarplicht in de Wijziging van de Telecommunicatiewet en de Wet op de economische delicten (WO 31.145), dat de evaluatie die in september 2010 is voorzien, zal leiden tot min of meer ingrijpende wijzigingen die tot een aanmerkelijke verlichting van de inspanningen van de met de uitvoering van de bewaarplicht belaste ondernemers kunnen leiden. De motie verzoekt de regering daarom over het bewaren van internetgegevens overleg te gaan voeren met de in Nederland gevestigde Internet Service Providers (ISP) ten einde onnodige kosten te voorkomen.[171] Franken becijfert dat voor een kleine ISP met ongeveer 2,5% marktaandeel deze provider tien storage devices (€ 7 miljoen) nodig zal hebben, waarvan de kosten doorbelast zullen worden aan de consument.[172] Het is te verwachten dat de evaluatie in 2010 ook een doorwerking zal hebben op de Richtlijnen 95/46/EG en 2002/58/EG. Dat zal weer gevolgen hebben voor het ontwerp van het privacyveilige informatiesysteem.

De Richtlijn 2006/24/EG heeft gevolgen voor de bereidheid om persoonsgegevens adequaat met privacy enhancing technologies (PET) te beschermen. De DRD is geen stimulans voor privacyveilige systemen. In een nog niet gepubliceerd onderzoek van Godel & Conlon (oktober 2009) over the economic benefits of privacy enhancing technologies wijzen zij op: "the lack of political imperative (…) limiting the deployment of PETs". De data protection authorities in de EU meenden dat op schaal van 1 (oneens) tot 5 (eens) het gebrek aan politieke drang 3,22 was, het bedrijfsleven scoorde op deze schaal 3,50 en de consumentenorganisaties waren het sterkst overtuigd dat de politieke drang (wil) vrijwel ontbrak. Zij scoorden 4,33 op deze schaal.[173]

169 Ball e.a., 2006.
170 Peissl, 2003, p. 19-24; Hosein, 2006.
171 EK 31 145, O; zie ook http://govinfo.nl/tag/dataretentie/.
172 H. Franken, 2007, p. 97.
173 Godel & Conlon 2009, p. 65.

Blijft de vraag of in de toekomst anonimiserende en pseudonomiserende technieken om persoonsgegevens te beveiligen nog wel wettelijk toelaatbaar zullen zijn na de invoering van de DRD in nationale wetgeving van de lidstaten? Temeer als er privacyveilige telecommunicatiesystemen zijn ingericht om de hoeveelheid verwerkte en opgeslagen gegevens tot een minimum te beperken.

2.10. Enige kritische kanttekeningen

Vanuit verschillende hoeken wordt regelmatig kritiek geleverd op de EU privacyrichtlijnen. Enerzijds wordt de tekst als weinig effectief, complex en te algemeen geformuleerd beschouwd. Anderzijds wordt een bureaucratische aanpak verweten. Bovendien blijken veel burgers niet op de hoogte van deze wetgeving en wordt de wetgeving en de toezichthouders hierop door anderen als een papieren tijger gezien[174]. Ten slotte menen de experts dat de wetgeving toe is aan herziening ten gevolge van de technologische ontwikkelingen van de laatste tien jaar. Hieronder wordt op bovenstaande punten ingegaan.

2.10.1. Vertrouwelijkheid is niet synoniem aan privacy

Hoewel de universele privacybeginselen in de EU algemeen er- en gekend zijn, zijn de afgelopen jaren vanuit de technologische, sociale, economische en juridische hoek de privacyrealisatiebeginselen ter discussie gesteld. Het dagelijks bewustzijn over privacy is overigens bij de 'man in the street' en in de organisatie laag. Slechts 50% van de verantwoordelijken voor de verwerking van persoonsgegevens zijn op de hoogte van de wettelijke normen. In het RAPID onderzoek in 2002 bleken bedrijven uit het midden- en klein bedrijf veel bepalingen uit de privacywetgeving niet te kennen en niet uit te voeren. Dat was in 2009 nog zo.[175] Alvorens op de kritiek op de wetgeving in te gaan, moet vastgesteld worden dat er ook veel verwarring bestaat over het begrip privacy. Uit interviews die ik in het kader van dit proefschrift had met medewerkers van internationale bedrijven in Zweden, het Verenigd Koninkrijk, Nederland en Zwitserland over de bescherming van privacy, bleek dat de er belangrijke verschillen in opvatting bestaan over de begrippen privacy, vertrouwelijkheid en beveiliging.

Privacybescherming wordt met name in de bancaire sector als een synoniem van het handhaven van de vertrouwelijkheid gezien. Banken richten hun beveiliging op het bewaren van vertrouwelijkheid in en niet specifiek op het kunnen uitoefenen van de privacy realisatiebeginselen. In de ict-industrie stelt men vaak privacy gelijk met informatiebeveiliging.

---

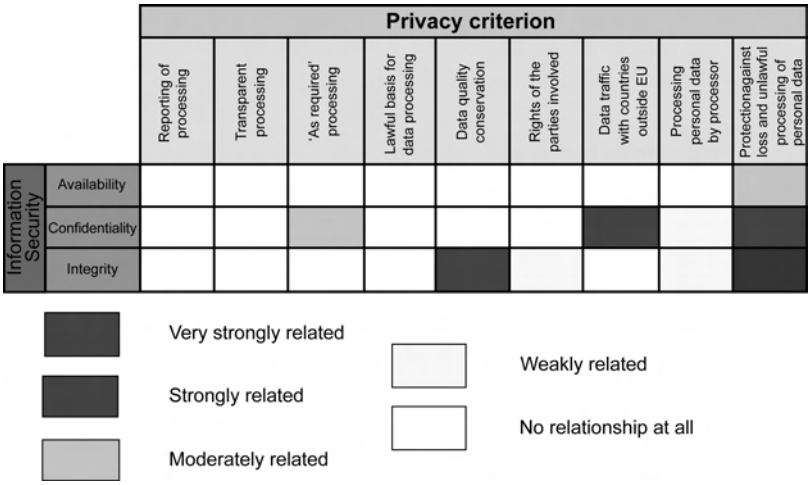
174 Kielman, 2010, p. 189-190: "De Wpolg biedt een duidelijke oplossing voor het tandeloze-tijgergehalte van het CBP (…) conclusie (…) dat controle en toezicht door het CBP tekortschieten(…)."

175 Special Eurobarometer 2003 no. 60. EU citizen views on privacy, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.

Bij vertrouwelijkheid gaat het niet over persoonsgegevens behorend tot een direct of indirect identificeerbaar persoon, maar over gegevens die geheim moeten worden gehouden of die slechts met van te voren bepaalde personen of organisaties mogen worden gedeeld. Gewoonlijk betreft het gegevens met een commerciële, technische, wetenschappelijke, militaire of octrooieerbare achtergrond die niet openbaar gemaakt mogen worden. Vertrouwelijkheid en informatiebeveiliging gaat geheel voorbij aan de rechtmatigheid van de te verwerken gegevens. Vertrouwelijkheid is één van de aspecten van informatiebeveiliging naast de andere aspecten van integriteit en beschikbaarheid waarvoor verwezen wordt naar hoofdstuk 4. Het is van belang de verschillen en overeenkomsten met de begrippen privacy, vertrouwelijkheid en beveiliging goed uit elkaar te houden. De overlapping en het verschil tussen privacy en informatiebeveiliging en vertrouwelijkheid, zijn gevisualiseerd in figuur 2.2 die is ontleend aan het PISA-project.[176]

In de horizontale kolom onder de term 'privacy criteron' worden negen privacy-realisatiebeginselen vermeld. Toestemming en verzet ontbreken. Toestemming kan onder 'lawful basis for data processing' gerangschikt worden, gegevensminimalisatie valt onder 'as required processing' en verzet is een onderdeel van 'rights of parties involved'. Deze beginselen worden afgezet tegen de in de verticale kolom vermelde begrippen 'availability' (beschikbaarheid), 'confidentiality' (vertrouwelijkheid) en 'integrity' (integriteit). Deze begrippen komen uit het domein van de informatiebeveiliging.

Figuur 2.2: Verschillen tussen privacy, confidentialiteit en beveiliging; naar een analyse in het EU PISA project 2003.



176 Borking, Giezen & Verhaar, 2001, p. 25.

Figuur 2.2 laat zich als volgt lezen. Informatiebeveiliging dekt in zijn totaliteit (meest linker verticale kolom) nergens volledig het domein van de privacybescherming. De drie velden worden met informatiebeveiliging, noch met confidentialiteit bestreken. Dat zijn de melding, de transparantie en de rechtmatige verwerking van persoonsgegevens inclusief het toestemmingsvereiste. Beschikbaarheid wordt slechts door één privacyrealisatiebeginsel redelijk gedekt, namelijk 'protection against loss and unlawful processing of personal data'.

Vertrouwelijkheid ('Confidentiality') raakt slecht vier privacyrealisatiebeginselen:

1. Doelbinding ('as required processing') in een redelijke mate.
2. In zeer sterke mate 'data traffic with countries outside EU'.
3. In lichte mate het beginsel betreffende de verwerking door de verwerker in opdracht van de verantwoordelijke ('processing personal data by processor').
4. In zeer sterke mate 'protection against loss and unlawful processing of personal data'.

Integriteit van data (integrity) heeft in meer of mindere mate ook betrekking op de vier privacy realisatiebeginselen, namelijk 'data quality conservation', 'rights of the parties involved', 'processing personal data by processor' en 'protection against loss and unlawful processing of personal data'.

2.10.2. Is de privacywetgeving effectief?

Vanuit het juridisch perspectief zijn er bij de effectiviteit van de huidige wet- en regelgeving ernstige vragen gesteld. Bovendien zijn er door allerlei 'stakeholders' initiatieven genomen om het traditionele juridische raamwerk door middel van gedragscodes, gebruikersrichtlijnen, certificering en keurmerkprogramma's, en privacystandaardisatievoorstellen, aan te vullen. Tot op de dag van vandaag is er twijfel of het individu zijn persoonlijke informatie met de wet in de hand wel goed kan beschermen. Dit geldt te meer voor zijn gegevens op internet, terwijl de gepredikte transparantie voor de meeste burgers zowel wat betreft de gegevensverzameling bij de overheid als bij het bedrijfsleven ver te zoeken is. De impact van het regelgevende kader moet verder verbeterd worden, met name voor wat betreft de bevoegdheden van de toezichthouder op de bescherming van de persoonlijke levenssfeer. Tijdens de behandeling van de Wet bescherming persoonsgegevens werd door leden van de Tweede Kamer opgemerkt dat: "in de discussie die de laatste maanden, in het bijzonder vanuit het bedrijfsleven over het wetsvoorstel wordt gevoerd, twee elementen naar voren lijken te komen: beduchtheid voor te ver gaande juridisering van de privacybescherming en beduchtheid voor een niet op de praktijk afgestemde toepassing daarvan. In dit verband wordt niet zelden gewezen op de voordelen die de ontwikkeling van elektronische producten en diensten ook voor burgers en consumenten kunnen

gaan opleveren. Een te strakke inkadering van deze ontwikkeling door wettelijke regels en toezicht zou de samenleving als geheel niet ten goede komen".[177]

Door Dumortier en Goemans[178] is dan ook de vraag gesteld of de verhouding tussen de verschillende vormen van regelgevende instrumenten en mechanismen ten behoeve van de bescherming van persoonsgegevens juist is om voldoende effect op het dagelijkse leven te verzekeren. Onderzoek[179] van de National Consumer Council in Groot Brittannië toont aan dat bijna vier van de vijf (78%) consumenten zeggen, dat zij de controle over hun persoonlijke informatie hebben verloren en niet weten hoe organisaties hun gegevens verzamelen en gebruiken. Ook het onderzoek[180] van Westin in de Verenigde Staten in 2005 bevestigt dit.

Al eerder werd door Waters twijfel geuit dat de aanpak in het Europese model met zijn bureaucratische boventoon achterhaald zou zijn.

1. In de wetgeving wordt niet rekening gehouden met de privacy binnendringende technologieën.
2. Er wordt te veel geloof te hechten aan het gezag en de effectiviteit van de nationale toezichthouders.
3. Er is een andere (culturele/sociaal-politieke geïnspireerde) visie op of andere interpretatie van de waarde van het grondrecht op privacy in vele delen van de wereld buiten Europa.[181]

Er is volgens Waters wel een politieke steun voor privacybeginselen te vinden maar die is dan niet meer dan 'broad and shallow'.[182] Zelfregulering of beter coregulering met een belangrijke rol weggelegd voor de industrie, zou een oplossing kunnen zijn omdat zo'n aanpak meer rekening zou houden met de cultuur dan nu het geval is met de van bovenaf opgelegde Europese wetgeving.

In dit kader geldt ook als kritiek, dat de partijen betrokken bij de privacybescherming (de stakeholders) niet allemaal voldoende worden ingeschakeld bij het ontwikkelen van de wet- en regelgeving.

Ook de werkgroep IPSE (Initiative on Privacy Standardization in Europe) van de Europese standaardisatie organisatie CEN in Brussel, rapporteert onvolkomenheden in de effectiviteit van de bescherming van privacy, met name op het gebied van de nakoming van de wettelijke verplichtingen en het gebrek aan bewustzijn en begrip van de privacyrechtsregels door de organisaties.[183]

---

177 Nota van wijziging inzake het voorstel voor de Wet bescherming persoonsgegevens (Tweede Kamerstukken, 1998-1999, 25 892, nr. 6 en 7).
178 Dumortier & Goemans, 2004, p. 191.
179 Lace, 2005.
180 Westin, 2005.
181 Waters, 2000, p. 3, 6.
182 Waters, 2000, p. 7.
183 IPSE final Report, On Data Protection, Brussels, 2002, www.cenorm.be/isss/Projects/DataProtection/dp.default.htm.

Tijdens de op 19 en 20 mei 2009 door de Europese Commissie georganiseerde Data Protection Conference uitten verschillende sprekers kritiek op Europese privacy richtlijnen. Zo zouden er grote verschillen zijn in de implementatie en interpretatie binnen de EU: "The rules are not technology current, ignore existing business and market realities, create administrative burdens and compliance proves to be difficult and complex."[184]

2.10.3. Een papieren tijger?

In interviews en workshops die in het kader van deze dissertatie zijn uitgevoerd, werd op de vraag of de kans op ontdekking van het overtreden van de privacywetgeving als handhavingsbevorderend werd ervaren, vaak schouderophalend af gedaan. In het interview in Zweden bij een multinational werd door de betrokken managers na discussie over een zeer ernstig privacyincident meegedeeld, dat vier jaar procederen en enige miljoenen euro's schadevergoeding verwaarloosbaar zijn in verhouding tot de schade veroorzaakt aan de reputatie van het bedrijf: "In terms of overall impact on the business, costs are not an issue since we have to fix it to earn back trust."[185]

Volgens de Richtlijn 95/46/EG is de verantwoordelijke aansprakelijk, hetgeen inhoudt dat uiteindelijk de aandeelhouders voor de boetes en schadevergoedingen opdraaien. In interviews in Nederland bij twee multinationals werd op de vraag over de aansprakelijkheid zoals die in de Richtlijn 95/46/EG is geregeld als antwoord gegeven dat het veel effectiever en afschrikwekkender werd geacht, wanneer net als in de Sarbanes-Oxley Act de verantwoordelijke manager zelf aansprakelijk wordt gesteld voor de privacy inbreuken. De Sarbanes-Oxley Act van 2002 maakt CEO's en CFO's (signing officers) persoonlijk aansprakelijk, niet alleen voor de accuraatheid van hun financiële mededelingen, maar ook, conform het bepaalde in artikel 302 lid 4(A), voor: "(…) establishing and maintaining internal controls". Als iets dergelijk voor de privacybescherming in de Wbp of Richtlijn 95/46/EG zou staan, dan zou dat veel verschil kunnen maken voor de handhaving van de privacywetgeving.[186] De privacy officer van een Nederlanse multinational deelde mee: "Sarbanes-Oxley makes a CEOs and CFOs manager personally liable. SOX only covers privacy, if the financial risk of privacy risks is going over a certain threshold. If it is going over a certain level I have to report my boss and eventually (above 10 Million Euros) it becomes a board issue. Privacy in itself is almost never raising a big financial issue under SOX. Privacy is much more a compliance issue and is a lawyer's problem. Privacy is not considered as a serious risk issue. SOX, however, is about risk issues! The Euro privacy law doesn't ask for a privacy risk analysis."[187]

---

184 Terstegge, 2009, p. 1.
185 Borking, 2008, p. 2-3.
186 Ribbers, Dijkman, & Borking, 2007, p. 6.
187 Ribbers, Tjeng, & Borking, 2008, p. 4.

Tijdens de workshop in Bristol (V.K.) bleek dat het midden- en klein bedrijf slecht op de hoogte is over de wettelijke verplichtingen tot bescherming van persoonsgegevens, laat staan over het feit dat zij aansprakelijk zou zijn: "AF (participant): There do not seem to be enough privacy intermediaries available to small businesses who don't know the laws to go ask someone what is required of me. In certain industries there are, if you're in the financial industry, the medical industry, if you've ever looked at invalids, retail or manufacturing, there's not a trade associate to turn to".[188]

Bax van het Bureau Européen des Unions de Consommateurs deelde tijdens de Data Protection Conference, die in mei 2009 door de Europese Commissie werd georganiseerd, mee dat uit onderzoek in 2008 was gebleken, dat 79% van de Europese burgers niet wisten dat zij met hun klachten over privacyincidenten bij de nationale Data Protection Authority terecht konden.[189] Bovendien rapporteerde de Eurobarometer nummer 225 betreffende gegevensbescherming in 2008, dat 63% van de Europese burgers ongerust zijn over de bescherming van hun persoonsgegevens.[190] Anderzijds klaagt men erover dat de toezichthouder (in Nederland het College Bescherming Persoonsgegevens) niet zijn tanden laat zien wanneer er publiekelijk een belangrijk privacyvraagstuk aan de orde wordt gesteld. Het duurt vaak erg lang voordat er een reactie komt. Dit blijkt bijvoorbeeld uit de eerder besproken afgifte aan de Verenigde Staten van Europese bankgegevens door SWIFT, de doorgifte van de PNR (passenger, name, record) gegevens door de luchtvaartmaatschappijen, het opslaan van de communicatiegegevens van alle Europese burgers door de nationale overheden,[191] het slecht beveiligde elektronisch patiëntendossier en de kwestie rond de onrechtmatig vertoonde videobeelden van de zoenende actrice/presentatrice Y. C. van K. en de voetballer W.S.[192] Volgens Krisch komt dit onder meer omdat "Data protection authorities have insufficient financial resources, insufficient personnel resources and a very low oversight over commercial data processing."[193]

2.10.4. Wetsaanpassing door de ontwikkeling van de technologie

Dumortier en Goemans trekken als conclusie dat de privacywet- en regelgeving gebreken vertoont en wat betreft de zich ontwikkelende informatiemaatschappij met de komst van *ambient intelligence* in de kinderschoenen staat.[194] De EU-Commissie ontkent niet dat er geen ruimte zou zijn voor verbetering en de noodzaak voor meer wetenschappelijk onderzoek om de regelgeving effectiever te maken, maar het moet

188 Fairchild & Borking, 2008, p. 6.
189 Bax, 2009, p. 5.
190 Het volledige rapport is beschikbaar op http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm.
191 Krisch, 2009, p. 6 http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm.
192 *De Volkskrant* 25 mei 2009, Liefde en Privacy, column Forum, p. 9.
193 Krisch, 2009, p. 7.
194 Dumortier & Goemans, 2004, p. 197.

uitgesloten worden geacht dat de EU-Commissie zou kunnen doen alsof het weer met een onbeschreven stuk papier nieuwe privacywetgeving zou kunnen ontwerpen, mede gezien het feit dat de lidstaten zijn gebonden aan de EVRM en Privacy Verdrag 108 van de Raad van Europa.[195]

Hustinx stelde tijdens de door de Europese Commissie georganiseerde Data Protection Conference in 2009 dat slechts een "gradual expansion of the privacy directives" mogelijk was met enerzijds minder administratieve rompslomp met name op het gebied van de melding van de verwerking van persoonsgegevens, maar anderzijds met een verplichte melding van beveiligings- en privacyincidenten en additionele eisen voor risicovolle verwerking van persoonsgegevens waaraan effectieve sancties bij overtreding zijn gekoppeld.[196]

Schermer meent dat de wetgever zich genoodzaakt zal zien om het wettelijk kader aan te passen ten gevolge van de mogelijkheden die de technologie van software agenten biedt.[197]

Poullet meent dat een derde generatie van de wetgeving ter bescherming van persoonsgegevens noodzakelijk is.[198] Deze opvatting is een gevolg van de technologische ontwikkelingen voor zowel wat betreft de privacybevorderende, als de inbreukmakende technologieën. De doorbraak van de *ambient intelligence* en het hebben van een veelvoud aan elektronische identiteiten staat voor de deur. In hoofdstuk 8 volgen hierover aanbevelingen. Toch moet, ondanks alle kritiek die er op de Europese Richtlijnen is gegeven, geconcludeerd worden dat de kritiek zich niet richt tegen de universele privacybeginselen,[199] en ook niet de privacy-realisatiebeginselen, maar tegen de bureaucratie, de traagheid van aanpassing van de wetgeving aan de technologische ontwikkelingen en het gebrek aan kennis, bevoegdheden[200] en daadkracht van de nationale toezichthouders.

2.11. Standaardisatie van privacyrealisatiebeginselen

De drie landen, die de pioniers zijn op het gebied van de wettelijke bescherming van persoonsgegevens, waren de Duitse deelstaat Hessen, Zweden en Frankrijk die tot de Romeins/Frans/Duitse rechtsfamilie horen. Hun wetgeving heeft als inspiratiebron zowel formeel als materieel als basis gediend voor de nationale en internationale wetteksten die later in andere Europese landen werden aanvaard om tenslotte uit te monden in de Richtlijn 95/46/EG. De structuur van deze richtlijn met zijn systematische aanpak en met algemeen voorschrijvende en abstracte teksten weerspiegelt de traditie van de Europese continentale rechtsfamilie en

195 Bolkenstein, presentatie tijdens de Conference on the implementation of Directive 95/46/EG Brussel, 30 september, 2002.
196 Hustinx, 2009, p. 4.
197 Schermer, 2007, p. 200-201.
198 Poullet, 2009, p. 2.
199 Terstegge, 2009, p. 2: "The concepts underlying the privacy principles still appear valid, but economic, social and technological changes will seriously challenge the existing legislation".
200 Aldhouse, 2005, www.ico.gov.uk/upload/documents/2005/dpa_conference_1.pdf.

concretiseert de algemeen aanvaarde visie van de bescherming van de persoonlijkheid zoals die al eerder in de Grondwet en in de daarvan afgeleide wetten in de verschillende Europese landen was vastgelegd.

Past deze Romeins/Frans/Germaanse rechtsaanpak van de bescherming van persoonsgegevens ook in de andere rechtsfamilies? Cottier concludeert dat in beginsel alle rechtssystemen in meer of mindere mate de idee van privacy erkennen[201] maar dat ten gevolge van politieke, culturele en religieuze gevoeligheden pas op de lange termijn wereldwijd geharmoniseerde en gelijkwaardige wetgeving kan worden bereikt. Hij meent, dat harmonisatie van privacybeschermende regels in de verschillende rechtsstelsels zou kunnen worden versneld door de wijn te verdunnen, dus door de vereisten te matigen en de Richtlijn 95/46/EG niet als absolute norm te nemen.[202]

Gegeven het feit dat in landen die privacybescherming als grondrecht onderschrijven, verschillende en afwijkende regelingen worden toegepast en de manier waarop en de mate waarin die regels worden afgedwongen, van land tot land verschillen, is het noodzakelijk in het kader van de mondialisering, internet en het kunnen toepassen van overal werkende privacyveilige informatiesystemen een wereldwijd geldende oplossing te zoeken. Terstegge stelt dat "Globalization of the digital economy requires a harmonization of various data protection frameworks around the world".[203] Het opnemen van de universele privacybeginselen en de privacyrealisatiebeginselen in ISO-standaarden,[204] zou ertoe kunnen leiden dat op termijn wereldwijd een privacyveilige gegevensuitwisseling tot stand kan komen. Door integratie van de ISO-privacystandaards in Cobit[205] of ITIL[206] zullen professionals, zoals softwareontwerpers en EDP auditors, deze standaards als professionele norm in hun werk toepassen. Door de massatoepassing van informatiesystemen, die ontworpen worden met behulp van ISO-, Cobit- of ITIL-standaards, kan deze aanpak binnen een relatieve korte tijd voor alle gebruikers een wereldwijde ingebouwde preventieve bescherming van persoonsgegevens in velerlei producten en diensten opleveren. Het onderzoek van de Technische Universiteit Dresden toont aan dat de economische gevolgen van een dergelijke standaardisatie voor ondernemingen en de maatschappij als geheel tot significante kostenvermindering leidt en het economische risico van de R&D-activiteiten (mede op het gebied van privacybescherming) van ondernemingen vermindert. Het leidt voorts tot versnelde overdracht van technologie met een positieve invloed op innovatie. Het zorgt er ook voor dat producten en diensten die niet voldoen aan de privacystandaards van de markt zullen verdwijnen.

201 Cottier, 2005, p. 10.
202 Cottier, 2005, p. 17.
203 Terstegge, 2009, p. 2.
204 Borking, 2005: www.weblaw.ch/Jusletter/Artikel.asp?/ArtikelNr=4237.
205 Control Objectives for Information and related Technology (COBIT) is een framework voor het gestructureerd inrichten en beoordelen van een IT-beheeromgeving (ITGI 1992).
206 ITIL (Information Technology Infrastructure Library) is ontwikkeld als een referentiekader voor het inrichten van de beheerprocessen binnen een ict-organisatie.

Bovendien drukt het de kosten voor de (wereldwijde) naleving van de privacywetgeving voor multinationals en lokale bedrijven. Bovendien wordt de vrijwillige naleving van de privacywetgeving versterkt door gebruik van de producten en diensten waar privacybescherming is ingebouwd.

Winn[207] bepleit ISO- en CEN-standaards als ondersteuning voor wet- en regelgeving. De Europese Commissie heeft een mandaat aan de CEN gegeven om hieraan te werken, maar de industrie blokkeert de werkzaamheden. Winn verwacht dat de ontwikkelingen rond RFID, e-invoicing en de Single Euro Payments Area (SEPA) de opstelling van de industrie noodzakelijkerwijs coöperatiever zal maken.[208] Dat standaards een belangrijke ondersteuning kunnen zijn van wetgeving, blijkt onder meer uit de Sarbanes-Oxley Act die refereert aan de ISO-standaard 17799/27001 (Information Security Management Standards) en ISO 15408 (Common Criteria for Information Technology Security Evaluation), waarover in hoofdstuk 5 meer. Binnen de ISO-organisatie vindt in werkgroep 5 van het Sub Committee 27 (ISO/IEC JTC 1/SC 27/WG 5) al voorbereidend werk plaats om privacy standaards voor identiteitmanagement en Privacy Enhancing Technologies te ontwikkelen.[209] Het ontwikkelingsproces van deze standaarden gaat traag en zal naar het zich laat aanzien zeker nog enige jaren in beslag nemen.

Een belangrijke voorwaarde voor de standaardisatie van de privacybeschermende beginselen is dat de ontwerpbeginselen voor privacyveilige systemen zijn ontwikkeld en in de praktijk bewezen hebben effectief een adequate privacybescherming waar te kunnen maken.

Technische normen zijn als zodanig niet als rechtsnormen te beschouwen. Wel kunnen zij formeel-juridische gelding krijgen bij opname of verwijziging in regelgeving. Veelal zal er geen strikt juridische dwang bestaan tot het volgen van technische normen, maar zal er een praktische dwang daartoe ontstaan; normen bezitten dan een feitelijke gelding.[210]

2.12. Invloed van persoonlijke en wettelijke beperkingen op het ontwerp van informatiesystemen

Bij het ontwerpen van een informatiesysteem dat persoonsgegevens verwerkt, dient rekening gehouden te worden met de privacy voorkeuren van het individu of met de mogelijke beperkingen die het individu kan stellen. De universele privacybeginselen houden in dat het individu naar zijn eigen inzicht kan beslissen met wie het zijn persoonlijke informatie wenst te delen. In de praktijk zal aan het

---

207 Winn, 2007, p. 5-8.
208 Winn, 2007, p. 9.
209 www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=63157&cmsareaid=63157&languageid=en.
210 Stuurman, 1995, p. 130-139: "Technische normen zijn als zodanig niet als rechtsnormen te beschouwen. Wel kunnen zij formeel-juridische gelding krijgen bij opname of verwijziging in regelgeving. (…) veelal zal er geen strikt juridische dwang bestaan tot het volgen van technische normen(…) maar zal er (…) een praktische dwang daartoe ontstaan; normen bezitten dan een feitelijke gelding. (…) een maatstaf zijn voor technisch juist handelen."

delen van de persoonlijke informatie (een set van persoonsgegevens) een aantal beperkingen en verplichtingen worden gekoppeld. Die restricties worden sterker naar mate de 'DAT BEN IK data' worden vervangen door de 'IK BEN data'.[211]

Bij analyse van het dagelijkse sociale verkeer tussen mensen onderling en tussen mensen en organisaties blijkt de uitgangpositie anonimiteit te zijn, die bij het intensiveren van de persoonlijke of zakelijke relatie steeds meer wordt vervangen door het uitwisselen of vrijgeven van persoonsgegevens.[212]

Bij het afgeven van persoonlijke informatie zullen privacyvoorkeuren of gebruiksbeperkingen gelden. De eenmaal vrijgegeven set van persoonsgegevens gaat in theorie blijvend vergezeld van de door het individu initieel aangegeven privacyvoorkeuren of gebruiksbeperkingen. Deze set van voorkeuren of beperkingen gelden bovenop de bepalingen in de wetgeving betreffende de bescherming van persoonsgegevens. Deze set van voorkeuren en beperkingen dient een van de uitgangspunten bij het ontwerp van een privacyveilig informatiesysteem te zijn. Na oplevering van het systeem kan tijdens de verwerking van persoonsgegevens rekening worden gehouden met de lijst van voorkeuren en beperkingen van het betrokken individu. In hoofdstuk 5 en 6 zal ik hierop nader ingaan. Bij het niet onderkennen van de persoonlijke privacypreferenties kunnen privacy bedreigingen ontstaan die kunnen leiden tot ongewild verlies van persoonlijke informatie aan derden en inbreuk op de persoonlijke levenssfeer.

Er zijn vijf beperkingen die het (privacybewuste individu) zou kunnen stellen:

1. Beperkingen met betrekking tot de verwerking.
Deze beperking is het gevolg van het universele privacybeginsel dat het individu slechts zijn persoonsgegevens ter beschikking van een verantwoordelijke stelt, als het doel van het gebruik van de data van tevoren is bekendgemaakt. Ander gebruik en verwerking, bijvoorbeeld in combinatie met andere persoonsgegevens van dezelfde persoon of van andere mensen of voor andere doeleinden is niet toegestaan, tenzij het individu zijn toestemming heeft gegeven dat verdere verwerking en combinatie valt binnen de applicatie die op het informatiesysteem draait. Deze set van beperkingen is vervat in de privacyrealisatiebeginselen betreffende rechtmatige verwerking van persoonsgegevens, finaliteit en doelbinding.

2. Beperkingen met betrekking tot de verspreiding.
Het individu legt met deze beperking aan de verantwoordelijke en zijn mogelijke opvolgers op waar, wanneer en naar wie de persoonsgegevens kunnen worden verspreid. Hij kan dit verbijzonderen door aan te geven dat zijn gegevens uitsluitend naar die landen mogen worden verspreid die een bepaald niveau van

211 Cfr. paragrafen 2.2.2 en 2.2.3 van dit boek.
212 Van Blarkom, Borking, & Olk, 2003, p. 147-148.

privacybescherming garanderen. Hij kan ook aangeven dat hij wil weten aan wie zijn persoonsgegevens zijn doorgegeven.

3. Beperkingen met betrekking tot de opslag.
Met deze beperking geeft het individu zijn voorkeur aan door aan de verantwoordelijke duidelijk te maken de termijn waarbinnen zijn persoonsgegevens gebruikt, verveelvoudigd en doorgegeven kunnen worden.

Dit kan in het ontwerp van het informatiesysteem zijn vastgelegd, bijvoorbeeld voor een periode, met een einddatum of gerelateerd aan een gebeurtenis. De beperking kan slaan op één gegeven of een set van gegevens van een persoon of in combinatie met andere personen. Het individu kan deze beperking uitoefenen door gebruik te maken van zijn rechten, zoals inzage, wijziging verzet e.d. (zie paragraaf 2.5.9).

4. Beperkingen met betrekking tot het gebruik van onjuiste of verouderde gegevens.
De beperking tot het gebruik van onjuiste en of verouderde gegevens kan als verplichting worden gekoppeld aan de persoonsgegevens van het individu in het informatiesysteem van verantwoordelijke en zijn mogelijke opvolgers. De verplichting kan voor de verantwoordelijke inhouden dat hij zich binnen een van tevoren vastgelegde periode (bijvoorbeeld na een jaar) vergewist van de juistheid en de volledigheid van de gegevens. De verantwoordelijke kan het individu vragen de over hem opgeslagen gegevens op juistheid en actualiteit te valideren. Als het individu zelf op de hoogte is waar zijn persoonsgegevens zich bevinden, kan hijzelf actie ondernemen om zijn gegevens te verifiëren. De verantwoordelijke en de verwerker heeft tevens de plicht het informatiesysteem zo in te richten dat het individu zijn persoonsgegevens kan inzien, wijzigen of verwijderen.

5. De beperkingen verbonden aan het beëindigen van de verwerking.
Als de verantwoordelijke en zijn mogelijke opvolgers de verwerkingsactiviteiten of de doeleinden van de verwerking van gegevens beëindigt of verandert, dan kan het individu eisen dat alle onder het begrip verwerking[213] vallende activiteiten met betrekking tot zijn persoonsgegevens wordt gestaakt. Hij kan de verantwoordelijke de verplichting opleggen, hoe de vernietiging van de persoonlijke informatie dient plaats te vinden, hoe het individu hierover wordt ingelicht en hoe met de eerder verveelvoudigde en verspreide persoonsgegevens wordt omgegaan. Helaas is het zo dat vrijwel geen enkele burger het bewustzijn heeft of de moeite neemt bij de afgifte van zijn persoonsgegevens de hiervoor vermelde vijf beperkingen aan de verantwoordelijke op te leggen.

213 Artikel 2b van de Richtlijn 95/46/EG.

Daarom dienen de privacyvoorkeuren en -beperkingen van het individu voor de afgifte van persoonsgegevens door de verantwoordelijke te worden vastgesteld en in het systeem aan de persoonsgegevens te worden gekoppeld. Dat kan inmiddels door middel van P3P, Sticky Electronic Privacy Policies, Data Tracking, en Obligation Management Systems. In hoofdstukken 5 en 6 paragrafen 5.11 t/m 5.13 en 6.4 kom ik hierop terug.

Nu alle privacyrealisatiebeginselen en de daarbij behorende EU Richtlijnen zijn besproken volgt hieronder een opsomming van juridische specificaties waarmee tenminste rekening moet worden gehouden bij het ontwerp van informatiesystemen.

2.13. Juridische Specificaties

Sommige van de privacyrealisatiebeginselen hebben een direct gevolg voor de ontwikkeling en de technische specificaties van het informatiesysteem of de applicatie (bijvoorbeeld gegevensminimalisering, transparantie, beveiliging, recht van toegang en inzage). Andere zijn meer algemeen van aard en vereisen organisatorische oplossingen die de technische specificaties aanvullen om naleving van de Richtlijn 95/46/EG te bevorderen. In de voorafgaande paragrafen van dit hoofdstuk is het positieve recht geanalyseerd om tot een antwoord op de eerste onderzoekvraag (OV 1) te komen. In een artikel[214] stelde ik gezien de complexiteit en uitgebreidheid van de wetgeving dat: "privacy rules are a horrendous challenge for developers". De ontwerper van informatiesystemen moet met heel veel zaken rekening houden.

De volgende zes juridische specificaties zijn een antwoord op onderzoeksvraag 1 (OV 1) en dienen in het ontwerp van privacyveilige systemen te worden meegenomen:

1. *Beginselen die aan de basis van een privacyveilig systeemontwerp ten grondslag liggen*:

a. Gegevensminimalisatie (waar mogelijk streven naar maximale anonimiteit, zo min mogelijk gegevens en zo vroeg mogelijke verwijdering van data).

Dit specificatieonderdeel is behandeld in paragraaf 2.5.6 en betreft de artikelen 6(1)(b, c, e) van Richtlijn 95/46/EG en 14(3) van Richtlijn 2002/58/EG.

b. Transparantie of openheid betreffende de verwerking.

Dit specificatieonderdeel is besproken in paragraaf 2.5.2 en heeft betrekking op de artikelen 6 (1)(a), 10 en 11, en Overweging 25 van de Richtlijn 95/46/EG.

c. Beveiliging aan de hand van een privacyrisico-, bedreiging- of effectanalyse. Dit specificatieonderdeel is toegelicht in paragraaf 2.5.10 en regardeert artikel 17 en overweging 46 van de Richtlijn 95/46/EG, en artikel 4 van Richtlijn 2002/58/EG.

214 Borking & Foukia, 2008.

2. *Beginselen betreffende de rechtmatige verwerking*:
De verwerking in het informatiesysteem dient zodanig te zijn ingericht dat de volgende beginselen worden gerealiseerd:
a. Rechtmatigheid (ondermeer: toestemming en doelbinding).
Dit specificatieonderdeel is behandeld in paragraaf 2.5.3 (toestemming) en 2.5.4 en betreft de artikelen 7 (a), (b)(c) (d) (e)(f) en 8 lid (2) (4) en (6) van de Richtlijn 95/46/EG.

b. Speciale categorieën persoonsgegevens.
Dit specificatieonderdeel is besproken in paragraaf 2.2.3 en betreft artikel 8 lid (2) (4) en (6) en artikel 8 (2) (a) (b) (c) (d) (e) van de Richtlijn 95/46/EG. Voor medische gegevens is artikel 8 lid 3 van toepassing; voor strafrechtelijke gegevens geldt 8 lid 5 en 6. Voor het verwerken van nationale nummers voor identificatie en andere algemene identificerende nummers gaat het om artikel 8 lid 7 van de Richtlijn 95/46/EG. Ten behoeve van de journalistiek dient met artikel 9 van de Richtlijn 95/46/EG rekening gehouden te worden.

c. Finaliteit, doelbinding van de te verwerken persoonsgegevens.
Dit specificatieonderdeel is toegelicht in paragraaf 2.5.5 betreft de artikelen 2(b) en 6 (1) (b) (e) van de Richtlijn 95/46/EG.

3. *Kwaliteit van gegevens.*
Dit specificatieonderdeel is toegelicht in paragraaf 2.5.8 en wordt geregeld in Artikel 6(d) van de Richtlijn 95/46/EG.

De volgende ontwerpvoorwaarden moeten in acht worden genomen:
a. Middelen om nauwkeurigheid en volledigheid van data te verzekeren en de mogelijkheid voor het doen van onderzoek naar data-input.
b. De duur van de opslag met waar mogelijk automatische vernietiging als de termijn is verjaard.
c. Periodieke schoning van gegevens.
d. Informatie over verbeterde gegevens aan derden aan wie deze gegevens eerder zijn overgedragen.
e. De mogelijkheid tot het nagaan van de logica achter de geautomatiseerde besluiten.
f. Maatregelen om fouten te minimaliseren of om te voorkomen dat noodzakelijke gegevensinput niet plaatsvindt en/of om fouten tijdens gegevensinput te ontdekken. Er moet in een correctieprocedure van onjuiste gegevens zijn voorzien.

4. *Rechten van het persoonsgegevens genererende individu.*
Deze specificatie is toegelicht in paragraaf 2.5.9 en wat betreft de mogelijkheid tot verzet, in paragraaf 2.5.7. Het gaat hier om de overweging 38 en de artikelen 10, 11, 12 van de Richtlijn 95/46/EG. Voor verzet is artikel 14b en 15(1) van 95/46/EG van toepassing.

Het systeemontwerp moet kunnen onderscheiden of de persoonsgegevens worden verkregen van de betrokkene, of dat de persoonsgegevens worden verkregen op een andere manier. De inrichting van het systeem dient zodanig te zijn dat voldaan wordt aan:
a. Informatie vereisten o.a. over de verantwoordelijke.
b. Melding van de verwerking van persoonsgegevens.
c. Inzage, correctie, verwijdering, blokkering.
d. Verzet tegen verwerking.

5. *Gegevensverkeer met landen*[215] buiten de EU en EEA[216].
Deze specificatie is besproken in paragraaf 2.8 en wordt geregeld in artikel 25 f van de Richtlijn 95/46/EG. De overdracht van persoonsgegevens aan een derde land (d.w.z. niet een lidstaat van de EU) is slechts toegestaan als het land in kwestie een adequate mate van bescherming biedt. Derhalve dient in het systeem de bestemming van de gegevens geverifieerd te worden en wanneer de gegevens niet verzonden mogen worden, dient de verwerking te worden geblokkeerd.

6. *Specifieke restricties op bepaalde vormen van gegevensverwerking op grond van de Richtlijn 2002/58/EG*[217] en speciale eisen uit de Richtlijn 2006/24/EG.
Deze specificatievereisten zijn besproken in paragraaf 2.6 en zijn geregeld in de Artikel 4(2), 5 lid (1), (2), (3), 6(4), 7, 8, 9, 11 en 12 van de Richtlijn 2002/58/EG.
Voorts dient het systeemontwerp rekening te houden met:
a. Verplichte informatie over beveiligingrisico's.
b. Confidentialiteit van de communicatie.
c. Het recht om informatie te ontvangen over het gebruik van *cookies* en andere informatie opgeslagen in de terminal.
d. Verwerking van verkeersgegevens en locatiegegevens (wanneer van toepassing).
e. Het recht om niet gespecificeerde rekeningen te ontvangen (wanneer van toepassing).
f. Het recht van weigering betreffende weergave van het opgeroepen en oproepende nummer (calling line en/of connected line identification) en het automatisch doorschakelen (waneer van toepassing).
g. Rechten met betrekking tot abonneelijsten. Abonnees dienen kosteloos op de hoogte te worden gesteld van de doeleinden van gedrukte of elektronische abonneelijsten die voor het publiek beschikbaar zijn voordat zij in de abonneelijst worden opgenomen. Bovendien dienen abonnees de gelegenheid te krijgen zelf te bepalen of, en zo ja welke, persoonsgegevens in een openbare abonneelijst worden opgenomen (wanneer van toepassing).

---

215 Verspreiding van gegevens naar Derde Landen: artikel 25 f van de Richtlijn 95/46/EG.
216 EEA staat voor: European Economic Area, zie hoofdstuk 2 van dit boek.
217 Artikel 3 (1) van de Richtlijn 2002/58 betreffende de toepasbaarheid. Zie ook artikel 2 van de Richtlijn 2002/21/EG. Uitzonderingsregel over toepasbaarheid zie artikel 5(3) van de Richtlijn 2002/58/EG.

Van belang hierbij is Overweging 46 van Richtlijn 95/46/EC waarin wordt gestipuleerd dat vooraf en niet achteraf met informatiebeveiliging en gegevensminimalisatie moet rekening gehouden worden: "the protection of the rights and freedoms of the individuals with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself" en Overweging 30 van Richtlijn 2002/58/EC waarin staat dat "systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum".

In hoofdstuk 6 komen de juridische specificaties weer aan de orde.

2.14. Slotbeschouwing

In dit hoofdstuk zijn de begrippen 'privacy' en 'identiteit' kort verkend en volgde een beschrijving van het (zich steeds ver uitbreidende) positieve recht, waarmee ontwerpers van informatiesystemen in hun architecturen en programmatuur rekening moeten houden. De ontwikkelingen staan niet stil. Poullet voorziet dat de ict-ontwikkelingen een derdegeneratieprivacywetgeving noodzakelijk zullen maken. Deze ontwikkeling is met de e-privacy Richtlijn 2002/58/EG en de universele diensten Richtlijn 2002/22/EG[218] in feite al in gang gezet. De structuur en de rechten die aan de gebruiker worden toegekend, wijzen daarop. De derdegeneratieprivacywetgeving zal een "increased protection of the intimate sphere beyond DP directive" met zich meebrengen.[219] In dit hoofdstuk heeft de eerste onderzoeksvraag zes juridische specificaties opgeleverd. Naast de Europese Richtlijnen die de persoonsgegevens van burgers online en offline beschermen, dient de ontwerper ook rekening te houden met de privacyvoorkeuren van het individu en de door hem gewenste beperkingen.

Ontwerpers van systemen hebben ook rekening te houden met de hoogst noodzakelijke informatiebeveiliging. Dit vereist enerzijds dat systemen beveiligd zijn tegen onrechtmatige toegang tot bijvoorbeeld elektronische dossiers, maar anderzijds moeten systemen voldoen aan de wettelijke eis tot inzage van eigen persoonsgegevens. Deze conflicterende vereisten gaan doorgaans ten koste van de transparantie en de toegang van de gebruiker tot zijn persoonsgegevens om deze in te zien, te corrigeren of te actualiseren. Voor productaansprakelijkheid lijkt zich een consensus af te gaan tekenen. Net zoals producenten van onveilige auto's aansprakelijk gesteld kunnen worden, zou dit ook voor ontwerpers van privacy onveilige informatiesystemen moeten gelden. In hoofdstuk 8 wordt hierop teruggekomen.

---

218 OJ L 108, 24.4.2002, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

219 Poullet, 2009, p. 18; Poullet, 2009 (A), p. 3.

Het is de ontwerper van systemen niet ontgaan dat in de afgelopen jaren het grondrecht van de bescherming van de persoonlijke levenssfeer steeds meer onder druk is komen te staan. Niet in het minst door dat veel apparaten inmiddels volledig digitaal werken. Ze worden ook steeds kleiner, moeilijker om met het blote oog te ontdekken en ze zijn steeds meer met elkaar, het internet of andere netwerken verbonden. Inbreuk op de grondrechten, en met name inbreuk op de bescherming van de persoonlijke levenssfeer, in de naam van de openbare veiligheid en terrorisme bestrijding staat sinds 9/11 sterk ter discussie. Politieke activiteiten ten gevolge van de "war on terror" sinds 9/11 hebben tot erosie geleid van een aantal belangrijke beschermingsmechanismen van de privacy. Wereldwijd zijn honderden antiterrorismewetten in het parlement aangenomen en geïmplementeerd.[220] Nas meent dat de privacybescherming te veel terrein zou hebben moeten prijsgegeven ten behoeve van de rechtshandhaving en openbare veiligheid.[221] Dat is op zichzelf niets nieuws. Het evenwicht tussen veiligheid en privacy is nooit statisch geweest, want in de loop van de afgelopen tientallen jaren sloeg de balans wel eens meer door naar de openbare veiligheid wanneer de samenleving met ernstige bedreigingen werd geconfronteerd.

De vraag is wel of er een ontwikkeling gaande is waarbij de burgers bereid zijn om inbreuk op hun grondrechten en met name hun privacy te accepteren in ruil voor het persoonlijk en de collectieve gevoel van veiligheid? Is er sprake van een zero sum game,[222] dat wil zeggen betekent meer openbare veiligheid minder privacybescherming en vice versa?[223] Is dit de prijs die wij met zijn allen betalen voor de zich steeds sterker ontwikkelende toezichtmaatschappij?

De vijfde stelling bij het proefschrift van Schermer[224] luidt: "Over 20 jaar bestaat geen privacy meer". Heeft Schermer gelijk? Bestaat over twintig jaar privacy nog wel?

Bovenstaande vragen hebben geleid tot onderzoeksvraag 2 (OV 2): *Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding?*

In het volgende hoofdstuk zal tweede onderzoeksvraag worden behandeld.

220 Peissl, 2003, p. 19-24; Hosein, 2006.

221 Nas, 2004; Prins, 2006, beschikbaar via www.bof.nl/docs/dwars.pdf.

222 Teepe, 2007, p. 5: "This privacy debate is widely believed to have zero-sum characteristics. The wishes of those who defend privacy are (supposedly) fundamentally incompatible with the wishes of those who give priority to fighting crime and terrorism. The thought that describes this can be summarized as 'Either you infringe everyone's privacy, or you do not catch any terrorists'".

223 Boettke, 2003, p. 155: "When we attempt to exchange our freedom for security we may in fact get neither. Ultimately, our humanity is lost".

224 Schermer, 2007.

3. De risicotoezichtsmaatschappij

"Buckle your seatbelt, Dorothy,'cause Kansas is going bye-bye!"
G. Yeffeth (Ed.), Taking the Red Pill, Science, Philosophy and Religion in The Matrix, Dallas 2003, p. 7.[1]

In dit hoofdstuk wordt een antwoord gegeven op de tweede onderzoeksvraag (OV 2): *Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding?*

In paragraaf 3.1 komt de gangbare opvatting aan de orde dat met het van kracht worden van data retentie Richtlijn 2006/24/EG (DRD) een principieel paradigma uit onze rechtsorde is omgedraaid. Iedereen is sinds de DRD a priori verdacht. Het gevolg zal zijn dat onze informationele privacy in toenemende mate zal eroderen. Het leidend adagium hierbij is 'better safe than sorry'. In paragraaf 3.2 staat de verschuiving van onze samenleving naar de risicotoezichtmaatschappij centraal ten gevolge van de digitalisering van beeld, geluid en schrift. In paragraaf 3.3 worden vijf voorbeelden van elektronische surveillance besproken die het gevolg zijn van de in paragraaf 3.2 gesignaliseerde ontwikkeling van gegevensvolgende, gegevenskoppelende en gegevensontdekkende technologieën. In paragraaf 3.5 komt sociale uitsluiting en informatieapartheid als neveneffect van de risicotoezichtsamenleving aan de orde en in 3.6 wordt het falen van de toezichthoudende technologie gesignaleerd. Het hoofdstuk wordt met paragraaf 3.7 afgesloten. Deze paragraaf geeft het antwoord op tweede onderzoeksvraag (OV 2) en geeft een toekomstvisie op de gevolgen van de toezichtmaatschappij op de privacybescherming.

---

1 Dit citaat wordt uitgesproken door Cypher tegen Neo, die een rode pil heeft ingenomen om uit de Matrix naar de "echte wereld" te ontsnappen, in 9e scene van de film The Matrix, een Amerikaansesciencefictionfilm uit 1999, onder regie van de gebroeders Wachowski. Voor een uitvoerige beschouwing over de vele lagen van de Matrix: Yeffeth, 2003, p. 7.

3.1. Erosie van privacy?

Privacy watchers zijn er van overtuigd, dat terrorisme bestrijdende regelgeving, zoals de Richtlijn 2006/24/EG (DRD) van 15 maart 2006 die zich richt op het bewaren van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten of openbare communicatienetwerken[2], de bescherming van onze privacy eroderen. Bunyan[3] stelt dat de DRD "another nail in democracy's coffin" is.[4] In het post-9/11-tijdperk heeft de bestrijding van terrorisme en transnationale misdaad een hoge prioriteit voor de overheid gekregen. Zonder al te veel maatschappelijke discussie[5] en mogelijk geleid door latente gevoelens van angst,[6] hebben burgers en parlementsleden zich erbij neergelegd dat daarbij inbreuken in hun persoonlijke levenssfeer onvermijdelijk zijn. Sinds 9/11 heerst er in de westerse wereld een 'moral panic', dat wil zeggen een paniekstemming die ontstaat omdat een grote groep mensen het intense gevoel heeft dat de sociale orde en hun normen en waarden worden bedreigd. Vanwege deze 'moral panic' lijken de politici het gerechtvaardigd te vinden om ter bescherming van onze veiligheid, onze anonimiteit op te heffen en het recht op privacybescherming in te perken. Zij vinden het mede daarom onvermijdelijk het toezicht op de burgers te intensiveren. De Duitse Minister van het Bundesinnenministerium verklaarde in het kader van de bescherming van de persoonsgegevens: "Wer darf Daten zu welchen Zwecken unter welchen Voraussetzungen nutzen und wie lange müssen sie gespeichert werden? Es könne nicht angehen, den Staat 'blind' zu machen. Vielmehr sei eine 'Datenverkehrsordnung' erforderlich, die einen optimalen Informationsfluss gewährleiste und die notwendige Datenverarbeitung transparent mache. Dabei müsse man aus Fehlern Erkenntnisse ziehen. Wir sollten eine Grundlage schaffen, die Daten zu nutzen, um Mörder zu erkennen. Alles andere könne man der Bevölkerung nicht erklären."[7]

In het pre-9/11-tijdperk zouden zulke inbreuken snel door de privacytoezichthouders zijn gekwalificeerd als 'Orwelliaans' of als een teken dat de maatschappij zich ontwikkelt in een hightech-politiestaat. Los van de 'moral panic' lijkt er door 9/11 sprake te zijn van een verschuiving in het krachtenspel tussen de privacybescherming en de rechtshandhaving.[8] Het is tekenend voor de huidige *zeitgeist* dat het volgende krantenbericht zeer weinig ophef in Nederland heeft veroorzaakt. De Parlementaire Nieuwsbrief van 3 januari 2008 opent op de voorpagina met de

2 OJ 13.4.2006 L105/54.
3 Bunyan, 2005, www.statewatch.org/news/.
4 Thomas, 2009: "risks that arise as a result of excessive surveillance that affect us individually and affect society as a whole".
5 Vedder, e.a., 2007, p. 5.
6 Susser, Herman & Aaron, 2002, p. 70-78: "The psychological damage caused by the attacks of September 11 mirrored the physical destruction and showed that protecting the public's mental health must be a component of the national defense."
7 www.heise.de/newsticker: *Heise Newsticker* van 30-01-2007.
8 Galbraith, 1984; Snyder, 2008.

kop: "Slecht gesteld met privacy burgers" en vervolgt: "Nederland is hard op weg een politiestaat te worden. Dat concluderen de onderzoekers van het Britse bureau Privacy International, dat jaarlijks de privacy van burgers wereldwijd onderzoekt. Uit de lijst die Privacy International vandaag heeft gepresenteerd blijkt dat Nederland is ingedeeld in de categorie van landen die systematisch falen om de privacy van burgers te beschermen. Nederland scoort onder de maat vanwege de identificatieplicht. Ook de mogelijkheid om telefoongesprekken af te luisteren en de bewaarplicht van gegevens van internetgebruikers spelen een rol, evenals het verzamelen van DNA-gegevens van mensen die zijn veroordeeld voor het plegen van ernstige misdrijven."[9]

Informatie- en communicatietechnologie gaat een steeds belangrijkere rol in onze samenleving innemen. Dit zorgt ervoor dat mensen voor nieuwe ethische, sociale en politieke problemen komen te staan. Een van de problemen is de omgang met persoonsinformatie. Zoals in hoofdstuk 2 is uiteengezet, is het zowel in het belang van het individu als de democratische samenleving om ervoor te zorgen dat de persoonlijke levenssfeer van het individu tegen inbreuken wordt beschermd. Deze kernwaarden zijn in de nationale en internationale wet- en regelgeving vastgelegd. De bescherming van de persoonlijke levenssfeer houdt evenwel niet in, dat ten gevolge van een rechterlijk bevel, opsporings- en veiligheidsdiensten een individu niet zouden kunnen dwingen zijn privacybescherming en anonimiteit op te geven. Om te voorkomen dat de overheid deze bevoegdheid misbruikt, zijn garanties nodig met strikte voorwaarden. Een van deze voorwaarden is dat de overheid een sterk vermoeden moet hebben dat iemand een misdrijf heeft gepleegd.

Sinds het van kracht worden van de DRD[10] in de Europese Unie, is een principieel paradigma uit onze rechtsorde omgedraaid. Iemand hoeft nu niet meer verdacht te worden van een misdrijf. Integendeel, nu is iedereen (de onverdachte burger) in principe verdacht en kan de overheid van iedereen preventief en zonder dat die persoon er erg in heeft, alle verkeersgegevens verzamelen, analyseren en bewaren die tijdens het elektronisch communicatieproces geproduceerd worden. Duizenden jaren lang was surveillance: volg **deze** persoon! Nu is het: volg **alle** personen! Geen wonder dat zowel de nationale toezichthouders op het gebied van de bescherming van persoonsgegevens, als actiegroepen die vrezen dat de grondrechten zullen worden aangetast, als de telecommunicatie-industrie zich om economische redenen verzetten tegen de carte blancheregeling.[11] In hoofdstuk 2 paragraaf 10.1 is dieper op de bezwaren ingegaan. De protesten hebben niet mogen baten. Op 6 juli 2009 is de Wet bewaarplicht telecommunicatiegegevens[12] door de Eerste Kamer aangenomen. De kamerbreed aanvaarde motie-Franken[13] kan op termijn nog verbetering brengen. In deze motie wordt de regering verzocht

9 www.sdu.nl/.../parlementairenieuwsbrief.jsp.
10 OJ 13. 4. 2006 L 105 p. 54.
11 Kosta Valcke, 2006, p. 370-380; Schermer, 2007, p. 99.
12 www.eerstekamer.nl/wetsvoorstel/31145_wet_bewaarplicht.
13 Eerste Kamerstukken, 2008-2009, 31 145, H.

de Europese Commissie op de hoogte te stellen van de bezwaren van de Eerste Kamer en er bij de Commissie op aan te dringen dat in de reeds voorziene evaluatie van de Richtlijn dataretentie (2006/24/EG) uitgebreid aandacht zal worden besteed aan de effectiviteit van de opslag van internetverkeersgegevens.

In ieder geval staan nu de telefoon- en internet gegevens een jaar ter beschikking van Justitie.

Onbewuste gezagsgetrouwe burgers gebruiken steevast de verdediging van zulk overheidsoptreden met het adagium: "Ik heb niets te verbergen",[14] maar daar gaat het niet om. Solove merkt daar over op: "It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised in government surveillance and data mining programs. When engaged with directly, the 'nothing to hide' argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the 'nothing to hide' argument, in the end, has nothing to say."[15]

Hoe kan de burger zeker weten dat zijn opgeslagen gegevens onder bepaalde omstandigheden als gevolg van risicoprofilering of data mining plotseling in een ander daglicht komen te staan. Er zijn te veel voorbeelden dat er incorrecte informatie uit de gegevens wordt gedestilleerd, terwijl e-mails doorgaans niet erg nauwkeurig worden opgesteld om te dienen als sluitend opsporingsmateriaal.[16] Bovendien is het uitgangspunt bij privacybescherming dat de burger zelf bepaalt wat over hem wordt opgeslagen en niet anderen die op een of andere manier persoonlijke informatie van hem hebben verkregen. Terecht stelt Vedder e.a. dan ook, dat: "burgers er steeds minder van op aan kunnen, dat zij niets te vrezen hebben, dan wel buiten schot zullen blijven".[17]

Inmiddels zijn er wereldwijd al ruim achthonderd antiterrorismewetten (stand eind 2006) van kracht geworden.[18] Het belangrijkste kenmerk van die wetten is dat veel persoonsgegevens tijdens de elektronische communicatie moeten worden opgeslagen. Deze ontwikkeling gaat lijnrecht tegen een aantal in hoofdstuk 2 uiteengezette privacyrealisatiebeginselen en met name tegen het beginsel van dataminimalisatie, dat een van kernbeginselen van de informationele privacybescherming vormt.

Maar hebben de 'privacy watchers' gelijk? Is dit inderdaad het begin van het einde van onze privacy? Wie moeten we ervan beschuldigen dat onze privacy afbrokkelt? '9/11', de DRD of de daarvan afgeleide wetgeving? Is de overheid

14 Koelewijn, 2009, p. 15, meent dat burgers deze uitspraak doen omdat zij de verwerking van hun persoonsgegevens niet als een inbreuk op hun vrijheid of privacy ervaren en de gevolgen van verwerking niet direct voor hen zichtbaar zijn. "Dit leidt (…) tot onderschatting van de mogelijke gevolgen van een onbegrensd inzicht van de overheid in het privéleven van haar onderdanen."
15 Solove, 2007, p. 23.
16 Strik, 2009, p. 7.
17 Vedder, e.a., 2007, p. 16.
18 Hosein, 2006.

beter in staat terrorisme te bestrijden nu zij onze privacy minder goed beschermd? Is er sprake van een 'zero sum game',[19] dat wil zeggen: houdt (het gevoel van meer) openbare en persoonlijke veiligheid of meer beveiliging minder privacybescherming in en omgekeerd?[20] Of gaat het hier om het vraagstuk van de persoonlijke vrijheid versus controle over het individu in plaats van veiligheid versus privacy? Het is de vraag of is de hierboven gekenschetste ontwikkeling op zichzelf staand is. Vedder merkt op dat al vóór de aanslagen van september 2001 er vergevorderde plannen waren om in de antiterrorismewetgeving de bevoegdheden van politie, justitie en veiligheiddiensten uit te breiden,[21] niet alleen in Nederland maar ook in andere landen. Zo is bijvoorbeeld in het Verenigd Koninkrijk de controversiële Regulation of Investigatory Powers Act (RIP)[22] al in 2000 als Chapter 23 van de Acts of the United Kingdom Parliament van kracht geworden. Naast de voorafgaande vragen is wellicht de meeste saillante vraag of de burgers zich door het toegenomen toezicht[23] werkelijk veiliger voelen en of het toezicht werkelijk bijdraagt aan onze veiligheid?[24] Daarover is weinig bekend.

De Commissie Suyver concludeert na een evaluatieonderzoek dat er weinig tot geen samenhang is in de antiterreurmaatregelen die Nederland na de aanslagen van 11 september 2001 heeft genomen. De Commissie Suyver ondervroeg sleutelfiguren in de Nederlandse terreurbestrijding. Die vinden dat ze voldoende bevoegdheden hebben. Maar onduidelijk is wie waarvoor verantwoordelijk is. Dit komt volgens de commissie omdat er nooit sprake is geweest van een masterplan voor de aanpak van terrorisme. Wetgeving werd ongecoördineerd ingevoerd. Er bestaan nog veel onduidelijkheden over de effectiviteit en de privacyaspecten van de genomen maatregelen om zo door te gaan.[25] Uit onderzoek naar videotoezicht in het Verenigd Koninkrijk (dat de meeste videobewakingscamera's (CCTV) ter wereld heeft, namelijk één camera op veertien inwoners) is gebleken dat deze vorm de misdaad aanmerkelijk minder goed bestrijdt dan goede straatverlichting. Het Britse Ministerie van Binnenlandse Zaken (Home Office) concludeerde dat "further high quality research is needed into CCTV to find out more about how CCTV works and where it works best".[26] Het URBANEYE-rapport wijst erop dat het beschikbare onderzoek naar de effectiviteit van videocamera's bij misdaadbestrijding veel hiaten bevat en dat vele rapporten "highlight statistics

19 Teepe, 2007, p. 5.
20 Klüver, Peissl, &Tennøe, 2006, p. 85. De uitdaging voor de overheid is hoe (collectieve) veiligheid kan worden verschaft zonder inbreuk op de privacybescherming te maken.
21 Vedder, e.a., 2007,. p. 32-33.
22 Regulation of Investigatory Powers Act 2000, The Stationery Office Limited, London 2000.
23 Soares, 2009, p. 9 gebruikt in haar artikel 'Eyes on the Swine', de omschrijving "in the age of ubiquitous surveillance, the public has come to assume that someone or something is always watching, ready to spot trouble as it is happening".
24 Klüver, Peissl, &Tennøe, 2006, p. 29.
25 De Volkskrant 11 juli 2009 Binnenland p. 3. Evaluatie anti-terreurmaatregelen www.justitie.nl/.../A%20Rapport%20**Commissie**%20Suyver_15602_tcm34- 204136.pdf?
26 Welsh & Farrington, 2002 p. 44; p. vi: "In the city centre and public housing setting, there was evidence that CCTV led to a negligible reduction in crime of about two per cent".

in order to justify the effectiviness of CCTV".[27] Omdat we nauwelijks weten wat het psychologische effect is van CCTV-surveillance, is meer wetenschappelijk onderzoek noodzakelijk. Terugkijkend naar de afgelopen decennia kan geconstateerd worden, dat huidige informatiemaatschappij[28] zich in rap tempo ontwikkelt naar een toezicht- of bewakingsmaatschappij. Of wellicht kan men beter spreken van een risicosurveillancemaatschappij met het adagium 'better safe than sorry'. Kan in dat licht de DRD en de wetgeving die daaruit voortvloeit gezien worden als een symptomatische uiting van deze maatschappelijke ontwikkeling? Als dat zo is, dan geldt dat ook voor bijvoorbeeld de risicoanalyse voor ieder kind in zijn eerste vier levensjaren die Minister Rouvoet van Jeugdzaken voorstelde onder het motto 'alle kansen voor alle kinderen'. Om het risico te bepalen kent de Basis Dataset Jeugdgezondheidszorg versie 2.0 (mei 2007) dertig bladzijden vragen met 1200 vragen per kind, waarvan het aantal, de definities, de interpretatie en de doelgebondenheid van de op te nemen gegevenselementen onvoldoende omschreven en gemotiveerd zijn. Als de plannen van minister Rouvoet werkelijkheid worden, dan wordt de voorgestelde risicoanalyse een vast onderdeel van het elektronisch kinddossier (EKD) in de jeugdgezondheidszorg[29] dat per eind 2010 tezamen met de Verwijsindex Risicojongeren wettelijk verplicht wordt.[30] Is hier sprake van overkill?

3.2. Verschuiving naar de Risicotoezichtmaatschappij

Volgens Castells kenmerkt de huidige (netwerk)samenleving zich door de opkomst van wat hij het 'informatietechnologische paradigma' noemt.[31] Hij beweert daarmee dat in onze huidige westerse maatschappij beeld, geluid, schrift etc. vanwege hun digitalisering makkelijk kunnen worden gemanipuleerd en verspreid. Daarnaast wordt onze maatschappij gekenmerkt door allerlei vormen en combinaties van netwerktechnologie. Bovendien signaleert Kurzweil dat de opkomst van de nanotechnologie, genetica, neurofarmacologie en de multifunctionele robotica een belangrijke rol bij de toezichtsamenleving zullen gaan spelen. Bijvoorbeeld: gedrag kan beïnvloed worden door neurofarmacologische middelen, die de neurohuishouding van een individu op het maatschappelijk gewenste

27 www.urbaneye.net – On the Threshold to Urban Panopticon? – A comparative research project on CCTV in Europe.

28 Franken, Kaspersen & De Wild, 2004, p. 35-41; Franken heeft voor de informatiemaatschappij zes ontwikkelingkarakteristieken gedefinieerd, te weten dematerialisatie, globalisatie, turbulentie, horizontalisering, kwetsbaarheid en transparantie.

29 Beleidsverslag 2007 van het programmaministerie Jeugd en Gezin, p. 11.

30 Artikel 5 van de Wet pg. www.scribd.com/doc/15228223/Vraag-Antwoord-Kamervragen-EKD-Dezentje-Hamming-Code-Rood.

31 Castells, 2004, p. 11: "a technological paradigm based on the augmentation of the human capacity of information processing and communication made possible by the revolutions in microelectronics, software, and genetic engineering".

peil kan brengen en houden. Deze drie ontwikkelingen zullen ingrijpende maatschappelijke, politieke, culturele en economische consequenties hebben.[32]

Negroponte voorspelde al midden jaren negentig dat het economisch verkeer zich niet meer zou beperken tot het verplaatsen van atomen (goederen) maar dat de kern van de economische activiteit zou komen te liggen bij het verzenden van digitale bits en bytes (informatie).[33] Hij heeft daarin gelijk gekregen. Een van de gevolgen daarvan is dat vaste prijzen van goederen en diensten over vijf jaar tot het verleden zullen horen. In plaats daarvan zal hun prijs afhangen van het dagelijks ritme van de economie. In supermarkten zullen prijskaartjes van producten via internet in directe verbinding staan met de wereldmarkt.

De bovenstaande maatschappelijke ontwikkelingen hebben onder meer het ontstaan van de 'risicosamenleving'[34] tot gevolg gehad met de daarbij behorende vervlechting van technologische, sociale en fysieke netwerken. Vertrouwen tussen burgers speelt daarbij een nog belangrijkere maatschappelijke rol dan vroeger. Door de eeuwen heen hebben mensen geleerd hoe zij elkaar kunnen vertrouwen zonder daarbij zelf risico te lopen. Daarbij spelen lichaamstaal en andere zintuiglijk waarneembare signalen en conclusies die mensen daaruit trekken, een belangrijke rol. Dit vertrouwen leidt tot korte of langdurige verbintenissen in het zakelijke en persoonlijke verkeer. De netwerksamenleving zorgt ervoor dat binnen het wereldwijde web (internet) mensen steeds vaker virtuele gemeenschappen en ondernemingen oprichten. In deze virtuele wereld gaat het echter om hetzelfde vertrouwen als in de fysieke wereld.

Om ervoor te zorgen dat mensen elkaar in de virtuele wereld vertrouwen, is het belangrijk dat het dataverkeer tussen burger en overheid, tussen consument en leverancier of tussen zakelijke partners integer verloopt. Er is daarbij echter één belangrijke handicap. Directe sensorische waarneming is op internet vrijwel afwezig. Bovendien begrijpen veel internetgebruikers de technologie niet die eraan ten grondslag ligt. Gemis aan tastbaarheid en onbekendheid met de technologie, herbergen een gevaar in zich: mensen weten niet zeker of de identiteit van bedrijven, instanties of medeburgers wel klopt. Daardoor kan de vrees ontstaan dat hun persoonlijke gegevens weleens misbruikt zouden kunnen worden en dat hun transacties op zijn minst onzeker zijn. Dit kan doorslaggevend zijn voor het gebrek aan een sluitend vertrouwen, waardoor gebruikers van het internet afhaken of onverantwoorde (privacy) risico's nemen. De virtuele wereld zonder grenzen heeft ook gevolgen voor de bestaande structuren binnen de overheid. Staten ontwikkelen zich van een klassiek gecentraliseerde staat met landsgrenzen naar een horizontale en gedeterritorialiseerde staat.[35] Dit heeft weer consequenties voor het functioneren van de overheid c.q. de staat, omdat het 'territorium' als ordeningsgrondslag (bijvoorbeeld met betrekking tot de jurisdictie van de staat en

32 Kurzweil, 2003, p. 185-197; Yeffeth, 2003, voor meer ontwikkelingen.
33 Negroponte, 1995, p. 11-85.
34 Beck, 1986 p. 25: "In der fortgeschrittenen Moderne geht die gesellschaftlichen Produktion von Risiken."
35 Borking, 2001, p. 285-296; Frissen, 1999.

van staatsorganen) fundamenteel wordt uitgedaagd[36] en de binding tussen de politiek-bestuurlijke institutie en het territorium (het land) onder druk komt te staan.[37] Om de risico's voor de openbare orde en veiligheid te beperken wordt in alle welvarende landen ter wereld de burger in het dagelijks leven steeds vaker doorlopend geconfronteerd met toezicht dat steeds minder waarneembaar wordt.[38] Er bestaat inmiddels in de westerse wereld een complexe basisinfrastructuur voor gegevensverwerking waarbij mensen er automatisch vanuit gaan dat het van vitaal belang voor hun bestaan is dat bedrijven en overheidsinstanties hun persoonsgegevens verzamelen en verwerken.

Toezicht is uiteraard geen nieuw maatschappelijk fenomeen. Ook in vroegere tijden hielden mensen elkaar in de gaten, hetzij om voor elkaar te zorgen, hetzij om elkaar op zedelijk gebied te vermanen, hetzij om heimelijk informatie te verkrijgen. Vanaf de Renaissance is er echter een verandering zichtbaar. Toen begon men het werk op een 'rationele' manier te organiseren. Sociale netwerken werden hierdoor steeds minder informeel. Dit gold ook voor de manier van leiding geven waarop het alledaagse leven en bestuur steunden. Deze nieuwe organisaties, 'bureaucratieën' genaamd, moesten soepel hun werk kunnen doen. Omdat familiebetrekkingen en persoonlijke contacten daarbij een storende invloed konden zijn, verloren de vanouds bestaande maatschappelijke banden tussen mensen hun betekenis.[39] Deze onpersoonlijke en bestuursgerichte praktijken zorgden ervoor dat mensen steeds meer onder toezicht kwamen te staan. In onze huidige samenleving neemt dit toezicht steeds toe.[40] Dit is toe te schrijven aan nieuwe naoorlogse informatietechnologieën, waardoor het bureaucratisch bestuur in staat is sneller en beter te managen, te analyseren en coördineren. Een voorbeeld hiervan is Shenzhen, een stad van 12,4 miljoen inwoners, gelegen aan de grens met Hongkong in de provincie Kanton, in het zuiden van China. Hier is men bezig alle inwoners te voorzien van een inwonerskaart met een krachtige chip. In die chip zijn niet alleen de naam van de houder en zijn adres opgeslagen, maar ook het werkverleden, zijn religie, het aantal voortgebrachte kinderen (in verband met het 'één-kind-beleid'), zijn politiedossier, medische verzekeringsgegevens en telefoonnummers van bijvoorbeeld de verhuurder van zijn huis. Het stadsbestuur van Shenzhen onderzoekt of de gegevens op de kaart kunnen worden uitgebreid met het betaalgedrag van de kaarthouder, openbaarvervoerbewijzen en kleine aankopen.[41]

De aanslagen in New York (11 september 2001), op het metrostation in Madrid (2004) en de 'Underground' in Londen (2005) hebben twee katalyserende effecten

36 Bekkers, 2007, www.eur.nl/fsw/bsk/onderwijs/rpaos/state_and_network_society/.
37 Sampson, 1983, p. 186-203.
38 Weiser, 1991, p. 94-104: "the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it".
39 Ball, e.a., 2006, p. 1.
40 Pierson, 1996, p. 17, 39 en 148.
41 Bradsher, 2007, p. 1.

gehad. Enerzijds is hierdoor de 'moral panic' bij het grote publiek toegenomen. Anderzijds zijn mensen zich meer bewust geworden van hun eigen kwetsbare (gevoel van) veiligheid. Hierdoor is het voor de overheid makkelijker geworden de bevoegdheden van opsporingsdiensten uit te breiden en andere antiterrorisme-maatregelen te nemen.[42]

De opkomst van de netwerkmaatschappij die Castells heeft gesignaleerd is echter niet de enige verklaring voor het feit dat (commerciële) organisaties meer aandacht zijn gaan schenken aan risico's van hun bedrijfsvoering en deze hebben geprobeerd te gaan beheersen. In de decennia na de Tweede Wereldoorlog was er al een ontwikkeling in de samenleving gaande die op deze tendens wees. Het belang van ict is steeds meer toegenomen. Binnen de ict heeft een evolutie plaatsgevonden in vier in elkaar overlopende fasen: substitutie (stand-alone transactieverwerkende systemen), verrijking (ondersteunende management-informatiesystemen), transformatie (procesvormgevende strategische informatie-systemen) en transparantie (flexibele infrastructurele informatievoorzieningen).[43] ict is steeds meer een onderdeel geworden van de bedrijfsvoering en de maat-schappij. Organisaties en bedrijfsprocessen kunnen steeds beter worden bestuurd en dat leidde tevens tot verbetering van de concurrentiepositie.[44] De evolutie van de ict leidde tot een toenemende belangstelling voor risicobepaling en beheersing van processen.[45] Hierdoor is de belangstelling van het management om interne en externe risico's te bepalen en te beheersen steeds meer toegenomen, ja zelfs een wezenlijk onderdeel geworden van de bedrijfsvoering.

Lag bij de fase van de substitutie het risico slechts bij de onbekende technologie, in de loop van de ict-evolutie verschoof het risicospectrum van specificatie-onderzekerheid, naar organisatorische, strategische en infrastructurele risico's. Ook bij het opstellen van automatiseringscontracten is risicoanalyse is een van de leidende gedachten geworden.[46]

Parallel aan de ict-evolutie ontstond in de loop van de jaren negentig van de vorige eeuw in een relatief korte tijd de 'surveillance society', onder andere doordat bestanden steeds meer aan elkaar gekoppeld werden.[47] Tegelijkertijd is de nadruk steeds meer op bedreigingen,[48] van de samenleving en daarmee verbonden veiligheidsgevoelens komen te liggen. Volgens analisten neemt het risico van terroristische aanvallen toe, omdat terroristische groepen met minimale middelen maximale (im)materiële schade kunnen aanrichten.[49] Figuur 4.9 in hoofdstuk 4 illustreert dit.

---

42 Vedder, e.a., 2007, p. 33.
43 Van Irsel & Swinkels, 1992, p. 624-625.
44 Porter & Millar, 1985, p. 149-160.
45 Keen, 1991, p. 202-204; Little, 1991, p. 108-110.
46 Modelcontracten (BiZa) Den Haag 1991. De tekst in de preambule 0100-1 van de automatiseringscontracten luidt: "De tekst van de contracten geeft richting aan het proces van risicosignalering, risicoweging en de navenante verdeling van verantwoordelijkheden."
47 Voor een illustratief voorbeeld hiervan: de in 1998 uitgebrachte film The Enemy of the State, een Amerikaanse film geregisseerd door Tony Scott.
48 Op het begrip bedreigingen wordt in hoofdstuk 4 van dit boek uitvoerig op ingegaan.
49 Koops, e.a., 2005, p. 24.

De overheid is mede onder politieke druk erop gebrand om de risico's van terroristische aanslagen zo veel mogelijk te verkleinen. Risico[50] is een sleutelbegrip in de maatschappij geworden met als doel de gevolgen van de risico's voor te blijven.

De technologie om data te verzamelen, op te slaan en te verwerken zal zich de komende vijf tot tien jaar nog sterker gaan ontwikkelen. Gilbert van de Royal Academy of Engineering heeft een verscheidenheid aan relevante ict-technologieën geanalyseerd.[51] Hij signaleert drie verschillende lagen van technologieën, die steeds meer convergeren en elkaar versterken. Bij deze technologieën spelen persoonsidentiteiten een sleutelrol. De Royal Academy onderscheidt als eerste laag de 'Connection technologies', dat zijn technologieën die data volgen, bijvoorbeeld RFIDs en NFC.[52] Als tweede laag gaat het om de 'Disconnection technologies', dat zijn gegevens koppelende technologieën, zoals de SIM[53] kaart in mobiele telefoons en biometrische technologie, die de toegang tot data controleren. De derde laag zijn de 'Processing technologies', dat zijn technologieën die informatie ontdekken en extraheren, zoals data mining, data warehousing en tijd-ruimte 'Googleing' die mogelijk zijn door de goedkope massale opslag van gegevens en het Wereld Wijde Web.[54] Door middel van de hierboven vermelde technologielagen hebben wij onze toezichtmaatschappij inmiddels georganiseerd en gestructureerd. Door de terugkoppelingssystemen gebaseerd op de hierboven vermelde technologieën kunnen mensen in de gaten worden gehouden en worden al dan niet identificeerbare persoonsgegevens in de meest ruime zin verwerkt.[55] Doordat burgers onder digitaal toezicht staan, wordt er informatie over hun mobiliteit en activiteiten met behulp van dezelfde technieken opgeslagen. Organisaties en overheden kunnen vervolgens hun voordeel hier mee doen. De verkregen informatie wordt vervolgens gesorteerd, gezeefd, gecategoriseerd en gebruikt als basis voor beslissingen die direct de burger regarderen. Deze beslissingen bepalen onder meer of wij recht hebben op en toegang tot uitkeringen, werk, producten en diensten hebben en of wij een strafbaar feit hebben gepleegd. Ook kunnen zij betrekking hebben op onze gezondheid en ons welzijn als mede op ons gebruik van de openbare en particuliere ruimte.

Schermer[56] signaleert dat in de afgelopen jaren de overheid de groeiende behoefte heeft de risico's voor de openbare veiligheid te beheersen. Dit heeft een significante invloed gehad op het strafrecht dat hierdoor steeds meer uitgroeit tot een systeem van 'risk justice'. In zo'n systeem gaat het er niet primair om misdrijven op te lossen en te bestraffen, maar misdrijven te voorkomen en risico's

50 Het begrip risico wordt in hoofdstuk 4 en 7 behandeld.
51 Gilbert, 2007.
52 NFC staat voor: near field communication.
53 SIM staat voor Subscriber Identity Module is een smartcard waarop de gegevens staan van een gebruiker van een GSM- of UMTS-mobiele telefoon.
54 Gilbert, 2007, p. 14-18.
55 Schermer, 2007, p. 35-40.
56 Schermer, 2007, p. 113.

te reduceren. De sciencefictionfilm *Minority Report*[57] geeft hier sprekende voorbeelden van.

De afgelopen jaren is in de westerse samenleving een ontwikkeling zichtbaar om proactief initiatief te nemen bij de aanpak van risico's in plaats van risico's te voorkomen.[58] Met name het gebruik van data mining en profilering bij het identificeren van risico's heeft er toe geleid dat de overheid niet meer 'ex post' specifieke individuen in de gaten houdt, maar preventief toezicht houdt op de gehele bevolking. Daarbij worden de gedragingen van burgers op grote schaal doorgelicht en hun transacties geanalyseerd.[59] Een voorbeeld van massale preventieve screening is het USVISIT-grenscontrolesysteem,[60] waar iedere passagier die in de Verenigde Staten aankomt mee wordt geconfronteerd. De analyse van alle bankgegevens die binnen SWIFT[61] zijn gegenereerd op grond van bancaire transacties in Europa kan in dezelfde categorie worden geplaatst. Justitie kan de hierboven besproken manier van monitoring inzetten om te bepalen op welke manier zij het beste kan ingrijpen wanneer individuen en groepen mensen een risico vormen voor de samenleving. Daarbij is het van groot belang veel (persoonlijke) informatie van en over identificeerbare individuen te verzamelen en te analyseren. Dergelijke praktijken kunnen op gespannen voet komen te staan met de bescherming van de persoonlijke levenssfeer.[62] Hand in hand met deze ontwikkeling is surveillance een welhaast militaire exercitie geworden. Er cirkelt een groot aantal militaire kunstmanen om de aarde die allerlei 'verdachte' praktijken scherp in het oog houden.[63] Onze GPS (Global Positioning System) is ontwikkeld door en staat nog steeds onder (USA) militaire controle. Het ECHELON-netwerk dat door de Verenigde Staten, het Verenigde Koninkrijk, Canada, Australië en Nieuw-Zeeland wordt beheerd, is wellicht het meest prominente en wijdverspreide elektronische toezichthoudende netwerk. Aanvankelijk was het bedoeld om de communicatie tussen de Sovjet-Unie en de voormalige Oost-Europese staten te controleren, maar later in beginsel ook om alle privé- en niet-militaire communicatie te volgen van alle wereldburgers.[64]

---

57 'Minority Report' is een Amerikaanse sciencefictionfilm uit 2002, geregisseerd door Steven Spielberg.
58 Ball, e.a., 2006.
59 Valverde & Mopas, 2004.
60 United States Visitor and Immigrant Status Indicator Technology is sinds 2004 voor alle lucht- en zeehavens en grensovergangen in gebruik.
61 *Society for Worldwide Interbank Financial Telecommunication* (SWIFT); De verwerkte bankgegevens van Europese burgers worden op grond van Amerikaanse wetgeving doorgegeven aan de inlichtingendiensten (CIA en FBI) van de Verenigde Staten: www.edps.europa.eu/EDPSWEB/edps/site/mySite/op/edit/lang/en/pid/38 en www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/25.
62 Vedder, e.a., 2007, p. 67: "als de hierboven geschetste trends zich doorzetten – en gelet op de bevoegdheidsuitbreidingen die op stapel staan, is er weinig reden daaraan te twijfelen – komt de privacy van burgers in een aantal opzichten verder onder druk te staan."
63 Ball, e.a., 2006, p. 13.
64 Wright, 1998.

3.3. Van een niet-technologische naar elektronisch toezicht

Camp stelt dat het inherent aan de samenleving is om zich te beveiligen en dat beveiliging en surveillance, onafscheidelijk bij elkaar horen.[65] Het is twee kanten van één en dezelfde medaille. Bij de toezichtmaatschappij hoort een systematische en gerichte aandacht van de overheid voor persoonsgegevens om controle te kunnen uitoefenen, rechten aan burgers te verlenen, invloed uit te oefenen en bescherming te bieden. Er zijn grosso modo twee manieren om toezicht te houden. De eerste manier is ervoor te zorgen dat uitsluitend geautoriseerde personen toegang hebben tot het systeem en de tweede manier is het gebruik van het systeem in de gaten te houden en tegen aanvallen te bewaken. In hoofdstuk 4 wordt hierop ingegaan. Langs dezelfde lijnen kunnen beveiligings- en toezichthoudend gerelateerde technologische toepassingen worden gegroepeerd. Er zijn technologieën voor identificatie en autorisatie, zoals biometrie, contactloze identiteitskaarten, digitale gezichtsherkenning, irisscanning,[66] en er zijn surveillance (recherche) technologieën, zoals videocamera's (Closed Circuit Television (CCTV) en sensoren (RFIDs),[67] die sterk in opkomst zijn. AMI levert weer andere mogelijkheden op, bijvoorbeeld actieve microscopisch kleine sensoren (bijvoorbeeld in de vorm van 'smart dust') die luchtdruk, temperatuur, windsnelheid, geluid, versnelling, warmte, geur etc. meet en die in staat zijn bewerkingen op de geregistreerde data uit te voeren en deze op bepaalde momenten uit te zenden.

De persoonsgegevens, die door bovenstaande technologische toepassingen worden gegenereerd, kunnen vele vormen aannemen, waaronder videobeelden van bewakingscamera's, biometrische (registratie)gegevens, biometrische terugkoppelingsgegevens, of numerieke of categorische data. Veel gegevens van de laatstgenoemde categorie hebben betrekking op transacties, informatie-uitwisseling, rekeningen, statusinformatie en dergelijke. Clarke heeft deze gegevens samengevat onder de noemer 'dataveillance'.[68] Ict maakt dataveillance mogelijk. De activiteiten van of communicatie tussen mensen wordt met dataveillance gegevens geautomatiseerd in de gaten gehouden en gecontroleerd. Deze manier van toezicht blijkt veel goedkoper te zijn dan rechtstreeks of doelgericht elektronisch toezicht. Omdat deze manier van toezicht houden voordelen biedt, moedigt het organisaties aan om zulke systemen verder uit te breiden, ook al zijn meer gegevens niet echt nodig voor het initiële doel.

---

65 Camp, 2004, p. 216 "(…) it emerges from a simple reality: attacks are based more and more on human system weakness instead of on technological weaknesses."

66 Greenemeier, www.scientificamerican.com/article.cfm?id=hands-free-iris-biometrics&sc=DD_2009072. Carnegie Mellon University CyLab researchers ontwikkelen op verzoek van US Department of Defense een iris-scanning systeem dat irissen kan scannen en vergelijken tot op een afstand van 12 meter.

67 RFID staat voor Radiofrequency-identification. Zwenne & Schermer, 2005, p. 15: unieke identificatie op afstand van producten en personen.

68 www.anu.edu.au/people/Roger.Clarke/DV/: "Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"; Bennett & Raab, 2006, p. 23-26.

Voordat ict surveillance mogelijk maakte, gebruikte de mens al sinds jaar en dag andere technieken. Mensen werden door anderen afgeluisterd, in de gaten gehouden, achtervolgd, bespioneerd. Na de ontdekking van het schrift, werden gegevens van mensen vastgelegd in dossiers. Toezicht in sommige autoritaire regimes, zoals in voormalig Oost-Duitsland,[69] steunden op papieren archieven en op informanten. Veel meer dan dat was er niet. Geavanceerde technieken hebben echter voor nieuwe methodes gezorgd om toezicht te houden. Deze toezicht-technologieën zijn omvangrijker, krachtiger en indringender dan de oude. Ze maken het mogelijk van veel meer mensen tegelijk veel meer soorten persoonlijke informatie te verzamelen, digitaal op te slaan en met elkaar te verbinden en direct te analyseren. In tegenstelling tot tien jaar geleden functioneren ze nu 'real time'. Organisaties kunnen daardoor snel en efficiënt (inter)nationale databases gebruiken om gerichte gezondheidzorg aan te bieden, maar ook om politieke tegenstanders zwart te maken.[70]

3.4. Elektronische surveillance, vijf voorbeelden

Hieronder volgt een analyse van vijf manieren waarmee surveillance kan plaatsvinden, te weten: databanken (3.4.1), telecommunicatie (3.4.2), videotoezicht (3.4.3), biometrie (3.4.4.) en localisering (3.4.5).

3.4.1. Databanken

Voor dit proefschrift, dat zich richt op privacybeschermende architecturen en technologieën van informatiesystemen, is het van belang de elektronische databank en het informatiepakhuis (*data warehouse*) nader te beschouwen. Figuur 3.1 geeft de vijf dynamische gegevensstromen in een *data warehouse* weer.

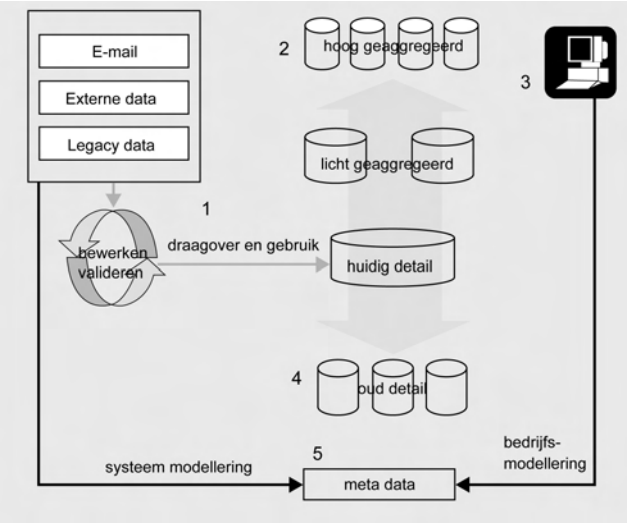
De eerste stroom 1 betreft de instroom van de gegevens in het data warehouse vanuit interne of externe operationele systemen. Deze gegevens kunnen ook bestaan uit gekochte bestanden. De gedetailleerde gegevens zijn afkomstig van bijvoorbeeld online transacties, e-mails, foto's, tekeningen etc. De tweede stroom 2 is de opgaande stroom. Na data reduplicatie worden de gegevens zonder redundantie opgeslagen. Dit niveau is doorgaans een aggregatieniveau hoger dan de operationele systemen. De tijdsdimensie wordt van datum-uur-minuut-seconde ingedikt naar bijvoorbeeld maandniveau. Dit aggregatieniveau kan nog verder worden ingedikt en in aparte bestanden worden opgeslagen. De derde

69 Een goed voorbeeld verschaft de film: 'Das Leben der Anderen', geregisseerd door Florian Henckel von Donnersmarck.

70 Bijvoorbeeld de in de USA ontketende zwartmakerij ('the borking of Bork') van R.H. Bork, toen president Reagan voorstelde hem te benoemen tot rechter van de Federal Supreme Court .

stroom 3 is de uitgaande stroom. Hier worden vanuit de inhoudelijke gegevens zo actueel en accuraat mogelijke rapporten gemaakt om het managen en het nemen van beslissingen te ondersteunen. Bij deze *outflow* komen de gegevens beschikbaar voor diverse gebruikers. De gebruikers gebruiken deze gegevens weer vaak voor data mining. De vierde stroom 4 betreft de neergaande stroom. Omdat er alleen maar gegevens aan het data warehouse worden toegevoegd is het noodzakelijk om onbeheersbare databases te voorkomen. Vandaar dat regelmatig delen van het data warehouse uit de operationele data warehouse worden weggehaald en afzonderlijk op schijven en andere gegevensdragers worden opgeslagen. Mochten deze gegevens weer nodig zijn dan kunnen de data weer worden toegevoegd aan het data warehouse. De vijfde stroom 5 is de meta-stroom. Metadata zijn gegevens over de gegevens in het data warehouse. Daarin kunnen bijvoorbeeld de oorsprong van bepaalde gegevenssoorten zijn vast-gelegd.

Figuur 3.1: Vijf dynamische datastromen in een data warehouse, Celko, 1995 (vertaald in Nederlands).



Organisaties kunnen tegenwoordig veel sneller en nauwkeuriger grote hoeveel-heden data verzamelen, in tabelvorm rangschikken en van verwijzingen voorzien dan met de ouderwetse papieren archieven die eens de moderne bureaucratie kenmerkten. Tot het midden van de jaren negentig van de vorige eeuw waren vaak de bestaande gegevensbestanden te groot en te complex en de gegevens te divers, onjuist en onvolledig. Hierdoor was op eenvoudige vragen, zoals “welke product-marktcombinaties doen het goed?”, geen correct antwoord te verkrijgen.

Doordat data mining en knowledge discovery in databases (KDD) een betere informatiewinning en kennisdistillatie mogelijk maken, is in de beantwoording van vragen zoals "welke product-marktcombinaties doen het goed?" grote verandering in gekomen. In drie stappen[71] kunnen uit de gegevens tegenwoordig patronen en verbanden worden ontdekt. Eerst worden de data door een onderzoeker geprepareerd (dat wil zeggen geschoond, geselecteerd en ondergebracht in gegevensdomeinen). Vervolgens kan de onderzoeker met zoekalgoritmen 'graven' (dat wil zeggen zeven, comprimeren en transformeren) in geselecteerde groepen gegevens. Daarna analyseert de onderzoeker de opgeleverde gegevens om te zien of hij nieuwe en vooral relevante informatie kan toevoegen aan de geselecteerde domeinen. Het gaat er dan met name om dat de onderzoeker nieuwe relaties en patronen binnen dataverzamelingen kan ontdekken.[72] Bijvoorbeeld, vele bedrijven in de particuliere sector proberen zoveel mogelijk gegevens over hun klanten te verzamelen en hun marketingstrategie daarop vervolgens specifiek (één-op-éénbenadering) af te stemmen. Een bankier in Maryland (USA) vergeleek openbaar beschikbare informatie over het ontslag van patiënten uit ziekenhuizen met zijn eigen cliëntenlijst om na te gaan of een van cliënten kanker had. Bij een positieve hit, beëindigde hij de door zijn bank verstrekte lening.[73] Organisaties combineren en verrijken transactiegegevens (gebruik van creditcards, mobiele telefoongesprekken, etc.) van een persoon met bijkomende gegevens. Die gegevens zijn afkomstig van klantenkaartprogramma's, klantonderzoeken, reclamewedstrijden, cookies van websites, productinformatie verzoeken, focusgroepen, callcenter contacten, feedback van consumentenfora en creditcardtransacties, etc. Zowel particuliere bedrijven als overheidsdiensten gebruiken enorme hoeveelheden opgeslagen persoonsgegevens over consumenten en burgers om op basis van de éénloketgedachte of de één-op-éénbenadering hun dienstverlening te verbeteren. Om personen en verdachte activiteitenpatronen te herkennen kan de politie verschillende gegevensverzamelingen met elkaar vergelijken. In forensische DNA-databanken liggen DNA-profielen en DNA-sporenmateriaal opgeslagen. Hiermee kan het DNA-profiel dat is aangetroffen op de plaats van het misdrijf worden vergeleken met profielen van eerder veroordeelde misdadigers. In de toekomst kunnen en zullen DNA-sporen op brieven, sigarettenpeuken, drinkglazen, maar ook verloren lichaamshaar door werkgevers gebruikt kunnen worden om mensen o.a. op hun werkplek te controleren en volgen.[74] DNA-sporen op brieven, sigarettenpeuken, drinkglazen, maar ook verloren lichaamshaar gebruikt worden. De sciencefictionfilm *Gattaca* (1997)[75] laat zien hoe dit mogelijk in zijn

71 Borking, 1999, p. 51-66.
72 Celko & McDonald, 1995.
73 Gerapporteerd in het artikel van C. Walter, A little Privacy Please over de research van Latanya Sweeney in *Scienific American* July 2007, p. 74-75.
74 Koops, e.a., 2005, p. 20.
75 Gattaca is een Amerikaanse sciencefictionfilm uit 1997. De regisseur is Andrew Niccols. Vincent, de hoofdrolspeler, neemt de identiteit van een genetisch perfecte man aan: Jerome Morrow. Jerome voorziet Vincent van haar, huid, bloed en urinemonsters, zodat Vincent alle dagelijkse toegangscontroles en keuringen doorstaat.

werk zal gaan en laat een mogelijk toekomstscenario zien. Met verfijnde technieken kunnen analisten gegevens ook 'uitdiepen'. Dit wil zeggen dat de gegevens tot grote diepte geanalyseerd worden om (tot dan toe onbekende) patronen te ontdekken die weer eventueel tot verder onderzoek leiden. Iedere transactie heeft een 'gegevenstraject', dat met een individu of een bepaald categorie behorend persoon of plaats verbonden kan worden. Daaraan voegt de analist vaak nog gegevens uit openbare bronnen toe, zoals statistische gegevens van bijvoorbeeld het Nederlandse CBS of EuroStat. Om de bestaande data te verrijken kan hij geodemografische profielen combineren met gegevens van non-profitorganisaties of bedrijven die gespecialiseerd zijn in gegevensverzameling.

Hiermee kan de analyst 'psychogrammen'[76] van individuen of profielen van groepen mensen maken. Heuristische kennisontdekking in databanken (KDD) kan patronen zichtbaar maken die ook voor de betrokken individuen verborgen en onbekend zijn en niet voor de hand liggen. KDD kan daarnaast gebruikt worden om toekomstig gedrag te voorspellen.[77] Via psychogrammen kunnen organisaties toekomstige transacties uitlokken en op een steeds persoonlijkere manier aan consumenten aanbieden. Een voorbeeld hiervan is de wijze waarop Amazon.com klanten boeken of dvd's aanbiedt die hen mogelijk bevallen op grond van eerdere aankopen.[78] Specifieke software maakt algoritmisch toezicht mogelijk door databases met andere toezichtsystemen te combineren. Hiermee kunnen opgenomen beelden of data vergeleken worden met gegevens die in de database zijn opgeslagen. Marketingbureaus, politierechercheurs en grensbewakers passen deze vorm van *dataveillance* dan ook uitgebreid toe. De overheid kan burgers hiermee als potentiële misdadigers of terroristen bestempelen.

Landsgrenzen worden 'slimme grenzen', omdat de grensbewaking ondersteund wordt door grote databases. Die verwerken informatie over individuen en hun reisgedrag. De visie hierbij is dat de grensbewaking "the last line of defense and the first" is.[79] Justitie gebruikt profielen uit deze databases om zwarte lijsten van gevaarlijk geachte passagiers op te stellen of om groepen personen te herkennen die een risico zouden kunnen gaan vormen voor onze samenleving.[80] De betrokken personen kunnen vervolgens zeer moeilijk van een dergelijke (niet-transparante) stigmatisering afkomen. Bovendien kan het leiden tot discriminatie van bepaalde bevolkingsgroepen omdat de profielen tot bepaalde aannames kunnen leiden. Sluitend is overigens een dergelijke grensbewaking niet.

---

76 Psychologische portretten gelardeerd met demografische statistieken, die zo gedetailleerd zijn dat de betrokkenen als zij ermee geconfronteerd worden, geschokt zijn over datgene wat buitenstaanders van hen weten.

77 Tot wat voor gevolgen profiling kan leiden is te zien in de in 2002 uitgebrachte de film Minority Report is een Amerikaanse sciencefictionfilm uit 2002, geregisseerd door Steven Spielberg.

78 Fink & Kobsa, 2000, p. 209-249.

79 www.digitalforum.accenture.com.

80 Ball, e.a., 2006, p. 23.

3.4.2. Telecommunicatie

Onder 'telecommunicatie' wordt verstaan het klassieke telefoonsysteem via de vaste lijn (gesprekken en faxberichten), mobiele telefonie (gesprekken, tekst, beeld, geluid en plaatsbepaalde informatie) en computercommunicatie (o.a. e-mail en internet via breedbandverbindingen). Toen het monopolistische staatsbedrijf PTT nog analoge telefoonsystemen exploiteerde, werden telefoons doorgaans afgetapt door de politie of veiligheidsdiensten. Dit was een probaat middel om mensen mee in de gaten te houden. Vandaag de dag zijn er echter drie zaken veranderd. Allereerst is telecommunicatie gedigitaliseerd (via mobiele telefoons, glasvezel, draadloos internet etc.). Dit genereert automatisch communicatieprofielen. Ten tweede zijn telecommunicatie en computeropslag en -verwerking (e-mail, websites, etc.) met elkaar verweven geworden. Ten derde is telefonie niet meer een staatsaangelegenheid, maar is de markt vrijgegeven en opereren er vele particuliere telecomaanbieders op de markt. Deze veranderingen vereisen een toegenomen interoperabiliteit van systemen en dit leidt tot een toenemende convergentie van technologieën, die in deze sector worden toegepast.

Door het gebruik van ontologieën kunnen verschillende elektronische toezichthoudende systemen met elkaar betekenisvol communiceren.[81] Zonder deze semantische[82] interoperabiliteit zijn de verschillende systemen niet in staat allerlei signalen of gegevens met elkaar uit te wisselen. Deze uitwisseling zorgt ervoor dat Justitie controle en toezicht kunnen uitoefenen, bijvoorbeeld door het lokaliseren van mobiele telefoons en het vastleggen van het bezoek aan websites. Hoe nauwer de telecommunicatietechnieken met elkaar verbonden raken, hoe meer informatie dit kan opleveren. Zoals in paragraaf 2.9 besproken, schrijft de Richtlijn 2006/24/EG (DRD), een bewaartermijn voor van maximaal twee jaar van verkeersgegevens. De opsporingsdiensten mogen in Nederland gedurende een jaar de 'digitale voetsporen' die een gebruiker achterlaat, als hij elektronisch communiceert, analyseren. Vrijwel iedere dag worden in Nederland honderden telefoongesprekken en andere vormen van communicatie via e-mail, Internet en sms door politie, justitie en AIVD afgetapt. Daarmee behoort de Nederlandse overheid tot de koplopers in de wereld op het gebied van aftappen en afluisteren. Volgens Van de Pol tapt Nederland verhoudingsgewijs zeer veel.[83]

Nationale Overheden tappen niet alleen telefoons af, maar filteren ook routinematig geweldige hoeveelheden telefoon-, telex-, e-mail- en faxverkeer om redenen van 'nationaal belang'. Het kan daarbij zowel om staatsveiligheid als economische belangen gaan. Het wereldwijde toezichtnetwerk 'ECHELON', dat door de Amerikaanse Nationale Veiligheidsinstantie wordt beheerd, onderzoekt

---

81 Het EU research PRIME project Contract No. 507591(2004-2008) is aangetoond dat formele ontologies succesvol kunnen worden ingezet voor "reasoning capabilities and rich and flexible policy and rule languages" voor gebruik in informatiesystemen, Deliverable W.P. 7.1 Brussels 2004.

82 Maedche, 2002, p. 3-4.

83 Van de Pol, 2006. Zie ook www.onderdetap.nl: op 3 september 2009 werd in het nieuws meegedeeld dat in Nederland 26.000 telefoontaps worden geplaatst tegenover 2000 in de VS.

automatisch en routinematig al het telecommunicatieverkeer van de hele wereld op sleutelwoorden en zinsdelen en gebruikt verfijnde algoritmes voor geavanceerde spraak- en betekenisherkenning.[84]

3.4.3. Videotoezicht

Voor toezicht in de openbare ruimte worden steeds vaker videocamera's gebruikt. Er hangen camera's boven de snelwegen, in het openbaar vervoer (tram, bus of metro) en op de treinstations. Ook hangen er veel bewakingscamera's in winkels, banken en tal van andere openbare ruimtes. Het gesloten televisiecircuit (CCTV) stamt al uit de jaren zestig van de vorige eeuw en diende oorspronkelijk om gebouwen te beveiligen.[85] Vanaf de late jaren tachtig verschenen camera's echter ook in de openbare ruimte. Het Verenigd Koninkrijk liep voorop in deze ontwikkeling. De verklaring hiervoor is tweeledig: aan de ene kant wilde de Britse overheid de achteruitgang van de winkelstraten in de binnenstad tegengaan en aan de andere kant terrorisme, misdaad en ongeregeldheden voorkomen. In Groot-Brittannië is er nu één camera op elke veertien mensen en iemand kan op meer dan driehonderd camera's per dag opgenomen worden. In veel Nederlandse gemeenten zijn inmiddels ook op meer of minder grote schaal videocamera's in gebruik, vaak in samenwerking met de plaatselijke politie. Ook een groeiend aantal bedrijven exploiteert camerasystemen voor de veiligheid van de klant en het personeel. Digitalisering heeft ervoor gezorgd dat videobewakingssystemen steeds meer automatisch gebruikt worden. CCTV wordt beschouwd als een multifunctionele technologie om risico's te beheersen. Uit onderzoek blijkt dat CCTV voornamelijk voor sociale controle (asociaal gedrag en misdaad) wordt ingezet. Dit heeft tot gevolg dat het systeem reageert op ingeprogrammeerde voorspelbare discriminatoire patronen, die kunnen leiden tot sociale uitsluiting van bepaalde bevolkingsgroepen.[86]

3.4.4. Biometrie

In de sciencefictionfilm *Minority Report* worden mensen binnen een milliseconde automatisch geïdentificeerd door een scan van hun irissen. Als individuen willen ontsnappen aan een dergelijke identificatie dan is er maar één mogelijkheid namelijk door van oogbollen te wisselen.[87] Er zijn drie mogelijkheden om de identiteit van iemand vast te stellen, namelijk door iets wat de persoon bezit, bijvoorbeeld een sleutel of een chipcard, of door iets wat de persoon weet, bijvoorbeeld een wachtwoord of een PIN, of door iets wat de persoon is, bijvoorbeeld menselijke (biometrische) kenmerken, zoals rood haar of groene ogen. Medisch onderzoek

84 Cambell, 1999.
85 De Mulder, Oey & Van Schelven, 2004, p. 714.
86 Hempel & Töpfer, 2004, p. 40-47.
87 Minority Report is een Amerikaanse sciencefictionfilm uit 2002, geregisseerd door Steven Spielberg en gebaseerd op het gelijknamige korte verhaal van Philip K. Dick.

heeft aangetoond dat ieder individu bepaalde unieke menselijke kenmerken heeft.[88] Dit kunnen lichamelijke kenmerken (vingerafdrukken) en gezichtsuitdrukkingen zijn, maar ook gedragspatronen zoals de druk die een pen uitoefent op het papier wanneer iemand zijn handtekening zet. Het gebruik van deze menselijke uniciteit wordt al lang toegepast bij politieonderzoek (vingerafdrukken) of bij identificatie van lijken (gebit). Sinds een tiental jaren worden specifieke lichamelijke kenmerken ook toegepast bij de elektronische informatie beveiliging. Onderzoek heeft ook aangetoond dat emoties invloed hebben op bepaalde biometrische kenmerken, zoals blijkt uit het gebruik van een leugendetector.[89] Nieuwe producten zijn in staat om verborgen emoties van mensen aan het licht te brengen wanneer zij met anderen spreken of wanneer ze aan het onderhandelen zijn. Stemanalyse heeft aangetoond dat de hoogte van de stem al verandert (dus indicatief is) voordat werkelijk met een voorstel wordt ingestemd.[90] Overigens werkt spraakherkenning nog niet perfect, met name als de stem getapt wordt.[91] DNA kan niet alleen onomstotelijk de identiteit van personen vaststellen maar ook ziekten van die persoon voorspellen. Vergelijking tussen verschillende biometrische kenmerken toont aan dat de irisscan en DNA een zeer grote betrouwbaarheid oplevert[92] voor identificatie (wie ben je?) en authenticiteit (ben je wie je zegt te zijn?).

Bijna alle nieuwe ID-systemen (paspoorten) maken gebruik van één of ander 'biometrisch' of lichaamskenmerk als kern en beginpunt om iemands identiteit vast te stellen. Voorbeelden hiervan zijn vingerafdruk, irisscan, gezichtstopografie, stempatroon en handgeometrische scans. Op 9 juni 2009 heeft de Eerste Kamer ingestemd met de gewijzigde Paspoortwet.[93] Door de aangenomen wet zullen, om fraude met reisdocumenten tegen te gaan, voortaan alle nieuwe paspoorten en identiteitskaarten voorzien worden van biometrische gegevens die in een chip in de paspoorten en de reisdocumenten worden opgeslagen. Het gaat om twee vingerafdrukken en een gezichtsscan van de houder. Alle landen van de Europese Unie moeten vingerafdrukken opnemen in hun reisdocumenten, zodat autoriteiten beter kunnen controleren of de bezitter van het paspoort ook de rechtmatige eigenaar is. Door het van kracht worden van de wet kan de overheid deze gegevens in een centrale databank opslaan die 24 uur per dag door Justitie te raadplegen is. Hierover is terecht maatschappelijke commotie ontstaan. De opslagtechnologie is nog niet goed ontwikkeld. Met de versleuteling van de gegevens kunnen vingerafdrukken worden gere-engineerd, en de databank kan worden gekraakt.[94] De privacyvereniging Vrijbit probeerde in september 2009 bij het Europese Hof voor de Rechten van de Mens een voorlopige voorziening af te dwingen waardoor de opslag zou moeten worden opgeschort. Het hof wees dit

88 Verhaar, Van Rhee & Borking, 1999, p. 9.
89 Juan, 2006; Gibbons, 1983.
90 Spreker herkenning moet niet verward worden met spraakherkenning, de interpretatie door machines van uitgesproken instructies, zoals: "Print dit document".
91 Van de Pol, 2006.
92 Hes, Hooghiemstra, & Borking, 1999, p. 25.
93 Eerste Kamerstuk, 2008-2009, 31 436, E.
94 Sprokkereef, e.a, 2009, p. 9.

echter af. De organisatie heeft nog een bodemprocedure bij het hof aangespannen. Hes, Hooghiemstra, & Borking hebben erop gewezen dat slechts verificatie gecombineerd met de decentrale opslag van het digitale patroon (template) (ernstige) privacy incidenten kan voorkomen: "(…) As a rule both the storage of templates and the verification process should be decentralised. In some specific cases and environments, the processing of personal data can be seen as a pure personal activity, (…) the protection of personal data can be realised by using different encryption keys and algorithms to encrypt the personal data (including biometrical data) in different databases. The original biometrics should (…) be destroyed after the derivation of the digital template; (…) Certification of the privacy-compliance of products will guarantee an adequate handling of the personal data of future users".[95] Het irisscansysteem op de luchthaven van Schiphol werkt op bovenstaande manier. Daarmee wordt voorkomen dat disproportionele identificatie plaatsvindt, terwijl niet meer dan verificatie van de passagier voldoende is.

Op dezelfde manier kan de controle van de vingerafdrukken in het paspoort plaatsvinden. Centrale opslag van vingerafdrukken in een databank is niet nodig om identiteitsfraude te voorkomen. Mocht opslag toch in een centrale databank plaatsvinden, dan wijzen Verhaar e.a. erop dat om privacyinbreuken te voorkomen: "that all templates (...) are processed with mathematical manipulations, using different parameters for every biometrics product in use. (...) The mathematical manipulations could be encryption algorithms or (one-way) hash functions. (...) Before the template is stored in the template database, the template is processed with the hash-function, generating a hash-value of the template. This hash-value will be stored in the template database. When verification of a human characteristic is needed, the digital representation of the characteristic will be hashed, resulting in a hash-value of the characteric. If the hash-value of the template matches the hash-value of characteristic (in the template database) the person involved is identified".[96]

De Nederlandse overheid heeft gekozen voor de vastlegging van de gegevens over biometrische kenmerken in een centrale reisdocumentenadministratie. Daarmee opteert zij voor grotere privacyrisico's en een niet gerede kans op de privacyinbreuken. Biometrie in combinatie met data mining wordt geacht de nauwkeurigheid van de vast te stellen identiteit te vergroten en de fraude te doen afnemen. Men kan zijn pincode en wachtwoord vergeten of verliezen, maar het lichaamskenmerk biedt een constante rechtstreekse verbinding tussen datgene wat over dat lichaamkenmerk en de persoon is vastgelegd. Dat wil overigens niet zeggen, dat met biometrische kenmerken niet te frauderen valt. Illustratief is het voorbeeld van de 'geleende' vingerafdruk in de James Bondfilm 'Diamonds are forever' uit 1971 waarmee Bond een andere identiteit aanneemt.

95 Hes, Hooghiemstra, & Borking, 1999, p. 55, 63.
96 Verhaar, e.a.,1999, p. 48-50.

Het biometrische toezicht houden is vooral na 9/11 door de Verenigde Staten gestimuleerd. De Verenigde Staten hebben zich sterk gemaakt voor wereldwijd gestandaardiseerde normen voor apparatuur die biometrische gegevens in paspoorten kan lezen. In het standaardisatievoorstel van de Verenigde Staten zullen niet alleen 'templates' van biometrische scans worden vastgelegd maar ook de biometrische beelden (bijvoorbeeld niet de topografische punten van een gezichtsscan maar het gezicht zelf).[97] Inmiddels moeten bezoekers aan de Verenigde Staten tijdens paspoortcontrole, naast een gezichtscan, een digitale afdruk laten maken van alle tien vingers. Inmiddels zijn miljarden biometrische scans in het 'Integrated Automated Fingerprint Identification System' van de FBI opgeslagen.[98] Naast identificatie kan biometrie ook gebruikt voor authenticatie.[99] Biometrische toegangssystemen beginnen thans norm te worden voor toegang tot vele kantoorgebouwen, en worden ook op een aantal vliegvelden toegepast, zoals bijvoorbeeld het Privium irisscannsysteem op het vliegveld Schiphol. Hiermee vindt overigens uitsluitend verificatie van het individu plaatst door vergelijking van de digitale template op de chipkaart met de feitelijke irisscan. Biometrie is ook steeds meer op straat te vinden. Steden zoals Newham (Londen), Birmingham en Manchester hebben geëxperimenteerd met detectiesystemen die automatisch gezichten herkent.[100] In verband met de Europese Kampioenschappen Voetbal in 2008 in Zwitserland en Oostenrijk, is gezichtsherkenning toegepast om de veiligheid van bezoekers van sportevenementen te verbeteren en om notoire relschoppers te verwijderen. Ook werd de gemoedstoestand van de bezoekers in de gaten gehouden. Als die veranderde van rustig naar agressief (armzwaaien, open mond, vuistballen, middelvinger opsteken, etc.), konden de autoriteiten in het stadion onmiddellijk maatregelen nemen.[101]

3.4.5. Plaatsbepaling, volgen en merken

Personen kunnen steeds nauwkeuriger worden getraceerd via hun mobiele telefoon. Het gsm-systeem[102] van de telecommunicatieaanbieder kan automatisch bij het tot stand komen van het gesprek bepalen in welke cirkel rond welke gsm-

97 Cavoukian & Stoianov, 2007, p. 9.

98 Cavoukian & Stoianov, 2007, p. 9: "Storing, transmitting and using biometric *images* (…) exacerbates the privacy concerns with large-scale identification systems, since a very important privacy protection afforded by templates is removed, namely, the inability to exactly reconstruct the original biometric image from the template. The image (…) can be converted into hundred of templates for matching and identification (…) purposes such as creating personal profiles and, (…) for committing identity theft. At this point the privacy implications explode."

99 In de meeste informatiesystemen maakt de gebruiker zich bekend (identificatie) voor de dienstverlener, waarop de dienstverlener de identiteit van de gebruiker controleert (authenticatie). Zie in dit boek hoofdstuk 5 paragraaf 5.1.

100 Ball, e.a., 2006, p. 24.

101 Gezichtherkenning door middel van het Happy Crowd System 2007 www.hln.be/hlns/cache/det/art_373362.html.

102 Gsm staat voor Global System for Mobile communications en is de wereldwijde standaard voor mobiele telefoons.

mast de mobiele telefoon zich bevindt. Personen kunnen in de gaten worden gehouden en gevolgd via GIS (Geographic Information Systems: geografische plaatsbepalingsystemen), GPS (Global Positioning Systems: wereldwijde plaatsbepalingsystemen), RFID (Radio Frequency Identification)-chips, slimme ID-kaarten, transponders of door de radiosignalen die door mobiele telefoons of draagbare computers worden uitgestraald.[103]

RFID's verdienen een korte nadere beschouwing, omdat deze chips beschouwd worden als voorlopers van (nano)microscopische sensors[104] die in de toekomst in ambient intelligente omgevingen[105] massaal door aanbieders van goederen en diensten zullen worden gebruikt om de consument te volgen en te dienen. Er zijn twee toepassingen van RFID's te onderscheiden:

1. Productgebonden toepassingen die producten en lastdragers (pallets, containers, dozen) identificeren.
2. Persoonsgebonden toepassingen om personen te identificeren.[106] Het individu draagt een of meerdere *tokens* bij zich.

Een 'token' is een opslagmedium dat informatie bevat die gebruikt kan worden voor identificatie, authenticatie en autorisatie. Voorbeelden van tokens zijn bankpassen, creditcards en toegangskaarten voorzien van een magneetstrip of chip. De in te voeren ov-chipkaart gebruikt contactloze tokens, dat wil zeggen dat de token op afstand kan worden gelezen, zelfs als deze nog in de portemonnee zit. Maar daar houden de toepassingen niet op. RFID-labels op voedsel, kleding, huishoudelijke apparaten etc. kunnen voor de consument gemak met zich meebrengen. Men kan verloren voorwerpen in huis gemakkelijk terugvinden, nagaan of in de koelkast de uiterste houdbaarheidsdatum van etenswaren niet verlopen is. Met diezelfde chips kunnen bedrijven echter ook gegevens over consumentengedrag verzamelen.[107] Door RFID-technologie binnen een personeelsvolgsysteem[108] te gebruiken kunnen werkgevers veelal makkelijker gegevens over de werknemers verzamelen en verwerken. Met behulp van RFID kan dit ook heimelijk gebeuren. RFID-chips kunnen ook worden geïmplanteerd in levende wezens. Chips die informatie bevatten over immunisatie en eigendom hebben geleidelijk de quarantainevoorschriften voor huisdieren in de EU vervangen.[109] Deze 'PETS-regeling' is daarna tot buiten Europa uitgebreid. In Japan slikken koeien RFID-*tags* in om de lichaamstemperatuur, ademhalingsritme, hartslag van de koe te meten en, bij zwangerschap, gegevens over het kalf bij

103 De Mulder, Oey & Van Schelven, 2004, p. 720.
104 De Mulder, Oey & Van Schelven, 2004, p. 723.
105 Zwenne & Schermer, 2005, p. 26.
106 Schermer, 2006, p. 8.
107 Zwenne & Schermer 2005, p. 63.
108 Een geautomatiseerd systeem waarin individuele en geaggregeerde gegevens van en over werknemers worden vastgelegd.
109 Verordening (EU) Nr. 998/2003 van 26 mei 2003 inzake veterinairrechtelijke voorschriften voor het niet-commerciële verkeer van gezelschapsdieren en houdende wijziging van Richtlijn 92/65/EG;
Commission Regulation (EC) No 911/2004 of 29 April 2004 implementing Regulation (EC) No 1760/2000 of the European Parliament and of the Council as regards eartags, passports and holding registers.

te houden.[110] Inmiddels worden RFID-chips bij bejaarde mensen in de Verenigde Staten toegepast die aan degeneratieve ziekten lijden. Bij zeventig van hen is een chip geïmplementeerd zodat hun verzorgers hen makkelijk kunnen terugvinden. Sommige onderzoekers en technofielen laten sinds enkele jaren chips bij henzelf implanteren. In februari 2006 heeft een beveiligingsbedrijf in Ohio, Verenigde Staten, bij twee van zijn medewerkers RFID-chips geïmplanteerd om hen toegang te geven tot de gebouwen en terreinen van het bedrijf.[111] De Baja Beach Club heeft zowel in Barcelona als in Rotterdam[112] VIP-bezoekers de mogelijkheid geboden om een RFID-chip (VeriChip) bij zichzelf te laten implanteren voor contactloze toegang (dus zonder nog een pasje bij zich te hoeven dragen) tot alle faciliteiten van de sportclub. Op sommige websites is zelfs een serieus debat gevoerd over het idee om bij kinderen chips onderhuids aan te brengen om hen snel te kunnen opsporen als zij zouden zoekraken.[113]

3.5. Sociale uitsluiting en Informatieapartheid

In de toezichtmaatschappij is sociale uitsluiting wijd verspreid. Discriminatie van mensen door de toegang tot bepaalde voorzieningen, producten of diensten te ontzeggen, komt steeds meer voor. Thomas waarschuwt hiervoor en stelt dat: "The risks that arise as a result of excessive surveillance affect us individually and affect society as a whole. There can be excessive intrusion into people's lives with hidden, unacceptable and detrimental uses. Mistakes can be made and inaccuracies can occur disrupting individuals' everyday lives. Breaches of security can have even more significant consequences and there is great potential for more discrimination, social sorting and social exclusion."[114]

Bij de overheid en in de marketing worden grote databases met persoonlijke informatie geanalyseerd en gecategoriseerd om risicobevolkingsgroepen en doelmarkten[115] te omschrijven. In de twintigste eeuw was het beleid van de overheid erop gericht om alle burgers in aanmerking te laten komen voor sociale voorzieningen. Vandaag de dag lijkt het echter alsof de prioriteit van het beleid van de overheid erop gericht is ongewenste elementen in de samenleving buiten te sluiten. Is men eenmaal ingedeeld in een bepaalde categorie, dan is het moeilijk er weer uit te komen. De in hoofdstuk 2 besproken 'no-fly list' is daar een voorbeeld van. In de VS is men ervan overtuigd dat deze 'sociale sortering' sinds '9/11' heeft bijgedragen aan meer veiligheid in het luchtruim. Tegelijkertijd heeft sociale sortering ertoe geleid dat de westerse overheden profielen van groepen hebben

110 Zwenne & Schermer, 2005, p. 63.
111 Waters, 2006, www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html.
112 Zwenne & Schermer, 2005, p. 24.
113 www.thewatcherfiles.com/articles/mark_beast.html.
114 Thomas, 2007, p. 6.
115 Een voorbeeld van de negatieve effecten hiervan: Rothfeder, 1992, p. 102-105: "living below the curve, as micromarketers indelicately call them". "These people are so disenfranchised that they don't even get good junk mail".

opgesteld, met name van mensen met Arabische namen, met een moslimachtergrond, uit de Maghreb en andere verdachte moslimlanden. Voor deze mensen geldt: "these systems tend to miliate against movement both within and between countries."[116] Het sociaal sorteren[117] bepaalt in toenemende mate de infrastructuur van de toezichtmaatschappij. Het sluit allerlei groepen uit van verschillende mogelijkheden. Mensen die bijvoorbeeld veel reizen en de financiële middelen hebben om een speciale ID-pas aan te schaffen kunnen sneller langs de douane en frequent flyers hebben voorrang wanneer zij een stoel in het vliegtuig reserveren en inchecken. Tegelijkertijd bieden bedrijven bij hun (gerichte) marketing de minder draagkrachtigen (die in bepaalde buurten wonen) niet dezelfde kortingen op hun producten aan als zij aan koopkrachtige mensen doen. Sociale sortering leidt in toenemende mate tot informatie-apartheid en zorgt er dikwijls voor dat de samenleving subtiel en soms onbedoeld geordend wordt.[118]

Toezicht kent twee gezichten. Aan de ene kant kan het leiden tot persoonlijke en sociale voordelen. Als het echter op grote schaal wordt toegepast kan dit belangrijke gevolgen hebben voor de vrijheid (de privacy) van het individu, voor innovaties en veranderingen in de samenleving.[119] Klüver[120] beschrijft het 'Big Mother Society'-scenario om aan te geven dat wij inmiddels in een maatschappij zijn aanbeland waarin veel afzonderlijke beslissingen tot doel hebben onze veiligheid te verhogen. Iedere afzonderlijke beslissing vormt weliswaar geen ernstige bedreiging voor de persoonlijke levenssfeer, maar het cumulerend effect kan resulteren in een Big Brotherachtig scenario.

Onzichtbare systemen als rekeningrijden en intelligente verkeersdoorstroming die steeds meer ingeburgerd raken, hebben zeker hun nut, maar bij beide wordt de stad of het land in sectoren verdeeld waarbinnen sommigen zich relatief ongehinderd kunnen verplaatsen (al dan niet tegen betaling), terwijl dat voor anderen moeilijker wordt. Tegelijkertijd kan met dit soort systemen de misdaad bestreden en de nationale veiligheid worden verhoogd. In Nederland hebben in 2001 de Registratiekamer en de Ministeries van Verkeer en Waterstaat en Financiën dit probleem onderkend. In het kader van het voorstel Wet kilometerheffing en later het wetsvoorstel bereikbaarheid en mobiliteit is een systeem voor rekeningrijden ontwikkeld dat het mogelijk maakt de privacy te beschermen en sociale sortering te voorkomen.[121] Of het in november 2009 door de Minister van Verkeer en Waterstaat te presenteren wetsvoorstel voor de kilometerheffing privacy van de autobestuurder goed beschermd is onbekend. Het is voorspelbaar dat de kilometerheffing veel privacycommotie zal gaan opleveren.

116 Ball, e.a., 2006, p. 43.
117 Ik gebruik de term sociale sortering als vertaling van social sorting i.p.v. sociale uitsluiting omdat het sorteren plastischer aangeeft wat er feitelijk gebeurt, nl. schiften van the haves and the have-nots.
118 Borking, 1998.
119 Beck, 1992.
120 Klüver, Peissl & Tennøe, 2006, p. 29.
121 De Registratiekamer, Den Haag, Brief van 6 maart 2001, Z2001-0336 inzake Wetsvoorstel bereikbaarheid en mobiliteit.

Ondertussen participeert de 'digitale generatie' van jonge mensen geboren na 1980 steeds meer in de virtuele samenleving.[122] In vele virtuele gebieden van die samenleving geldt 'zero tolerance' bij overtreding van de sociale regels. Chatroom conversaties[123] worden gelogd en gebruikt als bewijs om mensen te weren van websites en uit chatrooms. Conformeren is de regel. Mogelijk wordt dit op termijn een trend in de niet-virtuele samenleving. Chatroomconversaties zijn in Nederland ook al gebruikt als bewijsmiddel in rechtszaken.[124] Jongeren tussen de 15 en 24 jaar surfen er nochtans flink op los. Slechts 20% zegt in een onderzoek van de Eurobarometer (2008) dat zij zich van tevoren afvragen of het (ogenschijnlijk) veilig is hun persoonsgegevens via internet te versturen. Jongeren beseffen niet dat alles wat zij op internet via YouTube, Hyves etc. communiceren vastligt en zelfs nog jaren later als bewijs kan dienen, bijvoorbeeld om aan te tonen dat iemand ongeschikt is voor bepaald werk.

3.6. Het falen van de technologie

De beloofde technische prestaties van (innovatieve) informatiesystemen worden bijna nooit helemaal waargemaakt. Daarvan getuigen bijvoorbeeld de vele ict-arbitrages.[125] De biometrische technieken voor het USVISIT programma, bijvoorbeeld, zijn om logistieke redenen teruggebracht van de geplande irisscans tot digitale vingerafdrukken en scans van het gezicht van de reiziger. Evenzo zijn er uitvoeringsproblemen geweest met de biometrische onderdelen van het e-Borders programma van het Verenigd Koninkrijk. De prestaties van gezichtsherkenning blijken onvoldoende geschikt voor situaties die in de praktijk voorkomen.[126] Het *Criminal Records Bureau* in het Verenigd Koninkrijk (Instantie voor verschaffing van informatie betreffende strafregistraties) onthulde dat in haar systeem van circa 2.700 mensen ten onrechte was vastgesteld dat ze veroordelingen op hun naam hadden staan. Een aantal kreeg geen baan als gevolg van de foutieve informatie-'dubbelgangers'.[127]

Dit zal in Nederland niet veel anders zijn. De Registratiekamer onthulde al in de negeniger jaren dat door fouten vele Nederlanders in politieregisters stonden, die daar niet in thuis hoorden. Dit is niet zo verwonderlijk. Het is algemeen bekend dat databanken erg vervuild zijn. Met de toenemende profilering in de toezichtmaatschappij zal de groei van vals-positieve treffers toenemen. Hierdoor kunnen onschuldigen onterecht als gezochte crimineel te boek staan en gearresteerd worden.[128]

---

122 Van 't Hoff, Van Est, & Krom, 2005.
123 Een chatroom is een webbased forum waarvan de bezoekers (real time) informatie met elkaar kunnen delen.
124 Voor een bijvoorbeeld: Rechtbank 's-Gravenhage, 09/753596-03 betreffende verspreiding van kinderpornografische afbeeldingen in een MSN-groep, LJN:AY5348.
125 Franken & Borking, 2002.
126 Amoore, 2006, p. 336-351.
127 Norris, 2006, p. 8.
128 Schneider, 2003.

Fouten in databases kunnen de toegang tot plaatsen of diensten beperken, maar in andere gevallen, bijvoorbeeld bij medisch toezicht, kunnen ze levensbedreigend zijn zoals de sciencefictionfilm *The Net* op overtuigende wijze laat zien.[129]

3.7. Gevolgen voor de privacybescherming

De diepere oorzaak voor de toezichtmaatschappij met steeds meer antiterrorisme wetgeving is niet direct gelegen in '9/11' en daaropvolgende aanslagen, die wereldwijd hebben plaatsgevonden, maar in de sinds de zeventiger jaren van de vorige eeuw geleidelijk ingezette ontwikkeling van de netwerksamenleving waarbij de nadruk op risicoanalyse is komen te liggen. Om de collectieve veiligheid in de samenleving zo goed mogelijk te garanderen is daar vervolgens de risicosurveillance uit voortgekomen. Het staat buiten kijf dat de toezichtmaatschappij de burgers voordelen biedt. Er zijn echter ook negatieve gevolgen. Lyon waarschuwt dan ook terecht: "Surveillance fosters suspicion".[130]

De studie Veiligheid en Privacy in 2030[131] wijst erop dat panoptische technologie steeds vaker zal worden ingezet om mensen heimelijk in de gaten te houden. Omdat de sensoren (RFID's) die ons omringen steeds kleiner zullen worden, zal surveillance voor het individu steeds onzichtbaarder worden. Identiteitskaarten in 2030 zullen achterhaald zijn en hun functie zal door sensoren worden overgenomen, mogelijk op een manier zoals de film *Minority Report* (2002) laat zien.[132]

Adequate risicobeheersing in de moderne samenleving brengt met zich mee dat zo veel mogelijk kennis van de te analyseren situatie voorhanden is. Toegang tot persoonlijke gegevens wordt gezien als een voorwaarde om te weten waar de overheid de preventieve of curatieve middelen moet inzetten.[133] Risicoprofielen zijn snel te maken dankzij de grote interconnectiviteit van toezichtnetwerken. Sociale sortering zorgt ervoor dat de politie haar aandacht meer richt op overwegend niet-blanke of sociaal lager gekwalificeerde wijken en dat grote supermarkten en 'shopping malls' zich in de betere kapitaalkrachtigere buitenwijken bevinden, die makkelijker met de auto te bereiken zijn.[134]

---

129 The Net is een in 1995 uitgebrachte film van Irwin Winkler.
130 Lyon, 2003 (A), p. 45-48.
131 Koops, e.a., 2005, p. 18.
132 Minority Report is een Amerikaanse sciencefictionfilm uit 2002, geregisseerd door Steven Spielberg. Volgens deze film is de irisscanner voor 'eyedentification' als identificatiemiddel in de nabije toekomst algemeen gebruik.
133 Ball, e.a., A Report on the Surveillance Society, Manchester 2006, p. 47.
134 Borking, 1998 (A), p. 56-62.

In de Volkskrant van 7 november 2009 zegt Frissen: "(...) wij verdagen geen risico's meer. Het wetenschappelijk instrumentarium om risico's op te sporen en te voorspellen is een enorme industrie geworden. Wat we vroeger alleen deden op het terrein van de veiligheidsdiensten, dingen proberen te voorkomen, is nu uitgebreid naar het totale sociale- en welzijnsdomein".[135]

Het is maar de vraag in hoeverre individuen en groepen nog zelf kunnen bepalen hoeveel ze blootgesteld willen worden aan toezicht en hoezeer zij de persoonlijke informatie kunnen beperken die over hen verzameld en gebruikt wordt. Toezichtsystemen zijn voor een leek vaak moeilijk te begrijpen en gaan onzichtbaar en daardoor ongemerkt op in de alledaagse structuren en systemen van de maatschappij: op het werk, thuis, op school, op reis en bij communicatie en openbare diensten.[136] Bovendien is het informationele privacybewustzijn van de burgers laag. Pas nadat er op epidemische schaal '*data rape*'[137] met diefstal van identiteit is uitgebroken, zullen de burgers zich bewust worden hoe kwetsbaar zij zijn, in welke mate grote organisaties persoonlijke profielen over hen opstellen en welk effect dat op hen heeft. Gezien de complexiteit van de toezichthoudende middelen mag van de 'man in the street' niet simpelweg verwacht worden dat hij zichzelf kan beschermen tegen privacyinbreuken, maatschappelijke uitsluiting en informatiediscriminatie.

De toezichtmogelijkheden van de overheid zullen uitdijen. Dit zal leiden tot meer persoonsgegevens die de overheid vervolgens zal inzetten om de levensomstandigheden van de burger vorm te geven (bijvoorbeeld door (ongevraagd) gerichte subsidies toe te kennen of mensen te begeleiden) en hun keuzes te sturen.

Burgers kunnen slechts met veel moeite er achter komen wat er met hun persoonlijke gegevens gebeurt en wie deze wanneer en met welk doel hanteert. Er bestaat een informatie asymmetrie tussen het individu en degenen die het toezicht uitoefenen. Een voorbeeld hiervan is het videotoezicht dat steeds onzichtbaarder wordt.[138] Individuen zijn nauwelijks in staat de verschillende vormen toezicht te overzien en zich daartegen te beschermen,[139] zeker wanneer de rechter niet zorgt voor een effectief tegenwicht tegen de toezichtplannen van beleidsmakers.

Het toezicht met de inherente gegevensuitwisseling wordt voor een belangrijk deel door justitie en politie uitgevoerd. Koelewijn schrijft dat er vijf knelpunten zijn in de uitwisseling van politiegegevens. Namelijk: 1 moeilijk toegankelijke juridische kennis, die naleving door politieambtenaren bemoeilijkt; 2 ontoereikende gegevenscontrole, waardoor de juistheid, tijdigheid en volledigheid van de gegevens te wensen overlaat; 3 onvoldoende standaardisatie door de diversiteit

135 Van Hintum, 2009, p. 35.
136 Weiser, 1991, p. 94-104.
137 Rothfeder, 1992, p. 27-30 "people ... feel violated, vulnerable, ineffectual and deprived of their dignity."; Rothfeder, 1992, p. 210: "people will stop being productive citizen".
138 Bennett & Raab, 2006, p. 27.
139 Ball e.a., 2006, p. 6.

van de informatiesystemen waardoor de interne gegevensuitwisseling wordt belemmerd; 4 gesloten bedrijfscultuur waar het delen van informatie alles behalve van zelfsprekend is; 5 ontoereikende privacywaarborgen ten gevolge van tekortschietende controle en toezichtmechanismes via de privacyfunctionaris en het CBP, waardoor er nauwelijks prikkels zijn de privacyregels na te leven.[140]

Dat belooft weinig goeds voor onze risicotoezichtsamenleving.

De Britse Information and Privacy Commissioner waarschuwt voor het risico dat de toezichtmaatschappij voor de burger en de samenleving met zich meebrengt: "For individuals the risk is that they will suffer harm because information about them is: inaccurate, insufficient or out of date; excessive or irrelevant; kept for too long; disclosed to those who ought not to have it; used in unacceptable or unexpected ways beyond their control; or not kept securely. For society the wider harm can include: excessive intrusion into private life which is widely seen as unacceptable; loss of personal autonomy or dignity; arbitrary decision-making about individuals, or their stigmatisation or exclusion; the growth of excessive organisational power; a climate of fear, suspicion or lack of trust."[141]

De gegevensstromen die met het toezicht gemoeid zijn, zijn mondiaal. Wereldwijd wordt op de mobiliteit van mensen en hun activiteiten toezicht gehouden. Mondiale wetgeving op het gebied van toezicht bestaat (nog) niet. Om de privacy van mensen adequaat te beschermen is een meer geïntegreerde, mondiale wetgeving nodig. Als dat niet mogelijk is, dan zou langs de weg van standaardisatie een oplossing moeten worden gevonden. Gebruikers, consumenten, ontwikkelaars en beleidsmakers zouden bij deze uitdagingen betrokken moeten worden om een proportioneel toezicht met een opt-in of opt-outregeling te verwezenlijken. De ontwikkeling van de ict is in velerlei opzichten een niet-omkeerbaar fenomeen. Dit houdt in dat wanneer in het huidige ontwerp van ict-producten de bescherming van persoonsgegevens wordt genegeerd om wille van het toezicht of om andere redenen, dit de privacybescherming in de komende tien of twintig jaar negatief kan beïnvloeden.

De toezichtsamenleving is ook een niet omkeerbaar feit en zal niet meer verdwijnen. Zij maakt in toenemende mate georganiseerd en gestructureerd gebruik van op toezicht gebaseerde technieken met een complexe infrastructuur die veel persoonsgegevens verwerkt.

Gilbert[142] ziet drie mogelijke scenario's voor de nabije toekomst:

1. 'Big Brother', waarin met name de gegevensontdekkende technologieën domineren, zoals data mining en data warehousing. In dit scenario leidt de dominante technologie tot gigantische databanken met een zeer sterke speurkracht. Alles is voor eeuwig vastgelegd en digitale patroonherkenning in grote hoeveelheden data kan zeer snel geschieden. Dergelijke databanken worden

140 Koelewijn 2009, p. 129.
141 Thomas, 2007, p. 6.
142 Gilbert 2007, www.raeng.org.uk.

beheerd, hetzij door de overheid (Big Brother), hetzij door commerciële organisaties. Omdat de kosten van data processing scherp zullen dalen, zullen ook individuen in staat zijn om voldoende opslag- en speurcapaciteit voor henzelf en ten nadele van anderen in te zetten. De privacy is in dit scenario verloren.

2. Bij het tweede scenario 'Big mess' domineren de technologieën die data volgen, zoals RFID's en NFC (zie paragraaf 3.2). De chip in het paspoort, in de ov-chipkaart, in kleding en lichaam maken volledig toezicht mogelijk. In dit scenario zal het toepassen van de juridische ontwerpspecificaties (zie paragraaf 2.14) voor het verwerken van persoonsgegevens zeer moeilijk zijn af te dwingen en zal het moeilijk zijn om fraude vast te stellen. Vooral als deze technologieën gecombineerd worden met niet-robuuste (zwakke) technologieën die data aan elkaar koppelen (smart cards, SIM's in mobiele telefoons, biometrische technologieën zoals spreker identificatie) zullen er voortdurend op grote schaal privacy incidenten plaatsvinden. Persoonsgegevens zullen tegen de wens van betrokkenen door data te lekken publiek gemaakt worden en er zal op een misdadige manier van toezicht en persoonsgegevens gebruik gemaakt worden.
3. Het derde scenario is 'Little Sisters'. In dit scenario domineren de gegevenskoppelende technologieën. Persoonsgegevens zullen routinematig versleuteld worden en (digitale)identiteiten zullen worden gefragmenteerd. De sleutels tot deze gefragmenteerde identiteiten zullen beheerd worden door de 'Little Sisters". Dat zijn nu de ISP's en creditcard maatschappijen en straks zullen dat de 'identity management brokers' zijn, waar veel persoonsgegevens zullen zijn opgeslagen met mogelijke ernstige privacyinbreuken als gevolg.

Deze scenario's versterken het negatieve beeld van de risicotoezichtsamenleving.

Hoe kunnen wij ons tegen deze ontwikkelingen beschermen, die onze privacy steeds meer erodeert. Camp wijst erop dat: "Allowing individuals to gain control of surveillance is perhaps the only way for this (surveillance building) system to be accepted and to be maintained inside the democratic space as we know it (…) what we need are the keys to our own computer AND the permission to gain access (potentially) to the log files where every part of our body data lies."[143]

Gilbert[144] meent dat bij het ontwerp van informatiesystemen moet rekening houden met de gevaren die in de drie scenario's zijn geschetst. Het verlies en het lekken van data maakt het noodzakelijk dat de persoonsgegevens altijd versleuteld worden opgeslagen en dat er zo min mogelijk data wordt opgeslagen. De gevolgen van fouten in verwerkte data kunnen verkleind worden door in elk informatiesysteem de mogelijkheid in te bouwen, die burgers in staat stelt om hun persoonsgegevens altijd te kunnen inzien en te kunnen controleren op fouten.

143 Camp & Lewis, 2004, p. 218-221.
144 Gilbert, 2007, www.raeng.org.uk.

Bovendien dient de wetgeving er voor te zorgen, dat bij privacyincidenten de betrokkenen worden ingelicht en hun schade wordt gecompenseerd.

Gezien de in dit hoofdstuk geconstateerde feiten moet het antwoord op de tweede onderzoeksvraag: '*Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger door middel van ict-systemen preventief in de gaten te houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding*?' bevestigend beantwoord worden.

Als wij onze privacy willen behouden, dan zal het antwoord op de tweede onderzoeksvraag ontkennend moeten zijn. Dat kan alleen als de burger zelf controle (toezicht) kan houden op zijn eigen persoonsgegevens. Om dat te bereiken zullen informatiesystemen moeten worden gebouwd die onze privacy adequaat beschermen, het vertrouwen in de verwerking onze persoonsgegevens bevorderen en ons tegen de kwalijke gevolgen van de risicotoezichtmaatschappij beschermen. Technologieën die privacy bevorderen (PET) zijn geen panacee om alle privacyproblemen op te lossen, maar kunnen, wanneer PET systematisch zijn geïntegreerd in systeemontwikkeling, bijdragen aan een gebalanceerde relatie tussen toezicht en privacybescherming. De antwoorden op de onderzoeksvragen 4 (OV 4) en 5 (OV 5) in de hoofdstukken 5 en 6 moeten aantonen of een gebalanceerde relatie tussen toezicht en privacybescherming mogelijk is.

In ieder geval zou er veel gewonnen zijn als er wetgeving komt die opdrachtgevers voor en ontwerpers van informatiesystemen verplicht om voor de bouw van het informatiesysteem een privacybedreigingsanalyse of privacyimpactanalyse (PIA) uit te voeren. Zo kunnen zij de (potentiële) effecten van het verwerken van persoonsgegevens door het nieuw te bouwen informatiesysteem op de privacybescherming van de burgers en consumenten vaststellen en maatregelen nemen om de negatieve gevolgen te mitigeren of tegen te gaan. De PIA zou dan ook kunnen worden ingezet als een '*surveillance impact analyse*' met als doel niet alleen de privacybescherming te toetsen maar om het respecteren van alle relevante grondrechten in ogenschouw te nemen.

In dit hoofdstuk is in het algemeen vastgesteld dat de risicotoezichtmaatschappij bedreigingen voor de privacy inhoudt. Het volgende hoofdstuk zal hier dieper op ingaan en de onderzoeksvraag 3 (OV 3) behandelen: '*Met welke privacybedreigingen en -risico's moeten de burger en de ontwerper van systemen rekening houden*?'

Hierbij komt de privacybedreigings- en privacyimpactanalyse aan de orde.

4. De privacybedreigingen

"One of the lessons that science teaches us about physical reality is that its character is frequently surprising. Part of the excitement of doing research lies in the unexpected nature of what may be found lying around the next experimental corner."
J. Polkinghorne, Quantum Physics and Theology, New Haven 2007, p. 23

Dit hoofdstuk is gewijd aan de beantwoording van de derde onderzoeksvraag (OV 3). Deze luidt: '*Met welke privacybedreigingen en privacyrisico's moeten de burger en de ontwerper van systemen rekening houden?'*

In paragraaf 4.1 van dit hoofdstuk wordt betoogd dat de wetgeving niet anders uitgelegd kan worden dan dat een privacyrisicoanalyse wettelijk is verplicht. Om privacyrisico's en bedreigingen goed te kunnen beoordelen is een risicoanalyse nodig. Er zijn vele methoden om risicoanalyse uit te voeren. Ik behandel er zeven. In paragrafen 4.2. tot en met 4.4 komt de methode van de risicoklassen van de Registratiekamer/CBP aan de orde. In paragraaf 4.5 volgt de terugkoppelingsmethode van Belotti & Sellen en in paragraaf 4.6 de risicoanalyse van Hong. De privacybedreigingswereld van Solove wordt in paragraaf 4.7 uiteengezet. In paragraaf 4.8 wordt de door de Canadese autoriteiten ontwikkelde privacyimpactanalyse (PIA) toegelicht. Het EU PISA-onderzoeksproject heeft onder meer geleid tot een repeteerbare en verifieerbare methode om allerlei vormen van privacybedreigingen in kaart te brengen. Om dit mogelijk te maken is een pentagonale analyse van privacybedreigingen ontwikkeld en deze aanpak levert een opsomming van bedreigingen op. Deze methode wordt in de paragrafen 4.9 en 4.10 behandeld. In paragraaf 4.11 komt de innovatieve aanpak van Little & Rogova voor het voetlicht. Het gaat hier om een privacybedreigingsontologie met de drie kernelementen: a. intentie of motivatie, b. middel of bekwaamheid en c. gelegenheid. In paragrafen 4.12 tot en met 4.14 vindt de analyse van het ontologisch privacybedreigingsmodel van Little & Rogova plaats. Paragraaf 4.15 sluit dit hoofdstuk af met de constatering dat de privacy bedreigingen vooral de ongewilde identificatie en de onrechtmatige verwerking van gegevens betreffen. Er is een afdoende remedie hiertegen, namelijk PET-maatregelen.

4.1. Wettelijke verplichting tot beveiliging

De Financial Times van woensdag 21 november 2007 kopte op de voorpagina met "Massive data loss hits UK". De Britse Revenue and Customs Office had 25 miljoen gedetailleerde persoonsgegevens van kinderbijslaggerechtigden verloren door twee niet-versleutelde computerschijven niet aangetekend per post te versturen. De twee schijven kwamen vervolgens niet op hun bestemming aan.

Privacyincidenten komen vaak voor. Burgers en consumenten lopen een groot risico dat hun persoonsgegevens niet correct verwerkt worden of kwijt raken. Volgens het Privacy Rights Clearinghouse[1] dat de gegevens over privacyinbreuken dagelijks in de Verenigde Staten bijhoudt, werden er van 2005 tot en met 2007 alleen al in de Verenigde Staten 170.000.000 gegevensdragers met persoonsgegevens gestolen. ChoicePoint,[2] een bedrijf dat data aggregeert, bedrijfsinformatie verstrekt en databanken beheert met achtergrondinformatie (> 19 miljard documenten) over bijna alle Amerikaanse burgers, is een van de voorbeelden. Op 18 februari 2005 maakte ChoicePoint bekend dat 163.000 consumenten ernstige privacyrisico's zouden kunnen lopen doordat kort daarvoor gegevens uit verschillende databanken van het bedrijf waren gestolen.[3] Tenminste achthonderd gevallen van identiteitsdiefstal (fraude met andermans identiteit) waren daar het gevolg van. De Federal Trade Commission (FTC) gaf het bedrijf een boete van 15 miljoen dollar.[4] De Eurobarometer nummer 250 van mei 2009 rapporteerde dat persoonsgegevens van 5% tot 15% van de inwoners van de EU verloren gaan en dat de helft van de betrokkenen schade lijden.[5]

Binnen de Europese Unie zijn organisaties (de verantwoordelijke) verplicht om de persoonsgegevens die zij onder zich hebben, te beveiligen. De artikelen 17 van de EU Richtlijn 95/46/EG,[6] 4 van de EU Richtlijn 2002/58/EG[7] en de daarbij behorende overwegingen 46 respectievelijk 30 en artikel 3 (c) van de Richtlijn 99/5/EG[8] vormen binnen de EU de wettelijke grondslag hiervoor. De wettelijke verplichting houdt in dat organisaties passende technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen tegen verlies, ongewilde of onrechtmatige vernietiging, wijziging, vervalsing, niet toegestane openbaarmaking, onrechtmatige toegang en tegen enige andere vorm van onrechtmatige verwerking. Om persoonsgegevens adequaat te beveiligen moeten deze juridische normen worden 'vertaald' naar het ontwerp en de feitelijke inrichting van

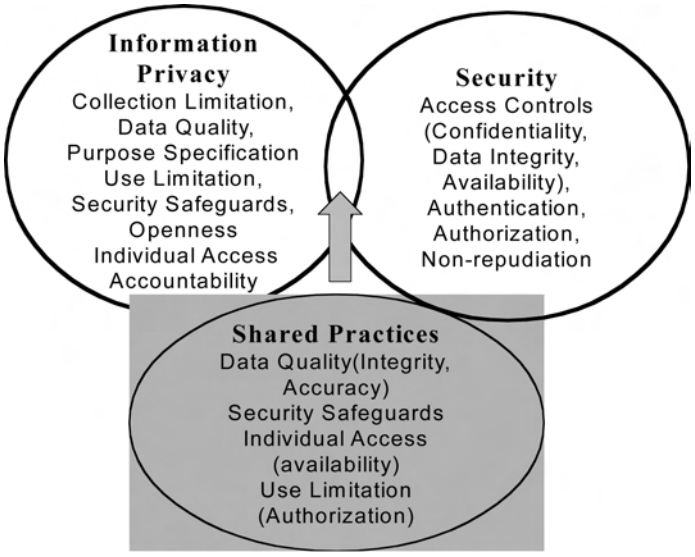
1 www.privacyrights.org/search.htm.
2 ChoicePoint verkoopt dossiers aan de politie, advocaten, journalisten en privédetectives.
3 www.msnbc.msn.com/id/6979897/.
4 www.ftc.gov/opa/2006/01/choicepoint.shtm.
5 http://ec.europa.eu/public.../eb_special_en.htm.
6 PbEG nr. L 281 van 23-11-1995, p. 31.
7 PbEG nr. L201 van 31-07-2002, p. 37.
8 Article 3 (3) (c) of Directive 99/5/EC: "The following essential requirements are applicable to all apparatus: (c) it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected".

informatiesystemen.[9] Koorn merkt hierover op: "de beveiliging die moet worden gerealiseerd, gaat verder dan informatiebeveiliging. Het is een misvatting te denken dat informatiebeveiliging een op een overeenkomt met bescherming van persoonsgegevens. Een bekend misverstand – met name onder ICT'ers – is het als bijna synoniem zien van beveiliging en privacy: 'Als we de beveiligingsmaatregelen hebben getroffen volgens de Code voor Informatiebeveiliging, dan hebben we direct de privacybescherming geregeld'. Dit is echter een misvatting, aangezien beveiliging slechts één van de zeven privacyprincipes kan invullen".[10]

Koorn gaat uit van zeven privacyprincipes, terwijl ik elf privacy realisatiebeginselen onderscheid. Dit is het gevolg van interpretatie. Uiteindelijk leiden beide interpretaties tot het zelfde resultaat, namelijk dat de persoonsgegevens optimaal worden beschermd. Informationele privacy en informatiebeveiliging is niet hetzelfde. Wel overlappen beide disciplines elkaar gedeeltelijk. Een belangrijk spanningsveld tussen informatiebeveiliging en informationele privacy betreft het privacyrealisatiebeginsel van transparantie (o.a inzagerecht) en de toegangsbeveiliging, omdat de inzage van documenten een beveiligingsrisico oproept.

Figuur 4.1 illustreert waar informationele privacy en informatie beveiliging elkaar deels overlappen (de verzameling shared practices):

Figuur 4.1: Gedeelde aandachtsgebieden van informatiebeveiliging en informationele privacy, Cavoukian, 2002, p.2.



9 Amendement Scheltema-de Nie en Wagenaar; Tweede Kamerstukken 1999-2000, 25 892, nr. 22.
10 Koorn, & Ter Hart, 2004, p. 18.

Alle vereisten betreffende de verwerking van persoonsgegevens moeten bij de informatiebeveiliging in aanmerking genomen te worden. Niet alleen die vallen binnen het ict-domein van de informatiebeveiliging, maar ook de additionele beveiligingsmaatregelen, die verzekeren dat de privacywet- en regelgeving worden nageleefd. In Overweging 46 van de Richtlijn 95/46/EG is bepaald dat de verantwoordelijke niet alleen met de beveiligingseisen rekening moet houden bij de gegevensverwerking, maar ook bij het ontwerp van informatiesystemen.[11] Concreet houdt dit onder meer in dat de verantwoordelijke al in de ontwerpfase voorzieningen moet treffen om onbevoegde toegang tot gegevens, programmatuur en apparatuur tegen te gaan. Degenen die opdracht geven tot de bouw van informatiesystemen zijn dus verplicht erop toe te zien dat zodanige beveiligingsmaatregelen in het ontwerp worden opgenomen, dat persoonsgegevens adequaat volgens de laatste stand van de techniek beveiligd zijn. Indirect zou dit voorschrift geïnterpreteerd kunnen worden als een ontwerpverplichting waar deskundige ontwerpers van systemen dan ook rekening mee hebben te houden. Het vereiste van een adequate beveiliging betekent feitelijk dat gebruikers van het informatiesysteem onderworpen zullen worden aan identificatie en authenticatie, wachtwoorden zullen moeten gebruiken en dat *logging* van de toegang tot persoonsgegevens noodzakelijk is.

Artikel 17 van de DPD is in de Wet bescherming persoonsgegevens (Wbp)[12] getransponeerd als artikel 13. Dit artikel 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 der 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".

Het begrip risico wordt niet in de Wbp gedefinieerd. Het begrip risico wordt veelvuldig gebruikt alsof het voor iedereen een eenduidig begrip is. Bij nadere beschouwing is dat nog maar de vraag. Gratt, voorzitter van de Amerikaanse Society of Risk Analysis (SRA) concludeerde na een tweejarige studie, dat "(...) a consensus was not being reached for the key definitions of risk and risk analysis".[13] Er zijn vele definities van risico in omloop. Miletti definieert bijvoorbeeld risico als "the probability of an event or condition occurring"[14] en Hewitt[15] als "an exposure to dangers, adverse or undesirable prospects, and conditions that

11 Overweging 46: "(…) the processing of personal data requires that appropriate technical (…) measures be taken, (…) at the time of the design of the processing system (…), particularly in order to maintain security and thereby to prevent any unauthorized processing".
12 Wet van 6 juli 2000, Stb. 2000, 302 houdende regels inzake de bescherming van persoonsgegevens.
13 Muller, 2004, p. 348.
14 Mileti, 1999.
15 Hewitt, 1997.

contribute to danger". Tettero[16] verstaat onder risico: "a probability that, due to a particular threat, a particular vulnerability is exploited causing damage to an asset". In de DIN-norm 31000,[17] wordt risico in artikel 1.1.1 onder e gedefinieerd als: "die Kombination aus der Wahrscheinlichkeit und der Schwere einer Verletzung oder eines Gesundheitsschadens, die in einer Gefährdungssituation eintreten können". Als definitie voor risico gebruik ik de volgende formule: het risico dat een organisatie loopt (r), is de waarschijnlijkheid van een gebeurtenis (in casu het beveiligings- of privacyincident) (p), vermenigvuldigd met de schade (e), dus: $r = p \times e$. Met deze formule kan het risico beter worden gekwantificeerd.

Om privacyrisico's vast te stellen en investeringen in beveiligingsmaatregelen te rechtvaardigen moet het risico ingeschat worden, zoals zal blijken uit de privacyrisico-, bedreiging- en effect- (impact)analyses, die in dit hoofdstuk en paragraaf 7.14 worden besproken. Door de risicoberekening moet duidelijk worden in welke volgorde van belangrijkheid, waar en op welke manier er geld en inspanningen (tegenmaatregelen) moeten worden geïnvesteerd om de risico's te voorkomen. De vraag, die telkens terugkomt bij het bepalen van privacybedreigingen is, hoe ernstig de consequenties zijn van de privacyinbreuk voor de persoon, die bepaalde persoonlijke informatie heeft verstrekt. Datzelfde geldt ook vanuit het oogpunt van aansprakelijkheid voor de organisatie, die de onderhavige persoonsgegevens beheert. Risicoanalisten wegen het risico door er een waarde aan toe te kennen. De waarde kan worden uitgedrukt in een willekeurige eenheid, liefst, wanneer dat mogelijk is, in een financiële eenheid, en anders in een eenheid, die weging mogelijk maakt. Het probleem is dat bij privacyrisico's het moeilijk is een waarde toe te kennen aan imponderabilia, zoals persoonlijke informatie en reputatieschade, omdat niemand weet hoeveel persoonlijke informatie precies waard is. Dat geldt ook voor andere beveiligingscomponenten.[18]

Een organisatie moet nagaan welke technische en organisatorische maatregelen zij moet nemen om persoonsgegevens op een passend niveau te beveiligen en behoorlijk en zorgvuldig te verwerken.[19] Organisatorische maatregelen zijn maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens (zoals toekenning en deling van verantwoordelijkheden, bevoegdheden, instructies, trainingen en calamiteitenplannen). Technische maatregelen zijn de logische en fysieke maatregelen in en rondom informatiesystemen (zoals toegangscontroles, vastlegging van gebruik en back-up). Het vereiste niveau van beveiliging van persoonsgegevens zal onder meer afhangen van de

16 Tettero, 2000, p. 22.
17 DIN 31000 (1979):VDE 1000: 1979-03 Allgemeine Leitsätze für das sicherheitsgerichtete Gestalten technischer Erzeugnisse. De zelfde tekst wordt gebruikt in de richtlijn 2006/42/EG.
18 Tettero, 2000, p. 96 "the value of the crucial security parameters is difficult to retrieve".
19 Artikel 6 Wbp. Het begrip "zorgvuldig" sluit aan bij de betamelijkheidsnorm in het Burgerlijk Wetboek (6:162) en het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur (Wet Algemeen Bestuursrecht afdeling 3.2).

door de verantwoordelijke ingeschatte risico's. In dertien WBP zijn de criteria: 'laatste stand der techniek' (the state of the art)[20] en 'de kosten van de tenuitvoerlegging van de maatregelen'[21] opgenomen. Deze zijn van invloed op de mate waarop door organisaties maatregelen en procedures moeten worden getroffen. Technische en organisatorische maatregelen dienen een onderling samenhangend en afgestemd stelsel te vormen, afgeleid uit een (informatie)beveiligingsbeleid, (informatie)beveiligingsplan en zijn terug te vinden in een stelsel van algemene maatregelen en procedures binnen de organisatie.[22] De onderlinge samenhang tussen risico's en de kosten wordt bepaald door het criterium: 'passende maatregelen', waarover later in dit hoofdstuk meer.

In het 'Raamwerk Privacy Audit' van de Registratiekamer (de voorloper van het College Bescherming Persoonsgegevens) wordt erop gewezen, dat een privacyaudit de vereiste graad van beveiliging moet vaststellen. In de privacyaudit kan niet het juiste niveau van beveiliging worden vastgesteld als de maatregelen niet tevens getoetst worden op de kwaliteitskenmerken:

1. Exclusiviteit (uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens).
2. Integriteit (de persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen).
3. Continuïteit[23] (de persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig daarover gemaakte afspraken en de wettelijke voorschriften).
4. Controleerbaarheid (de mate waarin het mogelijk is voor de gebruiker om te achterhalen dat de verwerking van persoonsgegevens overeenkomstig de hiervoor genoemde kwaliteitsaspecten is uitgevoerd).[24]

In de wettekst wordt vereist dat er passende maatregelen moeten worden getroffen. Bij de schriftelijke behandeling van de Wbp in de Eerste Kamer werd door de Minister van Justitie geantwoord dat hij onder het begrip 'passend' verstaat: maatregelen die in overeenstemming zijn met de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.[25]

Hij preciseert dat als volgt: "(...) de te nemen maatregelen moeten worden afgestemd op de risico's van onrechtmatige verwerking die zich in de betrokken organisatie voordoen, waarbij tevens rekening dient te worden gehouden met de stand van de techniek en de kosten om de betrokken maatregelen ten uitvoer te

20 Er moet gebruik worden gemaakt van beschikbare en in de praktijk getoetste methoden en technieken. Achterhaalde technieken worden als niet-toelaatbaar gekwalificeerd.
21 De kosten van de beveiliging moeten in proportie staan tot het te beveiligen belang en de aard van de gegevens.
22 Van Blarkom & Borking 2001, p. 15.
23 Continuïteit wordt gedefinieerd als de ongestoorde voortgang van de gegevensverwerking.
24 Leerentveld & Van Blarkom, 2000, p. 17-18.
25 Tweede Kamerstukken 1999-2000, WO 25 892, nr. 92c; Zie ook MvT 25 892, nr. 3 p. 98-99.

brengen. Dit criterium moet in het licht van de concrete omstandigheden worden ingevuld en is dan ook dynamisch. Het vereiste niveau van bescherming is hoger naarmate er meer mogelijkheden voorhanden zijn om dat niveau te waarborgen. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico voor de persoonlijke levenssfeer van betrokkenen inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd deze als «passend» moeten worden beschouwd, terwijl kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist".[26]

Wat de eindgebruiker zelf kan doen om zijn persoonsgegevens te beschermen komt in de Wbp niet aan de orde. Het lijkt mij niet ondenkbaar, dat de wetgever in de nabije toekomst de eindgebruiker (de digitale generatie geboren na 1980) een wettelijke verplichting zal opleggen om zijn persoonsgegevens in zijn computer te beschermen, analoog aan het eerder geldende beveiligingsvereiste van artikel 138a Sr in de Wet Computercriminaliteit (C.CR) I. Dit artikel stelde computervredebreuk[27] strafbaar. Dit vereiste is in de Wet C.CR II niet meer expliciet aanwezig. Wel ziet de Wet C.CR II het 'doorbreken van een beveiliging' als voorbeeld van het binnendringen van een computer.[28]

De individuele eindgebruiker kan over beveiliging en privacy veel informatie vinden op internet. Zo zijn er een negental basale aanbevelingen te vinden in de *CERT-guide* om persoonsgegevens te beschermen in de computer die thuis wordt gebruikt. De aanbevelingen komen neer op het installeren van antivirus, antispyware en Firewallprogrammatuur, het regelmatig maken van een back up, het gebruik van sterke wachtwoorden en pop-upblockers, encryptie en voorzichtig te zijn met e-mail met bijlagen en met het downloaden en installeren van programmatuur.[29] Omdat verwerking van persoonsgegevens binnen verschillende sectoren, markten, culturen en landen plaatsvindt, zullen de maatregelen die moeten worden getroffen voor de vereiste beveiliging van persoonsgegevens sterk variëren.

4.2. Risicoklassen

Bij het maken van de keuzes dient de verantwoordelijke te zoeken naar een balans tussen de hierboven vermelde criteria, de stand van de techniek en de kosten. Indien er met inachtneming daarvan een onderbouwde keuze is gemaakt,

---

26 Tweede Kamerstukken 1999-2000, WO 25 892, nr. 92c; Zie ook MvT 25 892, nr. 3 p. 98-99.
27 Computervredebreuk betreft het opzettelijk en wederrechtelijk binnendringen in een computersysteem of netwerk.
28 Koops, 2003. Per 1 september 2006 is de uit 1993 stammende wetgeving over computercriminaliteit ingrijpend veranderd. Rijkswet van 1 juni 2006, Stb. 2006, 299.
29 Zie www.cert.org/homeusers/HomeComputerSecurity/, versie10-10-2007.

is er sprake van een stelsel van passende technische en organisatorische maatregelen.[30] Omdat het maken van een risicoanalyse veel expertise vereist en die expertise bij de meeste organisaties in het midden- en klein bedrijf niet voorhanden is, heeft de Registratiekamer in 1994[31] en in 2001[32] samen met een groep van professionele informatiebeveiligingsexperts vormen van gegevensverwerking[33] geanalyseerd. Zij heeft op grond daarvan een algemene beveiligingsrichtlijn opgesteld met vier risicoklassen.[34] Daarin zijn een groot aantal maatregelen vermeld die genomen dienen te worden wanneer gegevens in een bepaalde risicoklasse worden verwerkt.[35] De opbouw van de risicoklassen is cumulatief: hogere klassen geven additionele normen aan die passen bij die hogere risicoklasse:
Risicoklasse 0 (geen risico)= publiek niveau;
Risicoklasse I = basis niveau;
Risicoklasse II = verhoogd risico;
Risicoklasse III = hoog risico.[36]

Het scala van risico's voor de betrokkene[37] bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens loopt van openbare persoonsgegevens, zoals in telefoonboeken, brochures, publieke internetsites etc., via verwerkingen van beperkte hoeveelheid persoonsgegevens, bijvoorbeeld lidmaatschappen (vereniging-lid), klantrelaties (hotel-gast), naar gevoelige gegevens. Voor bijzondere gegevens geldt een verhoogd en hoog risico, als de uitkomst van de risicoanalyse aantoont dat er extra negatieve gevolgen bestaan voor de betrokkene bij verlies, of onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. Het gaat dan bijvoorbeeld om de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene of om gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering of de gegevens die betrekking hebben op de gehele of grote delen van de bevolking.[38] Bij verwerking van bijzondere gegevens met een hoge gevoeligheidsgraad in het maatschappelijk verkeer geldt de hoogste risicoklasse, bijvoorbeeld wanneer

30 Van Blarkom & Borking, 2001, p. 19.
31 Borking, e.a., 1994. De Commissie bestond uit de experts: Borking, Van Rossum, Van Biene-Hershey, Koppes, Neisingh, Sneep & De Zwart. De zelfde experts met uitzondering van Van Rossum, die door Van Blarkom werd vervangen, voerden in 2001 de gegevensverwerkingsanalyse uit en stelden de te nemen beveiligingsmaatregelen voor.
32 Van Blarkom & Borking, 2001.
33 Onderzoek onder meer naar de aard, hoeveelheid en gebruik van gegevens.
34 Risico is in deze analyse het product van de kans op ongewenste gevolgen en de schade die dit kan veroorzaken voor de betrokkene, de verantwoordelijke of de bewerker. Hierbij moet worden uitgegaan van situaties die redelijkerwijs te verwachten zijn.
35 In Spanje is bij Koninklijk Besluit 994/1999 een beveiliging gebaseerd op een vergelijkbaar stelsel van risicoklassen (zie artikel 3) dwingend voorgeschreven.
36 Van Blarkom & Borking, 2001, p. 26-29.
37 Artikel 1 f van de WBP geeft voor betrokkene de definitie: betrokkene: degene op wie een persoonsgegeven betrekking heeft.
38 Huydecoper, e.a., 2006, p. 142.

het gegevens over levensbedreigende ziektes betreft, of persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is. Ook bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate vergroot risico voor de betrokkene opleveren dat het gerechtvaardigd is deze verwerking van persoonsgegevens in de hoogste risicoklasse te plaatsen. De maatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen. Dat geldt onder meer voor de verwerking van persoonsgegevens door opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt, bijvoorbeeld gegevens uit een DNA-databank.

4.3. Beveiligingsniveau

Van Blarkom & Borking geven aan dat er drie belangrijke aspecten zijn dat het beveiligingsniveau en de verwerking beïnvloedt.[39] In de eerste plaats betreft het de betekenis van de te verwerken persoonsgegevens binnen het maatschappelijk verkeer. Het gaat dan om de aard van de gegevens, dus persoonsgegevens die in combinatie met de omvang, het doel en het gebruik een verhoogde gevoeligheidsgraad hebben. De Wbp en de Richtlijn 95/46/EG kwalificeert die gegevens als bijzondere (gevoelige) persoonsgegevens (zoals gegevens over gezondheid, ras, religie etc.). Dergelijke gegevens rechtvaardigen een hoger niveau van bescherming en een andere manier van verwerking. Bijvoorbeeld: voor veel mensen is het onwenselijk dat gegevens omtrent hun financiële positie, erfrechtelijke aspecten of arbeidsprestaties bekend raken bij anderen. De gevoeligheidsgraad kan ook liggen in de gevolgen voor de persoon waarvan de gegevens ongeoorloofd of onzorgvuldig zijn verwerkt. De gevoeligheid (het risico) kan ook toenemen wanneer de hoeveelheid gegevens en de complexiteit van de verwerking groter wordt. Het kan gaan om het informatiegehalte, dat wil zeggen de mate van identificeerbaarheid: inhoudelijke kwaliteit en de hoeveelheid gegevens (gebruiksprofielen over langere tijd) en het kan gaan over hoeveel personen (specifieke) gegevens verzameld zijn. Hoe meer personen in de database(s) zijn opgenomen, hoe groter het informatiegehalte en hoe groter de kans op onzorgvuldig of onbevoegd gebruik. Het gebruik van gegevens is ook een bepalende factor: het gaat hier om de frequentie van de raadpleging (vele malen per dag of eens per jaar), het aantal personen dat toegang heeft tot de

39 Van Blarkom & Borking, 2001, p. 23-26.

gegevens (een persoon of honderden), het aantal locaties waar rechtstreekse toegang mogelijk is.

In de tweede plaats gaat het om het bewustzijn binnen een organisatie ten aanzien van (informatie)beveiliging van persoonsgegevens en privacybescherming. Nagegaan moet worden hoe het staat met het kennisniveau van de gebruikers van opgeslagen persoonsgegevens en de mate waarin een rechtmatige en behoorlijke omgang met persoonsgegevens gemeengoed is binnen de organisatie. Dat heeft te maken met de 'maturity' van een organisatie, waarover in hoofdstuk 7 meer.

In de derde plaats betreft het de ict-infrastructuur waarin de persoonsgegevens worden verwerkt. De gebruikte informatie- en communicatietechnologie (ict) verschilt qua gebruik, complexiteit, mogelijkheden en zal ook in 'the state of the art' variëren.

Onderstaande punten spelen tevens een rol bij het bepalen van de risico's en bij het definiëren van het toereikend niveau van de te nemen beveiligingsmaatregelen:

- De eigenschappen en organisatorische plaats van de computerapparatuur: PC of netwerk computer, client-server architectuur, mainframe, toepassingssoftware, RFID's, etc.
- De netwerken waarover wordt gecommuniceerd: intranet, extranet, internet etc. en de wijze waarop de verbindingen tussen de werkstations en de (externe) netwerken zijn gerealiseerd.
- De database en data retrieval technologieën die worden gebruikt voor de verwerking van persoonsgegevens (full textsystemen i.p.v. verwijzingsindex).
- De media waarop persoonsgegevens of toegangscodes tot die persoonsgegevens worden opgeslagen.
- De samenhang en de architectuur van de geautomatiseerde verwerking van persoonsgegevens en de daarvoor in te richten processen.

Aan de bepaling van de risicoklasse van persoonsgegevens hoort een privacyimpactanalyse (PIA) of privacybedreigingsanalyse vooraf te gaan, waarin de verantwoordelijke bepaalt welke risico's aan de verwerking van persoonsgegevens is verbonden. De PIA wordt in paragraaf 4.8 behandeld. Natuurlijk dient ook rekening gehouden te worden met de mate van exclusiviteit (alleen bevoegde personen hebben toegang tot gegevens), integriteit (de persoonsgegevens dienen in overeenstemming met de 'afgebeelde' werkelijkheid te zijn) en de continuïteit (de gegevens zijn zonder belemmeringen beschikbaar overeenkomstig de gemaakte afspraken en de wet).

Het onderstaand model (figuur 4.2) illustreert de onderlinge relatie van de risicoklassen en de toepassing op de verwerking van persoonsgegevens.

Figuur 4.2: Schema Risicoklassen – Van Blarkom & Borking, 2001 p. 21.

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	Aard van de verwerking		Conform 7-8 EU 95/46/EG artikel & 16 WBP
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse 0**	**Risicoklasse II**
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse I**	**Risicoklasse III**
Financieel en/of economische persoonsgegevens		**Risicoklasse II**	

De combinatie hoeveelheid persoonsgegevens en de aard van de verwerking bepaalt de risicoklasse. Wanneer het gevoelige (bijzondere) gegevens betreft wordt het risico bij privacyinbreuken groter en dat leidt tot een hogere risicoklasse.

4.4. Bedreiging

Bovenstaande schema geeft wellicht houvast ex post bij privacyaudits en voor de rechter, maar ex ante bij het ontwerpen van informatiesystemen om preventieve maatregelen in te bouwen teneinde privacybedreigingen en -inbreuken effectief te kunnen bestrijden, is het ontoereikend. Om de reële gevaren in kaart te brengen, alvorens het functionele ontwerp van een informatiesysteem te ontwikkelen dat persoonsgegevens adequaat kan beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, dient zoals eerder opgemerkt vooraf een privacybedreigingsanalyse of impactanalyse te worden uitgevoerd.[40] Onder een informatiesysteem wordt verstaan een systeem, dat de gebruikers voorziet van informatie die vereist is voor het uitvoeren van doelgerichte activiteiten. Het kan gaan om dat transactieverwerkende, geprogrammeerde beslissing nemende en beslissingondersteunende systemen. Schneier stelt onomwonden dat: “Threat Modeling is the first step in any security solution. It’s a way to start making sense of the vulnerability landscape. What are the real threats against the system? If you

40 Borking, 2003, p. 215-222; Flaherty, 2004.

don't know that, how do you know what kind of countermeasures to employ?"[41] Het begrip "bedreiging" is een fundamenteel concept voor de privacybescherming. Bedreigen en bedreiging[42] wordt in Van Dale omschreven als het hebben van de intentie om iemand leed, geweld aan te doen, een gevaar te vormen en iemand op gevaarlijke wijze te naderen. Tettero definieert bedreigingen als een gebeurtenis: "A threat is any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial-of-service."[43]

Op het begrip bedreiging wordt bij de bespreking van het privacy bedreigingsontologie in paragraaf 4.11 teruggekomen. Zonder de reële bedreiging voor de informationele privacy in kaart te brengen zou de keuze van te nemen privacybeschermende maatregelen een toevallige benadering zijn en zeer waarschijnlijk delen van de werkelijke bedreiging kunnen missen. Gezien het hierover bepaalde in de richtlijn 95/46/EG en Wbp, zou niet alleen het technische karakter van de te selecteren ontwerpmaatregelen moeten worden bekeken, maar ook de economische aspecten rond de keuze van de te nemen maatregelen door de kosten en voordelen tegen elkaar af te zetten.[44]

4.5. Terugkoppeling en controle

Er is in het begin van de jaren negentig van de vorige eeuw analytisch onderzoek gedaan naar de manier hoe risico's op privacyinbreuken voorkomen kunnen worden en privacy vriendelijke systemen gebouwd zouden kunnen worden. Xerox had in 1990 in Palo Alto (CA), Cambridge (UK) en Tokio 'media spaces' als werkplek voor haar onderzoekers gebouwd waar continue multimediaverbindingen tussen elke werkplek en de onderzoeker lagen.[45] De onderzoekers konden daardoor zelfs op grote afstand over de schouder van hun collega's meekijken naar het gezamenlijke onderzoek dat zij deden en direct daarop inbreken om suggesties te doen.[46] Belloti en Sellen viel het op dat nieuwe gebruikers en bezoekers van de 'media space' werkplekken zich niet prettig voelden bij de voortdurende observatie en vastlegging van alles wat zij deden zonder dat zij zich er van bewust waren.[47] Het bleek dat de permanent ingeschakelde videocamera's en microfoons al na enkele minuten niet meer bewust werden waargenomen en al snel werd vergeten.[48] Voor de onderzoeker

41 Schneier, 2000, p. 214.
42 Little & Rogova, 2006, p. 8: "Threat is a very complex ontological item, and therefore a proper threat ontology must be constructed in accordance with formal metaphysical principles that can speak to the complexities of the objects, object attributes, processes, events, and relations that make up these states of affairs."
43 Tettero, 2000, p. 21.
44 Een voorbeeld hiervan is te vinden in: Hussain 1984, p. 278.
45 Borking, 1995, p. 105-106.
46 Gaver, 1992, p. 28.
47 Bellotti & Sellen, 1993 (A), p. 5.
48 Hoe indringend media spaces kunnen zijn, is te zien op een door Sun Micro Systems in 1994 voor de afnemers uitgebrachte videofilm Starfire onder de regie van Bob Sweeney.

bestond de privacybedreiging uit de ongemerkte vastlegging van gegevens en het gebrek aan terugkoppeling over wat er met de geregistreerde gegevens werd gedaan.

Belotti en Sellen stelden vast dat onderzoekers en bezoekers van de 'media spaces' alleen gerustgesteld konden worden over de gevolgen van de voortdurende opname van beeld, geluid en andere gegevens voor hun persoonlijke levenssfeer, wanneer in 'media spaces' en in omgevingen waar veel sensoren en omgeving registrerende computers aanwezig zijn, terugkoppeling en controle over hun gedrag op elk moment mogelijk is,[49] "as there are no cues available which normally are noticeable in face-to-face meetings and have to be applied to each phase of the communication process."[50] Als gevolg van de ervaring van de onderzoekers met mediaspaces gold als extra voorwaarde in de Xerox researchgemeenschap de eis van wederkerigheid: "if you can see me, I can see you".[51] Bovendien kon de gebruiker de beeld-, data- en geluidskanalen op elk gewenst moment uit te zetten en aangeven wie wel en niet toegang had tot zijn 'media space' had. Deze aanpak werkte weliswaar in gesloten laboratoria met 'media spaces', maar het bleek dat de voorwaarden van terugkoppeling, controle en wederkerigheid bij 'open' informatiesystemen niet te realiseren waren. Neustaedter & Greenberg[52] deden in 2003 nader onderzoek naar mogelijke privacyinbreuken bij het gebruik van 'home media spaces' in de thuisomgeving bij telewerken. Ook hier staat de videocamera en de audioapparatuur op de thuiswerkplek altijd aan. Boyle, Edwards & Greenberg[53] hadden al vastgesteld dat in de kantooromgeving wanneer door middel van 'distortion filters' de ontvangen beelden algoritmisch zo worden bewerkt dat er een onduidelijk beeld ontstaat, dit de privacybescherming van kantoormedewerker aanzienlijk vergroot en dat, noodzakelijk voor de verrichte werkzaamheden, daarbij toch duidelijk blijft wie op een bepaald moment binnen de virtuele werkomgeving aanwezig is en bereid is te participeren in een werkinteractie.

In de thuiswerksfeer stelden Neustaedter & Greenberg via testen met proefpersonen evenwel vast, dat slechts bij het sterk wegfilteren van de video beelden (niveau 1 en 2 op een schaal van 1 (volledig grijs beeld) tot 10 (ongefilterd beeld)) privacybescherming effectief was. Minder filtering dan niveau 1 of 2 leverde genoeg informatie op om een bepaalde situatie te herkennen, zoals bijvoorbeeld het naakt zijn van de telewerker thuis. De keerzijde van de privacybescherming was, dat bij niveau 1 en 2 er niet meer kon worden vastgesteld of een thuiswerker

---

49 Bellotti & Sellen, 1993 (A), p. 5- 6. Onder controle door Bellotti wordt verstaan: "empowering people to stipulate what information they project and who can get hold of it"; Terugkoppeling is: " informing people when and what information about them is being captured and to whom the information is being made available".

50 Bellotti & Sellen,1993 (A), p. 6.

51 Gaver, 1992, p. 31

52 Neustaeder & Greenberg, 2003. http://guir.berkeley.edu/pubs/ubicomp2003/privacyworkshop/papers/Home-MediaSpaces_PrivacyWorkshop.pdf.

53 Boyle, Edwards & Greenberg, *2000*, p. 1-10.

in het 'home media spaces" netwerk bereid was interactief te participeren. Dat moment trad pas op tussen de niveau 3 en 5 en dan kon de privacy al geschonden zijn. Om privacy in de 'home media spaces" (HMS) goed te beschermen moet, aldus Neustaedter & Greenberg, in het ontwerp van HMS-aansluiting worden gezocht bij de manieren waarop individuen doorgaans hun privacy beschermen. Neustaedter onderscheidt vier categorieën:[54]

1. Verbaal gedrag: het gebruik, de inhoud en structuur van wat wordt gezegd. Voor het HMS betekent dit het produceren en daardoor bewust maken van de thuiswerker van waarschuwingssignalen of het introduceren van aankondigingssignalen zoals bellen, virtueel geklop op de deur of het piepend geluid bij het openen van een deur.
2. Non-verbaalgedrag: het gebruik van lichaamstaal bestaande uit gebaren en houding. Voor de HMS-verbindingen of voor de gebruikers van de virtuele HMS-omgeving houdt dit in dat de HMS reageert op herkenbare (vooraf in het systeem ingevoerde) lichaamstaal, zodat bij die signalen het HMS zich automatisch uitschakelt of uitlogt.
3. Omgevingsmechanismen: het zich verbergen achter barrières (muren, schotten, deuren), reageren op de ruimtelijke nabijheid van de bezoeker en het scheppen van tijdsduur tussen aankondiging van het contact en het feitelijk moment van contact. Dit heeft consequenties voor de installatie van de HMS, namelijk dat voor het installeren van HMS een ruimte in het huis wordt gebruikt, die doorgaans niet voor het privégebruik bestemd is. Voorts dat de videocamera op een zodanige plaats wordt opgehangen dat niet de gehele werkruimte kan worden bestreken met als standaardmogelijkheid dat de thuiswerker zelf de camera kan uitzetten, de beeldkwaliteit kan beïnvloeden of de opnamehoek van de camera kan bijstellen.
4. Culturele mechanismen: het gebruik van gangbare culturele en sociale gebruiken. Voor HMS-gebruikers betekent dit, dat er onderling een sociale code moet worden afgesproken over wie wat mag zien en beluisteren. Bij overtreding van zo'n code moeten er wel reële consequenties voor de overtreder aan verbonden zijn.

Er zijn in het laboratoriumontwerp van de HMS door het department of computer sciences van de universiteit van Calgary impliciete en expliciete controlemechanismen ingebouwd samen met visuele en auditieve terugkoppeling ten behoeve van het handhaven van het gewenste privacyniveau van de HMS gebruiker. Ook hier kan vastgesteld worden, dat deze aanpak bij 'open' informatiesystemen niet voldoende privacybescherming oplevert.

54 Neustaeder & Greenberg, 2003, p. 4-5.

4.6. De risicoanalyse van Hong

Hong e.a.[55] hebben met verwijzing naar het onderzoekswerk van Bellotti & Sellen een privacy risicoanalyse ontworpen voor de ambient intelligence (AMI) omgeving. De privacyrisicoanalyse kent twee delen: de risicoanalyse en het risicomanagement. De privacyrisicoanalyse richt zich op de sociale en organisatorische context van het systeem en de technologie die wordt gebruikt bij de implementatie van de applicatie. De risicoanalyse bestaat uit een aantal vragen die inzicht dienen te verschaffen over de manier waarop de applicatie verwacht wordt te functioneren bij normaal gebruik. Daarbij wordt tevens nagegaan wie de gebruikers en de gegevensdelers zijn, wie de gegevens bekijken en welke soort relaties (sociaal, juridisch, commercieel etc.) tussen hen bestaan. Deze inventarisatie geeft een indicatie hoe het best een adequaat niveau van vertrouwen en de voordelen van het delen van persoonlijke informatie gerealiseerd kan worden, terwijl de potentiële risico's tegelijkertijd kunnen worden verminderd. Speciale aandacht krijgt de manier waarop tegen privacyinbreuken kan worden geprotesteerd. Opvallend is dat de beveiliging van de gegenereerde persoonsgegevens niet in deze risicoanalyse voorkomt. Het tweede deel dat zich met het privacyrisicomanagement bezighoudt, geeft een weging aan de gevonden privacyrisico's. Bovendien geeft het voor de ontwerpers van het systeem oplossingsrichtingen aan om de risico's te ondervangen.

Hong e.a. refereert aan het Angelsaksische rechtsbeginsel *"reasonable care"*[56] als een nieuw element voor het managen van de privacyrisico's. Om de risico's te kunnen kwantificeren maakt hij de kosten/baten analyse een onderdeel van het privacyrisicomanagement. Hij laat zich leiden door een uitspraak van de befaamde rechter Learned Hand in de zaak *United States versus Carroll Towing Co.* (1947),[57] die drie factoren met betrekking tot het vaststellen van nalatigheid en aansprakelijkheid vaststelde. Deze factoren zijn door Hong e.a. aangepast om vast te stellen of de privacyrisico's wel proportioneel worden afgedekt. De eerste factor is L, die staat voor de waarschijnlijkheid dat een ongewenste openbaarmaking van persoonlijke informatie plaatsvindt. De tweede factor is de potentiële schade, weergegeven door de letter D, die ontstaat bij de openbaarmaking en de derde factor is C, de kosten die gemaakt moeten worden om een adequate privacybescherming te realiseren. Als C < LD (d.w.z. het risico en de schade van een ongewenste openbaarmaking zijn groter dan de kosten van

55 Hong, e.a., 2004, p. 91-100.

56 Hong, e.a., 2004, p. 96 : "reasonable care in law: the degree of care that makes sense and that is prudent, enough but not too much". Volgens Padfield, 1983, p. 224-225 wordt in het Engels recht onder *reasonable care* verstaan: "the care which a reasonable man would use or show in circumstances of the particular case under consideration. The degree or amount of care is variable. The test to be applied is: What is reasonable in the circumstances of the case, having regard to his particular profession or occupation?" Dit is bevestigd in onder meer de zaak Latimer vs. A.E.C Ltd (1953).

57 Circuit Court of Appeals, Second Circuit,159 F.2d Cir.1947; Feldman & Kim, 2002; www.audiocasefiles.com/cases/detail/case/8677/.

beschermingsmaatregelen), dan moeten maatregelen genomen worden ter wille van de privacybescherming. Zijn de kosten prohibitief hoog om privacy te beschermen, dan kan er volgens Hong e.a. op grond van het beginsel van "reasonable care" (gedeeltelijk) vanaf worden afgezien om een privacy beschermende investering te doen. Exoneratie van schadeaansprakelijkheid in de gesloten overeenkomsten zou de factor D kunnen verlagen, maar in veel gevallen zal exoneratie niet mogelijk zijn.[58] Hong e.a. hebben hun privacyrisicomodel getest op twee applicaties, nl. de Location-enhanced Instant messenger (een AT&T Wireless's Find Friends toepassing) en 911 BEARS Emergency Response Service[59] om de plaats van een ongeval te vinden. Het researchteam kwam tot de conclusie dat het voorgestelde model instrumenteel goed genoeg was om een aantal concrete privacyrisico's in de ambient intelligenceomgeving van beide applicaties op te sporen, maar van perfectie was geen sprake. Hoe de risico's op te lossen, kwam niet aan de orde.

4.7. De bedreigingswereld volgens Solove

Hoe ziet de privacybedreigingswereld voor informatiesystemen eruit? Wie en wat veroorzaakt de bedreiging? Om daar achter te komen zou men alle mogelijke vormen van privacyinbreuken in kaart kunnen brengen en vervolgens aan de hand van die opsomming kunnen redeneren wat er zou moeten worden gedaan aan het voorkomen van of het beschermen tegen privacyinbreuken. Solove[60] constateerde dat privacy voor iedereen wel een andere betekenis heeft en niemand precies kan zeggen wat het nu eigenlijk is. Om aan deze "embarras du choix" een einde te maken heeft hij samen met andere experts geprobeerd een taxonomie[61] op te stellen,[62] om op een gestructureerde niet-reductieve en contextuele wijze de maatschappelijke activiteiten die problematisch of inbreukmakend zijn voor de bescherming van privacy in kaart te brengen.[63] De onderzoeksmethode behelst om door middel van de taxonomie nauwkeuriger vast te stellen wat het probleem is. Voorts worden de ontdekte problemen in hun context geplaatst. Daarna wordt vastgesteld of het gaat om een uniek probleem

58 Hong, e.a., 2004, p. 96.
59 Hong, e.a., 2004, p. 97-99.
60 Solove, 2006 p.477-482: Hij ziet privacy niet "*as a unitary concept with a uniform value, which is unvarying across different situations*", maar stelt dat inbreuken op de privacy het gevolg zijn van een scala aan schade toebrengende of op zijn minst probleemveroorzakende activiteiten.
61 Tettero, 2000, p. 285 : "A threat taxonomy gives insight into the types of threats and the relations among the threat".
62 Solove had daarbij het voorbeeld van William L. Prosser in *Privacy, 48 Cal L.Rev.* 383.389 (1960) voor ogen die gebaseerd op het leerstuk over torts (onrechtmatige daad) een opsomming maakte over de betekening van het begrip 'privacy'. Prosser onderscheidde 4 categorieën die schade zouden kunnen doen aan iemands privacy: 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity that places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.
63 Solove, 2006, p. 485: "This taxonomy will aid us in analyzing various privacy problem so the law can better address them and balance them with opposing interests".

en hoe het verschilt van en gerelateerd is aan andere verzamelde problemen. Hij erkent dat twee belangrijke problemen bij het opstellen van een taxonomie zich voordoen, namelijk of bij het gesignaleerde risico inderdaad vermogensschade of immateriële schade (het verschil tussen de (nadeligere) positie die iemand heeft door het schadebrengende feit, en de positie die iemand anders zou hebben gehad zonder het schadebrengende feit)[64] zal optreden en in hoeverre een bepaalde activiteit het sociale of institutionele evenwicht negatief zal beïnvloeden.[65] Solove's taxonomie verkent in de jurisprudentie en federale- en staatswetgeving de verschillende opvattingen over privacy in de Verenigde Staten.[66] Hij tracht de verschillende sociaal herkenbare privacyinbreuken te identificeren en richt de aandacht op die activiteiten die hun invloed hebben op privacy. Het doel is tevens om bij te dragen aan de ontwikkeling van recht dat zich bezig houdt met privacybescherming en richting te geven aan het oplossen van implementatievraagstukken van de volgende generatie van privacybeschermende informatiesystemen. Het onderzoek leidt tot een taxonomie waarin vier basisgroepen van activiteiten worden onderscheiden, die schadelijk kunnen zijn voor de privacy.[67]

1. Het verzamelen van persoonlijke informatie.
2. Het verwerken van persoonlijke informatie.
3. Het verspreiden van persoonlijke informatie. En als consequentie van 1,2 of 3:
4. Het binnentreden in iemands levenssfeer.

Elke groep bestaat weer uit verschillende aan elkaar verwante subgroepen.

De subgroepen leiden concreet tot het vaststellen van risicogebieden. Solove onderscheidt zestien risicogebieden:

1. Surveillance.
2. Ondervraging.
3. Aggregatie van gegevens.
4. Identificatie.
5. Onzekerheid ten gevolge van onzorgvuldigheid met betrekking tot de verzamelde en opgeslagen informatie.
6. Gebruik van verzamelde gegevens voor een ander doel dan waarvoor verzameld.
7. Gebrek aan het geven van informatie aan het individu over wat over hem is opgeslagen.[68]
8. Het schenden van confidentialiteit.

---

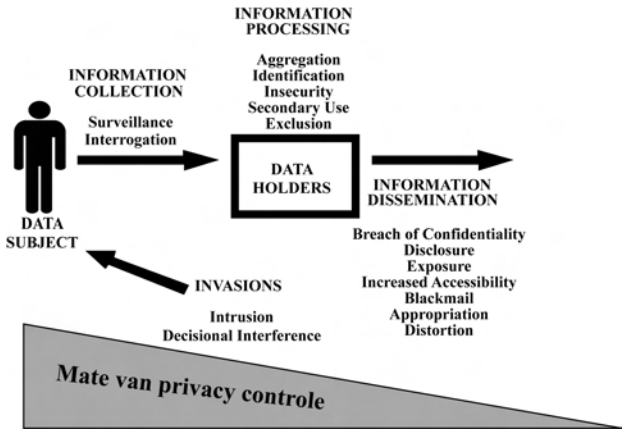
64 Het vonnis van het Gerechtshof 's-Gravenhage van 15 maart 2007, *LJN*:BA3669, R06/1401. Het hof hanteert een terughoudende toepassing van het schadebegrip in zaken betreffende privacy inbreuken.
65 Solove, 2006, p. 487.
66 In Hoofdstuk 2 van dit boek is aangegeven dat er wezenlijke verschillen zijn in de opvattingen over privacy in de VS en de EU.
67 Solove, 2006, p. 488.
68 Solove, 2006, p. 521-523.

9. Openbaarmaking.
10. Onthulling aan anderen van bepaalde fysische of emotionele eigenschappen van een persoon.[69]
11. Het in frequentie toenemen van (legale) toegang tot persoonsgegevens door derden met als risico ongewilde openbaarmaking.
12. Chantage.[70]
13. Het zonder toestemming van de betrokkene de naam of een afbeelding gebruiken voor eigen gebruik of profijt.[71]
14. Verdraaiing van feiten en gegevens.
15. Binnendringen in iemands privéleven.
16. Het door beslissingen zich mengen in iemands privéleven.

Hij verwijst als saillant voorbeeld van het laatste risicogebied naar de zaak Griswold tegen de Staat Connecticut, waar de Supreme Court in 1965 vonniste dat de staat Connecticut ten onrechte het gebruik van voorbehoedsmiddelen verbood aan getrouwde echtparen.[72] Ter illustratie van de taxonomie dient het model in figuur 4.3. Dit model start als uitgangspunt met een persoon met persoonsgegevens en onderscheidt vervolgens drie stadia, het verzamelen van gegevens, het be- en verwerken van persoonsgegevens door degene die de gegevens onder zich heeft (de verantwoordelijke) en de verspreiding van de persoonsgegevens. Het model geeft per stadium aan welke inbreuken in de privacy van een persoon kunnen optreden. Gegeven in dit model is dat naarmate het proces van de verwerking van persoonsgegevens verder gevorderd is (beginnend bij het verzamelen van gegevens, dan het be- en verwerken en tenslotte de verspreiding en opslag daarvan), de persoonsgegevens zich steeds verder verwijderen uit de controlesfeer van het desbetreffende individu. De aanname in het model is dat in beginsel een individu (enige) controle heeft of behoort te hebben over wat over hem wordt verzameld, zijn controle (sterk) afneemt wanneer de gegevens worden verwerkt en dat er nauwelijks nog van controle sprake is als de gegevens eenmaal zijn verspreid naar anderen.

69 Solove, 2006, p. 532-536.
70 Solove, 2006, p. 539-542.
71 Solove, 2006, p. 542 -546.
72 381 U.S.479, 485-86 (1965).

Figuur 4.3: Solovo's taxonomie model (gedeeld bewerkt door Borking), Solove, 2006, p.490.



Solove concludeert[73] dat de probleemgebieden en de activiteiten die de privacy schade kunnen berokkenen, aan elkaar zijn gerelateerd. Er blijkt evenwel geen gemeenschappelijke noemer te vinden te zijn die alle in kaart gebrachte privacyinbreukmakende activiteiten verbindt. De ict als faciliterend middel speelt bij het ontstaan van privacyproblemen in toenemende mate een belangrijk rol en maakt het mensen, bedrijven en overheden makkelijker opzettelijk privacy inbreukmakende handelingen te verrichten. Bovendien heeft ict een cultuur van sociale netwerken, webservices, 'mash-ups',[74] Web 2.0 en een virtuele samenleving mogelijk gemaakt, die van de participanten vereisen dat zij persoonsgegevens verschaffen, bij gebreke waarvan zij van deelname uitgesloten worden.[75] De door Solovo beschreven privacybedreigingswereld (vanuit de door hem onderzochte rechtszaken en wetgeving) om tot een betekenisvolle veralgemening van privacyproblemen te komen, is niet volledig en blijkt niet het gewenste resultaat op te leveren. Het draagt wel bij om een beter zicht te krijgen op de privacybedreigingen en kan gebruikt worden om een meer algemeen privacybedreigingsmodel te toetsen. Dyson merkt daarbij op dat veel bedreigingen die als privacybedreigingen zijn gekwalificeerd eerder bedreigingen van de beveiliging inhouden en indirect bedreigingen voor de privacy vormen.[76]

---

73 Solove, 2006, p. 558.

74 Voor uitleg van mash-ups zie http://webservicesmeshup.podomatic.com/: "One of the hottest trends in Web 2.0 is the development of mash-ups. The term mash-up originated in the music world – a music mash-up is a remix of two or more songs to create a new song. Similar to music mash-ups, a Web application mash-up combines complementary functionality from multiple Websites or Web applications".

75 Fritsch, 2008, p. 5.

76 Dyson, 2008, p. 27: "In many cases, what is called a breach of privacy is actually a breach of security or a financial harm (...)".

4.8. Privacyrisico- of Privacyeffectanalyse

Flaherty stelt uitdrukkelijk dat een privacy impact assessment (PIA) een essentieel beleidsmiddel is om persoonsgegevens preventief tegen inbreuken te beschermen.[77] In de EU privacyrichtlijnen en mutatis mutandis in Nederlandse wetgeving is geen expliciete bepaling betreffende een privacyrisicoanalyse opgenomen. Op grond van het bepaalde in artikel 13 WBP: "(...)gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen", zou evenwel kunnen worden geconcludeerd, dat ter rechtvaardiging van de keuze van de technische en organisatorische maatregelen, deze keuze dient te zijn gestoeld op een (gedocumenteerde) risicoanalyse van de effecten van het informatiesysteem op het beschermen van persoonsgegevens en de gevolgen van mogelijke privacyinbreuken bij het gebruik van het informatiesysteem. Tijdens de parlementaire behandeling is op geen enkele manier gerefereerd aan het verplicht maken van een privacyrisico- of privacy effect analyse. Wel is bij het nader aanduiden van het begrip 'passend' gewezen op de proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens.[78] Op zijn minst zou men dan ook mogen verwachten dat de aard van de te verwerken persoonsgegevens[79] wordt geanalyseerd, zodat bijvoorbeeld duidelijk wordt of er van gevoelige gegevens sprake is, die gezien de context zwaardere eisen stellen aan de beveiliging.

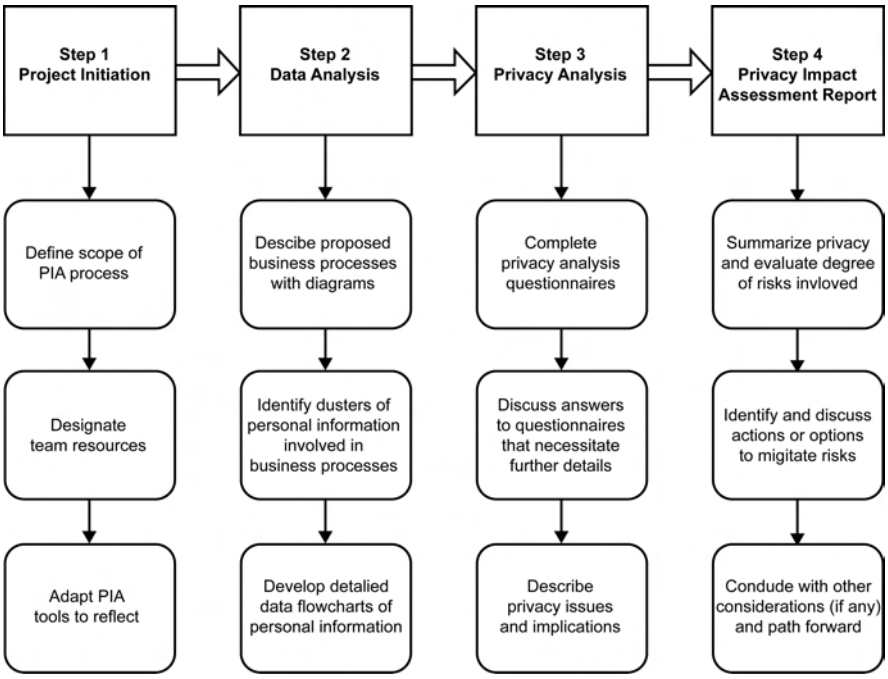
In Canada[80] zijn alle overheidsorganen verplicht[81] een PIA uit te voeren om vooraf de mogelijke privacyproblemen vast te stellen, die het gevolg kunnen zijn van nieuwe beleidsvoornemens, nieuwe (uitgebreidere) dienstverlening of door substantieel herontwerp van een beleidprogramma. Een PIA moet in ieder geval altijd uitgevoerd worden als de verzameling, het gebruik en de openbaarmaking van persoonsgegevens (in het kader van de integratie van beleidsprogramma's) met of zonder toestemming van de betrokken burgers toeneemt. Een PIA is ook vereist als de doelgroepen worden vergroot, een verschuiving van directe naar indirecte verzameling van gegevens plaatsvindt en persoonsgegevens voor meer beleidsprogramma's worden gebruik dan initieel voorzien. Als ondersteuning kan de 'Privacy Diagnostic Tool' (PDT)[82] worden gebruikt.

77 Flaherty, 2000, p. 85-90.
78 Roos, 2005, p. 120-121.
79 Artikel 17 (1) van Richtlijn 95/46/EC "the nature of the data to be protected".
80 Er zijn ook PIAs in Australië, maar die zijn aanmerkelijk minder diepgaand dan de Canadese PIA. www.privacy.gov.au/publications/pia06/mod-d.html.
81 Er is geen wettelijke verplichting in de Canadese privacy wetgeving voor organisaties om een PIA uit te voeren. Evenwel de Canadese Overheid heeft zich gebonden om een PIA uit te voeren op grond van de Treasury Board Privacy Impact Assessment Policy. Zie voor deze policy en de daarbij behorende richtlijnen www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp.
82 The Privacy Diagnostic Tool Workbook version 1.0 developed by the Office of the Information Commissioner of Ontario: www.ipc.on.ca/. Cavoukian, 2007, p. 165-170.

Rapportage van het resultaat van de PIA aan de Privacy Commissioner van de provincie of federale overheid is verplicht. De PIA onderzoekt op basis van het bepaalde in de Canadese Privacy Act en de Personal Information and Electronic Documents Act[83] of voldaan wordt aan de wettelijke eisen en of er privacyproblemen (te verwachten) zijn. Het is een gestructureerde manier om de essentiële componenten van het informatiesysteem en de stromen van persoonsgegevens in kaart te brengen. Het zorgt ervoor dat privacyvraagstukken gedurende het (her) ontwerp van systemen en programmatuur niet veronachtzaamd worden. Zoals uit het onderstaande model (figuur 4.4) blijkt, bestaat het Canadese PIA proces uit vier basiscomponenten: de project initiatie, de data-analyse, de privacyanalyse en het privacyeffectrapport. De PIA is niet eenmalig, maar volgt de ontwikkeling van het informatiesysteem gedurende zijn bestaan.[84] De PIA leidt tot een 'privacy risk management plan', dat onder meer een beschrijving geeft van de geïdentificeerde privacy risico's, een analyse van de mogelijkheden om de privacyrisico's te ondervangen of te verminderen, een lijst van overgebleven risico's die niet opgelost kunnen worden en een analyse van de mogelijke gevolgen van deze risico's voor wat betreft de reactie van het publiek en het succes van het voorgestelde beleidsprogramma.

83 Second Session, thirty-sixth parliament, 48-49 Elizabeth II, 1999-2000, Statutes of Canada 2000 chapter 5, Bill C-6.
84 Flaherty 2000, p. 89: "It is a protean document in the sense that it is likely to continue to evolve over time with the container development of a particular system."

Figuur 4.4: De stappen in het PIA proces in Canada; Treasury Board of Canada, 2007.



In de Verenigde Staten vereisen zowel artikel 208 van de E-Government Act (2002)[85] als artikel 222 sub 4 van de Homeland Security Act (2002)[86] dat er een Privacy Impact Assessment binnen de federale overheidsorganen moet worden uitgevoerd. De PIA analyseert hier op welke wijze "personal identifiable information (PII) is collected, used, disseminated and maintained".[87] Het stelt vast hoe de betrokken overheidsafdeling met de vastgestelde privacyproblemen gedurende de ontwikkeling, ontwerp en gebruik van een in te voeren (surveillance)technologie of regelgeving moet worden omgegaan c.q. is omgegaan. Daarbij dient de bescherming van PII zodanig te zijn dat het binnendringen in de levenssfeer van individuen zo veel mogelijk wordt beperkt, de rechtmatigheid van beslissingen van het overheidsorgaan zo groot mogelijk is en de legitieme verwachting van het individu met betrekking tot een afdwingbare vertrouwelijkheid van zijn persoonsgegevens wordt gerechtvaardigd. Het beleidsdocument

85 Pub.L.No.107-347.
86 Pub.L.No.107-296,116 Stat.2135 (Nov. 25, 2002).
87 Teufel 2007, p. 3.

behorend bij de wet wijst er op, dat er niet altijd een PIA uitgevoerd hoeft te worden. Er kan worden volstaan met een lichtere Privacy Threshold Analysis, op grond waarvan de 'privacy officer' beslist of er alsnog een PIA gedaan moet worden.[88] Onder punt 7.5 van het PIA-beleidsdocument van het US Department of Homeland Security komt specifiek de vraag aan de orde hoe de privacyrisico's worden ingeschat met betrekking tot het recht van toegang van het individu wiens persoonsgegevens worden verwerkt en tegelijkertijd hoe de risico's voor het systeem kunnen worden beperkt. Artikel 7.5.1: "Discuss how the redress and access measures offered in the system and collection of information are appropriate given the purpose of the system. For example, if the minimal redress procedures provided in the Privacy Act and the Freedom of Information Act are deemed inadequate please explain why additional redress measures offered are beneficial to the system." Het gehele proces geeft de indruk dat er een uitgebreide checklist moet worden afgewerkt met als mogelijk resultaat een privacy impact assessment report. Of dit rapport een lijst van privacyrisico's voor het individu ten gevolge van Homeland Security systeem oplevert, is niet duidelijk.

Inmiddels begint ook binnen de Europese Unie de belangstelling voor een PIA te groeien. Gezien de grote privacyrisico's die verbonden zijn aan het gebruik van RFIDs heeft de Europese Commissie een aanbeveling gedaan. De Commission Recommendation van 12 mei 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification legt in artikel 4 de verplichting aan de lidstaten op, dat "Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union".[89] Een gestandaardiseerde PIA is nochtans noodzakelijk wil een PIA gezag krijgen als input voor het bouwen van privacyveilige informatiesystemen. De Information Commissioner (ICO) van het Verenigd Koninkrijk[90] heeft op 7 januari 2008 in de EU het voortouw genomen met het publiceren van het privacy impact assessment handbook. De PIA is in Engeland vrijwillig en niet verplicht voorgeschreven. De ICO wijst erop dat: "The PIA process is considerably broader than just an audit of compliance with existing privacy related laws. A complementary process is needed to ensure that the project is legally compliant. That process can begin early, but cannot be finalised until late in the project life-cycle, when the design is complete (...) A PIA aims to prevent problems arising, and hence avoid

88 Teufel 2007, p. 6.
89 www.epractice.eu/files/recommendationonrfid2009.pdf.
90 http://news.zdnet.co.uk/security/0,1000000189,39291433,00.htm en zie hierbij het PIA-handboek: www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html.

subsequent expense and disruption."[91] Bij de privacybedreigingsanalyse dient de vooringenomenheid en de gemakzucht van de ontwerper te worden voorkomen. Het is dan ook noodzakelijk een systematische repeteerbare en verifieerbare methode toe te passen waarin de diverse facetten van het te ontwerpen informatiesysteem worden geanalyseerd op privacybedreigingen en de manier waarop deze potentiële bedreigingen of de gevolgen daarvan kunnen worden teniet gedaan of verminderd. Bovendien zou idealiter deze (gestandaardiseerde) methode, indien mogelijk, op een breed scala van privacygerelateerde, technologische systemen moeten kunnen worden toegepast. Als de EU-wetgeving een PIA zou voorschrijven zou dat een belangrijke stimulans kunnen betekenen voor het tijdig vaststellen van de gevolgen voor de privacy van de burger en consumenten van een nieuw informatiesysteem en de te nemen technologische maatregelen om de privacy te beschermen.

4.9. Naar een algemene privacybedreigings- en -risicoanalyse

Er zijn veel methoden om privacybedreigingen en risico's te analyseren. In dit hoofdstuk zijn inmiddels ter beantwoording van de derde onderzoeksvraag vijf methoden om privacybedreigingen en -risico's in kaart te brengen, besproken. In de paragrafen 4.2 tot en met 4.4 is de methode van de registratiekamer/CBP behandeld, in paragraaf 4.5 de terugkoppelingsmethode van Belotti & Sellen, in paragraaf 4.6 de risicocalculatie van Hong, in paragraaf 4.7 de bedreigingswereld van Solove, en in paragraaf 4.8 de privacy impact analyse (PIA) van de federale Canadese overheid. Geen van deze methoden geeft voldoende vertrouwen om er als ontwerper vanuit te kunnen gaan dat de privacybedreigingen afdoende in kaart zijn gebracht. De PIA lijkt het dichtst bij de volledige opsomming van privacyrisico's te komen.

Hieronder bespreek ik nog drie veelbelovende methoden, te weten in deze paragraaf de gecombineerde BSI-standaard 7799, CCTA- en ITSEC-aanpak, in paragraaf 4.10 de pentagonale PISA-analyse en in paragrafen 4.11 tot en met 4.14 de bedreigingsontologie van Little & Rogova.

Omdat binnen de privacybescherming, informatiebeveiliging[92] een belangrijke component vormt, is in het EU PISA project[93] gepoogd een algemene privacybedreigingsanalyse te ontwikkelen. In het project is als uitgangspunt genomen de beproefde methodes voor risicoanalyse voor informatiebeveiliging.

---

91 Information Commissioner, Privacy Impact Assessment Handbook Version 2.0, Manchester 2009, Online beschikbaar op www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/part1.html.

92 Tettero, 2000, p. 19: informatie beveiliging bestaat uit een complexe hoeveelheid maatregelen die de vereisten voor vertrouwelijkheid, integriteit en beschikbaarheid van het informatiesysteem op een adequate wijze waarborgen.

93 Privacy Incorporated Software Agent (PISA), EU research project RTD IST-2000-26038 (Brussels 2003).

Hierbij is gebruik gemaakt van de Britse standaard BSI 7799: "The Code of Practice for the Risk Analysis and Management Methodology", het Information Security Handbook of the Central Computers and Telecommunications Agency (CCTA1991[94]) en Information Technology Security Evaluation Criteria (ITSEC), gepubliceerd in 1991.[95]

De aanpak van de hiervoor genoemde methoden van risicoweging is aangepast en uitgebreid, omdat beveiliging maar één van de elementen van privacybescherming is. De wijzigingen resulteren in figuur 4.5, die weergeeft op welke methodologische wijze de privacybedreigingen in kaart gebracht kunnen worden en hoe de privacybescherming in informatiesystemen kan worden geconsolideerd.[96] Dat hier sprake is van een methode en niet van een opsomming van verschijnselen, zoals bij Solove, blijkt uit het feit dat deze aanpak voldoet aan de door Olle e.a.[97] geformuleerde criteria:

- De methode bevat een aantal opeenvolgende stappen.
- Het resultaat van ieder van deze stappen dient een specifiek doel en brengt goed onderbouwde resultaten voort.
- Het resultaat van iedere stap kan door onafhankelijke onderzoekers worden gevalideerd.
- Het aantal bronnen binnen iedere stap is beperkt.
- De expertise die noodzakelijk is om ieder stap te nemen, is homogeen en vereist een beperkt aantal verschillende deskundigen.
- De sequentie kan worden herhaald vanaf elk tussenliggend resultaat om het totale resultaat te verbeteren en te verfijnen.

Het in onderstaand figuur 4.5 weergegeven model van de privacybedreigingsanalyse bevat vijf niveaus:

1. Het eerste niveau is het veld Risk Reduction Regulations. Dit is de algemene benaming voor regelgeving die leidt tot risicovermindering. Het verkleinen van het risico van inbreuken op de informationele privacy wordt voorgeschreven door de privacywet- en regelgeving (in het model aangeduid als privacy regulation). Het tweede niveau in figuur 4.5 betreft de Risk Protection Ordination. Artikel 17 van de Richtlijn 95/46/EG legt de verplichting op (in het onderstaande model aangegeven met de term Privacy Protection Ordination) om zodanige maatregelen in het informatiesysteem te nemen dat de bescherming van persoonsgegevens is gewaarborgd, één en ander naar tevredenheid van de toezichthouder. De privacyrealisatiebeginselen, die in de Richtlijn 95/46/EG zijn uitgewerkt (zoals uiteengezet in hoofdstuk 2), zijn de facto de tegenmaatregelen van de wetgever om de

94 Tettero, 2000, p. 33: "Within scientific research, CRAMM is used more often than MARION (MARION 1983, Méthode d'Analyse de Risques Informatiques Optimisée par Niveau, by Club de la Sécurité Informatique Français) as reference material."
95 www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf.
96 Van Blarkom, Borking & Olk, 2003, p. 22-28.
97 Olle, Sol & Verrijn-Stuart, 1988.

privacy bedreigingen het hoofd te bieden. Helaas zijn de onderliggende bedreigingen niet expliciet in de overwegingen van de Richtlijn en de daarbij behorende documenten geformuleerd. Dat zou de ontwerpers een belangrijke leidraad geven bij het concipiëren van systemen en applicaties. Dat in deze methode direct bij het begin aan de privacy wet en regelgeving wordt gerefereerd, heeft ook een speciale reden. Het komt maar al te vaak voor, dat ontwerpers van informatiesystemen het bestaan van relevante wetgeving vergeten.

2. In het tweede niveau vindt de analyse van de '*assets'* en '*threats*' plaats. Onder *assets*[98] wordt verstaan de objecten en subjecten die persoonsgegevens bevatten en genereren (het individu in kwestie) en kwetsbaar zijn voor privacyinbreuken. Deze groep van *assets* wordt geëvalueerd om vast te stellen wat het belang ervan is om deze te beveiligen. Bovendien dient er een waarde aan toegekend te worden. De waarde kan worden uitgedrukt in een willekeurige eenheid, wanneer dat mogelijk is, in een financiële eenheid, en anders in een andere eenheid, die weging mogelijk maakt. Risico analisten voeren deze werkzaamheden uit.[99]

Vervolgens worden de bedreigingen (*threats*)[100] gevalideerd en het potentiële afbreukrisico van die bedreigingen beoordeeld. Deze factor vertegenwoordigt de waarschijnlijkheid van een inbreuk gemeten over een van te voren bepaalde periode. Het oordeel hierover wordt door een expert gedaan en bij voorkeur door middel van een statistische analyse.[101]

3. In het volgende niveau 3 vindt de risicoweging plaats. Zoals eerder in dit hoofdstuk is gesteld, zijn er vele definities van risico in omloop. In het PISA-project wordt onder risico verstaan: een risico is het product van de consequenties van de bedreiging vermenigvuldigd met de waarschijnlijkheid van het plaatsvinden van de bedreiging.[102]
4. Het vierde niveau 4 bepaalt de vereisten na het vaststellen van het privacyrisico's, welke geacht worden een adequaat antwoord te geven op geconstateerde privacyrisico's.[103] Deze tegenmaatregelen kunnen op zichzelf weer nieuwe secundaire risico's oproepen. Daarom dient de bedreigingsanalyse opnieuw te worden uitgevoerd, totdat geen nieuwe bedreigingen worden gevonden of verwacht.
5. Het laatste niveau 5 betreft het implementeren van de tegenmaatregelen om de privacy risico's af te dekken. Op basis van de ingeschatte risico's

98 Tettero, 2000, p. 2: "Information security is employed to prevent valuable things, called assets, from being damaged or to minimize the likelihood of damage. Examples of assets are buildings, a business strategy, customer data, network components (for example, routers and file servers), personnel, products and information about assets".

99 Voor meer informatie over de risico weging en calculatie: Fischhoff, e.a., 1981.

100 Tettero, 2000, p. 21.

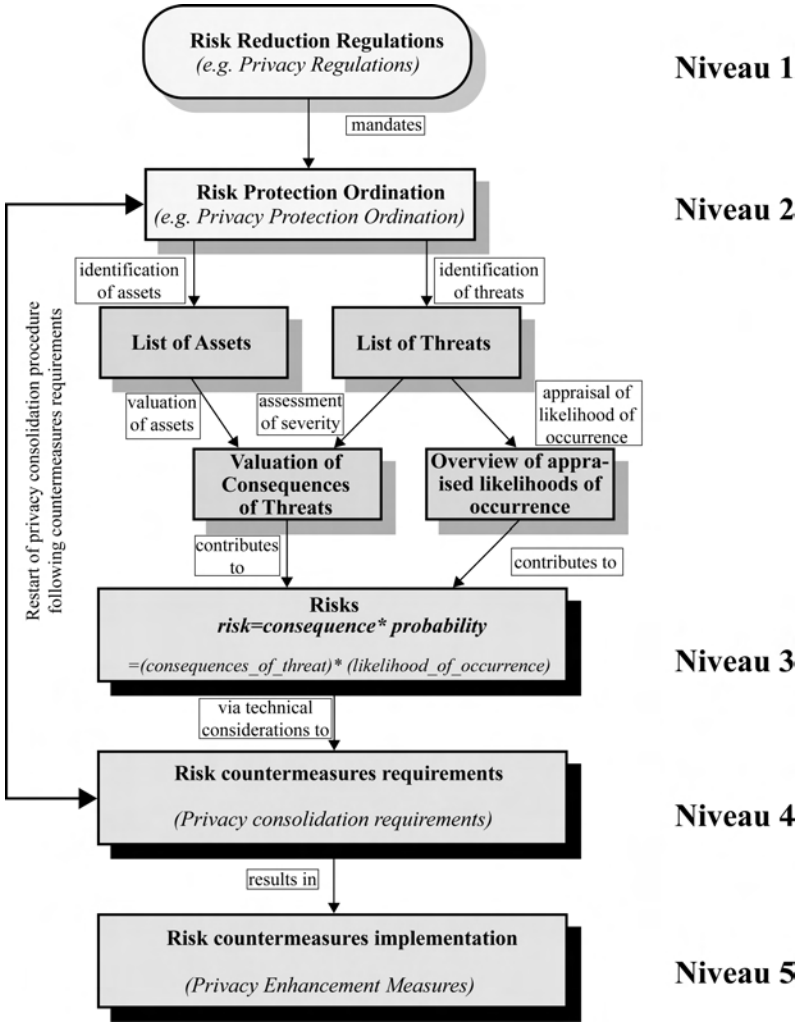
101 Borking e.a., 2001, p.18.

102 Van Blarkom, Borking & Olk. 2003, p. 23.

103 Tettero, 2000, p. 112: " The risk analysis is not only focused on the technical system. The risks for the User Organization, the stakeholder, are analyzed too".

moeten de gekozen beschermende maatregelen geen of een aanvaarbaar (rest) risico opleveren. Door nieuwe wetgeving kunnen er weer nieuwe risico's ontstaan. Het proces van risicoanalyse dient dan ook gezien het wettelijk beveiligingsvereiste van de 'state of the art' regelmatig gedurende het bestaan van het informatiesysteem uitgevoerd te worden. Bij de PIA gebeurt dat ook zo.

Figuur 4.5: Model Privacy Risico Analyse, Van Blarkom, Borking & Olk, 2003, p. 23.



4.10. De pentagonale aanpak

In het EU PISA-researchproject is na de ontwikkeling van het algemene privacy-risicoanalysemodel (zie figuur 4.5) een vijfhoekige aanpak voor de privacybedreigingsanalyse ontwikkeld in de verwachting dat door deze benadering zoveel mogelijk privacybedreigingen zouden kunnen worden opgespoord.[104] De methode wordt vervolgens geënt op het hiervoor besproken model en richt zich met name op het ontdekken van de specifieke privacybedreigingen die samenhangen met de aard van het informatiesysteem. Er zijn voor het opsporen van de bedreigingen vijf gezichtspunten toegepast, die moeten leiden tot het benaderen van de bedreigingen vanuit vijf verschillende richtingen. De vijfhoekig aanpak is schematisch weergegeven in figuur 4.6 [105] en dient te worden gelezen met de wijzers van de klok mee.

Het eerste gezichtspunt (dat al in de Risk Reduction Regulations aan de orde is gekomen) betreft de EU privacyrichtlijnen en de daarop gebaseerde nationale wetgeving ter bescherming van de persoonsgegevens. Kan het overtreden van de bepalingen in de richtlijnen worden vertaald naar concrete privacybedreigingen? Zo kan bijvoorbeeld het niet realiseren van de wettelijk vereiste doelbinding worden vertaald in de privacybedreiging die het systeem toelaat persoonsgegevens te verwerken zonder zich te houden aan de doelbinding. Bij het tweede gezichtspunt moet worden afgevraagd of de gevonden oplossing (de architectuur van het systeem om de privacy te beschermen) voor een bepaald probleem op zichzelf weer nieuwe privacybedreigingen oplevert. De privacybedreiging kan dan zitten in de algemene oplossing en niet in het systeem zelf. Bijvoorbeeld: de oplossing voor het vastgestelde doel van het systeem kan zijn het delen van informatie met software agents teneinde geautomatiseerde transacties uit te voeren binnen een publiek netwerk. De gekozen oplossing levert privacybedreigingen op.

Het derde gezichtspunt (threats emanating from use situation) komt voort uit de analyse van de situatie waarin het uiteindelijke systeem zal worden gebruikt (de omgevingsanalyse) en die de gevonden bedreigingen kunnen verergeren. Hier kan worden gedacht aan het gebruik van standaardprogrammatuur, die op zichzelf niet bedreigend is, maar dat wel wordt, bij het gebruik in een niet voorziene situatie.

Het vierde gezichtspunt betreft de toegepaste technologie. De bedreigingen kunnen dan voortkomen uit de manier waarop een systeem met bepaalde technologieën is verwezenlijkt en niet zo zeer uit het doel van het systeem zelf. Bij mobiele telefonie hoeft plaatsbepaling niet per se privacybedreigend te zijn, maar kan verwevenheid met de andere systemen in het netwerk privacybedreigingen opleveren.

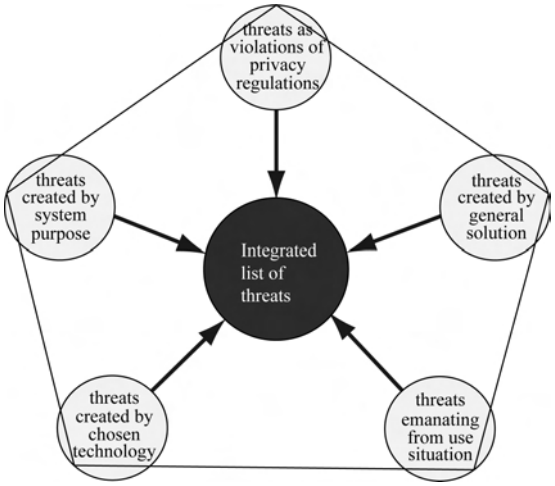
---

104 Van Blarkom, Borking & Olk. 2003, p. 24: "Five different perspectives, and hence five different lines of thinking, is more likely to reveal everything that there is to know about privacy threats."

105 Dit concept denkmodel is vooral het werk van Drs. J Giezen (TNO/TPD) een van de onderzoekers in het PISA research team als input voor deliverable 7 (Research team: J.J.Borking, R.Coolen, J.Giezen & P.Verhaar schreef: A Methodology for Threat Analysis, Deliverable 7 Privacy Incorporated Software Agent (PISA) (IST #2000-26038) project, Brussels 2001).

Het vijfde gezichtspunt betreft het doel waarvoor het systeem wordt ingezet. De vraag voor het vaststellen van de privacybedreigingen is of het doel problemen kan scheppen die de bescherming van persoonsgegevens raken. Het doel kan bijvoorbeeld zijn, dat het systeem wordt ontworpen om onbekende data te zoeken in onbekende bronnen teneinde het resultaat van de zoekactie te gebruiken om bekende data te verrijken of daarmee te vergelijken en op grond daarvan een (geautomatiseerde) beslissing te nemen.

Figuur 4.6: Pentagonale aanpak van privacy bedreigingen, Van Blarkom, Borking & Olk, 2003, p. 24.



Het gevolg van deze aanpak is dat de vijfhoekige analyse in de plaats komt van de niveaus 1 en 2 in het algemene model (figuur 4.5) en uitmondt in de bepaling van de waarschijnlijkheid van de vastgestelde bedreigingen. Daarna volgen de niveau stappen 3, 4 en 5. Hetzelfde gebeurt voor het identificeren van de assets en de inschatting van de consequenties van de bedreigingen voor de assets.[106] Deze aanpak leidt uiteindelijk tot een geprioriteerde lijst van bedreigingen die gebruikt wordt bij het vaststellen van de te nemen technologische en organisatorische maatregelen om de persoonsgegevens in het informatiesysteem te beveiligen. Daar waar technische maatregelen niet voldoende of niet haalbaar zijn, kunnen organisatorische maatregelen genomen worden.

De volgende bedreigingen[107] voor de persoonsgegevens en de persoonlijke levenssfeer zijn reëel bij het overtreden van de EU privacyregel- en wetgeving:

106 Van Blarkom, Borking & Olk, 2003. p. 26-27.
107 De opsomming is niet limitatief.

– Bedreiging 1: geheim bezit van of controle over persoonsgegevens.
De verantwoordelijke en de bewerker hebben controle over persoonsgegevens en er is geen melding van de verwerking van persoonsgegevens gedaan bij de nationale commissie voor de bescherming van de persoonlijke levenssfeer (Data Protection Authority (DPA))[108] van een lidstaat van de Europese Unie waar de verwerking plaatsvindt of bij een functionaris gegevensbescherming.

– Bedreiging 2: geheime verwerking van persoonsgegevens.
Er is een gebrek aan transparantie. De verantwoordelijke of de bewerker heeft de persoonsgegevens rechtmatig onder zich, maar de verdere verwerking geschiedt zonder dat de betrokkene daarvoor zijn toestemming heeft gegeven.

– Bedreiging 3: geheime verwerking van persoonsgegevens.
De betrokkene is niet op de hoogte van het bestaan van persoonsgegevens en de controle, die een onbekende verzamelaar van de persoonsgegevens heeft.

– Bedreiging 4: verwerking van persoonsgegevens in strijd met de wet.
Er is geen vrije, ondubbelzinnige en specifieke toestemming van de betrokkene voor de verzameling, het gebruik, de verwerking, de openbaarmaking en de verspreiding van zijn persoonlijke informatie.[109]

– Bedreiging 5: verwerking in strijd met de doelbinding.
De verwerking van persoonsgegevens vindt plaats in strijd met de privacy voorkeuren van de betrokkene of de verantwoordelijke beperkt de verwerking niet tot het opgeven doel van de verwerking (doelbinding).

– Bedreiging 6: onrechtmatige verwerking van persoonsgegevens.
De verwerking vindt in strijd met de wet plaats, is onrechtmatig (illegaal).

– Bedreiging 7: gebrek aan gegevensminimalisatie.
De verzameling van persoonlijke informatie wordt niet tot een strikt minimum beperkt. Er wordt meer verzameld en verwerkt dan strikt noodzakelijk is voor de realisering van het doel waarvoor de persoonsgegevens zijn bestemd.

– Bedreiging 8: excessieve identificatie van het individu.
De identiteitsgegevens zijn disproportioneel in verhouding tot de doeleinden van de verwerking van de gegevens noodzakelijk is. De inrichting van het informatiesysteem is zodanig dat de identificatie, observering en traceerbaarheid van het desbetreffende individu niet wordt beperkt.

---

108 In Nederland het College bescherming persoonsgegevens in Den Haag.
109 Artikel 13 van 95/46/EG bevat uitzonderingen en beperkingen op dit realisatiebeginsel.

– Bedreiging 9: verouderde gegevens.
Beslissingen vinden plaats op basis van onjuiste of verouderde gegevens. De persoonsgegevens worden niet correct, niet accuraat, ontoereikend, niet ter zake dienend verzameld en verwerkt.

– Bedreiging 10: verantwoordelijke is onvindbaar of weigert transparantie.
Geen of beperkte reactie van de verantwoordelijke op de aanmaning van de betrokkene. Personen over wie gegevens worden verzameld, krijgen niet de mogelijkheid om hun persoonsgegevens in te zien, te verbeteren, aan te vullen, te verwijderen of af te schermen of bezwaar te maken tegen de verzameling en verwerking van hun persoonsgegevens;

– Bedreiging 11: onbeveiligde datamanagement.[110]
Er zijn geen passende technische en organisatorische maatregelen genomen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking of om onnodige verzameling en verwerking van persoonsgegevens te voorkomen.

– Bedreiging 12: niet-vertrouwelijk en onzorgvuldige datamanagement.[111]
De vertrouwelijkheid van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten wordt niet gerealiseerd.

– Bedreiging 13: verkeersgegevens worden te lang opgeslagen.
De verkeersgegevens van abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst, worden wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, niet gewist of anoniem gemaakt.

– Bedreiging 14: niet toegestane verwerking buiten de EU.
Verzending van persoonsgegevens vindt plaats naar een land, dat geen (adequate) bescherming biedt zoals die geldt binnen de EU en EEA.

De gekozen technologie leidt tot specifieke bedreigingen. Hieronder volgen twee voorbeelden en betreffen de mobiele software agent en biometrische systemen:

---

110 ISO/IEC 15408-1: 1999; Evaluation Criteria for IT Security (ook bekend onder de naam Common Criteria for Information Technology Security Evaluation), International Organization for Standardization, 1999, csrc.nist.gov/cc/ccv20/ccv2list.htm. Voor deze bedreigingscategorie dienen de security objectives van ISO/IEC 15408 toegepast te worden.

111 Driml, 2003, *www.isaca.org/Template.cfm?Section=Home&Template=/Search/SearchDisplay.cfm.* Voor deze bedreigingscategorie dienen de securityobjectives van ISO/IEC 15408 toegepast te worden.

Voor mobiele software agents, die in hoofdstuk 6 aan bod komen, gelden de volgende extra bedreigingen:[112]

1. Verandering van de functionaliteit van de software agent.
2. Het klonen of dupliceren van de agent.
3. Het beschadigen van de agent.
4. Andere agenten doen zich voor met een andere identiteit dan die agenten normaliter hebben.
5. 'Masquerading', de gebruiker van een agent, gebruikt ten onrechte de identiteit van een andere eigenaar of houder van agent.
6. Niet of slecht beveiligde informatie die de agent bij zich draagt.
7. De mobiele software agent kan geen onderscheid maken tussen openbare en persoonlijke gegevens.
8. Het platform van waaraf de agent opereert, is niet veilig, waardoor een agent bijvoorbeeld geïnfecteerd kan worden met een computervirus.
9. Het platform waar de agent zich bevindt krijgt een niet voorziene controle over de agent, waardoor de agent tegen de instructies naar een ander platform kan worden gezonden waar hij de eerder ingeprogrammeerde opdrachten op andere plaatsen dan voorzien, uitvoert.
10. Door controle over de agent kunnen anderen ongewild binnendringen in de computer van de gebruiker.
11. De agent is door kwaadwillenden zo veranderd, dat de agent schadelijke acties tegen de oorspronkelijke eigenaar of houder van de agent uitvoert.
12. De agent is door een agent provider (te vergelijken met een ISP), ter beschikking is gesteld, en de provider corrumpeert de privacy van de gebruiker van agent.[113]

Er zijn nog veel meer bedreigingen. De bovenstaande lijst van bedreigingen is niet limitatief en dient toegevoegd te worden aan de lijst van bedreigingen die uit het overtreden van de Richtlijnen 95/46/EG en 2002/58/EG voortvloeien.

Voor biometrische systemen gelden onder meer de volgende bedreigingen:

1. 'Spoofing' (toegang door vervalste identiteit) door valse biometrische kenmerken aan te bieden.
2. Replay attacks door direct in het systeem een 'template' te installeren en daardoor de identificatiesensor te omzeilen.
3. Substitutieaanval door de bestaande rechtmatig vastgelegde 'template' van een gebruiker te vervangen door de template van de aanvaller en daarmee de identiteit te stelen van die gebruiker.
4. Tampering door de verificatienorm voor een bepaalde template in het systeem zo aan te passen dat er een hoge verificatiescore wordt gerealiseerd.
5. Maskerade aanval door een digitale template aan het systeem aan te bieden (bijvoorbeeld gestolen uit een database of nagemaakt) waardoor men zonder

112 Borking, Van Eck & Siepel, 1999, p. 23-31.
113 Van Blarkom, Borking, & Olk, 2003, p. 82-84.

dat het werkelijke biometrische kenmerk van de aanvaller hoeft te worden getoond elke keer weer toegang tot het systeem kan krijgen.

6. 'Trojaans paard' door bijvoorbeeld het vergelijken van het echte biometrische kenmerk met het opgeslagen template te vervangen door een Trojaans paard-programma waardoor het systeem altijd een positieve verificatiescore geeft.[114]

De vijfhoekige benadering bij het analyseren van privacyrisico's is in het PISA-researchproject uitvoerig getest. De PISA-onderzoekers geven toe dat deze methodische aanpak weliswaar werkt voor het vaststellen van de privacybedreigingen binnen de omgeving van mobiele software agents, maar (nog) niet aantoonbaar heeft geleid tot een gestructureerde, herhaalbare en verifieerbare methode om privacybedreigingen voor alle informatiesystemen voldoende volledig in kaart te brengen. Het ontbrak aan voldoende tijd en middelen dit uit te testen.[115] Het verdient aanbeveling de research met betrekking tot de pentagonale aanpak voort te zetten.

De derde onderzoeksvraag (OV 3) luidt: '*Met welke privacybedreigingen en –risico's moeten de burger en de ontwerper van systemen rekening houden?'*

Is de derde onderzoeksvraag nu voldoende beantwoord? Ik vind van niet. Omdat er geen gestandaardiseerde en algemeen geaccepteerde privacyrisicoanalyse bestaat, zijn er zo als eerder gesteld vele methoden in omloop. De innovatieve aanpak van Little & Rogova die de bedreigingen benaderen vanuit de een algemene bedreigingsontologie zou tot meer volledigheid van de waargenomen bedreigingen kunnen leiden. Het resultaat zou een betere beantwoording van de derde onderzoeksvraag tot gevolg hebben. De ideeën van Little & Rogova worden hieronder uiteengezet.

4.11. Privacybedreigingsontologie

Alle hierboven besproken privacyrisicoanalyses beschrijven op verschillende manieren hoe de privacyrisico's herkend kunnen worden en om de sterkte van de beschermingsmechanismen in het systeem te meten. Dit leidt tot een niet-limitatieve lijst van privacyrisico's zonder een redelijke zekerheid dat alle voor het systeem relevante privacyrisico's in kaart zijn gebracht. Dit gebrek aan voldoende 'volledigheid' kan ertoe leiden dat de mogelijk te nemen tegenmaatregelen hun beoogde doel geheel of gedeeltelijk zouden kunnen missen. Fritsch stelt, dat in de verschillende risicoanalyse methoden de classificatie van privacyrisico's en de hieraan gerelateerde kosten niet op een overtuigende manier is uitgevoerd.[116] Bovendien zijn de privacyrisico's in de bestaande literatuur niet goed gedefinieerd.[117]

---

114 Cavoukian & Stoianov, 2007, p. 12-13.
115 Van Blarkom, Borking & Olk, 2003, p. 29: "(…) a haphazard approach is not necessary (…) the presented approach (…) is just a first try and improvements and refinements are bound to follow".
116 Fritsch, 2007, p. 8.
117 Gellman, 2002.

Welke methode leidt dan wel tot een gestructureerd en nauwkeuriger overzicht van de privacybedreigingen? Felten adviseert dat bij een beveiligingsanalyse eerst het bedreigingsmodel moet worden doorzien: "Understand your threat model...if you don't have a clear threat model then you won't be able to think analytically about how to proceed. The threat model is the starting point of any security analysis."[118]

Om vanuit het kennisdomein 'bedreiging' een bedreigingsmodel te ontwikkelen is een ontologische benadering noodzakelijk.[119] Een ontologie kan beschreven worden als een formele hiërarchische gestructureerde en gedetailleerde beschrijving (vaak in de vorm van een beslissingsboomstructuur) van tussen experts gedeelde kennis over een bepaald kennisgebied. De ontologie heeft de bedoeling een abstract conceptueel model te creëren, dat kan worden geïmplementeerd in online semantic web[120] of in offline informatiesystemen en (semi)automatisch kan worden toegepast.[121] Maedche definieert het als volgt: "an ontology refers to an engineering artifact, constituted by a specific vocabulary used to describe a certain reality, plus a set of explicit assumptions regarding the intended meaning of the vocabulary".[122] De rigoureuze manier waarop een bepaalde werkelijkheid in een ontologie gedetailleerd in een data taal (bijvoorbeeld OWL)[123] wordt beschreven, lijkt op een woordenboek. In dit woordenboek worden alle toelaatbare concepten die in een bepaalde applicatie kunnen gebruikt, opgesomd waarbij aangegeven wordt welke mogelijke relaties er bestaan tussen de verschillende concepten, de zgn: 'Resource Description Framework' (RDF).[124] Een ontologie kan gezien worden als een model van de werkelijkheid voor een computer.[125]

Zo kunnen bijvoorbeeld de privacyontologieën, gebaseerd op de EU privacyrichtlijnen, na implementatie in informatiesystemen dienen als de ruggengraat voor dataverkeer over privacyvoorkeuren, voor het vergelijken van privacybeleid tussen verschillende organisaties, het uitwisselen van PII's en de automatische behandeling van persoonsgegevens in databanken overeenkomstig de voorkeuren van de persoon in kwestie of de wettelijke normen.

Ontologieën zorgen voor modellen die door informatiesystemen te 'begrijpen' ('vocabulaires') zijn. Deze vocabulaires zijn interoperabel en universeel

118 Felten, 2009.
119 Sotoodeh, 2007, p. 27.
120 Feigenbaum, e.a.,2007, p. 65-71: "Semantic Web: a highly interconnected network of data that could be easily accessed and understood by any desktop or handheld machine".
121 Uschold & Gruninger, 2005, p. 58-64.
122 Maedche, 2002, p. 11.
123 OWL staat voor Web Ontology Language.
124 Feigenbaum, e.a., 2007, p. 69: "Each piece of data and any link that connects two pieces of data, is identified by a unique name called a Universal Resource Identifier or URI."
125 Hogben, 2003, p. 2; "So XML schema for example is an informal ontology but it does not have a formal relationship to the world as semantics and therefore XML schemas fall short of what can be achieved by implementing a more rigorous semantic framework."

toepasbaar[126] in heterogene toepassingen. Een e-mail in een bepaalde databank is ook een e-mail in een andere databank. Om binnen een kennisgebied gezamenlijk aanvaarde ontologieën te krijgen, is de inbreng van niet-technisch geschoolde deskundigen van groot belang om de juiste interpretatie van de gebruikte concepten in te ontwikkelen ontologieën te bewerkstelligen. Zo dienen in de bescherming van persoonsgegevens deskundige juristen in discussie te treden met de ontologiebouwers over hun interpretatie van de privacywetgeving. Ontologieën dienen zodanig gestandaardiseerd te worden, dat zij in verschillende applicaties kunnen worden toegepast, herbruikbaar zijn en met elkaar in onderling verband staan. Bovendien dienen ontologieën zodanige logische en interfererende regels op te leveren dat deze over de gehele linie in heterogene informatieverzamelingen kunnen worden gebruikt.

Little en Rogova[127] hebben voor de Amerikaanse Luchtmacht een algemene bedreigingsontologie ontwikkeld. In de door hen geconcipieerde logische ontologische structuur van de bedreigingen worden de complexe objecten van bedreiging op metaniveau als geïntegreerde gehelen (wholes) gezien, waarbij is aangegeven hoe deze gehelen en hun attributen zich tot elkaar verhouden, hoe ze elkaar in processen en gebeurtenissen beïnvloeden, welke mogelijkheden zij bezitten en wat hun kwetsbaarheid is. Het doel is om de relaties tussen verschillende entiteiten, gebeurtenissen en relevant gedrag te begrijpen en te kunnen interpreteren.[128] Zij benadrukken het belang van het gebruik van mereotopologie. Mereotopologie is een combinatie van de mereologie, de combinatie van de logica van delen en deelrelaties, met de topologie, die de logica van de ruimtelijke omvang/reikwijdte en de onderlinge verbondenheid betreft. Mereotopologie wordt aangewend voor een formele ontologische taal om op een metaniveau de grote hoeveelheid complexe ontologische (deel)elementen met elkaar te verbinden.[129] Deze situatie doet zich onder meer voor bij het in kaart brengen van privacybedreigingen. In de mereotopologie wordt het belang van het onderkennen van de complexe relaties tussen objecten, eigenschappen, attributen, ruimten, tijdstippen benadrukt. Andere continue bestaande (zgn. Continuant of SNAP)[130] en in een bepaald tijdvak opkomende en zich ontwikkelende (zgn. Occurrent of SPAN)[131] elementen zijn hier tevens van belang. Door de verschillende ruimtelijke- en tijdsrelatievormen (in een bedreigingsveld) te onderkennen,

126 Sotoodeh, 2007, p. 3: "Interoperability issues arise when such technologies need to share information. Interoperability generally comes in three aspects: (1) technical: compatibility of message formats (2) semantic: terminology and definitions, and (3) organizational: practices and procedures".
127 Little & Rogova, 2006, p. 2.
128 Sotoodeh, 2007, p. 13.
129 Little & Rogova, 2006, p. 3.
130 Continuant: een entiteit dat een continue bestaan heeft en door de tijden heen blijft bestaan ondanks de verschillende veranderingen die optreden (bijv. Een menselijk orgaan, een nationale staat, een leger); SNAP: snapshot ontology.
131 Occurrent: een vier-dimensionaal bestanddeel dat louter binnen de tijd gebeurt en zichzelf openbaart gedurende een bepaalde tijdsperiode (bijvoorbeeld een gedachte proces, het vuren van een wapen, een militaire oefening); SPAN: spanning time ontology.

kunnen mathematisch de bedreigingen en de kwetsbaarheden beter worden gemodelleerd en het grote aantal relatiemogelijkheden beter worden ontrafeld. Bovendien verschaft de mereotopologie het middel om bij bedreigingen formeel de verschillende complexe deel-geheel relaties te beschrijven waarin de van elkaar afhankelijke relationele (foundational dependence) elementen zoals voornemen (intent), middelen (capability) en gelegenheid/omstandigheid (opportunity) een grote rol spelen. Als er een van deze elementen aantoonbaar is, bestaan de andere elementen volgens Little & Rogova ook op het metaniveau in de gehelen.

Bij deze ontologie wordt gebruik gemaakt van de volgende mereologische zinsconstanten als 'bouwstenen' (primitives),[132] te weten:

1. is noodzakelijk dat;
2. is een deel van;
3. afhankelijkheid van.

Bijvoorbeeld: x is een deel van y, dat kan dan betekenen: x is of een deel van y of x = y. Het in deze ontologie belangrijke sleutelbegrip: verbondenheid van delen van gehelen die over de tijd en ruimte verspreid zijn (als ware het in een kwantum veld), wordt als volgt gedefinieerd: als x y overlapt, dan is x verbonden met y. Het is evenwel mogelijk dat x wel verbonden is met y maar dat x geen enkel deel van y overlapt. Er is dan sprake van aanrakingspunt of externe verbinding.

Het eveneens hier belangrijke principe van monotoniciteit wordt als volgt gedefinieerd: als een bepaald object x een deel is van een bepaald object y, dan is alles wat verbonden is met x, ook verbonden met y.[133] Het concept van het overbruggend beginsel van monotoniciteit impliceert dat de mereologische overlapping een vorm van verbinding is. Deze relatievormen zijn van belang om bedreigingen en kwetsbaarheden te modelleren, omdat hiermee een voldoende decompositie van bedreigingsbestanddelen kan worden bereikt, waarbij alle relevante relaties tussen ruimtelijke en tijdsgebonden entiteiten aan bod komen.

Naast deze mereotopologische relaties wordt ook aandacht besteed aan de relaties die onafhankelijke ruimtelijke bestanddelen verbinden met hun tijdsgebonden processen, zoals: participatie, uitvoering, geduld en relaties die afhankelijke ruimtelijke bestanddelen verbinden met tijdsgebonden processen, als ook het realiseren van een bedreiging, en relaties die processen verbinden met hun onafhankelijke entiteiten of met hun afhankelijke eigenschappen zoals betrokkenheid in plaats van deelneming.

Een ontologie die wordt gebruikt voor een bedreigingsanalyse om een bedreiging te bestrijden, dient een onderscheid te maken tussen potentiële en levensvatbare c. q. uitvoerbare dreigingen. De aandacht bij de bedreigingsanalyse moet vooral gericht worden op de potentiële bedreigingen omdat deze bedreigingen nog niet

132 Von Kutschera &.Breitkopf, 1971, p. 49.
133 Little & Rogova, 2006, p. 3.

(volledig) bestaan (in the state of becoming).[134] Het gevolg van deze benadering is dat als men de juiste middelen aanwendt kan de bedreiging worden verkleind of afgewend en voorkomen worden dat de bedreiging levensvatbaar[135] en uitvoerbaar wordt (in the state of being).[136] Om de bedreiging te verkleinen of in de kiem te smoren is preventief handelen noodzakelijk, bijvoorbeeld door technologie in te zetten.[137] Daarbij is het noodzakelijk de kwetsbaarheden (zwakte) te begrijpen wanneer het gaat om intergerelateerde vormen van bedreiging die bestaan uit verschillende (deel)objecten die zijn verspreid over tijd en locatie en die op zichzelf onschuldig zijn, maar in combinatie een grote bedreiging en bij realisatie schade kunnen veroorzaken. Het klassieke voorbeeld is het afzonderlijk bezit van wielen, een motor, een stuur, een versnellingsbak etc. Het gaat om de combinatie. De bedreiging voor voetgangers ontstaat op het moment dat de onderlinge onderdelen gecombineerd worden om als een voertuig voor transport te gebruiken.

Handelen wanneer de *state of becoming* nog bestaat, is een van de redenen om binnen het kennisdomein privacybescherming privacy enhancing technologies (PET) in te zetten, omdat zolang de bedreiging zich nog niet volledig heeft ontvouwd, het een geschikte manier is om de privacybedreiging te matigen of zelfs in de kiem te smoren. Zo kan voorkomen worden, dat de bedreiging levensvatbaar en gerealiseerd wordt. Het gaat er met name om de gunstige omstandigheden voor de bedreiging uit te schakelen, want de relatie tussen bedreiging en doel wordt verbonden door de gunstige omstandigheden.

De door Little & Rogova ontwikkelde bedreigingsontologie, is in het PET-Webproject[138] toegepast bij de ontwikkeling van een privacybedreigingsontologie. Deze aanpak maakt het mogelijk de vele belangrijke elementen, hun onderlinge invloed en relaties die in privacywereld relevant zijn, weer te geven. Het resultaat levert een consistent en omvattend model op voor het inschatten van de mogelijke bedreigingen en hoe die bedreigingen zouden kunnen worden opgevangen. Bij het ontwerpen van informatiesystemen kunnen op grond van zo'n model beter onderbouwde beslissingen worden genomen en de gevolgen van de beslissingen voor de architectuur van het systeem beter worden ingeschat. Figuur 4.7 op de volgende bladzijde geeft schematisch de privacybedreigingsontologie weer. De bedreiging richt zich in dit model op de 'privacy objectives'. De verschillende bronnen voor de bedreiging leiden tot de 'threat actor', die in de ontologie de metabeschrijving is van het 'threat target' gecombineerd met de 'threat agent'. Vidalis en Jones verstaan onder threat agent het individu of

134 Little & Rogova, 2006, p. 5.

135 Little & Rogova, 2006, p. 5: "Viable threats exist when all three elements (intent, capability, opportunity) are present and form a tri-partite whole via relations of foundational dependence. Potential threats exist when at least one essential part (and its corresponding relations) is missing".

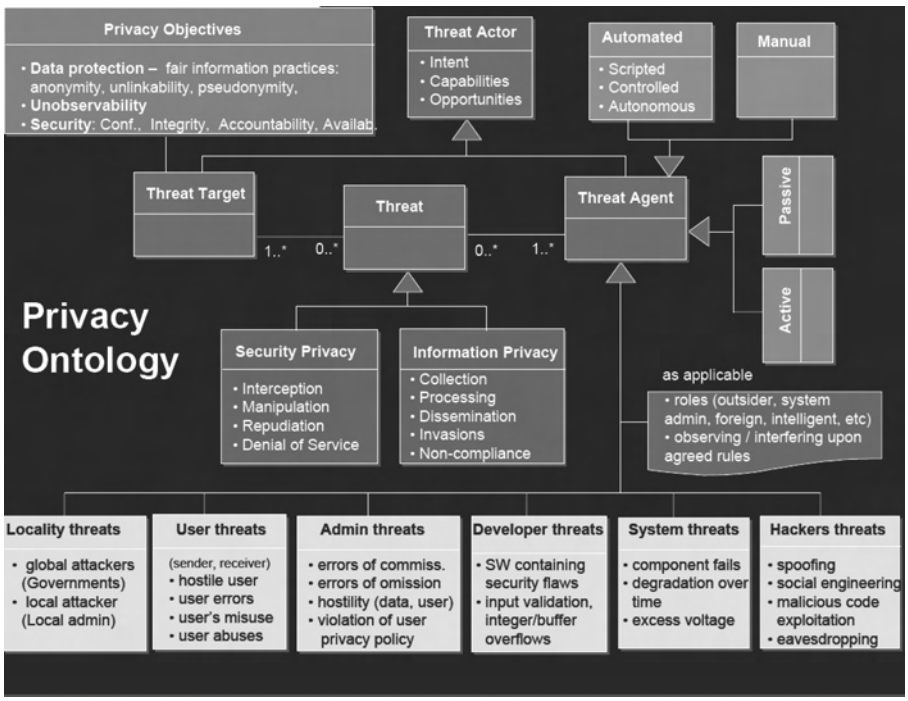
136 Little & Rogova, 2006, p. 4.

137 Voor privacybedreigingen kunnen privacy enhancing technologies (PET) worden ingezet.

138 Privacy Enhancing Technology for Webbased Services (PET-Web), "The primary objective is to devise a framework for facilitating the development of the next generation of privacy enhancing technologies in large-scale web-based services", Projectno. 180069/S10, Oslo 2007.

de groep dat een bedreiging kenbaar maakt of uitvoert.[139] Drie met elkaar in verband staande elementen zijn conform de ontologie van Little & Rogova van belang om de threat agent te kunnen opsporen. De 'threat agent' kan volgens het model zowel van binnen als van buiten de organisatie komen. In figuur 4.7. worden de elementen en hun intra- en interrelaties weergegeven. Deze zullen in paragraaf 4.12 worden toegelicht. Deze ontologische aanpak geeft een vollediger beeld dan de privacybedreigingsanalyses van Bellotti, Gaver, Neustaedter, Solove, en PISA, omdat het de bedreigingselementen in een elkaar beïnvloedende afhankelijkheidsrelatie in tijd en ruimte plaatst.

Figuur 4.7: PETWeb privacy bedreigingsontologie, Abie, 2007.



De lijn tussen Threat Target en Threat en tussen Threat en Threat agent geeft aan dat er een relatie bestaat tussen deze begrippen. De toelichting op dit model vindt hieronder in paragraaf 4.12 plaats.

139 Vidalis & Jones, 2005, p. 3.

4.12. Toelichting op het bedreigingsontologiemodel

Figuur 4.7 bevat vier bedreigingselementen met hun onderlinge relaties, namelijk het doel waarop de bedreiging zich richt: het ondermijnen van de privacy (threat target), de persoon die de bedreiging veroorzaakt (threat actor), de manier waarop bedreiging zich manifesteert (threat agent), en de bedreiging zelf (threat).

4.12.1. Privacydoeleinden

Uit het model blijkt dat er bedreigingen zijn voor privacydoeleinden of 'privacy objectives'. Hieronder wordt in dit model verstaan: de Europese en andere (inter) nationale wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens en de in hoofdstuk 2 besproken universele privacybeginselen betreffende persoonlijke informatie en de elf privacyrealisatiebeginselen. De hierboven vermelde privacybeginselen zijn niet de eerste kandidaten om het bedreigingsidentificatieproces mee te beginnen, maar de bedreigingen kunnen er van worden afgeleid, zoals in het EU PISA-researchproject is aangetoond.[140] In de groep privacy objectives hoort ook thuis de ISO-standaard 15408 betreffende 'anonymity', 'pseudonymity', 'unlinkability', 'unobservability'. Een aanval op anonimiteit, pseudonimiteit, niet-traceerbaarheid en het niet-observeerbaar kunnen de identiteit(en) van de gebruiker blootleggen en zijn privacy beschadigen. Anonimiteit[141] zorgt er voor dat de gebruiker van bepaalde diensten gebruik kan maken zonder dat zijn identiteit bekend wordt. Pseudonimiteit beschermt de identiteit binnen een bepaald gegevensdomein als anonimiteit niet kan worden aangeboden en de gebruiker in geval van fraude e.d. wel aansprakelijk gesteld dient te worden. Niet-traceerbaarheid verzekert de gebruiker van het feit dat hij van diensten kan gebruikmaken zonder dat anderen zijn gebruik van die diensten aan elkaar kunnen koppelen. Niet observeerbaarheid zorgt er voor dat een gebruiker van een dienst gebruik kan maken, zonder dat iemand in staat is om vast te stellen dat die dienst is gebruikt.[142] De Article 29 Working Party heeft omschreven wanneer er sprake is van anonieme en pseudonieme data.[143]

Het model geeft voorts aan dat bedreigingen kunnen optreden die de 'security objectives' kunnen corrumperen, namelijk vertrouwelijkheid (bij onderschepping en afluisteren), integriteit (bij manipulatie van gegevens), verslag kunnen doen over wat er in een systeem is gebeurd (zich niet kunnen verantwoorden)[144] en beschikbaarheid (niet kunnen beschikken over informatie). De notatie in het

140 Borking, e.a., 2001 p. 24.
141 Prins,1998.
142 Voor een uitgebreide discussie: Fischer-Hübner 2001; en http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.
143 Opinion WP 136 – Opinion 4/2007: on the concept of personal data, p. 18 (pseudonimiteit) en p. 21 (anonimiteit), http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/.
144 Bijvoorbeeld als de overheid door toedoen van een Israëlische toeleverancier niet kan beschikken over de broncode van bepaalde systemen (afluistersysteem).

model: 1..* en 0..* geven aan het voorkomen van de hoeveelheid van mogelijke specifieke met het onderwerp (bijvoorbeeld 'Threat Target') verbonden associaties of een bepaalde wiskundige waarde. Dus 0..1 betekent nul of één, 0..* betekent veel, 1..*, één of meer, en 1 betekent exact één. De twee punten (..) geven een klasse van objecten aan.

4.12.2. De threat actor

De privacybedreigingen worden veroorzaakt door een persoon, die de motivatie, de capaciteit en mogelijkheden bezit[145] om van persoonsgegevens, die hij al dan niet rechtmatig onder zich heeft, kennis te nemen of zonder toestemming te verwerken, te veranderen of te vernietigen of in strijd te handelen met de beperkingen die het individu ten aanzien van zijn persoonsgegevens heeft kenbaar gemaakt met het doel schade aan de ander toe te brengen.[146] Privacy bedreigingen[147] kunnen ontstaan, omdat er zich actoren (targets en agents) bevinden binnen de sfeer van de verwerking van persoonsgegevens, terwijl bovendien de bescherming van de persoonsgegevens al kwetsbaar is doordat persoonsgegevens op zoveel verschillende manieren worden blootgesteld aan de buitenwereld.[148]

Little & Rogova[149] en Vidalis & Jones[150] hebben beiden in de door hen ontwikkelde bedreigingsontologieen een vrijwel identiek drie dimensionaal matrixmodel gebruikt, om aan te geven aan welke noodzakelijke, aan elkaar gerelateerde attributen[151] een bedreiging en een uitvoerder van een bedreiging dient te voldoen om de potentie te hebben om een zwakke plek in het systeem te kunnen uitbuiten.[152] Omdat deze attributen binnen een bedreiging zo met elkaar verbonden en van elkaar afhankelijk zijn, is het gevolg van de verstoring of uitschakeling van één van deze elementen dat de bedreiging verdwijnt of zodanig wordt verstoord, dat de bedreiging niet meer effectief kan zijn. Daarom is het van belang om de rol van elk van deze attributen, 1 intenties of motivatie, 2 capaciteiten, 3 (gunstige) omstandigheden binnen een bepaalde dreiging goed te onderkennen. De hiervoor vermelde elementen van een bedreiging kunnen als extern- of intra- of intern gerelateerde delen van het geheel van een bedreiging bestaan:

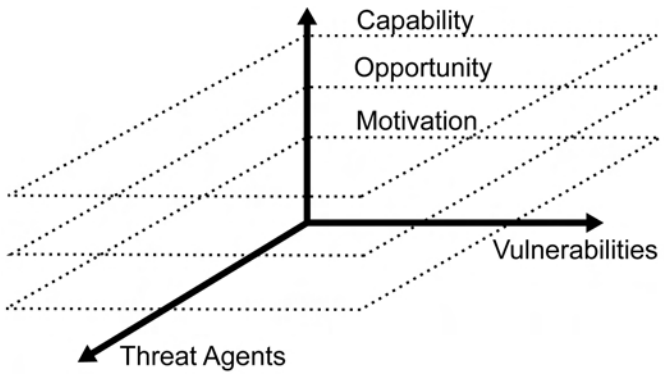
1. **Intentie of motivatie** – Intentie (het voornemen) bestaat volgens Little[153] uit plannen of doelstellingen die tot stand gebracht moeten worden. De intentie vertegenwoordigt de psychologische component van een bedreiging en kan

145 Vidalis & Jones, 2005, p. 2.
146 Groebel & Hinde. Aggression and War Cambridge 1989, p. 3: "Behaviour directed towards causing physical injury to another individual is labelled as aggressive behaviour".
147 Borking e.a., 2001, p. 39.
148 Met buitenwereld wordt de wereld buiten mijzelf, buiten de invloed van een persoon bedoeld.
149 Little & Rogova, 2006, p. 3.
150 Vidalis & Jones, 2005, p. 6.
151 Little & Rogova, 2006, p. 4.
152 Little richt zich meer op de omgevingsfactoren, terwijl Vidalis zich bezig houdt met de instelling van de agressor zelf.
153 Little & Rogova, 2006, p. 3.

sterk worden beïnvloed door iemands middelen en mogelijkheden. Vidalis[154] beschrijft motivatie als de mate waarin een agressor bereid is om een bedreiging ten uitvoer te brengen. Camp sluit zich daarbij aan.[155]

2. **Middel of bekwaamheid** – Hieronder verstaat Little de soorten objecten (bijvoorbeeld wapens), attributen van objecten (bijvoorbeeld projectielen of explosieven) of gedrag (bijvoorbeeld: bewegend, sensorische mogelijkheden), die een bepaald niveau van schade, verstoring of vernietiging aan een doel kunnen toebrengen (zoals vastgesteld door iemands intenties en mogelijk gemaakt door de gelegenheid). Vidalis[156] beschrijft dit begrip als de mate waarin iemand (de agressor) in staat is (de bekwaamheid heeft) om een bedreiging feitelijk ten uitvoer te brengen.
3. **Gelegenheid** – Hieronder verstaan zowel Little & Rogova als Vidalis & Jones de qua ruimte en tijd gunstige voorwaarden om de bedreiging effectief en met resultaat ten uitvoer te leggen, bijvoorbeeld toegang tot een systeem zonder autorisatie en authenticatie; de toegang tot een medewerker; op de hoogte zijn van de plannen van de tegenstander. Camp richt zich meer op de kwetsbaarheid van de infrastructuur. De opvattingen van Little & Rogova en Vidalis & Jones leiden tot het volgende matrix (figuur 4.8), waaruit een eerste zicht op de ernst van een bedreiging kan worden verkregen:

Figuur 4.8: Threat agent, kwetsbaarheid matrix, S.Vidalis & A.Jones, 2005, p. 6.



Wanneer deze matrix naar de wereld van de privacybedreigingen wordt vertaald, dan hangt de bekwaamheid om een specifieke bedreiging uit te voeren af van de bekwaamheid van de agressor om de middelen die nodig zijn om de bedreiging te effectueren, te ontwerpen, te ontwikkelen en in te zetten of aan anderen te leveren.

154 Vidalis & Jones, 2005, p. 2.
155 Camp & Lewis, 2004, p. 88-92.
156 Camp & Lewis, 2004, p. 88.

Intentie of voornemen wordt in het privacybedreigingsontologie model afgeleid uit beslissingspatronen van agressors en in vereniging samenwerkende groepen van agressors. Als er een predispositie is voor agressieve beslissingen, dan zal die meer voorkomen in een groep waar het groepsdenken ('groupthink') dominant is.[157] Bovendien blijkt het 'Prisoner's Dilemma' een rol te spelen in het nemen van een agressieve beslissing.[158] De bedreigingsontologie biedt een basis voor conclusies op basis van de in kaart gebrachte relevante relaties tussen entiteiten. In de ontologie wordt eveneens de zwaarte van de potentiële aanval op basis van kwetsbaarheid, tijd, expertise, omstandigheden, de kans en de te gebruiken middelen geëvalueerd.[159]

4.12.3. Passieve en actieve privacybedreiging door individuen en groepen

Er worden twee vormen van bedreiging onderscheiden: actief en passief.[160] Een passieve 'threat agent' is een aanval op het systeem waar een individu of groep ongeautoriseerd de communicatie (gegevensuitwisseling en opslag) tussen twee partijen volgt of afluistert zonder een poging te doen om de boodschap te veranderen, bijvoorbeeld door een passieve communicatielijn af te tappen. Een actieve 'threat agent' is een aanval waarbij de aanvaller ('attacker')[161] gegevens verstuurt naar een of beide partijen, of de gegevensstroom blokkeert in één of beide richtingen. De aanvaller kan zich indringen in een gegevenstroom tussen de communicerende partijen en zijn eigen data of die van anderen toevoegen aan de gegevensstroom, data uit een andere communicatie onderscheppen en toevoegen aan een andere gegevensstroom of gegevens verwijderen.[162] De binnendringer kan ook een 'man-in-the-middle-attack' (een specifiek voorbeeld van een actieve aanval) uitvoeren, waarbij hij zich nestelt in het midden van een communicatieverbinding, de boodschappen onderschept en vervangt door zijn eigen berichten. Hij kan daardoor aan de communicerende partijen de indruk geven, dat zij direct met elkaar communiceren, terwijl zij in werkelijkheid met de aanvaller communiceren.

4.12.4. Automatische en handmatige aanvallen

De ETSI (European Telecommunications Standards Institute) TIPHON (Telecommunications and Internet Protocol Harmonization over Networks)/TISPAN

157 Groebel & Hinde. 1989, p. 137.
158 Kerkmeester, 1989, p. 91-104 voor een uitvoerige beschouwing over prisoner's dilemma's.
159 Camp & Lewis, 2004, p. 89: "The likelihood that a potential vulnerability could be exploited by a given threat source can be described by high, medium and low" (NIST- U.S. National Institute of Standards and Technology 2001).
160 Davies & Price, 1994, p. 42-44.
161 Brands, 2000, p. 45-48 : Een attacker kan ook een interactief algoritme zijn: "that may deviate from its prescribed actions, for instance by deviating from its actions in the specified protocols or by wiretapping the protocol executions of others."
162 Tettero, 2000, p. 21.

(Telecoms & Internet coverged Services & Protocols for Advanced Networks)[163] bedreigingsanalyse kent vier soorten 'threat agents':

a. Manual Threat agents.
b. Scripted automated threat agent.
c. Controlled automated threat agents.
d. Autonomous automated threat agents.

a. Manual threat agent

Een manual threat agent is persoon die een schadetoebrengende aanval uitvoert op een asset (het object waarop de bedreiging zich richt en waardoor de bedreiging kan ontstaan (bijvoorbeeld de gebruikers, ISP, identiteitsverschaffer).

b. Geprogrammeerde of geautomatiseerde (scripted) aanval

Het betreft hier een geautomatiseerde aanval op het informatiesysteem die vervolgens over het internet wordt verspreid, waardoor personen met aanmerkelijk minder expertise (de zgn. script kiddies),[164] maar in het bezit van generieke pc-hardware, een aanval kunnen uitvoeren. Het gaat om een automatische methode die in een netwerk of informatiesysteem inbreekt op het niveau van 'point-and-click'.[165] Deze ontwikkeling houdt in, dat voor een geautomatiseerde aanval weinig expertise is vereist van systemen, er weinig tijd nodig voor is en er ook geen geavanceerde computers gebruikt hoeven te worden voor een dergelijke 'scripted' (geprogrammeerde) aanval.

c. Onder controle van derden staande threat agents (Botnet)

Botnet is een verzameling van software robots, ook wel bots genoemd, die zelfstandig en automatisch hun werkzaamheden uitvoeren door middel van zgn. 'zombie' computers die op afstand worden beheerd door hackers via commando en gecontroleerde infrastructuur. Deze geautomatiseerde aanval vereist geen interactie van de gebruiker. Als de aanval in werking is gezet, wordt de aanval verder overgenomen door 'zombie' computers die een gecoördineerde veelvoud van nieuwe opvolgende aanvallen oplevert. Het grote gevaar van een Botnet is dat er veel meer rekenkracht, bandbreedte en IP-adressen voor een aanvaller beschikbaar zijn. Hierdoor is het mogelijk bepaalde aanvallen uit te voeren die normaal niet mogelijk zijn. Dit kan leiden tot 'Distributed Denial of Service'

163 ETSI TR 187 014. V. 2.1.1 (2009); http://portal.**etsi**.org/docbox/.../2009/.../TVRA_006_TVRA_web_user_-guide.pdf.
164 Hieronder wordt verstaan een onervaren kwaadwillige hacker, die programma's gebruikt die door andere hackers zijn ontwikkeld om informatiesystemen aan te vallen en websites te bekladden; www.honeynet.org/papers/enemy/.
165 Keanini, 2003.

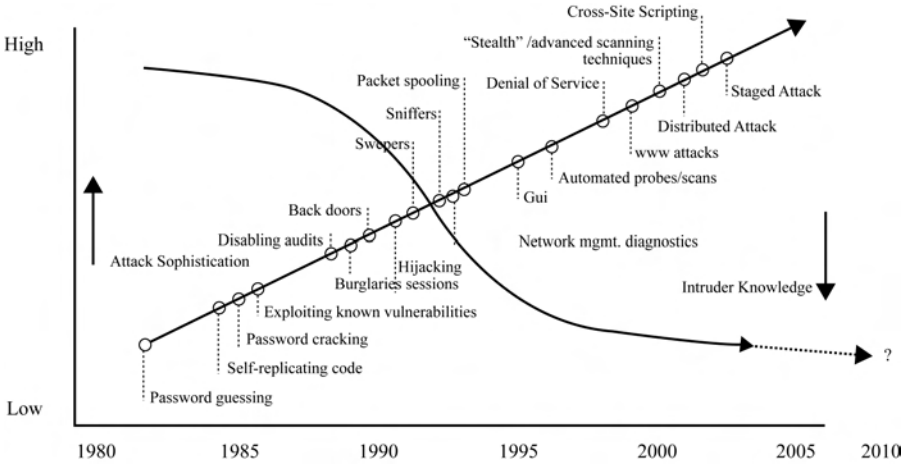
(DDoS)[166] aanvallen, maar dergelijke geconcentreerde aanvallen kunnen ook voor andere doeleinden worden gebruikt, zoals 'Distributed password cracking'. Bovendien is het veel lastiger om aanvallen te detecteren of tegen te gaan wanneer deze van verschillende IP-adressen afkomstig zijn.

Ernstiger is het dat deze vorm van aanval zonder interventie van een gebruiker op een systeem nog minder kennis van de aanvaller vereist dan die nodig is om een 'scripted' aanval te downloaden en uit te voeren. Het wordt steeds makkelijker om een (ro)botnet op te zetten, waardoor het niveau van potentiële bedreiging hoger wordt. Bovendien is het gevolg van dergelijke gecoördineerde aanvallen aanmerkelijk ernstiger, dan de aanvallen die sequentieel worden uitgevoerd.[167]

Omdat informatietechnologie steeds strategischer voor organisaties aan het worden is, worden organisaties en daarmee ook de persoonsgegevens steeds kwetsbaarder voor aanvallen.[168] Algemeen wordt verwacht dat steeds minder kennis van de aanvaller nodig is om een ernstige bedreiging uit te voeren (zie figuur 4.9).[169] Van de Weijer meldt in de Volkskrant van 21 april 2009 over 'CAPTCHA'S' (Completely Automated Public Test to Tell Computers and Humans Apart) (dat is plaatje met verdraaide en doorgestreepte letters en cijfers) die door service providers meegestuurd worden om door ontvangers van bepaalde diensten ontcijferd te worden, geen bescherming meer tegen spam bieden. 'Spammer bots' kunnen deze CAPTCHA's zo goed ontrafelen dat zij de bescherming tegen spam doorbreken. Google stuurt nu afbeeldingen die de gebruiker vervolgens weer rechtop moet zetten. Dat kan de spambot nog niet.[170]

166 F.Lau, e.a.; 2000, p. 2275- 2280: "A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. Examples (...) include attempts to flood a network thereby preventing legitimate network traffic, attempts to dispute connection between two machines thereby preventing access to a service, attempts to prevent a particular individual from accessing a service and attempts to disrupt service to a specific system or person."
167 www.ejure.nl/exturls/dossier_id=264/id=1088/show.html.
168 Kankanhale, e.a., 2003, p. 19-154.
169 B-J. Koops, e.a., 2005, p. 24.
170 Van de Weijer, 2009, p. 9.

Figuur 4.9: Ontwikkeling van aanvallen op systemen. Stippellijn toegevoegd Borking;[171] In 1980 ging het nog om het raden van wachtwoorden waar veel kennis voor nodig was, maar in de loop van dertig jaar zijn de aanvallen steeds verfijnder geworden, terwijl er steeds minder kennis voor nodig is.



d. Autonome geautomatiseerde threat agents (worm/virus)

Een geautomatiseerde aanval kan met een worm[172] of een virus[173] worden uitgevoerd. Iemand hoeft geen directe controle over zo'n aanval uit te oefenen, want de aanval wordt gestart op basis van een bepaalde kloktijd in de computer of een bepaalde tijd nadat de computer met een worm of virus is geïnfecteerd of zelfs door een externe gebeurtenis door bijvoorbeeld een bepaald sleutelwoord op de hoofdpagina van een (openbare) website. Dit type aanval kan zowel plaatsvinden vanuit internet als een gesloten netwerk. Het is mogelijk dat een worm of virus een gesloten netwerk binnendringt. Het virus kan tijdenlang een slapend bestaan leiden totdat het virus een computer met een bepaald IP-adres of domeinnaam bereikt en dan pas actief wordt. Dit gebeurde met de Confickerworm die wereldwijd meer dan tien miljoen computers infecteerde en op 1 april 2008 plotseling actief werd. Moyer beschrijft het mechanisme als: "a worm takes advantage of security holes in ubiquitous software - in this case Microsoft Windows – to spread copies of itself. It uses flaws in Windows software to

171 Allen, 2001.

172 www.sciam.com/article.cfm?id=code-red-worm-assault-on.

173 www.sciam.com/article.cfm?id=computer-viruses-are-25-years-old: "The first computer virus wasn't much of a threat. Created by a mischievous Pittsburgh high school student, Elk Cloner annoyed unwitting Apple II users with a brief poem extolling its power to proliferate: *It will get on all your disks, It will infiltrate your chips, Yes it's Cloner!* …The year was 1982. The IBM personal computer had only been born the year before (its first virus would not crop up until 1986)".

co-opt machines and links them into a virtual computer that can be commanded remotely by its authors".[174] Geïnfecteerde gegevensdragers (bijvoorbeeld een USB-sleutel besmet met een USB-stickvirus)[175] kunnen in een beveiligde ruimte worden binnengebracht en kunnen daardoor binnen het overigens goedbeveiligde netwerk een aanval openen.

4.12.5. Zwakke plekken

Zwakke plekken in informatiesystemen zijn per definitie onbekend, totdat het informatiesysteem of het netwerk wordt blootgesteld aan bedreigingen.[176] Afgezien van bedreigingen door toevallige en externe omstandigheden, zoals brand, het uitvallen van stroom, overstroming, blikseminslag zijn de volgende bedreigingen uit eerdere ervaringen onderkend.

a. De plaats van de aanval (Locality attackers)

Een 'global attacker' is een aanvaller die in staat is om de communicatie binnen het gehele netwerk op enig moment te onderscheppen, door bijvoorbeeld van verschillende partijen de gegevens op te vragen of te compromitteren. Dit zouden bijvoorbeeld speciale diensten van de centrale overheid van een land kunnen zijn of een terroristische aanvaller die een hele branche, land of regio kan beheersen. Onder een 'local attacker/eavesdropper' wordt verstaan een aanvaller die alleen de communicatie van en naar een specifieke groep computers binnen een organisatie in de gaten kan houden of slechts de gegevens van één bedrijf kan bemachtigen. Het gaat dan om alle binnenkomende en uitgaande boodschappen betreffende een bepaalde groep van netwerkknooppunten. Het verschil kan duidelijk worden gemaakt aan de hand van het volgende voorbeeld. Wanneer een webshop de anonimiteit van haar klanten wil waarborgen, kan zij bijvoorbeeld een bestelling aannemen via het internet, een token (willekeurig nummer) genereren voor deze bestelling, dit nummer geven aan de medewerker in het magazijn die de goederen in een doos doet en er dit nummer opplakt, en vervolgens dit nummer ook aan de bezorgdienst geeft met het adres. Een 'local attacker' in het magazijn of bij de pakketdienst weet nu niet wat de klant heeft gekocht, maar een 'global attacker' met zowel mogelijkheden in het magazijn als bij de pakketdienst kan dit wel.

b. Privacybedreigingen vanuit de verantwoordelijke

Hieronder vallen onder meer het schenden van de privacyvoorkeuren van de gebruiker van het systeem door de verantwoordelijke. Het inbreuk maken op de

174 Moyer, 2009, p. 18.
175 Leyden, 2007.
176 Camp & Wolfram, 2000, p. 31-39.

algemene privacybeginselen betreffende persoonlijke informatie en de privacy uitoefeningbeginselen, zoals besproken in hoofdstuk 2, zijn in het algemeen bedreigingsmodel onder gebracht in het veld 'information privacy'.

c. Bedreigingen vanuit de systeem- of programmatuurontwikkelaar

Er zijn vele mogelijkheden waarop een ontwikkelaar privacyinbreuken kan veroorzaken. De ontwikkelaar kan al dan niet opzettelijk software schrijven die beveiliging en privacygebreken veroorzaakt. Hij zou bijvoorbeeld 'back doors' kunnen plaatsen. Het ontwerp van de architectuur kan eveneens privacyinbreuken bevorderen of mogelijk maken.

d. Bedreigingen vanuit de gebruiker

In veel risico analysemodellen wordt de gebruiker als bedreiging vergeten. Er zijn een veelheid van handelingen die de privacy van het individu kunnen schaden, zoals: de gebruiker kan vijandige handelingen verrichten die kunnen leiden tot privacyinbreuken. De gebruiker kan de toestemming om data te verzamelen, te wijzigen of te verspreiden, misbruiken. De gebruiker kan vergissingen of fouten maken die de oorzaak kunnen zijn van privacyschendingen. Door al dan niet bewuste fouten van de gebruiker kunnen data niet meer benaderbaar zijn en dergelijke fouten kunnen de beveiliging van het systeem ondermijnen. Er kunnen (door infiltratie) onbetrouwbare en misdadige gebruikers binnen het informatiesysteem aanwezig zijn, die ontkennen dat zij berichten hebben ontvangen, verstuurd en transacties hebben uitgevoerd. Interne aanvallen kunnen door kwaadwillige en misnoegde personeelsleden worden uitgevoerd.

e. Bedreigingen vanuit de hacker

1. Aanvallen gericht tegen het informatiesysteem, zoals bijvoorbeeld het veranderen van de bestemming van informatie of de bron van informatie.
2. Aanvallen op het informatiesysteem, zoals niet geautoriseerd gebruik, toegang op systeemniveau, onjuist[177] of overmatig gebruik leidend tot 'denial of service', waarbij of de functie door het systeem niet kan worden uitgevoerd of derden het uitoefenen van een bepaalde dienst blokkeren.
3. Bedreigingen binnen het netwerk, zoals 'masquerade'; het doen voorkomen dat berichten van een andere bron komen dan de werkelijke bron; 'snooping', het onderscheppen van berichten om kennis te nemen van de inhoud en met die kennis al dan niet te handelen, bijvoorbeeld door berichten te veranderen.

177 Het kan gebeuren dat iemand een systeem crasht door slechts één verkeerd commando uit te voeren.

f. Bedreigingen vanuit de beveiliging en informationele privacybeginselen

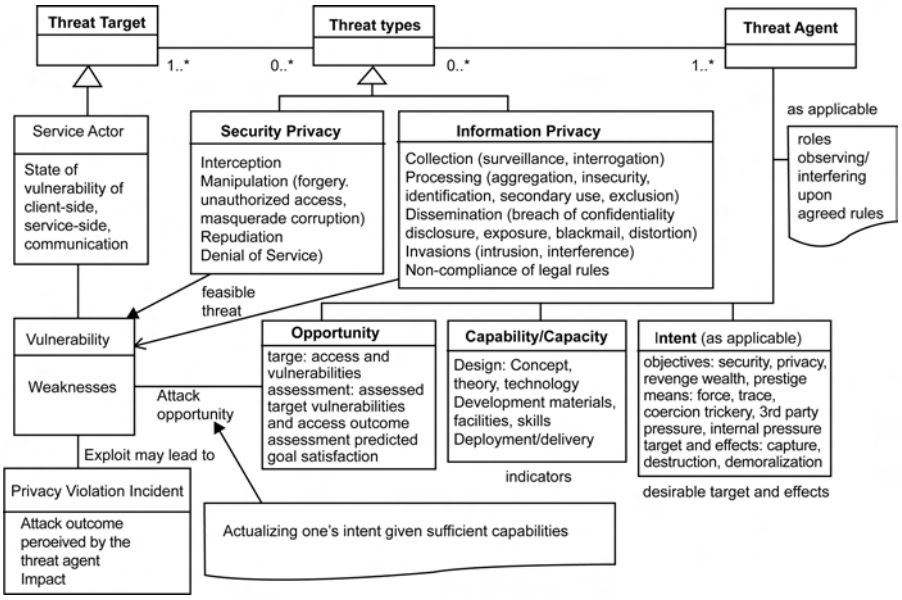
Over beveiliging is in dit hoofdstuk al het nodige geschreven. De term 'Security privacy' in figuur 4.7 is dat deel van de beveiliging dat een directe rol speelt bij bescherming van de persoonsgegevens. Vanuit dit domein kunnen de gegevens worden onderschept, gemanipuleerd en kan de ontvangst van berichten worden ontkend. *Information privacy* is in hoofdstuk 2 behandeld. In dit domein kan onrechtmatige verzameling, verwerking, verspreiding, inbreuken en overtreden van rechtsregels plaatsvinden. De term 'non compliance' is in deze opsomming opgenomen, niet alleen omdat het een ernstige bedreiging vormt, maar ook om ontwerpers van informatiesystemen op het bestaan van relevante privacywetgeving te wijzen.

4.13. Ontologische analyse van privacybedreiging

Het hiervoor besproken ontologische bedreigingsmodel (figuur 4.7) wordt toegepast op en verfijnd naar het functionele ontwerp van het systeem en de systeemomgeving (bijvoorbeeld een Internet Service Provider, die een bepaalde dienstverlening aanbiedt). Het nieuwe 'threat model' gaat uit van: a het feit dat privacybescherming ongelijk is aan informatiebeveiliging; b de parameters van Little & Rogova te weten: 1 intentie, 2 voornemen of motivatie, 3 mogelijkheid, middel en bekwaamheid; c kwetsbaarheid en zwakte, en d (gunstige) aanvalomstandigheden. Eveneens zijn in het model opgenomen de 'assets', de actoren en de bedreigingen.[178] In de hieronder weergegeven figuur 4.10 kan bij toepassing bijvoorbeeld van de 'threat agent' aangegeven worden of er sprake is van wraak, welvaart, druk van derden, lidmaatschap van terroristische organisatie, wat het doel van de bedreiging vanuit de 'threat agent' kan zijn, zoals bemachtigen, vernietiging en demoralisering. In de analyse worden de (potentiële) middelen opgenomen waarmee een bedreiging door de agent kan worden uitgevoerd en waar de gunstige omstandigheden voor een aanval kunnen liggen, gegeven de intentie, de bekwaamheid en de middelen.

178 Skomedahl, 2008, p. 14.

Figuur 4.10: PET-web ontologische privacybedreigingsanalyse, Abie 2007.



Deze analyse heeft geleid tot een gekwantificeerde weging van de bedreigingen met betrekking tot de website Min side (norge.no), die in het PET-Web project werd ontwikkeld. Het betreft dan de weging van de 'assets', het object waarop de bedreiging zich richt en waardoor de bedreiging kan ontstaan (bijvoorbeeld de gebruikers, ISP, identiteitsverschaffer), de mogelijkheden van de toegang tot het systeem, de 'threat agents' (bijvoorbeeld de beheerders, de ontwikkelaars, de hackers), en de motieven van de aanval (intentie, motieven, middel, bekwaamheid, gelegenheid). Vervolgens worden de bedreigingen aan de hand van de impactweging gerangschikt. Het gewogen resultaat dient als input voor de te nemen beslissingen om het functionele ontwerp aan te passen en meer privacybeschermend te maken. Kortom deze analyse spoort de zwakke plekken op.

In figuur 4.10 zou een 'attack tree'[179] kunnen worden gemaakt op basis van de formule: verwacht verlies = kans x impact van een bedreiging. Voor iedere bedreiging wordt vastgesteld wat de grootste impact is van deze bedreiging (in termen van kosten), en wat van elke bedreiging de grootste kans van slagen is (geschat in procenten). Deze getallen worden per bedreiging vastgesteld en met

179 www.schneier.com/paper-attacktrees-ddj-ft.html. www.cs.ru.nl/~petervr/secorg2007/slides04.pdf. www.cs.ru.nl/~petervr/secorg2007/attacktreetalk.pdf.

elkaar vermenigvuldigd. Dit leidt tot de verwachte verliezen per bedreiging. Vervolgens wordt gekeken wat per bedreiging de kosten zijn om ze op te lossen, en of de investeringskosten om de bedreiging te mitigeren de moeite waard zijn. Bij de economische behandeling van investeringsbeslissingen in PET in paragraaf 7.13 wordt op deze calculaties dieper ingegaan.

4.14. Evaluatie van de gebruikte ontologie en het ontwikkelde model

Er bestaat geen gestandaardiseerde methode om een ontologie te evalueren op inconsistenties en redundanties. Teneinde de kwaliteit van het ontwerp te beoordelen, raadt Sotoodeh[180] aan de beginselen van het software ontwerp als leidraad te gebruiken, zoals "abstraction, modularity, separation of concerns, generality, anticipation for change, and rigor and formality".

De researchers van het PET-Web project hebben het 'privacy threat impact model' getest op de applicatie van de Noorse overheid MyPage.[181] MyPage biedt iedere Noorse burger de mogelijkheid vrijwel alle gegevens die door de overheid over die individuele burger heeft opgeslagen, elektronisch vanuit zijn eigen computer in te zien. Evenwel, de toepassing van dit model is sterk beperkt ten gevolge van het hoge niveau van onzekerheid over het bepalen van de waarde van de 'assets' en het effect van een aanval op de verschillende elementen vermeld in het model. Terugkoppeling naar de structuur van het ontologisch model door middel van interviews met beveiliging- en privacyexperts die het model hebben getoetst aan hun kennisdomein, leidde tot het theoretisch inschatten van vele parameters, omdat er nog geen empirisch bewijs voor handen is. Zolang er geen verplichting bestaat privacyincidenten te rapporteren aan de nationale DPA, zullen de noodzakelijke empirische gegevens niet voorhanden zijn. Wel werd duidelijk dat gezien de geconstateerde bedreigingen het noodzakelijk is PET maatregelen in de architectuur van Min side of MyPage in te bouwen omdat anders het niet mogelijk was de identiteit van de burger in MyPage en zijn persoonsgegevens adequaat af te schermen.

4.15. Slotopmerkingen

De Europese privacyrichtlijnen en de daarop geënte nationale wetgevingen van de EU lidstaten schrijven de beveiliging van persoonsgegevens voor met een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Om dergelijke data adequaat te beschermen, dient duidelijk te zijn welke privacyrisico's er ontstaan bij het

180 Sotoodeh, 2007, p. 23.
181 http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3639.

verwerken van persoonsgegevens en het introduceren van nieuwe informatiesystemen. Daarvoor is een objectieve methodologische privacybedreigings- of -impactanalyse nodig.

Gezien het bepaalde in artikel 17 van 95/46/EC: "(...)Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.(...)", kan dit niet anders geïnterpreteerd worden dan dat een privacybedreigings- of -impactanalyse een sine qua non is voordat van persoonsgegevens worden verwerkt. Dit wettelijk vereiste wordt evenwel massaal genegeerd alsof deze verplichting niet zou bestaan. Feit is dat slechts 5% van de organisaties in Nederland bij de verwerking van persoonsgegevens niet in strijd met de WBP handelt[182] en dat privacyinbreuken op grote schaal plaatsvinden. Toegegeven, in de rechtstheoretische besprekingen van artikel 17 van de Richtlijn 95/46/EG is aan dit aspect voorbij gegaan en wordt dientengevolge bij het ontwerp van systemen vooraf nauwelijks een privacybedreigings- of -impactanalyse uitgevoerd. Het gebrek aan discussie hierover heeft er toe geleid, dat er (nog) geen algemeen aanvaarde methode is ontwikkeld om privacybedreigingen en -risico's te evalueren. In dit hoofdstuk zijn de meest bekende privacybedreigings- en -risicoanalyses besproken. De pentagonale aanpak om privacybedreigingen in kaart te brengen en de privacybedreigingsontologische methode van Little & Rogava verdienen de voorkeur.

Beide methoden voldoen aan de door Olle e.a.[183] geformuleerde criteria:
- De methode bevat een aantal opeenvolgende stappen.
- Het resultaat van ieder van deze stappen dient een specifiek doel en brengt goed onderbouwde resultaten voort.
- Het resultaat van iedere stap kan door onafhankelijke onderzoekers worden gevalideerd.
- Het aantal bronnen binnen iedere stap is beperkt.
- De expertise die noodzakelijk is om ieder stap te nemen, is homogeen en vereist een beperkt aantal verschillende deskundigen.
- De sequentie kan worden herhaald vanaf elk tussenliggend resultaat om het totale resultaat te verbeteren en te verfijnen.

Vanuit de behoefte om een consistente en veelomvattende privacybedreigingsanalyse uit te voeren, verdient de ontologische aanpak van de bedreigingen en risico's de voorkeur boven een vanuit de praktijk opgestelde niet-limitatieve opsomming van privacyinbreuken met de daarmee verbonden bedreigingen en risico's. Te meer daar Little & Rogova een nieuwe element aan de bedreigings- en risicoanalyse hebben toegevoegd nl. dat er drie attributen zijn (intention, capability en opportunity) en hun onderlinge relaties, die bepalen of een bedreiging de

182 Koorn, & Ter Hart, 2004, p. 15-22.
183 Olle, Sol & Verrijn-Stuart,1988.

potentie heeft vanuit de 'state of becoming' verwezenlijkt ('the state of being') te worden. Scheiding van deze drie elementen c.q. voorkomen dat er een relatie kan ontstaan tussen deze drie domeinelementen kan de bedreiging voorkomen of uitschakelen. Een probleem bij alle risicoanalyses is de weging van de 'assets' en de waarschijnlijkheid van de aanval. Het is wellicht mogelijk de risicoweging mede te baseren op geleden of mogelijk te lijden schade. Daarvoor staat echter te weinig gedetailleerd feitenmateriaal ter beschikking. Schneier stelt terecht dat: "It is not enough to simply list a bunch of threats, you need to know how much to worry about each of them. This is where risk assessment comes in. The basic idea is to take all the threats, estimate the expected loss per incident and the expected number of incidents per year, and then calculate the annual loss expectancy (ALE)".[184] Daarvoor zijn empirische gegevens over privacyincidenten nodig en die zijn niet voorhanden, omdat privacyincidenten (nog) niet geregistreerd worden. De financiële inschatting van de privacyrisico's komt ter sprake in hoofdstuk 7.

Een andere aanpak is wellicht de privacyrisicoweging niet vanuit een technisch of economisch perspectief te zien, maar vanuit het individu. Theoretische modellen over privacy suggereren dat individuen bij de perceptie van privacyrisico's een interne privacyrisicoberekening ('privacy calculus')[185] gebruiken om de kosten en de baten vast te stellen wanneer zij persoonlijke informatie prijsgeven.[186] Onderzoek van Dinev en Hart[187] wijst in de richting van een kosten-baten-weging wat betreft het geven van persoonlijke informatie bij online transacties. Hoe hoger het niveau is van gepercipieerde internet privacyrisico's, hoe minder men bereid is om persoonlijke informatie te verstrekken ter wille van een internettransactie, en omgekeerd.[188] Vertrouwen beïnvloedt sterk de bereidheid tot het overdragen van persoonsgegevens.[189] Het onderzoek van Dinev wijst er onder meer op dat ervaring met internet transacties de perceptie van privacyrisico's kan veranderen. Bovendien is wereldwijd gebleken dat door culturele verschillen de inschatting van privacyrisico's substantieel kunnen afwijken.[190] Wat betreft het privacybewustzijn van de internetgebruiker is in Noorwegen in 2006-2007 vastgesteld dat er een sterke correlatie bestaat tussen gebruik van beveiligingssoftware en privacybewustzijn. In de groep van gebruikers die privacybeschermende maatregelen nemen gebruikt bijna iedereen (92,1%) antivirussoftware, 72% gebruikt 'firewalls', 66% 'pop-up blockers', en 52% gebruikt 'anti-spy' software.[191] Omgekeerd is het zo dat bij gebrek aan

184 Schneier, 2000, p. 225.
185 Culnan & Bies, 2003, p. 323-342. De privacy calculus is gebaseerd op onderzoek naar de bereidheid om persoonlijke informatie te delen met winkeliers van R.S. Laufer & M.Wolfe 1977.
186 Chellappa & Shivenda, 2008, p. 193-225.
187 Dinev & Hart, 2006, p. 61-80.
188 Dinev & Hart, 2006, p. 33.
189 Dinev & Hart, 2006, p. 73.
190 Dinev, e.a., 2006, p. 389-402.
191 Andreassen, 2007.

bewustzijn er vrijwel geen bescherming op de computer door gebruikers wordt toegepast. Zo bleek in het 2e kwartaal van 2006 bij 90% van alle thuiscomputers (ongewild) 'spyware' software door derden tijdens het internetbezoek te zijn geïnstalleerd.[192]

Geen enkel beveiligings- of privacybedreigingsmodel is perfect. Volgens Camp & Wolfram[193] is het onmogelijk een systeem zo te beveiligen, dat alle bedreigingen worden ondervangen. Een (gestandaardiseerde) privacybedreigingsmethode stelt de ontwerpers van systemen evenwel in staat om de proportionaliteit van de applicatie, het proces of systeem en de organisatorische inbedding van het systeem te toetsen. Bovendien dient ook rekening gehouden te worden met de privacyvoorkeuren van de gebruikers, de te ondervangen potentiële risico's, het passend maken van de toe te passen technologische oplossingen,[194] de in te bouwen controle en terugkoppelingsmechanismen en de middelen om de dataverwerking te herstellen en verloren gegevens terug te vinden. Voorwaarde is natuurlijk wel dat de bedreigingen niet verkeerd worden ingeschat. Schneier merkt op over "getting the threat wrong" dat de Amerikaanse militaire communicatiesystemen tot voor kort primair beveiligd werden tegen "(…) eavesdrop (…) but completely missed the hacker threat. Hackers aren't interested in eavesdropping (…) they want to poke at systems for fun and see how they fall over. They want to brag to their friend and maybe get their names in the newspaper."[195]

De in het PET-Web project op basis van Little & Rogova ontwikkelde 'privacy threat impact analysis' is alleen in de casestudy 'Min Side' getest.[196] Of deze privacybedreigingsanalyse toepasbaar is op andere informatiesystemen kan alleen worden vastgesteld door deze methode vele malen empirisch te toetsen en het model op grond van de resultaten te kalibreren. De Noorse overheid heeft haar goedkeuring en subsidie voor een opvolgend researchproject in juni 2009 verleend om onder andere dit aspect verder te testen. In 2013 worden de resultaten verwacht. Om identificatie te voorkomen en waarborgen tegen onrechtmatige verwerking van persoonsgegevens te scheppen, worden versleuteling en logische toegangsbeveiliging toegepast. Binnen logische toegangsbeveiliging zijn met name het goede beheer van uniek identificerende persoonsgegevens en bijbehorende autorisatiegegevens van belang. Bovendien blijkt het automatiseren van privacymaatregelen veelal effectiever en efficiënter te zijn, dan het louter steunen op organisatorische procedures en handmatige activiteiten.[197]

---

192 Skomedahl, 2008, p. 4-9.
193 Camp & Wolfram, 2000, p. 31-39.
194 Iachello & Abowd, 2005, p. 91-100.
195 Schneier, 2000, p. 227.
196 http:// ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3639.
197 Koorn, e.a., 2004, p. 5-8.

Voor het risicoklassensysteem van de Registratiekamer biedt in de risicoklassen II (verhoogd risico) en III (hoog risico) het gebruik van Privacy Enhancing Technologies de beste mogelijkheden tot een optimale bescherming van persoonsgegevens. De Minister van Justitie antwoordde tijdens de schriftelijke behandeling van de Wet bescherming persoonsgegevens in de Eerste Kamer, dat "(...) gedacht kan worden aan gedeeltelijke of algehele anonimisering, bijvoorbeeld door persoonsgegevens te ontdoen van identificerende kenmerken of door deze af te schermen voor bepaalde toepassingen of gebruikers of om 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 toepassing van Privacy Enhancing Technologies (PET). Dit soort regels sluiten aan bij de zich ontwikkelende informatietechnologie".[198]

Om de belangrijkste risico's af te dekken toonde de PISA-privacybedreigingsanalyse aan, dat de mobiele software agent zowel gedurende de communicatie tussen gebruiker ('master') en agent en tussen agenten onderling de opslag van persoonsgegevens in de agent volledig afgeschermd dient te zijn. Bovendien mogen (gedeelten van) persoonsgegevens niet dupliceerbaar zijn, voor het geval de agent wordt onderschept. De technische oplossing om bedreigingen het hoofd te kunnen bieden en met name om de identiteit van 'master' en de persoonsgegevens die de mobiele agent op het internet met zich meeneemt, af te schermen, ligt in de toepassing van geavanceerde PET-maatregelen.[199]

De researchers van het PET-Web project kwamen na de privacybedreigingsanalyse van 'Min Side' tot de conclusie, dat het noodzakelijk was om PET-maatregelen in de architectuur in te bouwen. Het betreft onder meer de scheiding van identiteitsdomeinen (waarover meer in hoofdstuk 5), omdat het anders niet mogelijk bleek de identiteit van de burger in 'Min Side' en zijn persoonsgegevens afdoende te beschermen.[200]

De beantwoording van de derde onderzoeksvraag '*Met welke privacybedreigingen en –risico's moeten de burger en de ontwerper van systemen rekening houden?'* heeft een aantal methoden voor het bepalen van de privacybedreigingen en privacyrisico's opgeleverd. De pentagonale risicoanalyse in paragraaf 4.9 heeft geresulteerd in een lijst van generieke bedreigingen, die rechtstreeks uit de Richtlijn 95/46/EG kunnen worden afgeleid. Bovendien is in de paragrafen 4.11 tot en met 4.13 vastgesteld dat de bedreigingsontologie ontwikkeld door Little & Rogova tot een volledigere vaststelling van privacybedreigingen en

198 Tweede Kamerstuk 1999-2000, 25 892, nr. 92c.
199 Catrysse, Van der Lubbe & Youssof, 2002, p. 16-32.
200 Abie, 2007, p. 15.

-risico's zou kunnen leiden door rekening te houden met intentie of motivatie, middel of bekwaamheid en gelegenheid van de bedreiger en hun onderlinge relaties.

Uit de hiervoor besproken privacyrisico- c.q. bedreigingsanalyses, zowel van de Registratiekamer (classificatie van risicoklassen), als in het EU PISA-research-project en Noorse PET-web project komt als dominante bevinding naar voren dat de bedreigingen met name liggen op het gebied van ongewilde identificatie en onrechtmatige verwerking van persoonsgegevens. Volgens Ponemon zijn in de Verenigde Staten de meest gebruikte technische beveiligingsmiddelen om dit te bestrijden: "Encryption, Identity and Access Management, Endpoint security controls, Security event management, Perimeter controls".[201]

In hoofdstuk 5 zal vierde onderzoeksvraag (OV 4): '*Wat houdt het concept Privacy Enhancing Technologies (PET) in?'* worden behandeld. Tevens komt het theoretisch gedeelte van de onderzoeksvraag 5 (OV 5): '*Is het mogelijk privacy-veilige architecturen en systemen te ontwerpen en te bouwen?*' aan de orde.

De beantwoording van beide onderzoeksvragen zal zich richten op het aantonen dat PET-maatregelen de identiteits- en andere persoonsgegevens effectief kan loskoppelen van de bron en dat alleen met bepaalde PET-hulpmiddelen de koppeling tussen de identificerende gegevens en de overige persoonsgegevens kan worden gemaakt.

201 Ponemon, 2007.

5. Privacy enhancing technologies voor privacyveilige systemen

"***L'essentiel est invisible pour les yeux.***"
A. de Saint-Exupery, Le Petit Prince, Paris 2007, p. 92

Dit hoofdstuk richt zich op de vierde en het theoretisch gedeelte van de vijfde onderzoeksvraag (OV 4):

'*Wat houdt het concept Privacy Enhancing Technologies (PET) in?*' respectievelijk (OV 5) '*Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen?'*

In paragraaf 5.1 wijs ik op de technologische consequenties van de privacywetgeving. Paragraaf 5.2 behandelt het theorema van Chaum, dat de basis vormt voor privacy enhancing technologies (PET). In paragraaf 5.3 worden drie mogelijkheden gegeven om privacyveilige systemen te ontwerpen. In paragrafen 5.4 en 5.5 worden de voorwaarden voor informatiesystemen geanalyseerd, waarbinnen geen persoonsgegevens worden verwerkt. In paragraaf 5.6 wordt de noodzaak van identiteit in het informatiesysteem aan de orde gesteld en geconcludeerd dat het mogelijk is om volledig functionele privacyveilige informatiesystemen te bouwen zonder dat de identiteit van de gebruiker voor alle interne processen binnen het systeem nodig is, waardoor identificerende gegevens niet behoeven te worden verwerkt. In de paragrafen 5.7 tot en met 5.13 wordt beschreven wat onder 'privacy enhancing technologies' (PET) moet worden verstaan. In deze paragrafen is de definitie van PET opgenomen, alsmede de functionaliteiten van PET. In paragraaf 5.8 komt de hoeksteen van PET, de identityprotector met zijn functionaliteiten aan de orde en de manier waarop deze is te implementeren. In paragraaf 5.9 volgt hoe fraude door het gebruik van de identity protector kan worden bestreden. De consequentie van PET en het daarmee verbonden gebruik van een identiteitsbeschermer (IDP) is, dat elke keer wanneer een gebruiker in een privacyveilig informatiesysteem inlogt er een nieuwe IDP moet worden aangemaakt.

In paragraaf 5.10 wordt betoogd dat het beheer van identiteiten, het Identity Management (IM)[1] een onontkoombare en belangrijke ontwikkeling naast PET is.

---

1 Baladi, e.a., 2006: "Identity and Access Management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources".

In paragraaf 5.11 worden de bouwstenen voor privacy en identiteitsbeheer onder de loep genomen, zoals transparant privacybeleid; kleefbeleid of 'sticky policies'; en de mogelijkheid om de verspreiding van eigen persoonsgegevens door middel van 'data track' te kunnen volgen. In paragraaf 5.12 volgt het privacymanagementsysteem dat ingezet kan worden bij het verwerken van identiteitsrijke niet-vercijferde gegevens een en ander strikt binnen de wettelijke voorschriften. Om privacywetgeving in systemen in te bouwen zijn privacyontologieën nodig. Deze komen in paragraaf 5.12.4 aan de orde. In paragraaf 5.12.5 volgt de 'vertaling' van rechtsregels ('legal instantiation') door middel van 'privacy knowledge engineering'. Als voorbeeld wordt het privacyrealisatiebeginsel transparantie uitgewerkt. Een dergelijke bewerking is tijdrovend en vereist intensief overleg tussen de privacyjurist en de systeemontwerper. Vandaar dat gepoogd is om de productie van privacyontologieën te automatiseren. In paragraaf 5.12.6 wordt dit proces beschreven. Een belangrijk element in de architectuur is de overdracht van persoonsgegevens aan derde systemen. Daarvoor zijn de in paragraaf 5.13 beschreven overdrachtsregels nodig. Hierbij is weer het beginsel van transparantie als voorbeeld genomen. Paragraaf 5.14 sluit het hoofdstuk af met de samenvattende beantwoording van onderzoeksvraag 4 en de voorlopige beantwoording van onderzoeksvraag 5.

5.1. De technologische consequenties van de privacywetgeving

De implementatie van de (e)privacyrichtlijnen 95/46/EG en 2002/58/EG[2] in de wetgeving van de EU lidstaten heeft gevolgen voor de geautomatiseerde verwerking[3] van persoonsgegevens voor alle organisaties. Gezien de privacyrealisatiebeginselen (zie hoofdstuk 2) moet er meer gebeuren dan het nemen van de gebruikelijke organisatorische en technische beveiligingsmaatregelen. Artikel 11 en 13 Wbp richten zich specifiek tot de verantwoordelijken voor persoonsgegevens, de bewerkers en de systeemontwikkelaars en de manier waarop de persoonsgegevens moeten worden verwerkt. Canon stelt terecht dat "regulations are changing the way companies do business".[4] De verantwoordelijken[5] in de zin van de wet moeten ervoor zorg dragen, dat overeenkomstig de wettelijke voorschriften de bescherming van de persoonsgegevens op de geëigende manier wordt uitgevoerd.[6] De uitvoering van deze wettelijke verplichtingen vereist een doelgerichte aanpak.[7]. Tevens dient de verantwoordelijke, zoals in hoofdstuk 4 is

2 Zo vereist bijvoorbeeld 2002/58/EG artikel 14.3 dat elke apparaat en dienst zo moet zijn gemaakt/ingericht dat gebruikers hun privacy kunnen beschermen en controle daarover kunnen uitoefenen.
3 Deze voorschriften betreffen ook de handmatige verwerking.
4 Canon, 2005, p. 42.
5 Artikel 1 onder d WBP verstaat onder verantwoordelijke als 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.
6 Borking, 2001, p. 607-615.
7 Wijkstra, 1998, p. 6-11.

uiteengezet, rekening te houden met de resultaten van de privacyrisico- en bedreigingsanalyse,[8] en de privacyvoorkeuren van de gebruikers.[9] Privacymanagement behoort een geïntegreerd onderdeel te zijn van de bedrijfsprocessen van organisaties die persoonsgegevens verwerken.[10]

Dat betekent niet dat de wettelijke eisen een onevenredige verzwaring voor de verwerking van persoonsgegevens met zich meebrengt. Vele van de te nemen verwerkingsmaatregelen en -procedures moeten, ongeacht of er persoonsgegevens verwerkt worden, ter bewaking van de bedrijfsprocessen genomen worden. De voorzieningen dienen evenwel in samenhang met de specifieke beschermingsmaatregelen die voor de verwerking van persoonsgegevens noodzakelijk zijn, gerealiseerd te worden. Zij dienen derhalve geïntegreerd te worden in de vereiste verwerkings- en beveiligingsmaatregelen. Wil men binnen een organisatie tot een evenwichtig verwerkingsbeleid voor persoonsgegevens komen en dit adequaat implementeren en onderhouden, dan zal het beleid dat gericht is op privacybescherming niet alleen moeten streven naar totale kwaliteit,[11] maar zal ook een belangrijke plaats in de management cyclus[12] moeten innemen.[13] Het eerste en tweede lid van artikel 17 van de Richtlijn 95/46/EC luiden:

> "1 Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
>
> 2 The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures".

---

8 Het niet uitvoeren van een privacybedreigingsanalyse of een PIA kan beschouwd worden als een handelen in strijd met de wet. Willens en wetens geen gebruik maken van het resultaat is verwijtbaar zoals in het Tweede Vogelpestarrest (HR 20 februari 1976 NJ 1976/486) is vastgesteld.

9 Iachello & Abowd, 2005, p. 91-100.

10 De Rooij, 2003, p. 206.

11 Bij bedrijven (bijvoorbeeld Philips) waar '*sustainability*' onderdeel is van de ondernemingsvisie zal maatschappelijk verantwoord ondernemen een extra drijfveer hiervoor zijn.

12 Voor de beheersing van (ict-beheer)processen wordt vaak gebruik gemaakt van een managementcyclus die ook wel bekend is als de kwaliteitscirkel van Deming. Kenmerkend voor ITIL (Information Technology Infrastructure Library), en elke andere procesgerichte methode, is dat een dergelijke managementcyclus continu moet worden doorlopen. Zie www.kennisportal.com/main.asp?ChapterID=1481.

13 Leerentveld & Van Blarkom, 2000, p. 12.

Deze bepaling is in de Wet bescherming persoonsgegevens (Wbp)[14] getransponeerd als artikel 13. Bij de schriftelijke behandeling van de Wet bescherming persoonsgegevens in de Eerste Kamer antwoordde de Minister van Justitie:[15]

> "(...) 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 deze af te schermen voor bepaalde toepassingen of gebruikers of om het gebruik tot bepaalde doeleinden te beperken.[16] 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 Technologies (PET). Dit soort regels sluiten aan bij de zich ontwikkelende informatietechnologie."[17]

Welke technologische maatregelen moeten worden geïmplementeerd om aan het bovenstaande te kunnen voldoen, vergt een zorgvuldige afweging. De voortdurende groei in de capaciteit van en het aantal onderlinge verbindingen tussen computernetwerken leidt binnen organisaties wereldwijd tot een exponentiële toename in het verzamelen, verwerken en uitwisselen van informatie. Steeds meer persoonsgegevens worden vastgelegd via publieke ict-netwerken en internet, in onderling verbonden databanken waarvan door allerlei organisaties voor uiteenlopende doelen gebruik wordt gemaakt. Deze ontwikkeling noopt tot een voortdurende aandacht voor de beveiliging van geautomatiseerde informatiesystemen en het terugdringen van identificerende gegevens om persoonsgegevens zo goed mogelijk te beschermen. Interviews die in het kader van deze dissertatie met het management van de verantwoordelijken zijn gehouden, tonen aan dat informatie-intensieve bedrijven de controle op de verwerking van de gegevens aan het kwijt raken zijn.[18] Kelly signaleert dit verschijnsel op een veel grotere schaal.[19] De EPTA (European Parliamentary Technology Assessment Organization)[20] wijst er in zijn studie over ict en privacy op, dat nieuwe technologieën krachtige middelen kunnen verschaffen om persoonsgegevens te beschermen. Er is evenwel geen aanwijzing dat privacybedreigende en privacyversterkende mogelijkheden automatisch elkaar in evenwicht houden. Het lijkt er eerder op dat zonder gericht

---

14 Wet van 6 juli 2000, Stb. 2000, 302 houdende regels inzake de bescherming van persoonsgegevens.
15 Tweede Kamerstuk vergaderjaar 1999-2000, 25 892, nr. 92c. p. 16.
16 De Minister van Justitie ziet over het hoofd dat naast anonimisering ook versleuteling of loskoppeling tot de mogelijkheden horen (zie in dit hoofdstuk paragraaf 5.2 en in het bijzonder paragraaf 5.3).
17 Borking, 2001, p. 608-609. Het is vooralsnog niet nodig bestaande wetgeving voor de invoering en het gebruik van PET aan te passen, maar het zou de discussie vergemakkelijken als de Europese Commissie een standaard zou publiceren met vereiste PET functionaliteiten. Zie Klaver, e.a 2002, p. 104.
18 Hierover wordt gerapporteerd in Hoofdstuk 7.
19 Kelly, 1994.
20 Leden van EPTA zijn de Europese organisaties, die Technology assessment studies uitvoeren voor en in opdracht van parlementen. De EPTA is gevestigd te Geneve.

beleid en maatregelen er veel meer applicaties op de markt komen die de persoonlijke levenssfeer binnendringen, dan dat er privacybeschermende toepassingen voor handen zijn.[21]

5.2. Het theorema van Chaum

Chaum heeft in verschillende publicaties[22] in het midden van de tachtiger jaren van de vorige eeuw aangetoond dat met behulp van wiskundige benaderingen om gegevens te vercijferen,[23] het mogelijk is de echtheid en de vertrouwelijkheid van de communicatie tussen mensen te garanderen binnen een wereld waar elke transmissie naar zijn oorsprong kan worden getraceerd. Aan de hand van zijn theorema[24] bewees Chaum, dat of nu de versleuteling met een eenmaal te gebruiken sleutel of met publieke sleutels wordt uitgevoerd de communicatie langs cryptografische[25] weg veilig gemaakt kan worden.[26] Chaum stelde dat:

> "(…) those having only the public information and a set of keys seeing some anonymity set can learn nothing about the members of that anonymity set except the overall parity of their inversions".[27]

Hij realiseerde zich dat om ontdekking van de communicatie te voorkomen het in de praktijk bij het verzenden van informatie over netwerken noodzakelijk is, afhankelijk van de te verzenden boodschap, de juiste sleutellengte toe te passen.

Chaum had al eerder gedemonstreerd als voorloper op zijn algemene bewijs dat in een 'mix-net' door middel van 'mix-nodes' in openbare telecommunicatie en andere netwerken, gegevens in 'transit' tussen afzender en ontvanger kunnen worden beschermd.[28] Door een reeks nodes te installeren en bepaalde encryptie/decryptietechnieken te gebruiken, is het mogelijk om gegevens in transit te wijzigen en te hergroeperen zodat het voor een onbevoegde partij vrijwel onmogelijk is te bepalen of een bericht wordt verzonden of wordt ontvangen, en met die vaststelling de data in het netwerk te analyseren.[29] Een mix-node is een processor die als input een bepaald aantal berichten ontvangt en in een willekeurige volgorde weer verzendt.[30]

---

21 Klüver, Peissl & Tennøe, 2006, p. 16.
22 Chaum, 1988, p.65-75. Zie ook Waidner, 1990, p. 302-319.
23 Van der Lubbe, 1994.
24 Chaum, 1988, p. 69: Het theorema luidt: "*Let* a *be in GF(2)n. For each* i *in GF(2)n, which is assumed by* I *with nonzero probability and which has the same parity as* a, *the conditional probability that* A = a *given that* I = i *is 21-m. Hence, the conditional probability that* I = i *given that* A = a *is the* a priori *probability that* I = i."
25 Kleve, 2004, p. 86-92 voor een verhandeling over single pad en asymmetrische encryptie.
26 Chaum, 1988, p. 68-69.
27 Chaum, 1988, p. 67.
28 Chaum, 1981, p. 84-88.
29 Pfitzmann & Hansen, 2008, p. 19:"DC-net (Chaum) are mechanisms to achieve sender anonymity and relationship anonymity, respectively, both against strong attackers. If we add dummy traffic, both provide for the corresponding unobservability".
30 Berthold, Pfitzman & Standtke, 2000, p. 27-42; Berthold, Federrath & Kopsell, 2000, p. 101-115.

Kritiek op Chaum en andere cryptografen kwam van Anderson die stelde, dat:

> "Designers of cryptographic systems are at a disadvantage to most other engineers, in that information on how their systems fail is hard to get: their major users have traditionally been government agencies, which are very secretive about their mistakes. (…) the results of a survey of the failure modes of retail banking systems, which constitute the next largest application of cryptology (…) turns out that the threat model commonly used by cryptosystem designers was wrong: most frauds were not caused by cryptanalysis or other technical attacks, but by implementation errors and management failures".[31]

Waidner[32] heeft Chaum's theorema nauwkeurig onderzocht en komt tot de conclusie dat Chaum's bewijs dat de niet-traceerbaarheid van de zender en de ontvanger van boodschappen volkomen ('unconditional') juist is. Maar, aldus Waidner, Chaum nam ten onrechte aan dat er sprake was van een "reliable broadcast network, i.e. each message broadcast by an honest participant is received by each other participant without being changed" en dat zo'n netwerk niet door middel van cryptografische middelen kan worden afgedwongen. Een serie tegenmaatregelen die als 'fail-stop broadcast schemes'[33] (gebaseerd op 'Byzantine Agreement Protocol')[34] worden aangeduid, kunnen als aanvulling op Chaum's bewijs ook bij oneerlijke participanten (aanvallers) de 'unconditional traceability' realiseren.[35] Bovendien stellen Pfitzmann & Hansen dat 'dummy traffic' tot 'unobservability' kan leiden,[36] mits er tussen de 'nodes' van het netwerk 'dummy traffic' wordt verzonden ook als op dat moment geen informatie voor verzending wordt aangeboden. Een verdere verfijning op het bovenstaande waarbij de zender en ontvanger van een bericht gezamenlijk kunnen aantonen dat er sprake is van een vervalst bericht, is door Ismail & Hasan aangetoond.[37]

Chaum toonde in 1992 aan, dat de privacy van burgers ernstig gevaar loopt, wanneer bij het verzamelen en verwerken van persoonsgegevens door verschillende organisaties eenzelfde identificerende nummer, (bijvoorbeeld het burgerservicenummer), wordt gebruikt. Bij gebruik van zijn cryptografische uitvinding, bekend als de blinde digitale handtekening en het daarop gebaseerde 'Digital

---

31 Anderson, 2003, p. 215- 227.
32 Pfitzman & Waidner, 1986, p. 245; zij hadden in 1986 het theorema van Chaum onderzocht met betrekking tot boodschappen via het zich ontwikkelende internet en mobiele telefonie.
33 Pfitzmann & Hansen, 2008, p.19: " Broadcast is a mechanism to achieve recipient anonymity against strong attackers. If we add dummy traffic, both provide for recipient unobservability."
34 Lamport, Shostak & Pease, 1982, p. 382-401.
35 Waidner, 1990, p. 302-319. http://64.233.183.104/search?q=cache:QQzPncvUcZIJ:www.semper.org/sirene/publ/Waid_90fail-stopDC.
36 Pfitzmann & Hansen, Dresden 2008, p.19: "A mechanism to achieve some kind of anonymity appropriately combined with dummy traffic yields the corresponding kind of unobservability. Of course, dummy traffic alone can be used to make the number and/or length of sent messages undetectable by everybody except for the recipients; respectively, dummy traffic can be used to make the number and/or length of received messages undetectable by everybody except for the senders".
37 Ismail & Hasan, 2007, p. 9-21.

Cash'[38] (DC) netwerksysteem, kan de persoonlijke informatie worden beschermd, wanneer door de verwerkende organisatie aan de gebruiker/consument bij iedere transactie een verschillend (maar verifieerbaar) digitaal pseudoniem wordt gegeven. Tegelijkertijd kan hiermee de mogelijkheid van fraude door het zelfde individu worden voorkomen.[39] Voor alle duidelijkheid: een pseudoniem is een vaststeller van de identiteit ('identifier') van een subject anders dan aan de hand van een van de echte namen van het subject.[40]

Chaum bewees voorts aan de hand van verschillende situaties dat bij gebruik van de DC-netwerkoplossing door middel van een blinde digitale handtekening het tevens mogelijk was frauduleuze transacties te voorkomen zonder dat daarvoor de identiteit van een persoon bekendgemaakt hoefde te worden.[41]

5.3. Conceptuele modellen voor bescherming van persoonsgegevens

De door de Registratiekamer in 1994 uitgevoerde omgevingsanalyse (SWOT)[42] leverde als belangrijkste bevinding op, dat de technologische ontwikkeling met name van de informatie- en communicatietechnologie (ict) en de daarmee gepaard gaande informatisering, van grote invloed was (en is) voor het voortbestaan van een handhaafbare privacybescherming. De SWOT maakte duidelijk dat het beleid van de Registratiekamer gebaseerd op klachtenbehandeling ten gevolge van privacyincidenten, voor het preventief beschermen van de persoonlijke levenssfeer niet erg effectief is en dat er een structurele oplossing moest worden gevonden in plaats van ex post de Wet persoonsregistraties bij klachten toe te passen.[43] Onderzoek van de Registratiekamer in 1994 wees uit,[44] dat wanneer organisaties wordt gevraagd welke maatregelen zij hebben getroffen om de privacy te beschermen, zij erop wijzen dat zij zich hebben ingespannen om de persoonsgegevens te beveiligen, net zoals zij dat met andere gegevens in het kader van informatiebeveiliging doen. Hoewel het gebruik van beveiligingsmaatregelen om ongeautoriseerde toegang tot persoonsgegevens te voorkomen een belangrijke component van privacybescherming is, houdt een dergelijke beveiliging niet hetzelfde in als privacybescherming.[45] Immers bij informatiebeveiliging wordt geen rekening gehouden met de noodzaak of de rechtmatigheid van de verwerking van persoonsgegevens.

---

38 Met Digital Cash (Digicash) was het mogelijk om digitaal geld uit te geven zonder dat de ontvanger wist van wie het afkomstig was. De bank kon ook niet traceren van wie het geld afkomstig was en waar het was uitgeven. Wel was het mogelijk bij frauduleus handelen de identiteit van de gebruiker te achterhalen.

39 Chaum, 1992, p. 96-101: "Achieving electronic privacy, a cryptography invention known as a blind signature permits numbers to serve as electronic cash or to replace conventional identification."

40 Pfitzmann & Hansen, 2008, p. 20.

41 Klaver, e.a., 2002 p. 37.

42 Borking & Vriedhoff, 1995, p. 22-34. SWOT staat voor: Strenght, Weakness, Opportunity, Threat.

43 Wet van 28 december 1988, Stb. 665.

44 Borking, e.a. 1994, Het onderzoek vond plaats in het kader van deze publicatie.

45 H. van Rossum, e.a. 1995, p. 2, 17.

Als gevolg van het resultaat van de SWOT maakte de Registratiekamer de strategische keuze om in plaats van reactief op de omgeving te reageren proactief oplossingen voor privacyproblemen aan te bieden.[46] Dit leidde in 1994 tot het 'technology assessment' onderzoek om na te gaan welke mogelijkheden de aanpak van Chaum en Bellotti & Sellen[47] bood om het gebruik van identificerende gegevens binnen informatiesystemen terug te dringen, de verwerking van persoonsgegevens binnen het wettelijk kader te bevorderen en de burger meer zeggenschap en vertrouwen te geven over de verwerking van zijn persoonsgegevens. In het 'technology assement' onderzoek van de Registratiekamer werd ook de vraag onderzocht of informatiesystemen, waarbij de identiteit van de consument voortdurend wordt gebruikt, ook als het niet noodzakelijk is, zo zou kunnen worden geconstrueerd dat het gebruik van persoonsgegevens (de kern van de informationele privacybescherming) geheel of gedeeltelijk zou kunnen worden geëlimineerd, zonder de functionaliteit van informatiesystemen te verminderen. Met andere woorden: hoe kan de ict-technologie er toe bijdragen dat de persoonlijke levenssfeer juist beter gewaarborgd wordt, waardoor de schadelijke invloeden van technologische ontwikkelingen door aanvullende technologische maatregelen worden gecorrigeerd?[48]

Zouden er privacyveilige informatiesystemen kunnen worden ontwikkeld met ingebouwde privacybescherming, waarbij alleen in het geval van bedrog de identiteit van de gebruiker/consument bekend dient te worden gemaakt? De Registratiekamer realiseerde zich in 1994 dat het kunnen openbreken van het privacyveilige informatiesysteem, wanneer een misdrijf met het systeem was gepleegd, een belangrijke voorwaarde zou zijn om privacyveilige systemen maatschappij breed geaccepteerd te krijgen. Als bij de verwerking persoonsgegevens geëlimineerd of aanmerkelijk verminderd zouden kunnen worden, zou dat naast de verbeterde privacybescherming ook een aanzienlijk betere bescherming tegen de in hoofdstuk 4 besproken bedreigingen en risico's kunnen opleveren.[49] Bovendien als de te verwerken gegevens van direct of indirect geïdentificeerde of identificeerbare natuurlijke personen volledig en onomkeerbaar worden geanonimiseerd, dan is er geen sprake meer van persoonsgegevens en vallen de aldus geanonimiseerde gegevens buiten de wettelijke bepalingen betreffende de bescherming van persoonsgegevens.[50]

---

46 Borking & Friedhoff, 1995, p. 12 -15, 32; Kohnstamm, 2009, p. 5: inmiddels verdedigt in 2009 de voorzitter van het CBP Kohnstam het omgekeerde: "DPAs need to be selective in order to be effective: thus shift focus from ex ante to ex post."

47 Bellotti & Sellen, 1993, p. 51: "ict-systems should be open and transparent to data subject; the system should be comprehensible; feedback be provided at a time when control is most likely to be required and effective; feedback should be noticeable, not distract or annoy and not involve information that compromises the privacy of others; the system should warn users when omitting to take the required action to protect their privacy and should have flexibility in order to be adjustable to the privacy level as required by the user due to the context and interpersonal relationships."

48 Borking, 2002, p. 196-202.

49 Watts & Macaulay, 2000, p. 11: "Hes & Borking have looked at PETs in the context of EU DP legislation, with a view to engineering a complete solution that respect both the efficiency and effectiveness of an information system and the conditions for processing of the data."

50 Arendzen, e.a., 2007, p. 278.

Er zijn zes technisch realiseerbare mogelijkheden die zouden kunnen leiden tot een privacyveilig informatiesysteem.

1. De eerste mogelijkheid is het niet opvragen, niet genereren en niet vastleggen van welke gegevens in welke vorm dan ook.[51] Het ontbreken van identificerende gegevens maakt het niet of vrijwel niet mogelijk om de resterende gegevens te relateren aan een natuurlijk persoon. Deze oplossing is alleen mogelijk indien voor de doeleinden van de dienstverlening het verwerken van persoonsgegevens niet noodzakelijk is.[52]
2. De tweede mogelijkheid is het anonimiseren dat op verschillende manieren kan geschieden, zodat of de situatie van anonimiteit[53] blijft gehandhaafd of ontstaat. Voor anonimiteit wordt in dit kader definitie van Pfitzmann & Hansen[54] gebruikt: "Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set."[55] Eén en ander hangt natuurlijk wel af van de grootte van de verzameling.
3. Als de persoonsgegevens tijdelijk nodig zijn, dan worden de gegevens in eerste instantie verwerkt en daarna zo snel mogelijk vernietigd of door middel van cryptografische technieken losgekoppeld van de overige gegevens. Het vernietigen en/of loskoppelen van data moet wel onomkeerbaar gebeuren.[56] Zouden de persoonsgegevens en overige gegevens weer gekoppeld kunnen worden dan is er geen volledige anonimiteit bereikt.
4. Een andere mogelijkheid is de scheiding van gegevens waarbij persoonsgegevens wel worden verwerkt, maar de identificerende persoonsgegevens direct worden losgekoppeld van de overige persoonsgegevens.
5. Om de privacy te beschermen kan binnen het informatiesysteem bij verwerking van persoonsgegevens ook automatisch de wetgeving betreffende de bescherming van persoonsgegevens en het privacybeleid van de verantwoordelijke (zie paragraaf 2.7) worden toegepast. De verwerking moet dan zo geschieden, dat verwerking in strijd met de wettelijke verplichtingen of de 'privacy policy' leidt tot het af- of onderbreken van de verwerking.[57] Deze laatste mogelijkheid is met name van belang voor informatieprocessen binnen de overheidsinstanties, banken en verzekeringsbedrijven die over het

51 Burkert, 2001, p. 128 "the first question to be asked in PET design is whether personal information is needed at all".
52 Koorn, e.a., 2004, p. 38.
53 Prins, 2000, p. 153-157. Prins stelt in dit artikel op pagina 153: "Een recht op regie over de persoonsgegevens (*zie de nota van Min. BiZa 2000:"Contract met de toekomst"* – cursief: toevoeging Borking) komt in de buurt van een recht op anonimiteit. Immers, uitgangspunt bij een recht op regie is anonimiteit en niet kenbaarheid".
54 Pfitzmann & Hansen, 2008, p. 8.
55 Deze definitie is afgeleid uit de standard ISO 15408 (1999): "Anonymity ensures that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity. Anonymity is not intended to protect the subject identity. [...] Anonymity requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation". De definitie van Pfitzman en Hansen is ruimer dan definitie van anonimiteit in ISO 15408 omdat, deze definitie is niet beperkt is tot het identificeren van gebruikers, maar alle subjecten bevat.
56 Een voorbeeld hiervan is de Nederlandse meta-zoekmachine Ixquick (www.ixquick.com) (zie hoofdstuk 6).
57 De Rooij, 2003, p. 206-212.

algemeen zeer identiteitsrijk zijn en ook op grond van wettelijke bepalingen niet zonder identificerende gegevens kunnen.

6. Er zouden ook als zesde mogelijkheid deelmaatregelen kunnen worden genomen zoals het inbouwen van een beperkte houdbaarheid van elektronische data. Dit zou de verspreiding van persoonlijke informatie via koppelingen van instanties kunnen verminderen.[58]

5.4. Informatiesystemen zonder persoonsgegevens

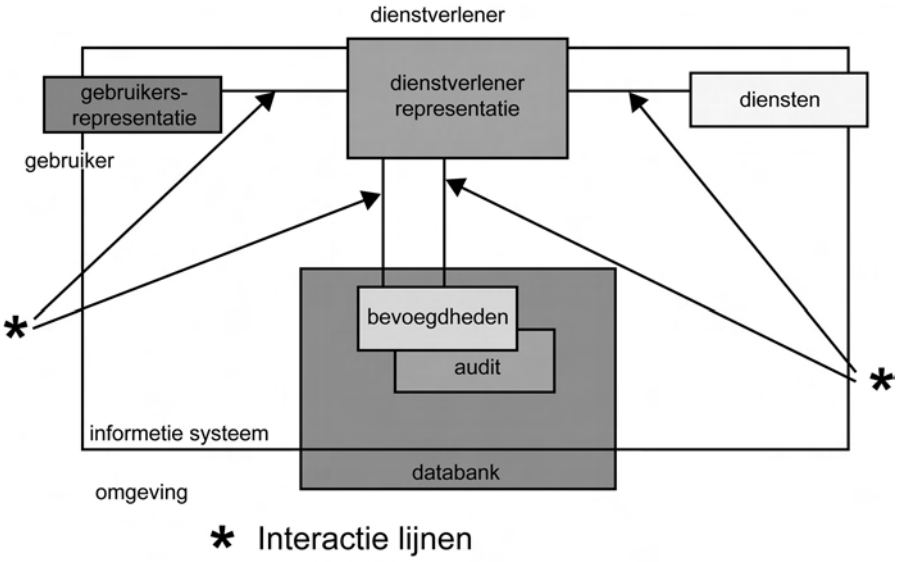
In een informatiesysteem en een communicatiesysteem (zoals VoIP,[59] browser e.d.), kunnen vier elementen[60] worden onderscheiden: organisatie, personeel, procedures en technologie.[61] Alle genoemde componenten zijn van belang voor een juiste werking van een informatiesysteem. In dit onderdeel wordt het accent op de technische inrichting van informatiesystemen gelegd. De wijze waarop aan dit aspect vorm is gegeven bepaalt de mate waarin de privacy van de burger/consument kan worden beschermd.[62] Het hieronder gepresenteerde figuur 5.1 en de daarvan afgeleide figuren is gebaseerd op architectuurmodel met drie lagen, bestaande uit infrastructurele datasystemen, rationele informatiesystemen en sociaal systemen van actoren.[63]

Om te bepalen of de identiteit van een gebruiker ook daadwerkelijk nodig is voor de werking van een informatiesysteem, moet het functioneren van een informatiesysteem worden onderzocht. Vragen die hierbij een rol spelen zijn: bij welke modules en voor welke processen binnen het informatiesysteem is het absoluut noodzakelijk dat de identiteit van de gebruiker aangewend moet worden?[64] Hes en Borking[65] onderscheiden binnen het informatiesysteem een viertal modules, te weten: a de gebruikersrepresentatie; b de dienstverlener representatie; c de databank; en d de te leveren/verleende diensten. Tussen deze modules bestaan interactielijnen. Bovendien is het informatiesysteem gedeeltelijk ingebed in de omgeving van de omringende wereld. Het figuur 5.1 hieronder geeft schematisch deze modules in het informatiesysteem aan.

---

58 Horlings, e.a., 2003, p. 36.
59 Voice over IP of VoIP wordt het Internet of een ander IP-netwerk gebruikt om spraak te transporteren.
60 Een andere indeling is ook mogelijk. Software ontwikkelaars gebruiken een drie deling, namelijk model, viewer, controller, waarbij de dienstverlening buiten de indeling valt. http://java.sun.com/blueprints/patterns/MVC-detailed.html.
61 Bemelmans, Deventer, 2000, p. 65: "Bij het ontwikkelen van een informatiesysteem voor een organisatie zal steeds eerst een analyse van de te besturen organisatie moeten worden gemaakt".
62 Hes & Borking, 2000, p. 16.
63 Dietz & Mulder, 1998; Mulder & Dietz, 2002; Dietz, 2006; Mulder, 2006.
64 Cavoukian, 2007, p. 228: "When accessing the need for identifiable data during the course of transaction the key question one must start with is: how much personal information/data is truly required for the proper functioning of the information system involving this transaction? This question is rarely asked at all since there is such a clear preference in favor of collecting identifiable data, 'the more, the better'".
65 Hes & Borking, 2000, p. 16.

Figuur 5.1: Technisch model van een informatiesysteem.



5.4.1. Gebruikersrepresentatie

De gebruikersrepresentatie[66] is de representatie van de consument, gebruiker of een natuurlijk persoon binnen het informatiesysteem. Een gebruikersrepresentatie zal doorgaans een proces zijn dat op verzoek van de gebruiker bepaalde functies verricht. De gebruikersrepresentatie bestaat veelal uit een technische 'interface'[67] tussen het informatiesysteem en de (eind)gebruiker. Via deze 'interface' kan de consument de gebruikersrepresentatie besturen, bijvoorbeeld een geldautomaat.

5.4.2. Dienstverlenerrepresentatie

De representatie van de aanbieder of dienstverlener[68] is de interne representatie van de organisatie of het bedrijf binnen het informatiesysteem waarvan de gebruiker zijn dienst betrekt, bijvoorbeeld een bank. De representatie van de dienstverlener binnen het informatiesysteem vertegenwoordigt de verantwoordelijke (bijvoorbeeld de eigenaar) van het informatiesysteem. In deze rol behartigt de representatie van de dienstverlener de belangen van de organisatie die zij vertegenwoordigt. Een belangrijke functie van de representatie van de dienstverlener is het controleren

66 Van den Broeck & Desmet 2003.
67 Een interface is een intermediair waarmee twee systemen met elkaar communiceren.
68 Hes & Borking, 2000, p. 17.

van toegang tot de diensten. Een representatie van een dienstverlener kan tevens een verzameling van bedrijven of organisaties vertegenwoordigen.

5.4.3. Diensten

De diensten moeten worden opgevat in de breedste betekenis van het woord. In veel gevallen zullen deze diensten bestaan uit informatie of uit het bewerken van informatie. Voorbeelden van diensten zijn: databanken voor informatievergaring; het lezen en schrijven van documenten op een computernetwerk; communicatiediensten; verrichten van betalingen; uitbetaling van het opgevraagde geld bij een geldautomaat; medische hulpverlening etc. Een dienst kan ook een koppeling zijn met andere (externe) informatiesystemen.

5.4.4. Databank

De database, gegevensbank of databank is een digitaal opgeslagen archief, ingericht met het oog op flexibele raadpleging en gebruik. De databank vormt de interne (elektronische) administratie van het informatiesysteem en bestaat ondermeer uit gegevens die nodig zijn voor het functioneren van het informatiesysteem. De databank is bedoeld voor de opslag van gegevens binnen het informatiesysteem en wordt daarom niet tot de diensten van het informatiesysteem gerekend. De databank bestaat uit tenminste twee bestanden:[69] een bevoegdheden (privileges)bestand en een auditbestand. In het bevoegdhedenbestand zijn de bevoegdheden van de gebruikers (equivalent aan de bevoegdheden van de gebruikersrepresentaties) vastgelegd. De gebruiker zal door middel van de gebruikersrepresentatie (via de module representatie van de dienstverlener die de bevoegdheden controleert in de bevoegdhedenbestand) wel of geen toegang krijgen tot de diverse diensten in het informatiesysteem. In het auditbestand wordt het gebruik van het informatiesysteem vastgelegd. Met het auditbestand kan bijvoorbeeld de gebruiker/consument worden afgerekend voor het gebruik van een informatiesysteem of kan worden nagegaan wie het informatiesysteem heeft gebruikt, wanneer het informatiesysteem is gebruikt en waarvoor het is gebruikt. Voor elke module van het schematische model is het mogelijk dat deze zich gedeeltelijk buiten het (geautomatiseerd) informatiesysteem bevindt. Alle elementen van het informatiesysteem kunnen een interface (‘verbinding’) hebben met de omgeving waarin het informatiesysteem functioneert, zoals weergegeven in figuur 5.1. Een auditbestand kan bijvoorbeeld worden afgedrukt op papier.

69 Overbeek & Sipman, 1999, p. 115-117.

5.4.5. Interactielijnen

Elke lijn die twee modules van het technisch model van het informatiesysteem met elkaar verbindt is een interactielijn.[70] Over een interactielijn kunnen de aanliggende modules een interactie afwikkelen, bijvoorbeeld gegevens uitwisselen. Elke interactielijn kan dan ook een potentiële bedreiging voor de privacy van de gebruiker/consument vormen, omdat over elke lijn de identificerende gegevens van de gebruiker/consument verspreid kunnen worden binnen het informatiesysteem. Een interactie tussen de modules zal veelal deel uitmaken van een proces dat wordt doorlopen bij het gebruik van een informatiesysteem. Om te kunnen bepalen of de identiteit van de gebruiker voor deze processen nodig is moet duidelijkheid worden verschaft over de processen die binnen een informatiesysteem worden uitgevoerd en over de functies die deze processen vervullen.[71]

5.4.6. Omgeving

Het woord 'omgeving' in figuur 5.1 staat voor het feit dat elk informatiesysteem een omgeving heeft, te weten gedeelten van de omringende wereld. Het systeem en de omgeving vormen de ruimte waarin het systeem opereert.[72]

5.5. Processen in het informatiesysteem

Bij het gebruik van informatiesystemen wordt er een aantal processen[73] doorlopen, namelijk:
1. identificatie en authenticatie;
2. autorisatie;
3. toegangscontrole;
4. audit, monitoring, logging;
5. accounting.

De uitwisseling van gegevens wordt weergegeven door interactielijnen die de modules onderling verbinden. De processen kunnen onafhankelijk van elkaar plaatsvinden waarbij een proces gebruik kan maken van de gegevens die voortkomen uit de andere processen.[74]

---

70 Hes & Borking, 2000, p. 18.
71 Hes & Borking, 2000, p. 18.
72 Pfitzmann & Hansen, 2008, p. 7.
73 Een proces is een uitwisseling van informatie tussen twee of meer modules binnen het informatiesysteem, zoals hierboven is aangegeven.
74 Hes & Borking, 2000, p. 18-19.

De processen: identificatie en authenticatie; toegangscontrole en audit spelen zich geheel binnen het informatiesysteem af. De processen autorisatie en accounting hebben een interface met de omgeving.

5.5.1. Identificatie en authenticatie

Identificatie[75] is het kenbaar maken van de identiteit van een subject (een gebruiker of een proces). De identiteit wordt gebruikt om de toegang van het subject tot een object te beheersen. Een object is bijvoorbeeld een computerbestand of een record in een database. Dit proces wordt uitgevoerd wanneer een gebruiker, middels de gebruikersrepresentatie toegang wenst tot het informatiesysteem. In de meeste informatiesystemen maakt de gebruiker zich bekend (identificatie) voor de dienstverlener, waarop de dienstverlener de identiteit van de gebruiker controleert (authenticatie). De gebruiker maakt voor identificatie en authenticatie gebruik van de interface die de gebruikersrepresentatie biedt.

Een veel voorkomende wijze van identificatie is het intoetsen van een zogenaamd gebruikersnaam (user-id), bijvoorbeeld XSHS/536810. De authenticatie geschiedt door de gebruiker een wachtwoord ('password') in te laten toetsen. Het wachtwoord is een code die alleen aan de gebruiker bekend is. Identificatie en authenticatie kan niet alleen geschieden aan de hand van wat de gebruiker weet (het wachtwoord), maar ook op basis van een kenmerk van de persoon (vingerafdruk, stem, iris) of op basis van het bezit van een bankpas tezamen met een persoonlijk identificatie nummer (pin)code[76] en/of met een biometrische scan, waarvan het resultaat vergeleken wordt met de template die in de chip op het bankpasje is aangebracht.[77] Een pseudoniem kan gebruikt worden om de authenticiteit van het individu of het informatiesysteem te verifiëren zonder dat daarvoor diens identiteit moet worden onthuld. Cryptografisch kan bij de toegangscontrole gebruik gemaakt worden van een 'challenge-response sequence', zoals bijvoorbeeld gebeurt bij het elektronisch bankieren.[78] Identificatie en autorisatie zijn nodig om te voorkomen dat ongeautoriseerde personen toegang krijgen tot netwerken en (delen van) bestanden waarin privacygevoelige data worden bewaard.[79] Het belang van een dergelijke bescherming is ondermeer aangetoond in het Noorse researchproject 'Privacy Enhancing technology for Webbased Services', waar als testcase het virtual private network 'Min Side' werd gebruikt.[80] Identificatie en autorisatie zijn van groot belang voor de

75 Overbeek & Sipman, 1999, p. 114, 126.
76 Overbeek & Sipman, 1999, p. 114.
77 Een voorbeeld hiervan is de verificatie van de houder van de Privium kaart van de Schiphol Group bij de paspoort controle. Voor meer informatie: Hes, Hooghiemstra & Borking, 1999, p. 52-54.
78 Overbeek & Sipman, 1999, p. 230, 235.
79 Horlings, e.a., 2003, p. 4-5. Dit rapport is in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties geschreven, maar als intern document niet gepubliceerd.
80 Privacy Enhancing Technology for Webbased Services (PET-Web), "The primary objective is to devise a framework for facilitating the development of the next generation of privacy enhancing technologies in large-scale web-based services", Projectno. 180069/S10, Oslo 2007, waarbij Min side als een casestudy fungeerde.

betrouwbaarheid en integriteit van systemen. Pas na de authenticatie kan de toegang tot het informatiesysteem plaatsvinden. In de tekst van artikel 3:15a eerste lid BW wordt de term 'authentificatie' gebruikt:

"Een elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, indien de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval".

Met authenficatie worden identificatie en authenticatie ten onrechte samengetrokken tot een proces.

5.5.2. Autorisatie van de gebruiker

Autorisatie is het proces waarin een subject (een persoon of een proces, hierna gebruiker) rechten of bevoegdheden krijgt op het benaderen van een object (een bestand, een systeem). Voordat een gebruiker voor de eerste keer gebruik kan maken van een informatiesysteem, bepaalt de dienstverlener c.q. objecteigenaar wat de bevoegdheden zijn van de gebruiker (dat kan de consument of klant zijn).[81] Hij mag bijvoorbeeld een bepaald bestand lezen of een programma starten.[82] De dienstverlener legt de bevoegdheden van de gebruiker vast in een bestand van de databank. De bevoegdheden kunnen worden bepaald op basis van kenmerken en/of eigenschappen van de gebruiker.[83] Als resultaat krijgt de gebruiker de beschikking over een gebruikersrepresentatie in het informatiesysteem. De representatie van de dienstverlener associeert de bevoegdheden van de gebruiker met de interne representatie van de gebruiker, bijvoorbeeld het bij een bank opgeslagen rekeningnummer. Het leidende principe daarbij is 'need-to-know': een persoon mag alleen zien wat die persoon uit hoofde van zijn functie nodig heeft. Het 'need to know'-principe kan uit het bepaalde in de artikelen 8 en 9 van de Wbp[84] worden afgeleid.

5.5.3. Toegangscontrole

Toegangscontrole is een continu proces en één van de belangrijkste middelen voor preventieve beveiliging.[85] Bij elke aangevraagde dienst controleert de representatie van de dienstverlener of de gebruiker via de gebruikersrepresentatie hiertoe gerechtigd is. Zo voorkomt de representatie van de dienstverlener ongeautoriseerd gebruik van diensten of acties die voor het informatiesysteem ongewenst zijn. Overbeek & Sipman wijzen erop, dat toegangscontrole bij databasesystemen op het niveau van velden in de 'records' is ingebouwd en ook plaatsvindt op het

81 Overbeek & Sipman, 1999, p. 115.
82 Ribbers, 2007, p. 26.
83 Versmissen, 2001, p. 31.
84 Artikel 61 lid 5 van de WBP voor de doorbreking van de geheimhoudingsplicht door het CBP.
85 Overbeek Sipman, 1999, p. 115

niveau van computers en netwerken om vast te stellen of deze met elkaar mogen communiceren en met welke applicaties. Bijvoorbeeld e-mail vanaf een computer kan wel worden toegelaten maar interactieve toegang niet.[86]

5.5.4. Audit/Monitoring/Logging

De meeste systemen hebben mogelijkheden om gebeurtenissen in het systeem te registeren en alarm te slaan.[87] Ook hier is sprake van een continu proces. De representatie van de dienstverlener kan gegevens bijhouden van een gebruiker waaraan hij diensten verleent. De representatie van de dienstverlener kan bijvoorbeeld vastleggen van welke diensten gebruik is gemaakt en hoe lang. Deze gegevens, monitoring-, logging- of auditgegevens[88] genaamd, worden opgeslagen in het auditbestand in de database. De dienstverlener bepaalt welke gegevens opgeslagen worden in het auditbestand. Een voorbeeld van auditgegevens zijn de telefoontikken die een telefoonmaatschappij voor het afrekenen vastlegt.

5.5.5. Accounting

Onder deze term vallen verschillende begrippen zoals: afrekening, verantwoording en 'monitoring compliance'. In dit proces worden de acties en handelingen van de gebruiker door de dienstverlener verrekend. Bijvoorbeeld, de consument moet betalen voor het gebruik van een dienst. De dienstverlener verrekent het gebruik op basis van de auditgegevens. 'Accounting' vindt doorgaans na gebruik van de dienst plaats. Echter, accounting kan ook plaatsvinden tijdens gebruik van een dienst. Het informatiesysteem kan bijvoorbeeld direct actie ondernemen zodra het auditproces een alarm afgeeft.[89] Een voorbeeld van accounting is wanneer bij het meermalen achtereenvolgens fout intoetsen van de pin bij het elektronisch betalen de transactie door het systeem wordt afgebroken of zelfs de pas wordt 'ingeslikt'.[90]

5.6. De noodzaak van identiteit in het informatiesysteem

Analyse van de in de voorgaande paragraaf geschetste processen binnen informatiesystemen toont aan dat in zeer veel gevallen gebruik wordt gemaakt van de identiteit van de gebruiker. Binnen het autorisatieproces bijvoorbeeld wordt de identiteit gebruikt voor het vaststellen en vastleggen van de bevoegdheden en

86 Overbeek & Sipman, 1999, p. 116.
87 Overbeek & Sipman, 1999, p. 116.
88 Hes & Borking, 2000, p. 19 spreken van audit en auditing. Waters, 1995: in de bespreking van het rapport van de Registratiekamer: Privacy Enhancing Technologies: the path to anonymity, meent dat het om verwarring te vermijden beter is om te spreken van "transaction record", dan van "audit", omdat de bedoelde functie primair wordt gebruikt in een "monitoring-compliance context".
89 Overbeek & Sipman, 1999, p. 117.
90 Hes & Borking, 2000, p. 19.

plichten van een gebruiker. Op deze manier wordt de identiteit van consumenten geïntroduceerd in het informatiesysteem. Doordat alle verschillende modules van het informatiesysteem betrokken zijn bij de vijf hierboven vermelde processen, wordt daardoor de identiteit van de gebruiker/consument verspreid door het informatiesysteem.[91] Voor elk van de genoemde processen kan de vraag gesteld worden of het noodzakelijk is de identiteit van de gebruiker te kennen voor de uitvoering van de processen en de werking van het informatiesysteem.[92]

5.6.1. Autorisatie

In het autorisatieproces kent de dienstverlener privileges (bevoegdheden) aan een (toekomstige) gebruiker toe. Of een identiteit nodig is voor de autorisatie hangt af van de manier waarop de dienstverlener de bevoegdheden van de gebruiker bepaalt.[93] De dienstverlener zou op basis van bepaalde individuele kenmerken van de gebruiker bevoegdheden kunnen verlenen. In dat geval moet de gebruiker de gevraagde karakteristieken aantonen. Te denken valt bijvoorbeeld aan het lid zijn van een groep (Flying Blue Frequent Flyers), club (Priority Club Intercontinental Hotels) of vereniging of de gebruiker heeft een aanbeveling nodig van iemand die de dienstverlener kent en vertrouwt of de status of de leeftijd van gebruiker is bepalend.[94] Van Rossum e.a. hebben vastgesteld dat in de meeste gevallen voor het toekennen van bevoegdheden het niet nodig is de identiteit van de gebruiker te kennen.[95] Omdat het bij autorisatie om het toekennen van bevoegdheden gaat, kan geconcludeerd worden dat de identiteit van de gebruiker niet strikt noodzakelijk is voor het verlenen van autorisatie. Wettelijk kan evenwel vereist worden dat de identiteit van de gebruiker bekend is. Bijvoorbeeld om een visum aan te vragen zal de gebruiker zijn paspoort moeten overleggen. Om een bankrekening te openen zal men in de Europese lidstaten zijn identiteit kenbaar moeten maken. In Nederland is dit geregeld in de Wet identificatie bij financiële dienstverlening 1993 (Stcrt. 17). Deze wet is onder meer ingevoerd ter gedeeltelijke implementatie van de Richtlijn van 10 juni 1991, 91/308/EEG ter voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld. Deze richtlijn draagt de lidstaten op ervoor te zorgen dat financiële instellingen bij het aangaan van zakelijke betrekkingen of het verrichten van transacties boven een bepaalde drempel, de identiteit van hun cliënten vaststellen om te voorkomen dat degenen die geld witwassen van hun anonimiteit profiteren om criminele activiteiten te verrichten.[96]

---

91 Hes & Borking, 2000, p. 20.
92 Morssink, 2002, p. 218.
93 Hes & Borking, p. 21.
94 Zie paragraaf 3.5 Sociale sortering en informatieapartheid van dit boek.
95 Rossum, e.a., 1995, p. 9.
96 In de Wijziging van de Wet op de identificatieplicht van 1 januari 2005 werd dit nog eens bevestigd in de memorie van toelichting bij het wetsontwerp 29218 vermeldde: "Bij het openen van een bankrekening, het aanvragen van een uitkering of bij de notaris is geen reden te volstaan met vluchtige controle, maar zal altijd controle van de geldigheid identiteitsbewijs moeten plaatsvinden."

5.6.2. Accounting

Wat betreft de vraag of identiteit noodzakelijk is voor het proces accounting concluderen Van Rossum e.a. dat het in bepaalde gevallen nodig is dat de identiteit bekend is, bijvoorbeeld in het geval dat een gebruiker rekenschap moet geven over het gebruik van het informatiesysteem. Dit kan bijvoorbeeld het geval zijn als de gebruiker misbruik of oneigenlijk gebruik heeft gemaakt van het informatiesysteem en hiervoor aansprakelijk is. Echter, zolang de gebruiker zich aan de regels houdt, hoeft zijn identiteit niet bekend te worden.[97]

5.6.3. Identificatie en Authenticatie

Zoals hiervoor is beschreven verstaan de informatici onder authenticatie het proces waarbij een persoon, een computer of applicatie nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Het opgegeven bewijs van identiteit wordt gecontroleerd met echtheidskenmerken, bijvoorbeeld het een in het systeem geregistreerde bewijs. Als de dienstverlener de gebruiker heeft geaccepteerd, dan krijgt de gebruiker de beschikking over de interne representatie (bijvoorbeeld een code of een vercijferd of eenmalig wachtwoord) die hij kan gebruiken binnen het informatiesysteem.[98]. Met die interne representatie kan de gebruiker zich identificeren binnen het informatiesysteem. Wanneer de interne representatie elke keer wanneer iemand inlogt verandert, wordt het moeilijk de identiteit te achterhalen. Ook hier kan vastgesteld worden dat identiteit niet altijd noodzakelijk is om de processen identificatie en authenticatie om het informatiesysteem correct te laten werken.

5.6.4. Toegangscontrole

Bij de toegangscontrole kan eveneens de interne gebruikerspresentatie gebruikt worden in plaats van de identiteit van de gebruiker. Dit proces controleert immers of de gebruikerspresentatie de gebruiker toestaat bepaalde activiteiten uit te voeren. Geconcludeerd kan worden dat ook hier de identiteit van de gebruiker niet nodig is.[99]

5.6.5. Audit

Ook hier geldt dat de interne gebruikerspresentatie voldoende is. Immers het is alleen nodig om vast te leggen wat de gebruikersrepresentatie in het systeem uitvoert en dat maakt de identiteit van de gebruiker overbodig.[100]

---

97 Van Rossum, e.a.,1995, p. 9.
98 Overbeek & Sipman, 1999, p. 115, 231.
99 Hes & Borking, 2000, p. 20-22.
100 Van Rossum, e.a., 1995, p. 9.

5.6.6. Conclusie

Uit het bovenstaande kan geconcludeerd worden, dat het mogelijk is een privacyveilig informatiesysteem te bouwen zonder dat de identiteit van de gebruiker voor alle interne processen nodig is, waardoor persoonsgegevens niet behoeven te worden verwerkt en er minder of geen identificerende gegevens worden vastgelegd. Hes & Borking toonden aan, dat er veel dienstverlening mogelijk is, waar thans de identiteit van de gebruiker wordt gevraagd, maar waarvoor het niet nodig is om de identiteit te prijsgeven.[101] Door ervoor te zorgen dat de identiteit van de gebruiker binnen het informatiesysteem slechts in uiterste noodzaak wordt gebruikt, wordt voldaan aan het wettelijk vereiste van gegevensminimalisatie.[102] Deze aanpak is volgens Koorn e.a haalbaar voor de dienstverlening van zowel de frontoffice (interactie tussen overheid/bedrijven en burgers/consumenten) als de backoffice (informatieprocessen en de administratieve activiteiten binnen de overheid/bedrijfsleven die niet zichtbaar zijn voor de burger/consument).[103] Het niet of zo min mogelijk gebruik van identiteit en identificerende gegevens mag natuurlijk niet ten koste gaan van de beveiligingsmaatregelen die worden ingezet om de privacybedreigingen te verminderen of het hoofd te bieden. Nochtans de noodzaak van de identiteit van de gebruiker in het informatiesysteem is ook afhankelijk van de relaties die bestaan tussen het informatiesysteem en zijn omgeving (de buitenwereld). Als in de omgeving van het privacyveilige informatiesysteem een ander niet-privacyveilig informatiesysteem bij de 'interfacing' om de identiteit van de gebruiker vraagt, dan kan het privacyveilige systeem niet zonder die identiteit van de gebruiker.

5.7. Privacy Enhancing Technologies (PET)

De uitkomst van de analyse dat het ontbreken van de identiteit de werking van een informatiesysteem niet nadelig beïnvloedt als antwoord op de eerder gestelde kernvraag of de identiteit voor alle verwerkingsprocessen vereist is,[104] opent de mogelijkheid om met gebruikmaking van de door Chaum ontwikkelde wiskundige benaderingen de identiteit van de gebruiker te scheiden van het gebruik van het informatiesysteem. Om dit te bereiken kunnen informatie- en communicatietechnologie (ict) als hulpmiddel worden ingezet teneinde de bescherming van de privacy van personen te vergroten, het individu meer zeggenschap te geven over het beheer van hun persoonsgegevens en het vertrouwen in de rechtmatige verwerking te verhogen.[105] Deze manier van het gebruik van ict ter bescherming van de persoonlijke levenssfeer, staat wereldwijd sinds 1995 bekend als 'Privacy

101 Hes & Borking, 2000, p. 20-21.
102 Zie paragraaf 5.6.
103 Koorn, e.a., 2004, p. 22-26.
104 Borking, 1996, p. 657.
105 M. Klaver, e.a., 2002, p. 34, 40.

Enhancing Technologies' (PET).[106] Het gehele PET-concept wordt in de paragrafen 5.7 tot en met 5.13 uiteen gezet.

5.7.1. Definities

Van Lieshout wijst erop dat PET doorgaans wordt gezien als het concept om een geheel aan ict-maatregelen in te zetten voor de versterking van privacy. Daarbij is er weinig aandacht voor de verschillende hoedanigheden waaronder PET zich kan voordoen en voor de bredere context waarin PET dient te functioneren.[107] In het TNO-rapport 'Privacy Enhancing Technologies en overheidsinformatiesystemen' wordt PET gedefinieerd als:

> "een verzameling van Informatie en Communicatie Technologieën, die eventueel in combinatie met organisatorische en/of fysieke maatregelen de bescherming van de persoonlijke levenssfeer van individuen binnen een informatiesysteem versterken door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens of door het bieden van middelen en maatregelen tot het vergroten van de controle van de betrokkene over zijn of haar persoonsgegevens".[108]

In andere definities wordt niet nadrukkelijk uitgegaan van specifieke technieken, maar wordt PET wel beschouwd als behorend tot het ict-domein.[109] Klaver e.a. stellen dat PET een generieke term is en refereert aan een groep van technische hulpmiddelen die de verbetering van de persoonlijke levenssfeer beogen. Het is niet van tevoren aan te geven welke technische middelen tot PET behoren, maar zal met name door de ontwikkelingen van de ict over de tijd variëren.[110] Hoewel PET uitsluitend naar de inzet van technologieën verwijst, zullen er in de praktijk aanvullende organisatorische en fysieke maatregelen noodzakelijk zijn om de PET-applicaties goed te laten werken. Bij PET gaat het overigens niet om technologieën ter beveiliging van data. Beveiliging is een belangrijk component voor de bescherming van privacy (om primair de exclusiviteit, integriteit en beschikbaarheid van gegevens te waarborgen) maar in hoofdstuk 2 en 4 heb ik aangetoond dat dit niet voldoende is. Het gaat bij 'Privacy Enhancing Technologies', zoals het woord 'enhancing' aangeeft, uitdrukkelijk om die technologieën die primair tot doel hebben om de privacy van het individu te verbeteren en de rechtmatigheid van de verwerking van de persoonsgegevens te borgen. De meeste

---

106 Proceedings of 17th International Conference on Privacy and Personal Data Protection, Copenhagen, 1995 p. 80. Borking, 2003: "The acronym PET (not PETs due to the double entendre in the Dutch, English and French language) coined in August 1995 in the report Privacy Enhancing Technologies- The Path to Anonymity, consists of three elements in combination with each other, namely: 1. P for Privacy for which exist many different formulations but includes here Personal Data Protection; 2. T for Technologies, all forms of ict inclusive information architectures; 3. E for enhancing that stands for to heighten, to intensify, to exaggerate, and to raise privacy."
107 Van Lieshout, 2002, p. 204.
108 Klaver, e.a., 2002, p. 43.
109 Horlings, e.a., 2003, p. 4.
110 Klaver e.a., 2002, p. 34.

definities die over PET[111] in de literatuur verschenen, sluiten meer aan bij de onderzoeksvraag in het plan van aanpak van de eerste technology assessment-studie van de Registratiekamer.[112] De onderzoekvraag richtte zich op de mogelijkheden om de informatie- en communicatietechnologie (ict) in te schakelen om de onrechtmatige verwerking van persoonsgegevens te voorkomen, en daarmee een bijdrage te leveren aan het oplossen van de privacyproblematiek, zonder afbreuk te doen aan de functionaliteit van informatiesystemen. In het in 1995 door de Registratiekamer (RGK) uitgebrachte rapport staat geen definitie van PET, maar wordt ter bescherming van de persoonlijke levenssfeer de inzet van encryptie, (blinde) digitale handtekeningen en digitale pseudoniemen noodzakelijk geacht.[113] Het ontbreken van een definitie leidde tot onterechte claims van leveranciers dat hun product of dienst PET-proof was. De definitie van de RGK komt later en luidt:

> "Privacy Enhancing Technologies (PET) zijn een samenhangend geheel van ICT maatregelen dat de persoonlijke levenssfeer (conform de richtlijn 95/46/EG en 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 functionaliteit van het informatiesysteem."[114]

In een uit dezelfde tijd stammende definitie van de RGK wordt PET omschreven als:

> "een systeem van maatregelen in de database, de applicatie en het proces waarmee de informationele privacy wordt beschermd en vertrouwen wordt geschapen door het verminderen of elimineren van identificeerbare of herleidbare persoonsgegevens en/of het voorkomen van onrechtmatige verwerking".

In de definitie van de Registratiekamer zijn twee elementen opvallend namelijk het in de eerste definitie van de Registratiekamer vermelde begrip "samenhangend". Dit slaat op het pakket van op elkaar afgestemde technologische en organisatorische maatregelen als een dwingende voorwaarde. Het tweede element is het vereiste dat de functionaliteit van het systeem niet verloren mag gaan. Dit vereiste was ingegeven, omdat de RGK niet terug wilde naar het tijdperk van de eerste computers met een uiterst beperkte functionaliteit en omdat er bij het nemen van maatregelen ter bescherming van persoonsgegevens noodzakelijkerwijs altijd een afweging dient plaats te vinden. Als de toepassing van PET in het bestaande informatiesysteem de uitvoering van bepaalde legitieme taken onmogelijk maakt, dan zal een afweging moeten worden gemaakt of de invoering van

111 Er waren op 21 maart 2008 via de zoekmachine van Google 311.000 hits op het begrip Privacy Enhancing Technologies, waarin een veelvoud aan gelijkluidende definities.
112 Borking, 2002, p. 196.
113 Van Rossum, e.a.,1995.
114 Van Blarkom & Borking, 2001, p. 19.

PET proportioneel is.[115] Dat wil niet zeggen dat er alsdan geen privacybeschermende maatregelen moeten worden getroffen, maar dat zullen dan andere PET-maatregelen zijn. Ten aanzien van nieuw te construeren systemen zal het bovenstaande proportionaliteitsargument moeilijker zijn aan te voeren omdat in het ontwerp met allerlei randvoorwaarden nog rekening kan worden gehouden.

Rotenberg stelt dat PET een grote verscheidenheid van technieken (dit is ruimer dan technologieën) omvat, die kunnen worden omschreven als protocollen, standaarden en *tools* (gereedschappen) die direct hulp bieden bij het beschermen van de privacy door de te verzamelen persoonlijk identificeerbare data tot een minimum te beperken en waar mogelijk zelfs volledig te elimineren.[116]

Ook Claerhout meent dat PET een grote verscheidenheid van technieken omvat die onder meer kunnen omschreven worden als protocollen, standaarden en 'tools' die direct hulp bieden bij het beschermen van de privacy door de in te zamelen persoonlijk identificeerbare data tot een minimum te beperken en waar mogelijk zelfs volledig te elimineren.[117]

In de Mededeling van de Europese Commissie aan het Europees Parlement en de Raad inzake de verbetering van de gegevensbescherming door technologieën ter bevordering van de persoonlijke levenssfeer[118] wordt gerefereerd aan de definitie in het door de Europese Gemeenschap gesubsidieerde PISA-project.[119] Hierin wordt onder technologieën ter bevordering van de persoonlijke levenssfeer (PET) verstaan:

> "een samenhangend systeem van ICT-maatregelen ter bescherming van de persoonlijke levenssfeer door persoonsgegevens of de onnodige en/of ongewenste verwerking van deze gegevens te elimineren of te verminderen zonder de functionaliteit van het informatiesysteem in gevaar te brengen".[120]

Deze definitie moet beschouwd worden als de definitie die de EU voor PET hanteert. De EU-definitie van PET stipuleert nochtans niet uitdrukkelijk dat de doelstelling van PET ook is het bieden van middelen tot het vergroten van de controle van het betrokken individu over zijn of haar persoonsgegevens. Het door de EU gesubsidieerde FIDIS (Future of Identity in the Information Society)

115 Klaver, e.a., 2002, p. 41.

116 Rotenberg & Agrawal, 2003: Statement for the record of Marc Rotenberg and Ruchika Agrawal, Workshop on Technologies for Protecting Personal Information: the Consumer Experience and Technologies for Protecting Personal information: the Business Experience before the Federal Trade Commission 2003. www.ftc.gov/bcp/workshops/technology/comments/rotenberg.pdf.

117 Claerhout, 2005, p. 3.

118 Communication From The Commission To The European Parliament And The Council On Promoting Data Protection By Privacy Enhancing Technologies (PETs), COM(2007) 228 Final, Brussels, 2.5.2007.

119 EU Projectnummer: IST-2000-26038; Projectnaam: PISA – Privacy Incorporated Software Agent, Building a Privacy Guardian for the Electronic Age; Onderzoeksperiode: 1999-2003. Doelstelling: PISA builds a model for software agents to perform actions on behalf of a person without compromising the personal data of that person.

120 Borking, 2001: Hierin wordt er op gewezen dat niet alleen de ongewenste verwerking van gegevens moet worden tegengegaan, maar ook dient zoveel mogelijk gegevensminimalisatie te worden toegepast.

project[121] onderscheidt in 2007 PET-systemen in systemen met 'transparency tools' en systemen met 'opacity tools' De 'transparency tool' dient om aan het individu inzicht in de gegevensverwerking te verschaffen over de manier waarop zijn persoonsgegevens worden verwerkt. Dat kan bijvoorbeeld door 'log files'. Bij 'opacity tools' gaat het om de identiteit van de gebruiker te verbergen of de verbinding tussen de de gebruiker en zijn persoonsgegevens af te schermen, bijvoorbeeld door pseudoniemen. De Deense MetaGroup onderscheidt PET in technologieën die de privacy beschermen en technologieën die de privacyverplichtingen managen.[122]

Clarke heeft een indeling gemaakt met vier categorieën, namelijk:

1. Pseudo-PET, zoals privacycertificaten en P3P (waarover in paragraaf 5.12.2).
2. 'Counter'technologie, counters one specific privacy threat e.g SSL encryption or spyware removal'.
3. Savage PET, die zorgt voor niet traceerbare anonimiteit.
4. Gentle PET, waarbij het gaat om "balanced pseudonimity tools with accountability, identity management".

Clarke heeft geen scherpe definities bij zijn indeling gegeven, noch een classificatie van bestaande PET-applicaties.[123]

Bij de behandeling van de Wet bescherming persoonsgegevens in de Tweede Kamer wordt naast de motie Scheltema-De Nie en Wagenaar[124] kamerbreed de motie Nicolaï[125] aangenomen. De regering wordt hierin verzocht als innovatieve aanbesteder ('launching customer') in haar eigen informatiesystemen wat betreft de verwerking van persoonsgegevens het voortouw te nemen om PET toe te passen. Uit de debatten bij de behandeling van het wetsontwerp kan geconcludeerd worden dat de bescherming van de persoonlijke levenssfeer al begint bij het ontwerp van het informatiesysteem. Artikel 13 Wbp vormt de grondslag van de inzet van PET, want het gaat conform dit artikel niet alleen om beveiliging van gegevens maar ook om onnodige verzameling en verdere verwerking te voorkomen. Daarbij gaf de toenmalige toezichthouder (RGK) de voorkeur aan technische voorzieningen boven organisatorische. Technische maatregelen zijn doeltreffender omdat het moeilijker is aan het effect ervan te ontkomen,[126] maar zonder samenhang met organisatorische maatregelen zal het niet tot een goed functionerende PET-applicatie kunnen komen.[127]

---

121 www.fidis.net.
122 Meta Group, 2005.
123 Clarke, 2007.
124 Tweede Kamerstuk 25 892 nr. 22, vergaderjaar 1999-2000. Dit belangrijke amendement heeft het toenmalige artikel 13 WBP uitgebreid met de zin: "De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."
125 Tweede Kamerstukken 1999-2000, 25 892, nr. 31.
126 Van Blarkom & Borking, 2001, p. 20.
127 Klaver, e.a., 2002, p. 41: "PET applicaties zullen in het algemeen onderdeel zijn van een bredere verzameling privacy enhancing maatregelen."

5.7.2. Vier PET-functionaliteiten

PET kunnen niet alleen defensief worden ingezet ter bescherming van de persoonlijke levenssfeer en afscherming tegen ongewenste bemoeienis van anderen (de overheid daarbij inbegrepen). PET bieden ook het individu de mogelijkheid meer zeggenschap en controle uit te oefenen (met inachtneming van de wettelijke regels en voorschriften) over het verwerken, het verspreiden en opslaan van zijn persoonsgegevens. PET verschaffen bovendien organisaties de middelen om er voor te zorgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad. Door PET ontstaan evenwel ook mogelijkheden de persoonlijke levenssfeer te verrijken en waardevoller te maken, door bijvoorbeeld onder een pseudoniem aan een organisatie persoonsgegevens beschikbaar te stellen om over bepaalde acties en activiteiten geïnformeerd te worden, zonder dat eigen levenssfeer wordt geschaad.[128] Burkert constateert dat:

> "PET as a concept have brought the social 'soft' concern of how to reduce personal data down to the level of 'hard' system-design considerations".[129]

Dat is belangrijk, schrijft hij, want door de technische beschrijving van privacy bescherming in PET "system-design specifications" zijn de privacyvoorvechters en -beschermers in staat om met systeemontwerpers over het systeemontwerp in dezelfde taal te praten. Bovendien snijdt het argument dat privacybescherming technisch onvertaalbaar is in de 'system engineering' geen hout.[130] Politici en de overheid kunnen zich dan ook niet meer achter het argument verbergen dat privacybescherming technisch onmogelijk is te realiseren. Burkert onderscheidt vier vormen van PET functionaliteit:

a. Subject georiënteerde PET.
b. Object georiënteerde PET.
c. Transactie georiënteerde PET.
d. Systeem georiënteerde PET.

a. Subject georiënteerde PET heeft volgens Burkert tot doel:

> "to eliminate or substantially reduce the capability to personally identify the acting subject (or interacting subject) in transactions or in their relationship to existing data".[131]

De persoonsgegevens worden geanonimiseerd of aan het individu wordt een willekeurige niet permanent pseudo-identiteit gegeven.

---

128 Klaver, e.a., 2002, p. 8, 33.
129 Burkert, 2001, p. 129.
130 Burkert, 2001, p. 129.
131 Burkert, 2001, p. 126.

b. Bij object georiënteerde PET wordt volgens Burkert de verbinding tussen subject en object verbroken omdat in het dagelijks leven vastgesteld kan worden, dat:

> "transactions often involve exchange or barter and the observation that an object given in exchange carries traces (not unlike fingerprints) that allow identification of the exchanging subjects….the aim is then to free the exchanged object from all such traces without eliminating the object itself".[132]

Zo worden in Chaum's 'digital cash' cryptografisch beveiligde nummers afgegeven die staan voor een eenmaal te gebruiken van tevoren bepaalde geldwaarde. Deze aanpak is te vergelijken met een chipkniptransactie, zij het dat de chipkniptransactie weliswaar niet in de winkel, maar wel in de 'backoffice' van de bank traceerbaar is omdat anders zou niet duidelijk zijn door welke bank het gechipte bedrag betaald moet worden.

c. Transactie georiënteerde PET richt zich op het verhullen van de transactie.
d. Systeemgerichte PET richt zich op de integratie van de drie hierboven vermelde categorieën waarbij, zoals Burkert het schrijft:

> "creating zones of interaction where the identity of the subjects is being hidden, where the objects bear no traces of those handling them, and where no record of the interaction is created or maintained".[133]

Er zijn een aantal risico's die door het subject georiënteerde PET-concept worden opgeroepen waarvan de eendimensionale anonimiteit het belangrijkste is. De individuele gebruiker/consument krijgt in dit concept bescherming om een machtsevenwicht te scheppen ten opzichte van de economisch sterkere dienstverlener. Maar het kan ook zo zijn dat de gebruiker een sterke inkooporganisatie is en de aanbieder een kleine onderneming. Deze vorm van PET introduceert hier een verkapte normatieve beslissing betreffende welke partij in de transactie bescherming krijgt. Voorzichtigheid is dan ook geboden bij bepaalde implementaties van dit concept. Burkert stelt dan ook:

> "(…) PETs; they may indeed enhance privacy as we cherish it, but they might also enhance unwanted secrecy" en "PETs may make it possible to maintain a given distribution of organizational power rather than to empower individuals in their dealings with such organizational power and thus enhancing the defense of their rights and freedoms and privacy".[134]

Caronni wijst ook op deze keerzijde van de medaille, maar stelt dat er vele voordelen tegenoverstaan:

---

132 Burkert, 2001, p. 127.
133 Burkert, 2001, p. 128.
134 Burkert, 2001, p. 131.

> "Dennoch: In Zeitraum der Untersuchung wurden viele wertvolle Nachrichten von Menschen befördert, die sich sonst kaum hätten unerkannt oder frei aussprechen können....Aufdecken von Mißständen in der Wirtschaft, in Behörden und Sekten (z.B. Scientology); Aussprachemöglichkeit für mißhandelte Ehepartner und Kinder; Foren für verfolgte Minderheiten (politische, religiöse und andere. Diese und andere ähnliche Nutzungen sind es wert, die Nachteile in Kauf zu nehmen als Preis für unser aller Freiheit."[135]

Dat ziet Burkert natuurlijk ook in. Afgezien van het feit dat afhankelijk van de omgeving waarin het PET systeem werkzaam is en de keuze van de gebruiker, er of anonimiteit of pseudonimiteit aan de gebruiker kan worden verschaft, kan er een oplossing voor het een dimensionale anonimiteitsprobleem volgens Burkert worden gefourneerd. De door hem aangedragen oplossing is dat:

> "one would have to ensure not only that individual PET systems were designed properly but also that their role in networks of PET and non-PET systems remained clearly identifiable".[136]

Transparantie is de beste waarborg tegen manipulatie. Er moet kunnen worden vastgesteld dat een PET-systeem inderdaad de persoonsgegevens beschermt en dat via de verwerking van de gegevens geen verborgen informatie voor anderen beschikbaar komt, waardoor het mogelijk wordt, zonder daartoe gerechtigd te zijn, de persoonsgegevens te ontcijferen. De vraag is dan wie gaat dat doen? In de eerste plaats zouden in het ontwerp proces individuen meer direct er bij betrokken moeten worden en, aldus Burkert:

> "Data-protection agencies could play an important role in adopting such procedures for the design and implementation of large personal-information systems and their PET components."[137]

Of de laatste suggestie realistisch is, valt te bezien. De meeste toezichthouders betreffende de bescherming van persoonsgegevens zien het niet als hun taak zich in te laten met het feitelijk technische ontwerp van informatiesystemen. Ook de Europese Commissie heeft dit ingezien. Zij ondersteunt verschillende projecten die de research naar privacybescherming bevorderen, zoals PRIME en EuroPrise. Zo heeft het PRIME researchproject onder meer tot doel:

> "PRIME will enable the users to effectively control their private sphere thanks to the PRIME Architecture that orchestrates the different privacy-enhancing technologies, including the human-computer interface".[138]

---

135 Caronni, 1998, p. 633-635.
136 Burkert, 2001, p. 133.
137 Burkert, 2001, p. 137.
138 Projectnaam: PRIME (Privacy and Identity Management for Europe) Contract No. 507591 Researchperiode 2004-2008.

Het Europrise researchproject heeft tot doel: "Introducing a European Privacy Seal for IT-products and services that have proven privacy compliance in a two-step certification procedure: an evaluation by specialized experts and an check of the evaluation report by an independent certification body", om de transparantie van de privacybescherming van producten en diensten voor de burgers en consumenten te vergroten.[139] Burkert ziet twee duidelijke verdiensten bij de implementatie van het PET concept in de architectuur van informatiesystemen: PET zorgt voor een betere gegevensminimalisering en voor de noodzaak van een weloverwogen toestemming.[140]

5.7.3. De PET-trap

PET manifesteren zich in vier vormen. Ieder vorm heeft specifieke functies met betrekking tot gegevensbescherming. De ene vorm biedt meer bescherming dan de andere. In figuur 5.2 zijn de verschillende PET-vormen gepositioneerd ten opzichte van de effectiviteit van de gegevensbescherming. Er is sprake van algemene PET-maatregelen, die voornamelijk bij de informatiebeveiliging worden toegepast, de scheiding van gegevens in verschillende identiteitsdomeinen met gebruikmaking van pseudo-identiteiten, privacymanagementsystemen en anonimisering. In een PIA ('privacy impact analysis'), (zie paragraaf 4.7) wordt vastgesteld of er sprake is van identiteitsrijke (dat wil zeggen dat identificerende persoonsgegevens zijn vereist), identiteitsarme (identiteit eenmalig nodig, maar één persoonskenmerk zoals leeftijd of beroep volstaat) of identiteitsloze verwerkingsprocessen waarbij geen identiteit nodig is. In figuur 5.2 zijn de belangrijkste eigenschappen van de PET vormen weergegeven. Koorn e.a. schrijven dat de PET-trap geen trap en ook geen groeimodel is. Het is dus voor een organisatie niet noodzakelijk om alle vier vormen te doorlopen. De geschiktheid van de verschillende PET-vormen is afhankelijk van de situatie.[141]

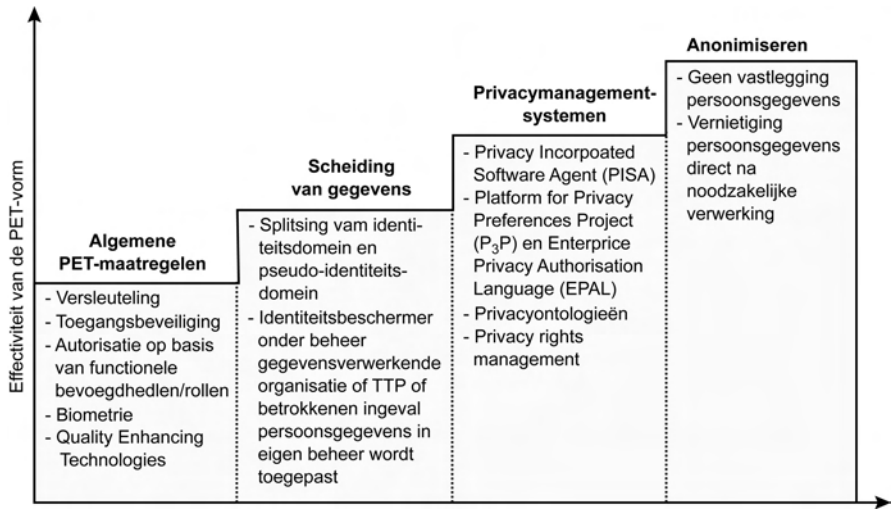
---

139 EuroPriSe is een Europees project gesubsidieerd door de Europese Commissie met 1,2 Miljoen euro onder het eTEN programma. Projectnaam: European Privacy Seal; project nummer: 046221. Onderzoeksduur 2007-2009. Het consortium bestaat uit negen Europese partners en wordt geleid door het Unabhängiges Landeszentrum für Datenschutz, ULD Schleswig-Holstein, Kiel.

140 Burkert, 2001, p. 138.

141 Koorn, e.a., 2004, p. 40.

Figuur 5.2: De PET-trap, Koorn, e.a. 2004, p. 40.



Sinds 2004 heeft de research nieuwe middelen ontwikkeld om de persoonsgegevens nog beter te beschermen. Er zijn 'detection tools', die het mogelijk maken om vast te stellen of data wordt verplaatst en of data wordt gebruikt in strijd met het doel waarvoor de persoonsgegevens door het individu zijn afgestaan. Het is mogelijk geheime 'watermerken' en biometrische kenmerken aan de eigen data toe te voegen. Als de data op het web opduikt, kan het individu tegen degene die de data onrechtmatig gebruikt actie nemen. Deze technologie is gebaseerd op 'Digital Rights Management' en wordt aangeduid met 'Personal Rights Management'.[142] Naast 'detection tools' zijn er ook middelen die het privacybeleid van de organisatie ondersteunen, de onderhandelingen over gewenste privacybescherming tussen de aanbieder van een bepaalde dienst en de afnemer mogelijk maken en het naleven daarvan kunnen afdwingen. Ten slotte zijn er 'opacity tools' ontwikkeld zoals de anonieme remailer Mixmaster (gebasserd op Chaum's MIX principe) die analyse van het dataverkeer onmogelijk maakt en e-mails anoniem of onder een pseudoniem kan versturen. Een voorbeeld van MIXmaster is http://secret101.com/anonymous101/index.htm. Het AN.ON (Anonymität Online) project van de universiteit van Dresden en de privacytoezichthouder voor Schleswig-Holstein in Kiel is ook een MIXmaster. In plaats van direct een verbinding te maken met een webserver, maken gebruikers een omweg

142 Deng e.a., 2006.

via verschillende tussenstations, de zogenaamde Mixes om de relatie tussen de verzonden e-mail en persoonsgegevens te ontkoppelen.[143]

5.7.4. De beleidsdoelstellingen van PET

De beleidsdoelstellingen van PET kunnen visueel het best weergegeven worden in een grafiek (zie figuur 5.3). Op de horizontale as is het identificerende gehalte van de gegevens aangegeven en op de verticale as de hoeveelheid vastgelegde gegevens. De informatiesystemen die niet gebruikmaken van gegevensminimalisatie en PET, leggen veelal veel gegevens vast van een hoog identificerend gehalte. De gegevens kunnen dan ook direct aan een natuurlijk persoon worden gerelateerd. Deze informatiesystemen bevinden zich in de rechterbovenhoek van de grafiek. De van PET voorziene informatiesystemen zullen zich dichtbij één van de assen van de grafiek bevinden. Wanneer er sprake is van voldoende niet identificerende gegevens kunnen die data niet aan een persoon gerelateerd worden. En omgekeerd als gegevens worden losgekoppeld van de identiteit, kunnen er geen gegevens gerelateerd worden aan een persoon. Een combinatie van deze twee mogelijkheden, bevindt zich in de 'wolk' nabij het kruispunt van het assenstelsel. De grafiek toont als ideaal voor optimalisatie van de bescherming van persoonsgegevens een asymptotische kromme. Nochtans door mij is niet bewezen dat bij optimaal gebruik van PET de directe of indirecte identificatie van een persoon leidt tot de functie: ID = f (qn,ql Δ) = y =1/x.

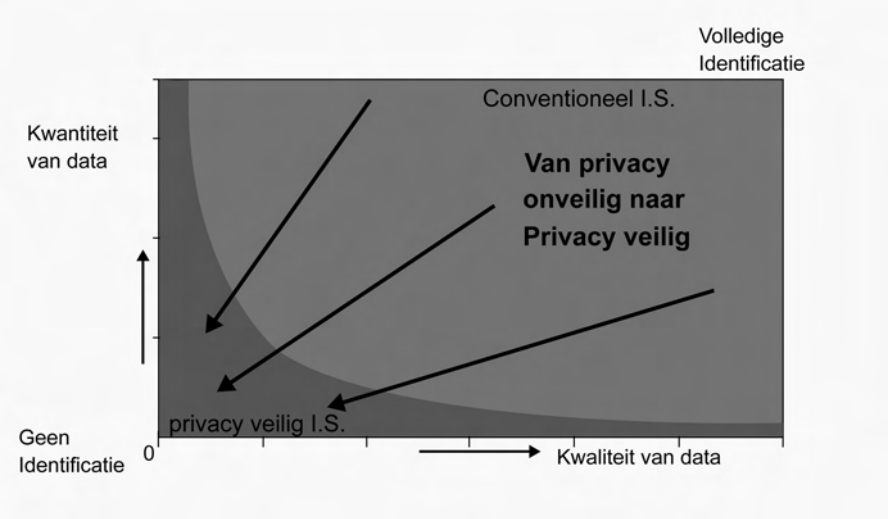
ID betekent in de formule: identificatie. Het symbool Δ staat voor persoonsgegevens en 'qn' en 'ql' staan voor kwantiteit respectievelijk kwaliteit van de data.

De doelstellingen worden evenwel visueel duidelijk weergegeven.

---

143 http://anon.inf.tu-dresden.de/index.html; Er zijn nog veel meer tools ontwikkeld zoals onion routing,TOR, TORPARK.Xerobank Browser, Cookie Cooker, Eternity service van Ross Anderson, Identity management tools, zoals IBM's IDEMIX en reach ability management tools om o.a SPAM mails en ongewenste telefoongesprekken te voorkomen. Fritsch, 2007, p. 30: "tools for unobservability and identity protection have reached a high level of maturity. Some concepts, such as trusted platforms, anonymous credentials or DRM technology application for information tracking have not yet entered the market yet."

Figuur 5.3: De ideale privacybescherming met PET.



5.7.5. PET, meer dan beveiliging

Klaver wijst erop dat de bescherming van de persoonlijke levenssfeer tweeledig is. Aan de ene kant moet gestreefd worden naar gegevensminimalisatie en aan de andere kant moeten de in het informatiesysteem aanwezige persoonsgegevens afgeschermd worden tegen ongeautoriseerde inzage, verwerking, wijziging, achterhouden en verwijderen. In beide gevallen kan PET gebruikt worden voor het verwezenlijken daarvan.[144] Burkert tekent hierbij aan dat PET bedoeld is "to enhance privacy"[145] en dus meer is dan informatiebeveiligingsmaatregelen, die de exclusiviteit, integriteit en beschikbaarheid waarborgen.[146] Beveiliging is wel een noodzakelijke, maar niet toereikende voorwaarde voor de bescherming van persoonsgegevens.

5.7.6. Privacywetgeving in programmacode

Het PET-concept kende vier kernfunctionaliteiten (Anonimiteit,[147] Pseudonimiteit, Niet-relateerbaarheid en Niet-observeerbaarheid),[148] vastgelegd in 1999 in de

144 Klaver, 2002, p. 42.
145 Burkert, 2001, p. 131.
146 Van Blarkom & Borking, 2001, p. 16.
147 Over het recht op anonimiteit is veel gediscussieerd. Zie bijvoorbeeld: Het advies van de Raad voor het Openbaar bestuur : ict en het recht om anoniem te zijn, Den Haag 2000; Roessler, 1998, p. 619-622 Demuth & Rieke, 1998, p. 623- 627.
148 Federath, 2000: "anonymity implies no identifiable data at all; Pseudonymity means identifiable for authorised users only; Unlinkability is no common identifier to link systems; unobservability requires anonymity until required for identification".

'Common Criteria Technology Security Evaluation' standaard-ISO 15408. Hoofdstuk 9 van deze standaard van de International Organization for Standardization (ISO) is gericht op het reduceren van persoonsgegevens in informatiesystemen. In deze ISO-standaard wordt PET gekoppeld aan beveiligingsvraagstukken. In dit verband is volgens Van Lieshout de opname van PET in artikel 13 van de WBP ten gevolge van de amendementen van de Tweede Kamerleden veelzeggend.[149] Maar PET is niet alleen bedoeld voor informatiebeveiliging. Door middel van onder meer vercijfering, geavanceerde toegangscontrolemechanismen, 'firewalls', domeinscheiding, anonimisering en andere technische beveiligingsmaatregelen kan PET een aantal van de in hoofdstuk 2 besproken privacyrealisatiebeginselen borgen. Het gaat dan om transparantie, doelbinding, dataminimalisatie, de rechtmatige verwerking van de persoonsgegevens, waarborging van de verplichtingen van de verantwoordelijke en de bewerker. In 2002 maakte het College Bescherming Persoonsgegevens (CBP) in zijn jaarverslag over 2001 bekend, dat PET meer inhoudt dan de in de ISO-standaard 15408 vermelde vier kernfunctionaliteiten aangevuld met de relevante organisatorische en fysieke maatregelen. Het CBP schrijft:

> "Privacy Enhancing Technologies (PET) voorkomen de onnodige verwerking van persoonsgegevens in informatiesystemen zonder dat verlies van functionaliteit optreedt. In plaats van de wet toe te passen op het systeem, wordt de wet in het systeem ingebouwd: 'privacy by design'".[150]

Het College refereert met deze uitspraak aan het EU gesubsidieerde PISA-project waarin het CBP van 1999 tot en met 2003 participeerde en dat als doelstelling had: "To prove and show that the privacy of user is protected in all kinds of processes by incorporating PET features in software agents". In dit onderzoeksproject vindt de 'vertaling' van normen uit de EU privacyrichtlijn in beschrijvingen van concrete softwarecomponenten plaats.[151] In het jaarverslag over 2003 deelt het College mee:

> "PISA was ook de afronding van een project dat een technisch 'proof of concept' moest leveren waarmee kon worden aangetoond dat abstracte en open normen uit de privacywet- en regelgeving technisch vertaald konden worden in werkende producten, die rechtmatig handelen afdwingen".[152]

Het inbouwen van de regel- en wetgeving in systemen moet dan ook worden beschouwd als een nieuwe loot aan de PET-stam. Klare (niet-vercijferde)

---

149 Van Lieshout, 2002, p. 204: "De relatie met beveiliging had vermeden kunnen worden door aansluiting te zoeken bij artikel 11 WBP".
150 CBP, 2001, p. 34.
151 CPB, 2002, p. 49.
152 CBP, 2003, p. 47. Het College deelde bij de afsluiting van het PISA project mede, dat "het CBP in de toekomst niet meer zo nadrukkelijk mede eindverantwoordelijk kan zijn voor dergelijke projecten. De toezichthoudende taak staat dat in de weg". Borking: "Het is evenwel zeer de vraag of de stelling van het CBP juist is. Participatie van de DPA's is juist geboden".

persoonsgegevens, die in veel verwerkingen nu eenmaal niet kunnen worden vermeden, kunnen zo worden verwerkt dat de grenzen van de privacywetgeving niet worden overschreden. Ging het vóór het PISA-project vooral om identiteitsbescherming, het tegengaan van onnodige identificatie en om datareductie met daaraan gekoppeld het anonimiseren en pseudonimiseren,[153] nu werd voor het eerst gepoogd de privacywetgeving in al zijn aspecten in digitale vorm op de gegevensverwerking toe te passen. De verwerking van persoonsgegevens in strijd met de wetgeving werd onmogelijk gemaakt door in het informatiesysteem de wettelijke regels te converteren naar een binaire code met dwingende beslissingsregels die de verwerking van persoonsgegevens beheersen. PET kan met deze nieuwe loot aan de stam een belangrijk hulpmiddel zijn, dat grotere technische zekerheid biedt voor een rechtmatige verwerking van persoonsgegevens en daardoor het vertrouwen van het individu in de verwerking van zijn gegevens kan vergroten.

5.8. De Identity Protector

De identiteitsbeschermer (IDP: 'Identity Protector', zoals deze functie internationaal bekend staat)[154] kan beschouwd worden als het hart van PET. Het is een systeemmodule die de uitwisseling van de identiteit van de gebruiker tussen de overige systeemmodules en processen beheerst.[155] Hoe de Identity Protector technisch moet worden ingericht, hangt af van het specifieke informatiesysteem. Een aantal van de manieren waarop dit dient te gebeuren zijn gebaseerd op de eerder besproken ideeën van Chaum.[156]

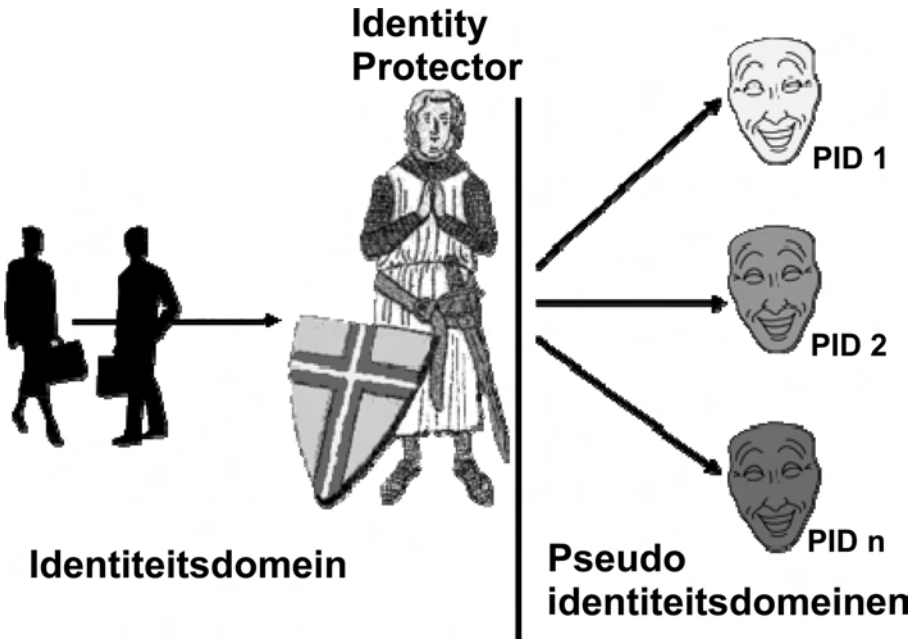
Figuur 5.4 geeft aan dat de Identity Protector de identiteit van de gebruiker in één of zo veel meer pseudo-identiteiten (in het figuur 5.4 weergegeven als maskers) converteert als er aantallen afzonderlijke transacties zijn binnen het informatiesysteem. Het zinsdeel "een of zoveel meer pseudo-identiteiten" slaat op het feit dat door het vele gebruik van een en dezelfde pseudo-identiteit, de ware identiteit toch achterhaald kan worden. Een bankrekeningnummer is bij eenmalig gebruik een goede pseudo-identiteit, maar niet als hetzelfde bankrekeningnummer een aantal keren wordt gebruikt. Wanneer verschillende pseudo-identiteiten door een persoon worden gebruikt, valt er geen patroon te ontdekken in de activiteiten van die persoon die op basis van de verschillende pseudo-identiteiten worden uitgevoerd.

De pseudo-identiteit is een alternatieve digitale identiteit die het individu kan krijgen, wanneer hij het informatiesysteem gebruikt. Alle gegevens die samenhangen met het gebruik van het systeem worden vanaf het moment dat de IDP

153 Claerhout, 2005, p. 4-6.
154 Borking, 1996, p. 654-658.
155 Van Rossum, e.a., 1995, p. 5.
156 Hes & Borking, 2000, p. 23.

een pseudo-identiteit heeft verleend aan de gebruiker, gekoppeld aan die pseudo-identiteit, waardoor er geen persoonsgegevens meer worden gegenereerd.

Figuur 5.4: De Identity Protector (Identiteitsbeschermer).

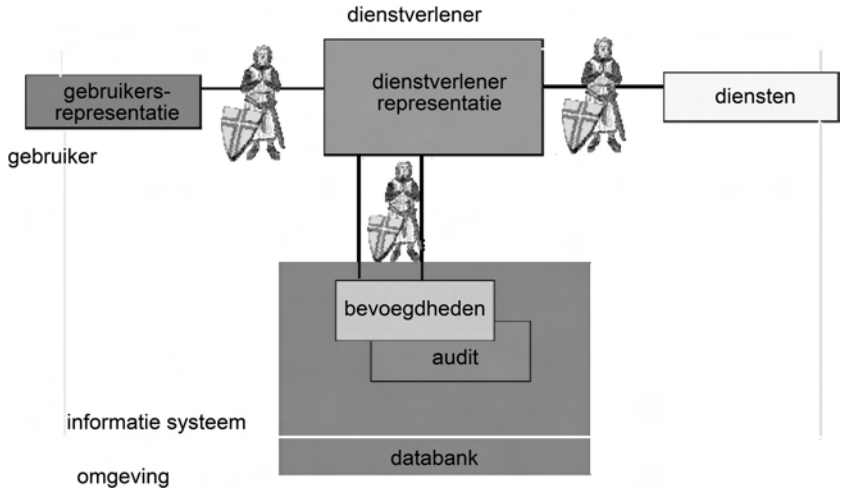


Ten behoeve van de noodzakelijke identiteitsuitwisseling tijdens de verschillende processen in het informatiesysteem wordt de IDP op een of meerdere interactielijnen in het informatiesysteem (zie figuur 5.5) geplaatst. De IDP kan overal waar in het informatiesysteem persoonsgegevens worden uitgewisseld, geplaatst worden. Hoe meer de identiteit en daarmee samenhangende persoonsgegevens van de gebruiker moeten worden beschermd, des te kleiner het identiteitsdomein (ID) dient te zijn en des groter het pseudo-identiteitsdomein (PID) in het informatiesysteem. Dus, de identiteitsbeschermer die direct na de gebruikersrepresentatie is geplaatst, creëert het grootste pseudo-identiteitsdomein. Een nog groter pseudo-identiteitsdomein zou kunnen worden gecreëerd door een smartcard met daarop de IDP te gebruiken bij het inloggen.[157] Het informatiesysteem is dan in zijn geheel een pseudo-identiteitsdomein voor de gebruiker geworden.

157 Koorn, e.a., 2004, p. 34.

Figuur 5.5 laat het effect van de plaatsing van de IDP in het informatiesysteem zien:

Figuur 5.5: Identity Protectors in het model Informatiesysteem.



De plaatsing van de IDP heeft tot gevolg dat de identiteit en de persoonsgegevens van de gebruiker niet meer naar het afgeschermde deel van het informatiesysteem verspreid kunnen worden. De persoonsgegevens worden dus bij de verwerking gescheiden van de niet-persoonsgegevens. Scheiding van gegevens houdt in dat persoonsgegevens wel worden verwerkt, maar dat de identificerende persoonsgegevens worden losgekoppeld van de overige gegevens. Deze gedachte vormt de basis voor de IDP. Uit figuur 5.4 kan worden afgeleid dat door het plaatsen van de IDP twee soorten domeinen binnen het informatiesysteem, ontstaan. Er is één domein waar de identiteit van de gebruiker bekend of toegankelijk is en er zijn één of meerdere domeinen waarin de gebruiker slechts bekend is onder een pseudo-identiteit die kan verschillen per verwerking.[158] De term 'identiteitsdomein' duidt het domein aan waar de werkelijke identiteit van de gebruiker van het informatiesysteem bekend is. De domeinen waar de identiteit van de gebruiker niet bekend zijn, worden aangeduid als 'pseudo-identiteitsdomeinen' (zie figuur 5.4). Personen die geautoriseerd zijn de IDP te gebruiken, kunnen hiermee toegang verkrijgen tot beide domeinen en de relatie tussen de twee domeinen zien. Personen die voor hun functie niet de beschikking hoeven te hebben over alle persoonsgegevens, krijgen alleen toegang tot die pseudo-identiteitsdomeinen waartoe zij gerechtigd zijn. De gebruiker moet er overigens vanuit kunnen gaan

158 Goemans, 2002, p. 5.

dat de dienstverlener in het domein waar de identiteit van de gebruiker bekend is, zijn persoonsgegevens conform het van tevoren door de gebruiker geaccepteerde privacybeleid c.q. de privacy wet- en regelgeving zal behandelen.

5.8.1. Functies van de Identity Protector

Zoals hierboven al uiteengezet is een belangrijke functie van de identity protector (IDP) het omzetten van de identiteit van een gebruiker in een pseudo-identiteit, meestal door het toekennen van niet-herleidbare identificatiecodes. Met de pseudo-identiteit (een digitale identiteit) kan de gebruiker vervolgens handelingen binnen het informatiesysteem verrichten. De IDP waarborgt de belangen van de gebruiker, met name houdt hij controle over de verspreiding van zijn identiteit en persoonsgegevens binnen het informatiesysteem. Bovendien zorgt de IDP er voor, dat de betrokkene niet kan worden getraceerd aan de hand van eerder verkregen persoonsgegevens en zorgt het pseudo-identiteitsdomein ervoor dat de persoonsgegevens niet kunnen worden gevonden aan de hand van de verkregen identiteit. Dat wil natuurlijk niet zeggen dat bij strafrechtelijk onderzoek deze bescherming niet opengebroken kan worden, zoals in de 'Campina-afpersing' zaak.[159] De gebruiker kan afhankelijk van zijn behoefte en de mogelijkheden binnen het informatiesysteem de IDP zo instellen, dat bij rechtmatig gebruik zijn identiteit, niet vrijgegeven wordt. Hij kan ook de IDP zodanig instellen, dat zijn identiteit alleen vrijgegeven wordt aan bepaalde dienstverleners. De IDP kan de identiteit van de gebruiker afschermen van zowel medegebruikers als van diensten die binnen het informatiesysteem geleverd worden. De koppeling tussen het identiteitsdomein en de pseudo-identiteitsdomeinen kan worden gemaakt indien dit noodzakelijk is voor het verwerkingsproces en hierin bij het ontwerp van het informatiesysteem is voorzien.[160]

Omdat in veel gevallen een informatiesysteem verschillende soorten gebruikers kent die slechts een beperkt aantal gegevens mogen inzien, kan de IDP verschillende pseudo-identiteitsdomeinen tot stand brengen. In ieder pseudo-identiteitsdomein wordt dan een deel van de informatie over een persoon verwerkt. De IDP kan ook tussen de gebruiker en verschillende informatiesystemen worden geplaatst, waardoor er per informatiesysteem een pseudo-identiteitsdomein wordt gecreëerd. Van Rossum e.a. geven als voorbeeld:

> "The service provider, say a hospital or doctor, wants to check whether a patient is insured for a particular treatment. The hospital and the insurance company know the patient by different pseudo-identities. Via the identity protector, which can translate pseudo-identities, the hospital can determine what coverage the patient has for which treatments."[161]

159 LJN: AR6799, Gerechtshof Amsterdam, datum uitspraak: 30-11-2004.
160 Koorn, e.a., 2004, p.32-35.
161 Van Rossum, e.a., 1995 p.17-18.

De IDP draagt op vier manieren bij aan de versterking van de bescherming van de persoonlijke levenssfeer:

1. Hij kan de identificeerbaarheid voorkomen of verminderen.
2. Hij kan ingesteld zijn op het voorkomen van de verdere verwerking van persoonsgegevens.
3. Hij kan gericht zijn op het ondersteunen van de privacyrealisatiebeginselen zoals besproken in hoofdstuk 2.
4. Hij kan de controle van het individu vergroten over zijn eigen persoonsgegevens.[162]

In de praktijk is een IDP een deel van een programma dat op een server kan staan. In het informatiesysteem kan de IDP gerealiseerd worden in de vorm van, bijvoorbeeld: een aparte functie geïmplementeerd in het informatiesysteem of informatieproces. Ook kan de IDP een apart informatiesysteem zijn, dat onder controle van de gebruiker of de burger (bijvoorbeeld via een smartcard) staat of onder controle staat van een door de dienstverlener (bijvoorbeeld de overheid) en de gebruiker vertrouwde partij (trusted third party of TTP).[163]

Samenvattend: De identiteitsbeschermer biedt de volgende functionaliteiten:

1. Melding van en controle met betrekking tot de vrijgave identiteit.
2. Het maken van pseudo-identiteiten op basis van de echte identiteit.
3. Het omzetten van pseudo-identiteiten in identiteiten, en vice versa.
4. Het omzetten van pseudo-identiteiten in andere pseudo-identiteiten.
5. Het koppelen van de pseudo-identiteit en de echte identiteit.
6. Het creëren van identiteit- en pseudo-identiteitsdomeinen.
7. Bestrijding van misbruik van de pseudo-identiteiten.[164]

Gezien de belangrijke functies van de identiteitsbeschermer is het van groot belang dat er zorgvuldig met de identiteitsbeschermer wordt omgesprongen. De autorisatie en authenticatie van personen is dan ook een kritisch proces om de effectieve werking van de identiteitsbeschermer te waarborgen. Het authenticeren kan bijvoorbeeld gebaseerd worden op een digitaal certificaat. De identiteitsbeschermer is tot nu toe beschreven als een abstracte functionaliteit, of anders gezegd een 'black-box' waarmee de ontwerper in staat is het informatiesysteem zodanig te modelleren, dat de identiteit van de gebruiker wordt afgeschermd en alleen voor bepaalde functies beschikbaar komt. De ontwerper wordt, bij de realisatie en implementatie van de identiteitsbeschermer, niet beperkt in zijn keuze voor het toepassen van speciale technieken. Hij kan in zijn ontwerp bijvoorbeeld gebruik maken van (blinde) digitale handtekeningen,[165] 'trusted third parties'

162 Klaver, e.a., 2002, p. 43.
163 Hes & Borking, 2000, p. 23.
164 Hes & Borking, 2000, p. 23.
165 Chaum, 1992, p. 96-101.

(TTPs),[166] en het gebruik van digitale certificaten ('credentials').[167] Om privacyinbreuken te voorkomen moet natuurlijk de identity protector wel betrouwbaar zijn, dus gecontroleerd worden. Dat kan geschieden door een organisatie (bijvoorbeeld Europrise)[168] die certificaten afgeeft waarin de betrouwbaarheid van de identity protector wordt gegarandeerd na het uitvoeren van een evaluerende privacyaudit.[169]

5.9. Fraudebestrijding door IDP

Eén van de meest gehoorde bezwaren tegen de IDP is dat deze bedrog of misbruik door de gebruiker mogelijk maakt doordat zijn identiteit is afgeschermd. Dit kan evenwel op een aantal manieren voorkomen worden, door gebruik te maken van de door Chaum ontworpen cryptografische detectiemethode. Zo kan dubbel gebruik van unieke digitale identiteiten worden voorkomen c.q. onmogelijk worden.[170] Chaum gebruikte deze methode voor het eerst om digitaal geld te maken dat slechts een keer uitgegeven kan worden. De eerste mogelijkheid om bedrog te voorkomen is de IDP zodanig te construeren, dat het voor de gebruiker niet mogelijk is misbruik te maken van zijn anonimiteit of pseudonimiteit. Een andere mogelijkheid gaat uit van een combinatie van detectie en correctie. De IDP constateert wanneer de gebruiker misbruik of onjuist gebruik maakt (probeert te maken) van zijn anonimiteit. Op het moment dat de IDP dit constateert, kunnen maatregelen worden genomen 'tegen' de gebruiker. Enkele maatregelen zijn: identiteit vrijgeven aan de betrokken dienstverlener, identiteit vrijgeven aan de wetshandhavende instantie (bijvoorbeeld het OM) of de handeling blokkeren. Wanneer misbruik of onjuist gebruik door de IDP wordt geconstateerd, is het noodzakelijk dat de IDP de gebruiker door middel van een signaal of mededeling waarschuwt en op de consequenties van zijn handeling wijst, namelijk het vrijgeven van zijn identiteit aan met name genoemde derden (bijvoorbeeld aan Justitie).[171].

Hes & Borking[172] geven als voorbeeld een IDP die constateert dat een gebruiker misbruik probeert te maken van zijn anonimiteit waarna de IDP de gebruiker corrigeert. Een consument verschaft zich door tussenkomst van een intermediair (bijvoorbeeld een 'digitale' notaris) toegang tot een bepaalde dienst. De intermediair treedt op als IDP. De dienstverlener wil de verleende dienst afrekenen en stuurt de rekening naar de intermediair. De intermediair ('identity broker') stuurt,

166 Duthler, 1998. Duthler heeft een uitvoerig onderzoek naar juridische modellen voor trusted third parties gedaan.
167 Brands, 2000.
168 www.european-privacy-seal.eu/about-europrise/fact-sheet.
169 Een voorbeeld hiervan is de Nederlandse meta-zoekmachine Ixquick (www.ixquick.com) (zie hoofdstuk 6).
170 Chaum, 1992, p. 96-101.
171 Hes & Borking, 2000, p. 30.
172 Hes & Borking, 2000, p. 30.

op zijn beurt, de rekening door naar de gebruiker. Wanneer de consument niet betaalt zal de dienstverlener bij de intermediair aandringen op betaling. Wanneer de gebruiker weigerachtig blijft, heeft de intermediair een aantal mogelijkheden om de gebruiker te benaderen. Een van de mogelijkheden is dat de intermediair, na toepassing van cryptografische technieken, de identiteit van de consument vrijgeeft aan de dienstverlener. De dienstverlener kan op deze manier direct of met behulp van een incassobureau contact zoeken met de consument. Een andere mogelijkheid is dat de intermediair zelf of met behulp van een incassobureau contact zoekt met de gebruiker om erop toe te zien dat de gebruiker alsnog betaalt. Voordat zijn identiteit wordt prijsgegeven moet de gebruiker altijd in de gelegenheid worden gesteld om aan te tonen dat hij goede redenen heeft niet te willen betalen (bijvoorbeeld hij heeft defecte goederen ontvangen) of om aan te tonen, dat hij ten onrechte wordt beschuldigd van misbruik. Het kan bijvoorbeeld mogelijk zijn dat de gebruiker de eerste rekening niet heeft ontvangen.[173]

Uit de uitspraak van het Gerechtshof te Amsterdam in 2004 in de strafzaak over afpersing van Campina blijkt, dat de anonimiteit die door de Internet provider www.surfola.com via een *anonymizer* wordt gegarandeerd niet waar werd gemaakt. De afperser maakte gebruikt van deze ISP die in zijn voorwaarden op de website belooft de anonimiteit van de gebruiker te waarborgen. De tekst luidt:

> "Prevent sites from tracking you! Surfola's Stealth Mode prevents others from knowing where you surf! Web sites, advertisers, ISPs, and employers can all watch what you do on the net. Surfola lets you protect your privacy."[174]

Het Internetbedrijf zegt nog steeds (in 2008) de privacy te waarborgen tegen 'tracking', maar er is nergens een certificaat te vinden dat dit ook uit testen blijkt waar te zijn. Ondanks deze pretentie werd de identiteit van de dader toch (via de FBI) bij Surfola achterhaald, hetgeen leidde tot een veroordeling van tien jaar.[175] Het hof overwoog dat:

> "Als – in het ongunstigste geval, hetgeen op grond van het vertrouwensbeginsel niet aanwezig mag worden verondersteld – de FBI inderdaad met voorbij gaan aan wettelijke regels over het internetadres van verdachte de beschikking heeft verkregen, dan betekent dat naar het oordeel van het hof en tegen de achtergrond van de belangen die op het spel stonden, zo'n geringe inbreuk op de privacy van verdachte dat daaraan geen gevolgen voor de ontvankelijkheid van het OM, de toelaatbaarheid van enig bewijs (verdachte heeft vrijwel onmiddellijk bekend dat hij zich van het met behulp van de FBI achterhaalde internetadres bediende) of in de sfeer van de straftoemeting verbonden zouden moeten worden."[176]

---

173 Van Rossum, e.a., 1995, p. 18-19.
174 www.surfola.com : "privacy surfing (…) and more".
175 *LJN*: AR6799, Gerechtshof Amsterdam uitspraak: 30 november 2004, Parketnummer: 21-001971-04.
176 Overweging 3 van het vonnis van het Gerechtshof Amsterdam uitspraak: 30 november 2004.

5.10. Management van (deel)identiteiten

De consequentie van PET en het gebruik van een IDP is, dat elke keer wanneer een gebruiker in een privacyveilig informatiesysteem inlogt er een IDP moet worden aangemaakt. Deze IDP mag (afhankelijk van de behoefte van de gebruiker) in principe niet dezelfde zijn als de IDP die al elders is gebruikt. Dit om profiling en traceerbaarheid te voorkomen. De gevolgen van het gebruik van een IDP laat zich niet alleen voor de gebruiker, maar ook in organisaties voelen.

Vandaar, dat het beheer van identiteiten, het Identity Management (IM)[177] een onontkoombare en belangrijke ontwikkeling is naast PET. Organisaties die in de cyberwereld willen functioneren zullen zich zo moeten inrichten, dat zij hun diensten toegankelijk maken voor een brede laag van gebruikers. Om online transacties met hun leveranciers, klanten, werknemers en bedrijfspartners direct af te handelen is een IM-systeem voor een organisatie onvermijdelijk. Ook de eindgebruikers zullen een IM-systeem nodig hebben om controle te houden over hun vele online identiteiten.[178]

IM-systemen worden geconfronteerd met belangrijke privacykwesties. Gebruikers kunnen zich gaan afvragen: wie beheert mijn netwerkidentiteit, wanneer en welke keuze moet ik maken om te bepalen aan wie ik mijn netwerkidentiteit geef? IM-systemen waarin PET wordt toegepast, vereisen technologieën die het gebruikers mogelijk maken om de afgifte van persoonlijke informatie en de koppeling van die informatie binnen verschillende IM-systemen onder controle te houden.[179] Bij het ontwerp van privacyveilige informatiesystemen moet dan ook een robuust identiteitsbeheersysteem meegenomen worden.

Iedereen bezit inmiddels in onze informatiemaatschappij vele (deel)identiteiten[180] en daarop gebaseerde digitale identiteiten[181] ('accounts') (zie figuur 5.6), waarvan de authenticatiegegevens zoals wachtwoorden of pincodes moeten worden onthouden of moeten worden toegepast zoals bijvoorbeeld biometrische kenmerken. De hoeveelheid digitale identiteiten zal per persoon in de komende jaren sterk toenemen zodat gebruikers (maar ook organisaties) een nog grotere behoefte zullen krijgen aan technische middelen voor het privacy veilig beheren van hun identiteiten en de daarbij behorende authentificatiegegevens. De term digitale identiteit wordt gewoonlijk gebruikt met betrekking tot twee met elkaar samenhangende concepten: Nyms en Partial Identities.[182] Wanneer gebruikers een interactie aangaan met andere partijen, dan kunnen zij verschillende 'nyms'

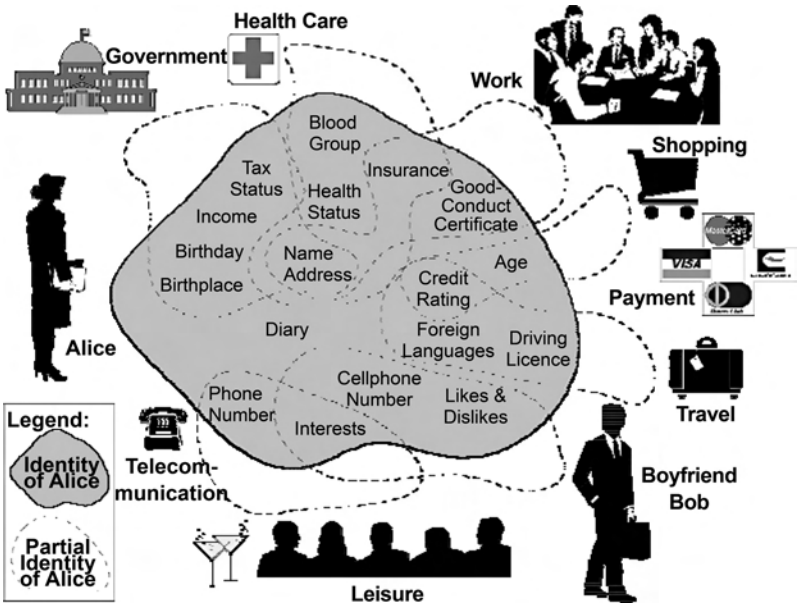
177 Baladi, e.a., 2006: "Identity and Access Management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources".
178 Herreweghen, e.a., 2003, p. 5-6.
179 Pfitzman, e.a., 2002.
180 Hansen, Schwartz & Cooper, 2008, p. 38: "The identity of an individual is a complex entity with many facets. In each situation only subset of this complete identity is needed – in essence, a partial identity. Individuals learn to manage their partial identities intuitively, telling others only what they are willing to disclose and separating contexts from each other where appropriate."
181 Clauß & Köhntopp, 2001, p. 206. Digital representations of partial identities are data sets comprised of attributes and identifiers.
182 Samarati, Damiani, & De Capitani di Vimercati, 2002, p. 4-5.

inzetten.[183] Elke 'nym' geeft een gebruiker een identiteit waarmee hij kan handelen. Nyms kunnen sterk aan een fysieke identiteit gerelateerd worden (dat wil zeggen: er bestaat een partij of een combinatie van verschillende partijen die het nym kunnen verbinden met een individu) of nyms hebben slechts werking binnen een bepaald systeem of zelfs voor één enkele transactie. Er zijn ook nyms die als zwak verbindend of niet identificerend kunnen worden gekwalificeerd en die bijvoorbeeld in 'peer-to-peer' informatie-uitwisselingsystemen worden gebruikt. Bij deelidentiteiten hebben gebruikers verschillende geassocieerde eigenschappen (bijvoorbeeld: naam, leeftijd, creditkaart, beroep, etc.). Elke subset van de eigenschappen vertegenwoordigt een deelidentiteit van de gebruiker. De deelidentiteit kan al dan niet met de werkelijke identiteit van de gebruiker worden geassocieerd.

In figuur 5.6 worden de deelidentiteiten van Alice vermeld. De wolk in het midden van deze figuur geeft de gehele identiteit van Alice weer en bevat persoonlijke informatie die binnen bepaalde groepen gedeeld wordt. De grenzen zijn met stippellijnen aangegeven. Deze grenzen geven een gedeelte van de identiteit van Alice aan. Voor elk gedeelte van de identiteit kan Alice voor een pseudo-identiteit kiezen. Figuur 5.6 geeft tien specifieke domeinen van activiteit weer, waarbinnen Alice een gedeelte van haar identiteit prijsgeeft. Alleen Alice kan alle attributen van haar identiteit samenvoegen. In dit voorbeeld kan Alice dus tien pseudo-identiteiten hebben. Om de juiste identeitsinformatie bij het juiste domein te houden is identiteitsmanagement nodig.

183 Berne, 1966, p. 69-181. De keuze van de nyms kan leiden tot leiden tot een voorspelbare uitkomst van de transactie.

Figuur 5.6: Voorbeeld van digitale (deel) identiteiten, Clauß & Köhntopp (2001) p. 207.

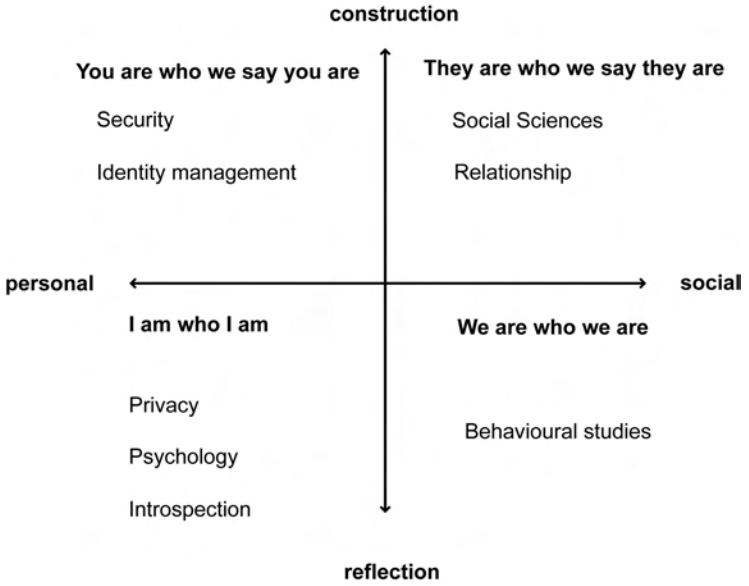


Omgekeerd zullen gebruikers ook privacybeschermende middelen nodig hebben wanneer zij digitaal door andere gebruikers of automatisch door informatiesystemen worden benaderd. Nu al beschikken veel gebruikers over een filtermechanisme om spam, e-mail of ongevraagde telefoongesprekken te blokkeren. De huidige digitale netwerken kunnen de authenticiteit niet garanderen en zonder het gebruik van een IDP is identiteitsdiefstal relatief gemakkelijk. In de digitale wereld is een van de meest belangrijke privacyzorgen de traceerbaarheid ('linkability'). Systemen die methodes voor authentificatie, integriteit en onloochenbaarheid ('non-repudiation') steunen, zoals digitale handtekeningen kunnen ongemerkt en onbevoegd gebruik van digitale identiteiten verhinderen.

Gebruikers laten, wanneer zij geen beschikking hebben over een IDP bij gebruik van het internet of andere digitale netwerken ongemerkt gegevenssporen achter en zonder IDP kunnen zij dit niet verhinderen. Ter bescherming van de persoonlijke levenssfeer zouden gebruikers zich moeten kunnen wapenen tegen ongewilde profilering door organisaties die hun persoonsgegevens beheren. De consequentie van het recht op informatiezelfbeschikking impliceert dat gebruikers feitelijk in staat moeten worden gesteld zelf te bepalen waar, wanneer en door wie welke persoonsgegevens worden opgeslagen, wanneer men het internet bezoekt of zijn

mobiele telefoon, pc of 'personal digital assistant' (PDA) gebruikt. De enige manier tot nu toe is gebruik te maken van technieken die de anonimiteit of pseudonimiteit van het individu verzekeren. Voor elke situatie zou een eigen gekozen (pseudo)identiteit kunnen worden gebruikt.[184] In figuur 5.7 is privacy en identiteitsbeheer gepositioneerd ten opzichte van de samenleving. Privacy staat voor 'I am who I am' en identity management en beveiliging worden weergegeven door 'you are who we say you are'.

Figuur 5.7: De positionering van Identity Management, Cofta, 2009.



De idee van het identiteitsbeheer beoogt de gebruiker in staat te stellen om in verschillende situaties onder verschillende identiteiten te handelen. Bij gebrek aan identificeerbare persoonsgegevens kan een derde niet een telkens wisselende pseudo-identiteit met een gebruiker verbinden. Zo wordt het moeilijker voor derden, zoals webdiensten of reclamebedrijven, om uitgebreide profielen over een gebruiker op te bouwen zonder de toestemming van de gebruiker.[185] Dergelijke identiteitsmanagementsystemen om de verschillende partiële identiteiten aan te maken en te managen zijn nog niet universeel operationeel. Een prototype is

184 Voor het beheren van de verschillende identiteiten is identiteitsmanagement nodig. Identiteitsbeheer is een logisch gevolg van PET.
185 Köhntopp & Pfitzmann, 2004, http://drim.inf.tu-dresden.de/index.html.en.

inmiddels in het PRIME research project[186] ontwikkeld als tegenhanger voor de door de overheid en bedrijfsleven gebruikte identiteitsbeheersystemen die zich over het algemeen richten op bedrijfsprocessen zonder de gebruikers de mogelijkheid te bieden hun persoonsgegevens te managen. De bronsystemen van de identiteitsmanagementsystemen bevatten broninformatie en/of deelinformatie over een digitale identiteit die procesmatig naar andere systemen worden getransporteerd. De meest gebruikte bronsystemen zijn HRM-, CRM- en andere identiteitbevattende systemen (bijv. Gemeentelijke Burger Administraties (GBA) en bedrijvenadministraties). Hansen stelt dat een identiteitsbeheersysteem (IMS) zodanig moet zijn ingericht dat de gebruiker in staat wordt gesteld om zijn recht op informationele zelfbeschikking uit te oefenen.

> "For this purpose it should recognize different kinds of social situations and assess them with regards to their relevance, functionality and their security and privacy risk in order to find an adequate role making and role taking Pseudonyms and credentials, i.e., convertible authorizations, are the core mechanisms for the handling or the representation of identities. The IMS should provide functions for context detection and support the user in choosing the appropriate pseudonym. A log function for all transactions of the IMS should give valuable input to the context detection module and inform the user about past transactions."[187]

In het algemeen wordt er onderscheid gemaakt tussen gecentraliseerde identiteiten ('centralized identity') en gefederaliseerde identiteiten ('federated identity'). De gecentraliseerde identiteiten worden verstrekt door een centrale IMS-provider die als één enkele toegangspoort voor het beheer van de identiteiten van de gebruiker optreedt. De gefederaliseerde identiteiten hebben meerdere IMS-providers. Deze laatste vorm komt steeds meer voor ten gevolge van de toenemende relaties tussen organisaties waardoor ketenintegratie en samenwerkingsverbanden op grote schaal ontstaan.[188] Teneinde processen van met elkaar samenwerkende organisaties op een metaniveau te integreren, is het nodig om zekerheid te verkrijgen over de identiteiten die betrokken zijn bij die processen. Het is echter niet altijd mogelijk om als organisatie alle identiteiten zelf te beheren. Om toch een betrouwbare registratie te verkrijgen, wordt meer en meer vertrouwd op de authenticatie van gebruikers door ketenpartners. Als een ketenpartner betrouwbaar[189] wordt gevonden, dan wordt ervan uitgegaan dat de medewerkers van die partner ook betrouwbaar zijn. Een privacycertificaat zoals dat van Europrise, waaruit dit blijkt is noodzakelijk. De organisatie zal dan ook gaan vertrouwen op de identiteiten die de ketenpartner zelf ook

---

186 Projectnaam: PRIME (Privacy and Identity Management for Europe) Contract No. 507591 Research periode 2004-2008.

187 Hansen, 2003, p. 2.

188 Grijpink, 1997.

189 Duthler, 1998, p. 108. In de behandeling van de juridische eisen waaraan een TTP moet voldoen, hanteert Duthler het betrouwbaarheidscriterium: "de mate waarop een TTP-afnemer zich kan verlaten op de dienstverlening en het informatiesysteem van een TTP". Dit criterium geldt mutatis mutandis ook in relatie tussen ketenpartners.

vertrouwt. Het 'federated identity' mechanisme maakt dat mogelijk. Door toepassing van protocollen als SAML[190] en WSTL[191] kan het identiteitenbeheer wordt overgedragen aan derden.[192] Het gecentraliseerde identiteitsbeheer is gemakkelijker en goedkoper te onderhouden, maar het schept ook een aantrekkelijk doel voor aanvallers[193] en wordt steeds meer beschouwd als niet realistisch. Het spreekt natuurlijk van zelf dat ook deze systemen moeten voldoen aan de wettelijke normen met betrekking tot het beschermen van persoonsgegevens. Voor het ontwerpen van architecturen van een onder controle van gebruikers staande IMS heeft 'The Center for Democracy & Technology' in 2007 'Privacy Principles for Identity in the Digital Age' gepubliceerd.[194] Deze publicatie beschrijft de juridische normen (VS wetgeving en de Europese richtlijnen voor de bescherming van persoonsgegevens) waaraan het IMS moet voldoen.

5.10.1. Het beheer van de levenscyclus van identiteiten

Efficiënte oplossingen van het identiteitsbeheer (IM) vereisen dat ook rekening gehouden wordt met de digitale levenscyclus van nyms en deelidentiteiten. Over het algemeen wordt de levenscyclus van de digitale identiteiten als een opeenvolgend proces gemodelleerd, lopend van het aanmaken van nyms tot de beëindigingfase met daartussen het voortdurend bijwerken en onderhouden. Samarati e.a. wijzen er op, dat een dergelijk sequentieel proces (nog) niet voldoet aan de vereisten die moeten worden gesteld aan veelvoudige betrouwbare identiteiten.[195] Daar moeten onderzoekers nog een sluitende oplossing voor vinden. Eén van de dringende problemen is revocatie van identiteiten. Immers, identiteiten kunnen verouderd of niet van toepassing worden en moeten daarom ingetrokken kunnen worden. Bijvoorbeeld, van een werknemer die een organisatie verlaat, dient automatisch zijn identiteitsinformatie met betrekking tot zijn functie automatisch te kunnen worden herroepen. Uit door mij uitgevoerde privacyaudits is gebleken dat organisaties vaak vergeten de digitale identiteit van de werknemer in te trekken, wanneer deze de organisatie verlaat.[196]

5.10.2. Identity 2.0

Tot nog toe worden identiteiten beheerd door de organisaties die zelf bepalen wie toegang mag hebben tot de applicaties van die organisaties. Daarbij registreert elke organisatie zijn eigen gebruikers. In de huidige internetcultuur is dit niet

190 Security Assertion Markup Language.
191 Web Services Trust Language.
192 DigiD is in Nederland een voorbeeld van federation binnen het overheidsdomein.
193 Hansen, 2003, p. 5.
194 Privacy Principles for Identity in the Digital Age v1.3, Center for Democracy & Technology, Washington DC (July 2007): http://cdt.org/security/20070716idprinciples.pdf.
195 Samarati, Damiani, & De Capitani di Vimercati, 2002, p. 9.
196 www.cbpweb.nl/Pages/pb_20020424_controleauditGBA.aspx.

langer een realistisch uitgangspunt. Niet alleen is het aantal potentiële gebruikers ongekend groot, maar gebruikers en consumenten, willen zelf hun identiteit beheren en zeggenschap hebben over het verstrekken van identiteitgegevens. Die ontwikkeling wordt gestimuleerd door de Web 2.0-gedachte. Voor het identiteitenbeheer betekent dat ondermeer dat sprake is van het User Centric Identity Management. De door Cameron geformuleerde Seven Laws of Identity, beschrijven de basis voor een "unifying identity metasystem", dat kan worden toegepast op het identiteitsgebruik op internet. Cameron stelt, dat:

> "1) Technical identity systems must only reveal information identifying a user with the user's consent; 2) The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution; 3) Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship; 4) A universal identity system must support both 'omni-directional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles; 5) A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers; 6) The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human/machine communication mechanisms, offering protection against identity attacks.; 7) The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies."[197]

De term die voor deze ontwikkeling wordt gebruikt, heet in navolging van Web 2.0 ook wel Identity 2.0.[198]

5.11. Bouwstenen voor privacy- en identiteitsbeheer

Zonder een helder privacybeleid van de organisaties waar het individu mee te maken krijgt wanneer hij binnen internet surft, kan hij onmogelijk weten hoe er met zijn persoonlijke informatie door die organisatie wordt omgegaan. Zijn vertrouwen in organisaties met een onduidelijk of afwezig privacybeleid zal er niet door toenemen. In paragraaf 5.11.1 stip ik het privacybeleid op de website aan met de daarbij voorkomende 'human computer interface' (HCI)problemen. In paragrafen 5.11.2 en 5.12.3 komt de vervolgvraag aan de orde of de website met de daarop gepubliceerde 'privacy policy' doet wat hij belooft. Om zeker te stellen dat de privacy preferenties van het individu ten aanzien van zijn persoonsgegevens worden gerespecteerd, kunnen 'sticky policies' en 'data track' systemen helpen.

---

197 Cameron, 2005.
198 Een goede uitleg van Identity 2.0 is te vinden op YouTube. www.youtube.com/watch?v=RrpajcAgR1E.

5.11.1. Het transparant privacybeleid

Dat organisaties hun privacybeleid op hun website vermelden, is niet bijzonder meer. Het komt helaas veel minder voor, dat het getoonde privacybeleid dient als 'modus operandi' voor de geautomatiseerde gegevensverwerking. Volgens Hansen mankeert er nog heel wat aan, met name wat betreft aan de informatie rond het verkrijgen van de toestemming[199] die vereist is, alvorens de persoonlijke informatie van gebruikers kan worden verwerkt.[200] *Machine-readable* privacybeleid (bijvoorbeeld in het P3P[201] formaat dat door het Consortium van World Wide Web (WWW) wordt gestandaardiseerd) maakt het mogelijk de privacyvoorkeur van de gebruiker automatisch te toetsen aan het privacybeleid van de organisatie. Voordat het zo ver is dat alle organisaties dit gerealiseerd hebben, zal er sprake moeten zijn van 'proven technology' waarvan zeker is dat die niet meer beveiligingsrisico's voor de organisatie oproept. In hoofdstuk 7 zal worden ingegaan op het feit waarom organisaties zo traag en aarzelend de verwerking van persoonsgegevens 'PET proof' maken.

Problemen zijn er ook met betrekking tot het snel toegankelijk en begrijpelijk maken van het privacybeleid in een omgeving van steeds meer connectiviteit. Mobiele telefoons hebben maar uiterst kleine schermen met een gelimiteerde ruimte om privacy boodschappen weer te geven. De opkomst van RFID's[202] en andere geavanceerde sensoren stellen de ontwerpers voor het vraagstuk hoe de gebruiker te waarschuwen voor privacy relevante situaties. Research in het PISA- en PRIME-project heeft zich ondermeer gericht op de hoogst noodzakelijke 'human computer interfaces' (HCI). In een oogopslag moet de grafische (of zelfs multimedia) representatie (digitale hiëroglyfen) van de inhoud van het privacybeleid te begrijpen zijn. Tijd is hierbij een belangrijke factor. Door middel van zeer eenvoudige en snel herkenbare visuele pictogrammen kan voorkomen worden dat gebruikers (als ze dat al zouden doen) lange teksten in juridisch jargon moeten lezen alvorens de beslissing te nemen naar de gewenste website door te klikken. In figuur 5.8 geeft Rundle[203] een voorbeeld van ontwikkelde digitale privacy hiëroglyfen.

---

199 Cfr.Artikel 7 van 95/46/EG.

200 Hansen, 2003, p. 6.

201 The Platform for Privacy Preferences (P3P), www.w3.org/P3P/2004/09-p3p_sw.html#ref-P3P. The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents.

202 Schermer & Durinck, 2005, p. 9 Radio frequency identification (RFID) is een technologie om met behulp van radiosignalen objecten te identificeren en van een afstand informatie op te slaan in en te lezen van zogenaamde RFID-'tags' die op of in objecten zitten.

203 Rundle, 2006, http://identityproject.lse.ac.uk/mary.pdf.

Figuur 5.8: Voorbeeld van digitale privacy hiëroglyfen. Rundle, 2006.

Extract of Creative Commons-like icons (Rundle 2006)

	You agree not to trade or sell this data.
	You agree to make available to me the data that you have on me without my having to pay for it/at a minimal charge.
	You allow me to address inaccuracies in the data and request its removal.
	You agree to take reasonable steps to keep my data secure.
	You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]

Inmiddels zijn in het PRIME-project de eisen voor de functionaliteit voor transparantie geformuleerd. De doelstelling is dat de gebruikers de gegeven informatie moeten kunnen begrijpen en op grond daarvan adequaat moeten kunnen handelen. Dat betekent dat de 'privacy policies' moeten worden getoond waarin de voorwaarden staan hoe de gegevens worden verwerkt. Bovendien moet de betrouwbaarheid van de partijen in de transactie aantoonbaar zijn. Voorgesteld wordt om de historische gegevens te tonen over de betrouwbaarheid van de (commerciële) partij waar zaken mee wordt gedaan. Bijvoorbeeld x% van de bezoekers van deze website zegt dat dit bedrijf zijn verplichtingen nakomt. Het privacybeleid op de website dient een duidelijke ondersteuning is voor het uitoefenen van de privacyrechten van het individu te bieden. Het zou mooi zijn als iemand zijn privacy kan beschermen met gebruik van een pseudoniem. Hansen meent dat informatie moet worden gegeven over het privacyveilig zijn van het netwerk om gegevens te verzenden en dat demonstratiemateriaal (instructie filmpjes) beschikbaar moet zijn om de gebruiker te leren hoe hij met de website om kan gaan, voordat hij werkelijk tot een transactie overgaat. Ook vindt zij dat aan de server-kant er sprake moet zijn van een volledige (maar afgeschermde) logging ten behoeve van het uitvoeren van privacyaudit.[204]

204 Hansen, 2008, www.prise.oeaw.ac.at/.

Bij het testen van IM-systemen dient nagegaan te worden of voldaan kan worden aan de vier 'human computer interface en interaction' (HCI) vereisten (de 4 C's),[205] te weten:

1. Comprehension: bijvoorbeeld: de gebruiker begrijpt wie zijn persoonsgegevens verwerkt en voor welke doeleinden.
2. Consciousness: bijvoorbeeld: de gebruiker weet wat er met zijn persoonsgegevens gebeurt als de bewaartermijn verloopt.
3. Control: bijvoorbeeld: de gebruiker is in staat om de manier waarop zijn persoonsgegevens worden verwerkt te controleren en zijn wettelijke rechten uit te oefenen.
4. Consent: bijvoorbeeld: de gebruiker geeft zijn vrije, ondubbelzinnige en specifieke toestemming aan de verantwoordelijke om zijn gevoelige gegevens te verwerken.

Voor de digitale hiëroglyfen of iconen gelden ook de 4Cs.

5.11.2. Kleefbeleid of Sticky policies

De kritische en privacybewuste websitebezoeker vraagt zich af of de verwerking van persoonsgegevens bijvoorbeeld wel conform de beloofde doelbinding plaatsvindt, wanneer een website optimale privacybescherming aan de bezoeker van de website biedt. Hoe kunnen gegevensverwerkingsystemen waarborgen dat de binding tussen het doel voor de gegevensinzameling en het daadwerkelijke gebruik van de gegevens niet wordt verbroken? Huidige systemen kunnen dat nog niet waarborgen, maar research heeft aangetoond dat door middel van cryptografische technieken privacyvoorkeuren aan de gegevens kunnen worden 'geplakt', zodat organisaties niet kunnen afwijken van de aan de website bezoeker toegezegde manier van gegevensverwerking.[206] De gevolgde aanpak lijkt op het door de muziekindustrie gebruikte digitaal auteursrechtenbeheer (DRM) om ongeoorloofde verveelvoudiging en exploitatie van de inhoud van het auteursrechtelijk werk tegen te gaan. Deze 'sticky policies' of kleefbeleid in gegevensbeheerssystemen kunnen een verwerking waarborgen dat de privacyvoorkeur van de betrokkene (in de zin van 95/46/EG) wordt gevolgd. Het kleefbeleid zorgt er voor dat conform de overeengekomen voorwaarden de persoonsgegevens worden verwerkt, In het informatiesysteem van de verantwoordelijke (in de zin van 95/46/EG) blijven de preferenties van de betrokkene aan de persoonlijke informatie gekleefd, zodat hij er toch op kan vertrouwen dat zijn privacypreferenties worden gerespecteerd.[207]

205 Van Blarkom, Borking & Olk, 2003, p. 254-265 voor een uitvoerige beschrijving van de beginselen van HCI.
206 Kenny & Korba, 2002.
207 Hansen, Schwartz & Cooper, 2008, p. 23.

Karjoth, Schunter & Waidner geven als voorbeeld hoe met deze techniek toestemming per persoon en per 'record' kan worden beheerd.

> "When submitting data to an enterprise, the user consents to the applicable policy and to the selected opt-in and opt-out choices. The form then associates the opt-in and opt-out choices as well as the consented policy with the collected data. This holds even if the data is disclosed to another enterprise."[208]

De 'sticky policy' aanpak maakt de afstand tussen het individu en de verantwoordelijke kleiner, waardoor de mogelijkheid van controle op de verwerking van persoonsgegevens wordt vergroot en het vertrouwen van het individu toeneemt.

5.11.3. Data track

Eén van de veel gehoorde verzuchtingen over de bescherming van persoonsgegevens is, dat burgers, consumenten en gebruikers van informatiesystemen niet weten wat er allemaal over hen wordt verzameld, waar die gegevens blijven en wat anderen over hen (al) weten. Het antwoord op deze vraag is het eerste vereiste voor het vertrouwen in de verwerking van persoonsgegevens en het beschermen van de privacy. Zo is er in het PISA-project voor elke software agent een audit trail ingebouwd. Zo kan men na te gaan aan welke software agent en op welk platform persoonsgegevens van de gebruiker van de software agent zijn uitgewisseld en welke beslissingen er na onderhandelingen tussen software agents zijn genomen.[209] Dat helpt ook bij het vaststellen van de aansprakelijkheid mocht er iets misgaan. Veel verder gaat de nog in de kinderschoenen staande research waar het gegevensspoor van de bezoeker van de website door die bezoeker kan worden opgevraagd. Dit gegevensspoor (*Data Track*) geeft de condities (inclusief de toestemming) waaronder de opslag en verwerking van zijn persoonsgegevens heeft plaatsgevonden aan de bezoeker van Internet weer. Hansen deelt mee, dat:

> "History functions such as the 'Data Track' in the PRIME project store all relevant information from online transactions, including a record of which personal information has been disclosed to whom and under what conditions. The stored data also includes information from the privacy policies of services requesting the data so that users can review it later on to understand what exactly they have consented to."[210]

De *Data Track* verschaft niet alleen transparantie voor gebruikers, maar stelt hen ook in staat om de verantwoordelijken (in de zin van Richtlijn 95/46/EG) later te vragen of zij werkelijk de gegevens zoals beloofd hebben behandeld. In de Europese Unie zou dit kunnen betekenen dat gebruikers hun rechten met

208 Karjoth, Schunter, & M.Waidner, 2003, p. 7.
209 Van Blarkom, Borking & Olk, 2003, p. 192-196.
210 Hansen, Schwartz & Cooper, 2008, p. 23.

betrekking tot hun persoonsgegevens effectief zouden kunnen uitoefenen. Wanneer de gegevens niet conform de wet of conform hun overeengekomen privacypreferentie zijn verwerkt, kunnen zij direct hun toestemming voor verdere verwerking in trekken. Langs dezelfde weg zou wellicht ook een waarschuwingssysteem kunnen worden gebouwd om degene die zijn persoonsgegevens aan anderen heeft toevertrouwd te alarmeren als zijn gegevens niet volgens de overeengekomen afspraken worden verwerkt.[211]

5.12. Privacymanagementsystemen

Een nieuwe loot aan de PET-stam is het privacymanagementsysteem (PMS), dat de verwerking van niet-vercijferde persoonsgegevens doet uitvoeren conform het privacybeleid van de organisatie of de privacywetgeving. In paragraaf 5.12.1 wordt uitgelegd hoe PMS werkt. In paragraaf 5.12.2 wordt het privacy preferences project (P3P) toegelicht, dat aan de basis ligt van PMS. In 5.12.3 wordt gewezen op de juridische vraagstukken die de ontwerper en de jurist bij het inbouwen van wetgeving kunnen tegenkomen. In paragraaf 5.12.4 wordt gewezen op de noodzaak van privacyontologieën en hoe deze tot stand komen. In paragraaf 5.12.5 wordt de '*legal instantiation'* van privacyrealisatie beginselen toegelicht en in paragraaf 5.12.6 de automatische productie van privacyontologieën.

5.12.1. Privacybeleid geautomatiseerd uitvoeren

Zoals eerder in dit hoofdstuk is uiteengezet, is in de periode rond het millennium naast Identity Managementsystemen een nieuwe vorm van PET ontwikkeld die wordt aangeduid als privacymanagementsysteem (PMS). PMS zorgt voor de geautomatiseerde toepassing van privacybeleid ('privacy policy')[212] van een organisatie in het geval het onmogelijk of wettelijk niet toegestaan is om een pseudo-identiteit te gebruiken of te anonimiseren. Het betreft hier programmatuur die als het ware als een schil om de verwerkingsprocessen van persoonsgegevens heen ligt en automatisch toetst of het verwerkingsproces plaatsvindt conform het vastgelegde privacybeleid geldend voor de desbetreffende database of het informatiesysteem. Het PMS zorgt er voor, dat er automatisch een inventarisatie plaatsvindt van persoonsgegevens in de databases van de verschillende 'legacy' informatiesystemen, van de rollen (functies) toegekend in de 'directory services'[213]

---

211 Hansen, Schwartz & Cooper, 2008, p. 24.

212 Karjoth, Schunter & Waidner, 2003, p. 5: "A privacy policy contains three elements. The first element is a header that contains information describing the policy such as a name, an author, and a version. The second element is the declaration that declares the used identifiers, such as PII types, operations, and purposes. The third element is the authorization rules. The authorization rules can express what operations for which purpose by which data user can be performed on a given PII type".

213 Centraal geautomatiseerd informatiesysteem waarin de resources van een organisatie worden vastgelegd vaak in de vorm van rollen (bijvoorbeeld de rol marketing). Directory services worden onder andere gebruikt voor de toegangscontrole (beveiliging) voor bedrijfstoepassingen.

en van de verwerkingsprocessen vastgelegd in de transactie logbestanden. Het privacybeleid en de verwerkingsprocessen worden door middel van een gestandaardiseerde elektronische privacytaal in de PMS-programmatuur ingevoerd.[214] Deze privacytaal werkt met specifieke privacybegrippen, begrippen en daarop gebaseerde ontologieën.[215] In het privacy management systeem worden de volgende privacy parameters gebruikt: 'actor(en)'; 'gegeven(s)' (speciale groepen van gegevens); 'activiteit(en)'; 'conditie(s)', 'doel(en)', 'attributen' en 'verplichtingen'.

Met deze parameters kan een organisatie zijn privacybeleid en de manier van verwerking beheren en modelleren. Bijvoorbeeld: toestemming van de betrokkene kan met een voorwaardelijke parameter worden gemodelleerd. De parameter 'verplichtingen' regardeert de consequenties van een handeling, bijvoorbeeld: informeer per e-mail; betaal € 200. De Rooij[216] geeft een aantal voorbeelden ter verduidelijking van bovenstaande begrippen:

Voorbeeld 1:
Toestemming is een belangrijk concept in de privacywetgeving. Betrokkenen moeten expliciet en ondubbelzinnig toestemming geven alvorens de persoonsgegevens van de betrokkenen voor een specifiek doel mogen worden verwerkt[217]. De toestemming van de betrokkene wordt bijvoorbeeld vastgelegd in een toestemmingenbestand. Dit bestand wordt gecombineerd met de doelbinding die is opgeslagen in een of meerdere informatiesystemen. De inrichting van de verwerking dient zodanig te zijn, dat naleving automatisch wordt afgedwongen. Dit gebeurt door 'privacy statements'.

Een voorbeeld van een 'privacy statement' in het PMS is: (cursief tussen haakjes staan de PMS elementen):

[ABC bank] (*PMS element: actor*) [mag] (*PMS element: conditie*) [klant telefoonnummer] (*PMS element: gegevens*) [openbaar maken] (*PMS element: acties*) aan [XYZ telemarketing dienstverlener] (*PMS element: actor*) voor [het aanbieden van nieuwe diensten] (*PMS element: conditie*) [als klant ABC bank toestemming heeft gegeven voor het telefonisch aanbieden van nieuwe diensten] (*PMS element: conditie*).

---

214 Koorn, e.a., 2004, p. 36-37.

215 Bench-Capon, 2007, p. 69: Bench-Capon refereert voor dit begrip aan Gruber, die en ontology omschrijft als "an explicit conceptualization of the domain".
Een ontologie een hiërarchische datastructuur die alle relevante entiteiten en hun onderlinge relaties en regels binnen dat domein bevat, zoals bij een domeinontologie het geval is. Mulder & Dietz (2002) constateren dat "ontological definitions are based on empirical observation of what a system is, distinct from other observable things. Teleological definitions are based on interpretation of observed behavior of a system". In onderdeel 5.14.4. 'Privacyontologieën' van dit hoofdstuk wordt nader op dit begrip in gegaan.

216 De Rooij, Privacymanagement en Enterprise Privacy manager, Privacy & Informatie, 6e jaargang nummer 5, 2003, blz. 213.

217 Artikel 13 van 95/46/EG bevat uitzonderingen en beperkingen op dit privacyuitoefeningsbeginsel.

Voorbeeld 2:
Een salarisbedrag op zich is een onschuldig gegeven maar gecombineerd met een naam of andere identificeerde gegevens kan een salarisbedrag een gevoelig persoonsgegeven worden. De 'privacy statement' hiervoor wordt: [salarisbedrag] (*PMS element: gegevens*)[mag niet] (*PMS element: conditie*) worden gebruikt in combinatie met [naam of telefoonnummer of adres] (*PMS element: gegevens*).

Privacybeleid en verwerkingsprocessen gedefinieerd en vastgelegd in de hierboven beschreven privacystatements (in specifieke programmeertaal) gaan een integraal deel uitmaken van de geautomatiseerde gegevensverwerking van organisaties. De elektronische privacystatements kunnen ook worden gebruikt om verwerkingsprocessen te controleren en/of de naleving van het privacybeleid in het informatiesysteem te volgen. Zodra het privacybeleid en de verwerkingsprocessen zijn beschreven en in het PMS zijn ingevoerd, worden deze geanalyseerd op tegenstrijdigheden, consistentie, conflicten en overtredingen. In onderstaande figuur 5.9 worden de analysemogelijkheden getoond. In de tabel worden twee privacystatements met elkaar vergeleken en geanalyseerd op tegenstrijdigheden, conflicten en overtredingen. De zesde regel van de tabel toont bijvoorbeeld een overtreding: een verwerkingsproces (privacystatement 1) verwerkt gegevens terwijl dit niet is toegestaan volgens de norm (privacystatement 2).[218]

Figuur 5.9. Analyse van privacy statements * Leeg = heeft geen gevolg. De Rooij, 2003, Nr. 5.

	Privacystatement 1	Waarde	Privacystatement 2	Waarde	Resultaat
1	Verwerkingsproces	Doen (+)	Verwerkingsproces	Doen (+)	Akkoord
2	Verwerkingsproces	Doen (+)	Verwerkingsproces	Niet doen (−)	Conflict
3	Norm	Mag (+)	Norm	Mag (+)	Akkoord
4	Norm	Mag (+)	Norm	Mag niet (−)	Conflict
5	Verwerkingsproces	Doen (+)	Norm	Mag (+)	Support
6	Verwerkingsproces	Doen (+)	Norm	Mag niet (−)	Overtreding
7	Verwerkingsproces	Niet doen (−)	Norm	Mag (+)	Neutraal
8	Verwerkingsproces	Niet doen (−)	Norm	Mag niet (−)	Support
9	Verwerkingsproces	Niet doen (−)	Leeg*	Leeg*	Geen dekking
10	Norm	Mag (+) of Mag (niet) (−)	Leeg*	Leeg*	Geen dekking

218 De Rooij, 2003, p. 216.

Met Support in de tabel wordt bedoeld dat de betreffende bewerking voldoet aan de norm en uitgevoerd mag worden. De bewerking in kwestie wordt 'gesupport' door de norm (het desbetreffende privacyrealisatiebeginsel).

De tabel vergelijkt hier drie zaken:

1. Wordt de norm nageleefd?
2. Zijn normen onderling consistent? En
3. Zijn verwerkingen in de praktijk onderling consistent? Punt 3 kan organisaties helpen te begrijpen wat ze in werkelijkheid met de verwerking van persoonsgegevens doen en waar dingen fout kunnen gaan:

– De norm met de praktijk.
– De ene norm ten opzichte van een andere norm.
– De ene bewerking in de praktijk met een andere bewerking in de praktijk.

Het gevolg kan zijn dat verschillende uitkomsten bij analyse kunnen bestaan. De in de analyse gevonden risico's en 'gaten' (geen dekking) kunnen worden aangepast door privacystatements inhoudelijk aan te passen, door bepaalde privacystatements prioriteit te geven over andere privacystatements, door condities stringenter te definiëren, door het bereik (reikwijdte) van een statement aan te passen en/of door filters toe te passen. Om een sluitende bescherming van persoonsgegevens te verkrijgen is het noodzakelijk PMS tezamen met de IDP te implementeren, om te voorkomen dat bestanden die de verwerking van gegevens registeren niet zelf weer persoonsgegevens bevatten, waarvan de verantwoordelijke met gebruikmaking van PET juist de verwerking probeert te voorkomen.

5.12.2. Platform voor Privacy Preferences Project (P3P)

De basis voor de PMS is gelegd door het Platform for Privacy Preferences Project (P3P). De P3P-standaard is ontworpen door het World Wide Web Consortium (W3C)[219] en maakt het mogelijk dat op een website de bezoeker duidelijk wordt gemaakt welke persoonsgegevens worden verzameld en op welke wijze de gegevens zullen worden gebruikt. Voor de website bezoeker is P3P[220] een hulpmiddel om op eenvoudige en gestandaardiseerde wijze over zijn privacyvoorkeuren te communiceren in een voor het informatiesysteem leesbare vorm. Binnen P3P wordt aangegeven wie de gegevens verzamelt, verwerkt en opslaat; welke gegevens worden verzameld en met welk doel ze worden verwerkt; of er opt-in en opt-out alternatieven zijn; aan wie de gegevens worden verstrekt; tot welke gegevens de verantwoordelijke toegang heeft; welke bewaarperiode voor de persoonsgegevens van kracht is; hoe conflicten over het privacybeleid van de

219 Karjoth, Schunter & Waidner, 2003, p. 3.
220 www.w3.org/P3P/ en P3P and Privacy – Center for Democracy & Technology/IPC Ontario www.cdt.org/privacy/pet/p3pprivacy.shtml.

verwerkende organisatie worden opgelost of beslecht; en waar het privacybeleid op de website te vinden is.

Op deze wijze wordt de transparantie over de gegevensverwerking voor de gebruiker sterk verhoogd. De internetgebruiker vult online een formulier in waarin de gebruiker zijn/haar privacyvoorkeuren vastlegt. Vervolgens kan deze gebruiker door feedback bij ieder website bezoek (mits P3P wordt toegepast) vaststellen of zijn/haar preferenties door het privacybeleid van de organisatie worden gerespecteerd. Op grond van de feedback kan hij beslissen of hij inderdaad de website gaat bezoeken.[221] Overigens is een dergelijke toepassing ook bruikbaar voor systemen die niet via internet verlopen, maar wel gebruikmaken van internettechnologie.[222]

Voor het definiëren van privacystatements zijn inmiddels praktische hulpmiddelen verkrijgbaar, bijvoorbeeld de Enterprise Privacy Authorization Language (EPAL). Daarnaast zijn ook de talen: APPEL, EPML, OWL, RDF, RDFS, RDQL en SWAPPEL[223] ontwikkeld, die allemaal hun eigen toepassing hebben. SWAPPEL wordt bijvoorbeeld gebruikt voor de specificatie voor privacypreferentieregels voor P3P, evaluatie van privacybeleid en voor de uitwisseling van privacypreferenties.[224] Verschillende softwareleveranciers hebben inmiddels privacymanagementsystemen ontwikkeld die de verwerkingen conform de vooraf gedefinieerde privacyregels laten plaatsvinden. Nadat in het PMS het door de organisatie vastgestelde privacybeleid is ingevoerd, vindt vervolgens de integratie met de verwerkingsprocessen plaats. Bij invoer van nieuwe verwerkingsprocessen en gegevens wordt automatisch geanalyseerd of het verwerkingsproces wordt gedekt door het eerder vastgestelde privacybeleid. Bovendien wordt vastgesteld of de verwerkingsprocessen van de verschillende organisatieonderdelen consistent zijn. De functionaliteiten kunnen worden uitgebreid naar de bewerkers, opt-in management en geautomatiseerde handhaving van het privacybeleid of de wetgeving.

Met behulp van logging en controle kan achteraf worden vastgesteld of het geïmplementeerde PMS adequaat functioneert. Hiervoor is het belangrijk om alle handelingen met betrekking tot persoonsgegevens die onder toezicht van de verantwoordelijke plaatsvinden, vast te leggen en te controleren. Een voorbeeld hiervan is om op persoonsniveau vast te leggen aan welke organisaties gegevens zijn verstrekt (inclusief waarom en wanneer). Er ontstaat daardoor een 'audit trail' (wie deed wat, wanneer, waar en waarom) waardoor de bewerkingen controleerbaar zijn en er vastgesteld kan worden of het privacybeleid wordt opgevolgd en de genomen PET-maatregelen goed werken. Met de regelmatige analyse van de logbestanden kunnen 'lekken' in PMS worden opgespoord en vervolgens gedicht worden. Op deze wijze draagt ook logging en controle bij tot het voorkomen van onrechtmatige verwerking van persoonsgegevens.

---

221 Koorn, e.a., 2004, p. 36-37.

222 Bijvoorbeeld door gebruik van het internet TCP/IP-protocol binnen de organisatie of over gesloten netwerken tussen organisaties of binnen een intranet.

223 Zie voor een verklaring van de afkortingen het afkortingen register in dit boek.

224 www.w3.org/P#P/2004/09-p3p_sw.html#ref-SWAPPEL.

Een bijkomend voordeel van logging en controle is dat voldaan kan worden aan de informatieplicht naar de burger/consument. Een burger kan aan een organisatie vragen welke gegevens de organisatie over hem heeft vastgelegd en aan wie deze informatie is verstrekt. Met behulp van de logbestanden kan de organisatie aantonen dat de informatie in het geheel niet is verstrekt of dat de informatie alleen maar is verstrekt aan geautoriseerde instanties of personen. Het is van belang dat de logbestanden niet gemanipuleerd kunnen worden, waardoor onbevoegden sporen zouden kunnen uitwissen. De logbestanden moeten wel afgeschermd blijven. Daarnaast moeten de logbestanden periodiek worden beoordeeld door bijvoorbeeld de beveiligingsfunctionaris of de functionaris gegevensbescherming (privacy officer), en moet het management hierover periodiek worden geïnformeerd. Een belangrijk aandachtspunt bij logging en controle is dat de logbestanden natuurlijk ook PET-proof moeten zijn.

Uit ervaring in Canada blijkt dat privacymanagementsystemen het vertrouwen van de burger aanzienlijk vergroten en het inzicht van het management in de verwerking en controle van gegevens doen toenemen. Vooral de geautomatiseerde handhaving is een belangrijk pluspunt en voorkomt kostbare privacyaudits om de naleving te controleren.[225]

5.12.3. Juridische vraagstukken bij het inbouwen van wetgeving

Het in dit hoofdstuk vermelde PISA-project[226] had naast de toepassing van de traditionele PET-componenten, zoals 'identity protectors' en het scheppen van domeinen van anonimiteit en pseudonimiteit, als een van de ambitieuze doelstellingen de privacywetgeving in mobiele[227] software agents te implementeren. Hiermee wordt voorkomen dat persoonsgegevens door andere agenten en platforms zouden worden verwerkt in strijd met de privacywetgeving en de privacypreferenties van de betrokkene, die de agent met een specifieke opdracht op het internetpad had gestuurd.[228] Deze ambitie had tot gevolg dat in de mobiele software agents niet alleen beslissing-, planning-, onderhandeling- en leereigenschappen moesten worden ingebouwd, maar ook de privacyrealisatie beginselen (zie hoofdstuk 2) en met name de eisen die gelden voor toestemming.[229] Speciale aandacht kreeg de beveiliging tegen aanvallers.

---

225 De Rooij, 2003, p. 206-212.

226 EU Projectnummer: IST-2000-26038; Projectnaam: PISA – Privacy Incorporated Software Agent, Building a Privacy Guardian for the Electronic Age; Onderzoeksperiode:1999-2003.

227 Borking, Van Eck & Siepel, 1999, p. 11. Mobiliteit refereert aan de mogelijkheid dat deze agenten zich kunnen bewegen vanuit de PC binnen netwerken. Zie ook Schermer, 2007, p. 24.

228 Van Blarkom, Borking & Olk, 2003, p. 142.

229 Artikelen 2 en 7 van de Richtlijn 95/46/EG vereisen een toestemming, die "freely" (artikel 2h), "specific"(artikel 2h), "informed" (artikel 2h), "unambiguously" (artikel 7a) en "explicit" (artikel 8 lid 2 a).

Wanneer het gaat om innovatieve technologie doen zich een aantal juridische vraagstukken voor, die nog niet eerder geduid zijn.[230] In het PISA-project moest uitgezocht worden of :

1. de software agent als gebruiker van de door hem verzamelde persoonsgegevens zelf als verantwoordelijke of bewerker gekwalificeerd wordt;
2. een agent zelf een betrokkene ex artikel 2a van de Richtlijn 95/46/EG kan zijn;
3. de vereiste toestemming voor de verwerking van persoonsgegevens door de agent zelf en/of namens de gebruiker van de agent kan generiek worden verleend;[231]
4. de wettelijke verplichtingen van de verantwoordelijke door zijn software agent kunnen worden uitgevoerd;
5. gezien de autonomie van de mobiele software agent aan hem een (juridische) persoonlijkheid kan worden toegekend;[232]
6. er bij de wetgever op aangedrongen moet worden op langere termijn aan een software agent een slavenstatus toe te kennen;
7. de software agent vergelijkbaar is met de slaaf als rechtsobject in het Romeinse Recht, die net als een software agent overeenkomsten kon sluiten en bezit kon verkrijgen waarvan de 'possessio naturalis' en de 'naturalis obligatio' erkend werden?[233]
8. het haalbaar was om door middel van privacyontologieën (de ingebouwde juridische know how) tijdens de werkzaamheden van de software agent de wettelijke privacy aspecten af te dwingen.

De (tentatieve) antwoorden op deze vragen waren direct van invloed op de te ontwerpen architectuur voor de mobiele software agent in het PISA-project. Voor de onderzoekers in het PISA-project was een extra moeilijkheid, dat er nog maar zeer weinig jurisprudentie over de interpretatie van de richtlijn 95/46/EG voor handen was. Bovendien:

> "problems that are due to changes in the law are well-known in conventional data processing: changes in tax law, for example, must be announced well in advance of coming into effect to ensure there is sufficient time for the considerable task of altering programs which have to apply these laws in payroll and other applications".[234]

Konden privacyontologieën aan deze problemen het hoofd bieden?[235] In hoofdstuk 6 wordt dieper op het PISA-project ingegaan.

---

230 Borking & Foukia, 2008, p. 7. www.theprivacynetwork.org/SSN/PrivacyTech/PET/default.aspx.
231 In hoofdstuk 6 wordt hierop ingegaan.
232 Solum, 1992.
233 Van Oven, 1948, p. 439.
234 Van Blarkom, e.a., 2003, p. 187.
235 Bench-Capon, 2007, p.70.

5.12.4. Privacyontologieën

Tussen enerzijds de privacywetgeving met de toezichthouder en anderzijds de verwerking van de persoonsgegevens met de organisatie, de burger/consument en informatiesysteem, bestaat een gaping wat betreft het voldoen aan de wetgeving. Deze gaping wordt gedeeltelijk overbrugd door het implementeren van privacybeleid en het doen van privacy-audits. Om de gaping geheel te overbruggen zijn privacyontologieën noodzakelijk, die de privacywetgeving in een algemeen conceptueel model vertalen, waardoor de wetgeving in informatiesystemen kan worden ingebouwd.[236] In paragraaf 4.11 van dit boek is een (domein)ontologie[237] beschreven als een formele hiërarchische gestructureerde en gedetailleerde beschrijving van tussen experts gedeelde kennis over een bepaald kennisgebied. Het is de bedoeling een abstract conceptueel model te creëren, dat kan worden geïmplementeerd in online of offline informatiesystemen en dat (semi)automatisch kan worden toegepast. Een privacyontologie is het product van een poging een uitputtend en strikt conceptueel schema te formuleren over het kennisdomein betreffende privacy. Het bevat een hiërarchische datastructuur met alle relevante entiteiten en hun onderlinge relaties en regels binnen het privacydomein.[238]. Hameed, Sleeman & Precee menen dat het ontwerpen van ontologieën moeten zijn gebaseerd op een consensusproces.[239] Daarbij is de stabiliteit van de normen binnen een domein van groot belang. Binnen het kennisdomein betreffende de bescherming van persoonsgegevens is in het PISA- en PRIME-project gekozen voor de in hoofdstuk 2 besproken privacyrealisatiebeginselen, want:

> "The privacy principles have been broadly accepted over a period of more than 20 years and, therefore, considered stable enough to be implemented in information systems".[240]

Voordat de bouw van de softwarecomponenten van IMS (identitymanagementsystemen) en PMS (privacymanagementsystemen) kan beginnen, is een grondige inbreng van ontwikkelaars, privacyjuristen, privacyontologen en eindgebruikers vereist om tot een werkbare privacyontologieën en adequaat 'rule based' systeem te komen. Het is bijvoorbeeld van groot belang dat alle 'browsers' privacyinformatie op een semantisch eenvormige manier worden weergeven. Dat is nuttig voor de transparantie en maakt de aansprakelijkheid van de verantwoordelijke

---

236 CEN/CWA 15263 – 2005 item 7.8.
237 Bench-Capon, 2007, p. 72-73: "lightweight, upper or top, core or domain and application ontologies".
238 T. R. Gruber. 1995, p. 907-928: "In the context of knowledge sharing, I use the term ontology to mean a *specification of a conceptualization*. That is, an ontology is a description (like a formal specification of a program) of the concepts and relationships that can exist for an agent or a community of agents. This definition is consistent with the usage of ontology as set-of-concept-definitions, but more general. And it is certainly a different sense of the word than its use in philosophy".
239 Hameed, Sleeman & Preece, 2001: "The paper is based on the principle that it is not possible to automate the entire process of ontology capture".
240 Van Blarkom, e.a. 2003, p. 173.

voor de gepresenteerde informatie aan de bezoekers van een website beheersbaarder. Browsers zouden bijvoorbeeld moeten kunnen aangeven welk niveau van privacybescherming het privacybeleid van de website biedt en wie degenen zijn die de persoonlijke informatie hebben ontvangen. De EU Richtlijn (95/46/EG) vereist dat de gebruiker bepaalde informatie over de uit te voeren gegevenstransactie krijgt, alvorens hij de transactie uitvoert. Om te bereiken dat de gebruikte begrippen eensluidend zijn, zodat er geen verwarring ontstaat,[241] kunnen er twee methoden worden gebruikt. Of er is een gezaghebbend orgaan, dat door de experts in een kennisdomein wordt erkend, dat de ontologieën aan de belanghebbenden voorschrijft (bijvoorbeeld als gevolg van een wet), of de ontologieën worden van onderaf geformuleerd door middel van het bereiken van consensus tussen de experts van het kennisdomein. Het gaat er dan vooral om de achtergronden en de procedurele kennis uit het privacykennisdomein in de ontologieën te incorporeren. Het proces van kennisvergaring over een domein is moeilijk.[242] Het gaat vaak om kennis die nergens tot dan toe is vastgelegd. Juist omdat men hiermee nog weinig ervaring heeft, is het individueel testen van de verkregen resultaten door de eindgebruiker vereist. Voor het vastleggen van waardevolle en unieke informatie uit het specifieke kennisgebied worden technieken uit de cognitieve wetenschap en de psychologie gebruikt en wordt er gewerkt met gebruikersscenario's binnen het kennis domein.

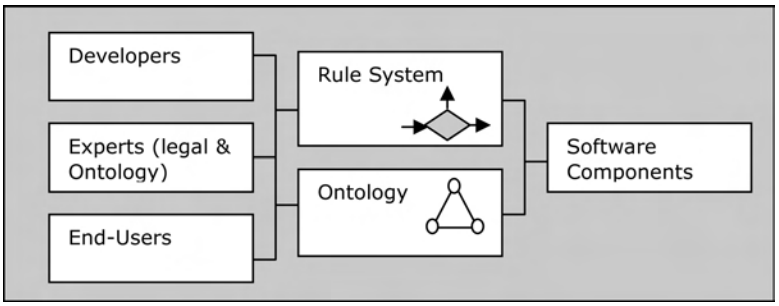
In het PISA- en PRIME-project heeft een uitvoerige analyse van privacyrichtlijnen plaatsgevonden, waarna verdere analyse van de wetsteksten is gebruikt om hogere niveauconcepten of principes te extraheren. Uiteindelijk leidt dit proces tot een reeks kandidaatontologieën, die door een kleine groep deskundigen besproken en aangepast worden. Vervolgens worden deze kandidaatontologieën weer ter beoordeling voorgelegd aan een grotere groep 'stakeholders' om te zien welke ontologieën het beste binnen het kennisdomein passen. Het te ontwerpen regelsysteem waaruit de verplichtingen voortvloeien en de daarop gebaseerde ontologieën moeten zodanig zijn, dat zij applicatie-onafhankelijk zijn en het 'rule system' de veranderingen in de ontologieën kan blijven volgen.

In het consensus-proces zal elke inconsistentie uit de gebruikte begrippen moeten worden gehaald, zodat noch dezelfde term voor een verschillend begrip (de verantwoordelijke is één rechtspersoon of verschillende partijen), noch een verschillende term voor het zelfde begrip (bijvoorbeeld: verantwoordelijke en verantwoordelijke entiteit) of verschillende termen voor verschillende begrippen worden gebruikt. Ook moet voorkomen worden dat er verschillende begrippen voor hetzelfde concept gedurende verschillende perioden gelden. Er kan pas van overeenstemming tussen de kennisdomein experts sprake zijn indien er geen verschillende termen voor het zelfde begrip in een zelfde context voorkomen en indien niet in een nauwelijks afwijkende context de zelfde term wordt

241 Maedche, 2002 p. 13-17.
242 Bench-Capon, 2007, p. 70.

gebruikt.[243] De ideale ontologie-aanpak zorgt er voor dat naast de ontwerpers van de systemen, de deskundigen en de eindgebruikers vooraf hun kennis inbrengen. Dit leidt tot het volgende schematische model (figuur 5.10):

Figuur 5.10: Ideale ontologie aanpak, Hogben & Vakalis, 2005.



Deze aanpak leidt tot de specificaties voor softwareontwikkeling en systeem-architectuur, en maakt het mogelijk nieuwe technologieën aan de hand van de ontwikkelde privacyontologieën te beoordelen op privacyvriendelijkheid.[244]

5.12.5. Privacyrealisatiebeginselen in het systeemontwerp

Het systeemontwerp dient de privacyrisico's die zijn vastgesteld in de privacy-bedreigings analyse, af te dekken. Uit de privacybedreigingsanalyse (zie in paragraaf 4.9 de pentagonale aanpak) is gebleken, dat de relevante bepalingen uit de privacywetgeving vaak door ontwerpers worden vergeten, terwijl uit de wetgeving rechtstreeks een aantal relevante bedreigingen zijn te distilleren. De privacywetgeving dient dan ook een sterke invloed op het ontwerp te hebben. De systeemontwerper zal de rechten en verplichtingen voortvloeiende uit de privacy-richtlijnen in het systeem zodanig moeten construeren dat deze in het verwer-kingsproces niet omzeild kunnen worden.[245] De onderzoekers in het PISA-project stelden vast dat de privacywetgeving complex is en vele uitzonderingen op de regels kent. De ontologie ontwerpers hadden geen softwaremiddelen tot hun beschikking om de complexe en verfijnde juridische taal één-op-één in de programmatuur in te voeren. De privacyrichtlijnen werden niet alleen als complex, maar ook als te abstract beschouwd om direct daaruit technische specificaties te genereren. Een te hoog abstractieniveau kan tot te veel van elkaar afwijkende interpretaties leiden. Dit kan ernstige fouten in de architectuur tot

243 Deze methodologie van het ontwikkelen van privacyontologieën is vastgesteld in Ispra, op 23 januari 2003 met de volgende onderzoekers: J.J. Borking, J. Huizenga, L. Vervenne, R. Meersman, J. Angele, A.Hameed, E. Damiani, P.Ceravolo, M. Wilikens, G. Hogben, I. Vakalis,P. Chawdry,R.Steinberger, B. Pouliquen.
244 Hogben & Vakalis, 2005, p. 2.
245 Borking & Foukia, 2008, p. 7.

gevolg hebben. De oplossing die de onderzoekers kozen, was om te werken met een vereenvoudiging van de wetgeving. Die werd voornamelijk gevonden in het gebruik van de stabiele privacyrealisatiebeginselen (zie hoofdstuk 2), zonder de mogelijkheid te verliezen om later meer aspecten van de wet te integreren wanneer de omstandigheden dat zouden vereisen. Bijvoorbeeld: medische persoonsgegevens worden beschouwd als privacygevoelige gegevens waarvan de wet vereist dat een strikt regime bij de verwerking van deze gegevens wordt gevolgd. De vertaling van de rechtsregels (door de onderzoekers als '*legal instantiation'* bestempeld)[246] door middel van '*privacy knowledge engineering'*[247] werkt als volgt:

Eerst wordt door de juridische experts de 'overbodige' tekst, die bijvoorbeeld in de overwegingen van de privacyrichtlijnen kan worden gevonden, verwijderd. Dit leidt tot de kerntekst (*corpus*) van de 95/46/EG en 2002/58/EG. Daarna vindt de verdere vereenvoudiging van de wettekst plaats door de aaneenschakeling ('*chaining*') van geselecteerde artikelen van deze richtlijnen, die de gekozen privacyrealisatiebeginselen[248] weergeven. Neem bijvoorbeeld het principe van transparantie, dat vereist dat de betrokkene geïnformeerd moet worden wat met er zijn persoonsgegevens wordt gedaan. Dit principe kan worden gevonden in de artikelen 10 a, b en c en 11, lid 1, a, b, c en 11, lid 2 en artikel 13, lid 1, a, c, d, e, f en g en lid 2 van de richtlijn 95/46/EG.[249]

Uit het corpus worden de regels en de uitzonderingen op de regels geselecteerd, nader geanalyseerd en van elkaar gescheiden. Vervolgens wordt de tekst opgesplitst in eenvoudige zinnen, zoals "individuen moeten over de verwerking van hun gegevens worden geïnformeerd"; "de individuen hebben het recht de gegevens te raadplegen"; "de individuen hebben het recht correcties te vragen" en "de individuen hebben het recht tegen de verwerking in bepaalde omstandigheden bezwaar te maken". De bron van deze zinnen wordt apart geregistreerd, bijvoorbeeld dat de bovenstaande zinnen zijn ontleend aan overweging 25 en de artikelen 10 en 11 van de Richtlijn 95/46/EG. Na de aaneenschakeling van de artikelen van

246 Maedche, 2002, p. 20.

247 Kenny & Borking, 2002, p. 13 "we define privacy engineering as a systematic effort to embed privacy relevant legal primitives into technical and governance design".

248 Het gaat om de privacyprincipes zoals die bijvoorbeeld die vermeld in de Convention 108 van de Council of Europe (1981) en uit de Organization for Economic Co-operation and Development (OECD) guidelines (1980). Zie hoofdstuk 2 van dit boek.

249 Kenny & Borking, p. 14:
"Such a principle is considered in anatomical terms emphasizing context and goal orientation. Subdivisions are made which possess orthogonality and regularity. To each subdivision is attached a numerical identifier, nesting as appropriate, affording documentation and controlling benefits, plus eases modeling work item interdependence".

de privacyrichtlijnen per privacyrealisatieprincipe, is de volgende stap de beginselen in de elementen te verdelen. Aldus worden de beginselen gedeconstrueerd in een reeks van elementen die de nadruk op de context (wat is de bron van deze tekst) en het doel (wat moet worden bereikt) leggen. Er wordt naar gestreefd de interpretatieruimte zo veel mogelijk te reduceren, zodat latere softwarerisico's voorkomen worden bij het opstellen van de bouwspecificaties.

Bijvoorbeeld: Om transparantie in het informatiesysteem te realiseren is het noodzakelijk dat:

1. De betrokkene ('Data Subject' = DS) zich bewust is wie zijn persoonsgegevens verwerkt en voor welk doel.
1.1 De verantwoordelijke (V) houdt bij welke verwerkingen plaatsvinden. 1.1.1 V stelt deze informatie ter beschikking van DS.
1.2 De 'personal identifiable information' = PII) is van DS verkregen.
1.2.1 Voorafgaand aan de verzameling van de PII van DS: DS is geïnformeerd over: de identiteit (ID) van V.
1.2.2 DS is geïnformeerd over de doelbinding (PS).
1.2.3 Voorafgaand aan de verzameling van de PII van DS, de ID van V en informatie over PS: DS is geïnformeerd over het feit dat PII speciale categorieën van gegevens bevat.
1.2.4 PII moet worden behandeld overeenkomstig de gevoeligheid die aan deze gegevens wettelijk is toegekend.
1.2.5 De PII van DS worden gemarkeerd met een van de overeengekomen gevoeligheidsniveaus: L (laag), M (gemiddeld), H (Hoog).
1.2.5.1 Medische gegevens (MS) van DS worden gemarkeerd met gevoeligheidsniveau H etc.[250]

Op dezelfde manier vindt vanuit de rol van de verantwoordelijke of vanuit de strekking van een bepaald privacyrealisatiebeginsel (bijvoorbeeld doelbinding) of betreffende de privacyvoorkeuren van de DS de uitsplitsing plaats. Bijvoorbeeld: met betrekking tot de expliciete toestemming van DS; de gebruiks- en bewaartermijn van de PII; de statistische verwerking van de gegevens; etc.[251] Voor dit werk zijn juridische deskundigen onmisbaar. Zij zorgen voor de argumentatie bij de juridische specificaties en de opsplitsing van de privacyrealisatiebeginselen. Ontwerpers zijn soms moeilijk te overtuigen van de juridische noodzaak.

De volgende stap wordt uitgevoerd door ontologie ontwerpers en is gericht op een verdere abstractie van de aldus verkregen korte privacybeschermende beschrijvingen. Deze privacystatements (beweringen) worden nu nog verder gereduceerd tot zeer eenvoudige zinnen die de essentie ('elementary fact') weergeven. Het criterium van een 'elementary fact' is dat de zin niet verder in kleinere bestanddelen is op te splitsen zonder zijn betekenis te verliezen. Dit proces leidt

250 Borking & Foukia, 2008, p. 7.
251 Van Blarkom, e.a., 2003, p. 188.

tot een set van generieke elementen ('instances') en 'triples'.[252] Een triple is een zo'n kort mogelijke zin met een onderwerp (subject) -,. werkwoord (verb), en voorwerp (object) (SVO) structuur.[253] Daarnaast vindt er regel (rule) abstractie plaats, waarbij de regel wordt gesubstitueerd met superklassen of supereigenschappen van deze regels en een samenvattende term, die staat voor de termen van de subklassen of voor de termen die de subeigenschappen weergeven. Bijvoorbeeld de term 'wit' kan samengevat worden in de term 'kleur' op een lager niveau en in een object beschrijving op hoger niveau bijvoorbeeld: 'trilling'. Het gehele proces eindigt in '*lexon engineering*'.[254] De basis voor de uiteindelijke privacyontologieën.

Wanneer dit voor alle privacyrealisatiebeginselen is uitgevoerd, dan is de grens van de 'privacy knowledge engineering' bereikt met betrekking tot het genereren van technische vereisten die uit de privacywetgeving voortspruiten. Een verdere verfijning is dan niet meer mogelijk en het meest elementaire niveau van het beschrijven van de Richtlijnen in specificaties is bereikt. De overgebleven artikelen die niet behoren tot het domein van de privacyrealisatiebeginselen worden niet in het systeemontwerp opgenomen. Deze artikelen spelen wel een vitale rol met betrekking tot de verklaring en interpretatie zoals bijvoorbeeld de artikelen 2 a tot en met h (definities), 3 lid 1, 3 lid 2, 4, lid 1 a, b, c, 4 lid 2, 5, 9, 15 lid 1, van de Richtlijn 95/46/EG en beïnvloeden indirect de systeemarchitectuur. Sommige artikelen zijn niet relevant voor de architectuur, zoals de vereisten voor de toezichthouder, de juridische remedies etc.

5.12.6. Automatische ontologieproductie

Uit het bovenstaande blijkt dat het ontwerpen van privacyontologieën een zeer tijdrovende en arbeidsintensieve zaak is.[255] Dit komt onder meer door het inschakelen van experts uit het betreffende kennisdomein (de privacybescherming). Dit uitvoerige proces van kennisvergaring is volgens Hameed onvermijdelijk, omdat er anders geen zekerheid kan ontstaan over de geldigheid van de te ontwerpen ontologieën binnen een bepaald kennisdomein.[256] Hogben, Spyns & Borking hebben in 2005 onderzocht of binnen een beperkte tijd en met minder menskracht sneller dan volgens de methode van Hameed kwalitatief hoogwaardige triples, de bouwstenen voor ontologieën, automatisch rechtstreeks uit de privacyrichtlijnen geëxtraheerd konden worden.[257] Gepoogd werd langs de weg van 'human language technology' (HLT) en 'information extraction technology'

252 Maedche, 2002, p. 20: "A knowledge base structure is a 4-tuple (O,I, inst, instr), that consists of an *ontology* (O), a *set* (I) whose elements are called instances, a function *inst* (C) called concept instantiation, a function *instr* (R) called relation instantiation.
253 Spyns & Hogben, 2005, p. 24.
254 Spyns & Hogben,2005, p. 3: Lexon, de vervolgfase van de triple wordt weergeven als < term1 (=head term), role, co-role, term2 (tail term)> en kan worden beschouwd als de combinatie van twee (RDF)-triples.
255 Spyns & Hogben, 2005, p. 1.
256 Hameed, Sleeman & Precee, 2001.
257 Spyns & Hogben, 2005, p. 1-14.

(IET) 'triples' te genereren. Als dat zou lukken, dan was de volgende vraag of de triples automatisch zodanig kunnen worden geëvalueerd, dat die evaluatie voldoet aan dezelfde kwaliteits- (kennis)standaarden van verschillende domeinexperts? Automatiseren was gewenst, want het evaluatiewerk blijkt voor experts zeer tijdrovend en afstompend te zijn. Zeker wanneer duizenden triples moeten worden gelezen, beoordeeld en van een kwalificatie moeten worden voorzien verdeeld over drie niveaus, lopend van 'valid' (+) (dus bruikbaar in de context van het ontwerpen van een privacyontologie), via 'neutral' (0) naar 'not-valid' (–).

Het experiment verliep als volgt: de triples werden geëxtraheerd uit het 'privacycorpus' (de tekst waarop de bewerking wordt uitgevoerd, i.c. de Richtlijn 95/46/EG) door een door de universiteiten van Antwerpen (CNTS) en Tilburg (ILK) ontwikkelde 'memory-based shallow parser',[258] een zogenaamde 'text miner'. Als controletekst voor de vaststelling van de juiste werking van de 'text miner' werd de tekst van de Wall Street Journal gebruikt.

De geproduceerde triples werden onafhankelijk van elkaar gevalideerd door twee kennisdomeindeskundigen, een privacyjurist en een 'knowledge-engineer' gespecialiseerd in privacy en vertrouwens-(trust)-vraagstukken. De eerste poging leverde heel veel 'not-valid' triples op. Na analyse bleek dat de meeste van 'not-valid' triples werden veroorzaakt door de overwegingen (de teksten die met 'whereas' beginnen) die vooraf gaan aan de eigenlijke tekst van de Richtlijn 95/46/EG. Vervolgens is de corpus door de jurist geschoond waarbij alle overbodige formuleringen werden verwijderd en vervolgens 'gelemmatized'. 'Lemmatize' houdt in dat de woorden worden gereduceerd tot hun meest basale vorm, bijvoorbeeld: working, works, worked wordt work, maar de tekst blijft verder ongewijzigd. De outputparameters van de 'text miner' werden na een aantal 'trial and error'-pogingen ingesteld op triples met de structuur:

1. "Subject-Verb-Object", zoals bijvoorbeeld: <third_country, ensure, level_of_-protection>.
2. Triples met de structuur: "noun phrase-preposition-noun phrase", zoals: <Treaty, on, European_Union>.
3. Triples met de structuur: "subject-verb-prepositional object", zoals: <controller, establish, in_Member_State>.

Dat leverde 22 producties op van tussen de 1.116 en1.223 triples. De 'text miner' werd zo ingesteld dat automatisch kon worden vastgesteld welke woorden relevant zijn in de triples. Zo verschenen 416 woorden eenmaal in de tekst van de Richtlijn 95/46/EG en één woord 1.163 keer. Uit fundamenteel onderzoek van Zipf,[259] een Amerikaanse taalkundige en filoloog die statistisch onderzoek deed naar woorden die in verschillende talen voorkomen, is gebleken dat wanneer een woord veel voorkomt, de betekenis daarvan afneemt. In het corpus komt het woord "the" 1.163 keer voor en op grond van Zipf's criteria houdt dit in dat dit

258 Reinberger, Daelemans & Spyns, 2005, p. 5-8.
259 Zipf, 1949.

woord geen of zeer weinig betekenis heeft. In tegenstelling tot het woord "assurance" dat in de corpus slechts één keer voorkomt en als zeer betekenisvol wordt gekwalificeerd. De frequentie van een woord in een tekst bepaalt de frequentieklas (FC). De frequentie klas van een woord wordt uitgedrukt in het aantal malen dat het woord voorkomt. Dus eenmaal voorgekomen levert de FC 1 op en bij 1163 keer levert de FC 1163 op. Uiteindelijk werden de woorden uit FC 1 tot en met FC 49 als relevant beschouwd.[260] Als alleen de 49 relevante FC's van het privacycorpus in aanmerking worden genomen, dan blijkt de herkenning van niet relevante triples te zijn: 'recall' 95,58%, precisie[261] 96,29%, en accuratesse[262] 95,04%. Er zijn 22 combinaties voor de triple productie uitgeprobeerd. De overall score voor alle FC's is wat betreft de *recall* 89,91%, de *precisie* 27,43% en voor de *dekking* (*coverage*[263]) 79,88%.[264] De experts rapporteerden, dat:

> "too many irrelevant results are produced – the text miner not being able to skip over sections that are only of marginal interest for the privacy topic."[265]

Het is mogelijk dat de resultaten zijn beïnvloed door het feit dat de in de Engelse taal gestelde wetteksten (EU-richtlijnen) termen bevatten, die alleen maar relevant zijn binnen het juridisch kennisdomein en niet daarbuiten, terwijl de 'unsupervised text miner' is ingesteld op allerlei soorten teksten (bijvoorbeeld in kranten).[266] De onderzoekers concluderen, dat vergeleken met de Hameedmethode de automatische evaluatiemethode in staat is om ongeveer in de helft van de gevallen, een geproduceerde triple terecht als geschikt te kwalificeren en een irrelevante triple te verwerpen. De onderzoekers menen dat hoewel de scores bescheiden zijn, de semi-geautomatiseerde aanpak bruikbaar is omdat er voldoende tijd wordt bespaard vergeleken met de conventionele methode (inschakelen van experts). Deze aanpak is interessant voor het modelleren van ontologieën. Ter mogelijke verbetering van de resultaten wordt voorgesteld om als controle tekst niet kranten te gebruiken, maar een aantal EU-richtlijnen te nemen, waardoor de classificatieproblemen tussen de domeinexperts en de experts die de 'unsupervised text miner' bedienen aanmerkelijk zouden kunnen afnemen. Een juridisch deskundige blijft zonder meer noodzakelijk om de wettekst te analyseren en zo nodig op te schonen. Vooralsnog is meer empirisch onderzoek nodig om het proces van 'triple mining' te verbeteren.

---

260 Spyns & Hogben, 2005 p. 4-5.
261 De triples zijn zinvol voor het kennisdomein.
262 De triples zijn niet te algemeen geformuleerd maar geven de belangrijke termen van het domein weer.
263 Coverage betekent: percentage van alle triples in de corpus.
264 Spyns & Hogben, 2005, p. 7.
265 Spyns & Hogben, 2005, p. 10.
266 Er is bewust maar één taalversie (Engels) gebruikt. De problemen zouden onoverkomenlijk zijn als richtlijnen in verschillende taalversies zouden worden gebruikt.

5.13. Overdrachtregels voor persoonsgegevens

Er zijn drie situaties waarbij de overdracht van persoonsgegevens plaatsvindt.
1. Bij de directe interactie tussen het individu en de organisatie (de verantwoordelijke in de zin van de wet) al dan niet via een *frontoffice* met opslag in de centrale en/of decentrale databanken.
2. Bij gebruikmaking van centrale of decentrale databanken ten gevolge van processen tussen de verschillende afdelingen binnen de organisatie.
3. Tussen afzonderlijke organisaties al dan niet in een keten.[267]

Als persoonsgegevens elektronisch worden overgedragen dan dient duidelijk te zijn dat de overdracht en de verwerking conform de wettelijke vereisten en de privacyvoorkeuren van het individu, waarop de gegevens betrekking hebben, plaatsvinden. Om die overdracht op een juiste wijze te laten plaatsvinden, dient in de privacymanagementsystemen (PMS) gerefereerd te worden aan de 'privacy statements', die zijn ontworpen op basis van de privacyontologieën. Een generiek abstract 'statement' over bijvoorbeeld transparantie wordt opgesplitst, zoals wij hiervoor hebben gezien, in de verschillende rechten die aan het individu volgens de wet of het privacybeleid van de organisatie worden toegekend. Vervolgens kunnen de regels (bestaande uit de privacyvoorkeuren en wettelijke vereisten) opgesteld worden, die gaan bepalen hoe de communicatie tussen de zender en ontvanger van de persoonsgegevens moet verlopen. Daarvoor worden matrices (protocollen) opgesteld die aangeven hoe binnen en tussen de informatiesystemen de taken moeten worden uitgevoerd. De transferregels voor de persoonsgegevens bestaan uit één of meerdere subregels per privacyrealisatiebeginsel. Alle regels, die gekoppeld zijn aan de te verzenden gegevens, evalueren elektronisch of de ontvanger hier aan voldoet. Als de evaluatie van de ontvanger positief uitvalt, dan vindt verzending naar de ontvanger plaats. Tegelijkertijd moeten met de persoonsgegevens ook de metagegevens over deze persoonsgegevens verzonden worden, waarin de privacyvoorkeuren van de zender zijn vastgelegd. Op die manier kan de ontvanger bij verzending van die persoonsgegevens op zijn beurt de rol van de eerste zender overnemen. In de regels worden positieve evaluaties weergegeven als: waar (T = true) en negatieve evaluaties als vals (F = false). Positieve evaluaties resulteren in het akkoord gaan met het verzenden (overdragen) van de persoonsgegevens. Alle regels moeten een positief evaluatieresultaat opleveren alvorens de persoonsgegevens wordt verzonden.[268]

De redenering die het systeem op grond van de transferregels moet volgen gaat bijvoorbeeld voor het privacyrealisatiebeginsel 'transparantie'als volgt: het individu kan in zijn privacyvoorkeur aangeven of hij voor de overdracht van zijn persoonsgegevens om transparantie wel (Y = yes) of niet (N = no) verzoekt. Er

267 Koorn, e.a., 2004, p. 22-26.
268 Van Breukelen, e.a., 2002, p.1.

zijn dan twee situaties mogelijk. De ontvanger kan geen transparantie (N) aanbieden of hij biedt wel transparantie conform de 95/46/EG (Y) aan.[269]

Dit leidt tot het volgende resultaat in de algemene transparantiematrix (figuur 5.11): de termen: t^{pref} staat voor privacyvoorkeur van het individu; en t^{pol} staat voor privacybeleid van de ontvanger; T staat voor true (positief resultaat) en F staat voor false (negatief resultaat).

Figuur 5.11: Algemene transparantiematrix.

t^{pref} / t^{pol}	**N**	**Y**
N	*T*	*T*
Y	*F*	*T*

Dit figuur moet als volgt worden gelezen: in de verticale linkerkolom staat de preferentie van het individu (de gebruiker) met betrekking tot de behandeling van zijn persoonsgegevens. In de bovenste twee horizontale velden rechts van de notatie t^{pref}/t^{pol} staat het privacybeleid van de ontvanger, namelijk hij biedt de gebruiker geen transparantie aan (N) of juist wel (Y). De 'N' in de linkerkolom betekent dat de gebruiker geen voorkeur voor transparantie heeft. Dit leidt in de naast gelegen velden onder de 'N' en de 'Y' tot het resultaat *T*. Dit wil zeggen dat indien de ontvanger geen transparantie aanbiedt, het ook voor de gebruiker geen probleem oplevert en de persoonsgegevens kunnen worden overgedragen en verwerkt. In het geval de ontvanger wel transparantie aanbiedt, is er geen probleem voor de gebruiker en kunnen de data worden verzonden. De Y in de daaronder gelegen linkerkolom betekent dat de gebruiker wel zijn voorkeur voor transparantie heeft uitgesproken. Het resultaat is dat wanneer de ontvanger geen transparantie aanbiedt er wel een probleem voor de gebruiker ontstaat, weergegeven als *F* (de verzending van de gegevens is dan niet mogelijk). De gebruiker heeft echter geen probleem als de ontvanger wel transparantie aanbiedt, want dat komt overeen met zijn eigen voorkeur, weergegeven in de laatste rechterkolom als *T*, met andere woorden zijn persoonsgegevens kunnen overgedragen worden. Het resultaat van een dergelijke matrix leidt tot de transferregel: $(\neg t^{pref} \wedge \neg t^{pol}) \vee (t^{pref} \wedge t^{pol}) \vee (\neg t^{pref} \wedge t^{pol})$[270]

In woorden luidt deze regel: dit is waar en alleen dan waar indien de volgende situatie zich voordoet: of er is noch een preferentie en noch een policy, of zowel de preferentie als de policy is aanwezig, of er is geen preferentie maar wel een policy.[271] De bovenstaande notatie geldt voor alle afzonderlijke onderdelen van het privacyrealisatiebeginsel 'transpararantie', zoals inzage, correctie, verwijderen, blokkeren, verzet en bezwaar.

269 In het PISA-project is de standaard-(default)-positie het bepaalde in de Richtlijnen 95/46/EG.
270 Borking & Foukia, 2008, p.8.
271 Von Kutschera & Breitkopf, 1971, p.17-55; Ollongren, Meyer & Deutz, 2009.

Een ander voorbeeld is de bewaartermijn. De betrokkene zoals gedefinieerd in de Wbp, kan in zijn privacypreferenties de uiterste bewaartermijn voor zijn persoonsgegevens aangeven. Na die datum moeten de data worden vernietigd. De consequentie van deze voorkeur is dat de verantwoordelijke de onderhavige gegevens niet langer mag bewaren. Dit is in één eenvoudig regel te vatten, namelijk dat de door het individu gewenste bewaartermijn ('data subject's retention period' = t_{pref}) gelijk of langer dient te zijn dan de door de verantwoordelijke gehanteerde bewaartermijn ('controller's retention period' = t_{pol}). Dit wordt weergegeven als: $t_{pref} \geq t_{pol}$.[272]

In het PISA-project werd, wanneer de persoonsgegevens een hoog beveiligingsniveau[273] hadden gekregen, de 'privacy incorpated software agent' voorzien van de volgende transferregel om de software agent te laten beslissen wanneer hij (agent 1 verzender) ingebouwde toestemming had voor de overdracht van persoonsgegevens conform het bepaalde in de Richtlijn 95/46/EG aan agent 2 ontvanger: "If APS-(1) matches DS-privacy-preference-(2) and APS-(2) matches DS-privacy-preference-(1) and PII level 2-(1) matches PII level 2-(2) then allow disclosure/exchange PII level 1-(1)."

In deze overdrachtsregel staat (1) voor agent 1 en (2) voor agent 2; APS betekent 'agents practices statement' (= privacybeleid) waaronder de software agent opereert; DS is data subject. PII level 2 zijn persoonsgegevens van de gebruiker van de mobiele software agent met een laag identificerend gehalte. PII level 1 heeft een hoog identificerend gehalte (zie paragraaf 6.9.1 a). Dergelijke transferregels kunnen in de architectuur van het informatiesysteem voor alle privacyrealisatiebeginselen worden opgenomen en zo een geautomatiseerde overdracht van persoonsgegevens bewerkstelligen conform de privacyvoorkeuren van de DS/betrokkene (zoals gedefinieerd in Richtlijn 95/46/EG respectievelijk Wbp).

5.14. Samenvatting

In dit hoofdstuk zijn een aantal belangrijke ontwerpelementen in samenhang met 'privacy enhancing technologies' besproken, die kunnen worden ingezet om privacyveilige systemen te ontwerpen en te bouwen. In de paragrafen 5.3 tot en met 5.6 is aangetoond dat het mogelijk is een privacyveilig informatiesysteem te bouwen zonder dat de identiteit van de gebruiker voor alle interne processen van het informatiesysteem nodig is. Dit houdt in dat dan ook geen of minder persoonsgegevens hoeven te worden verzameld, verwerkt en opgeslagen. Veel dienstverlening is mogelijk zonder dat de identiteit van de afnemer bekend hoeft te zijn, terwijl toch de afnemer naar zijn identiteit wordt gevraagd en zijn

272 Van Blarkom, Borking & Olk, 2003, p. 185.
273 Kenny & Borking, 2002, p. 18-19.

persoonsgegevens worden verwerkt. Daarmee wordt in strijd met het door de wet voorgeschreven beginsel van gegevensminimalisatie gehandeld.

De vierde onderzoeksvraag (OV 4): *Wat houdt het concept Privacy Enhancing Technologies (PET) in?*, is in de paragrafen 5.7 tot en met 5.13 beantwoord. De oorsprong van PET ligt in het theorema van Chaum waaraan in paragraaf 5.2 is gerefereerd. 'PET' is een technologisch concept en kan theoretisch gezien worden als een belangrijke aanvulling op het bestaande privacyrechtelijk kader en de organisatorische uitwerking daarvan. Met PET kan het gebruik van persoonsgegevens worden gelimiteerd, aanmerkelijk worden verminderd. De verwerking kan door toepassing van PET dwingend gebonden worden aan de wettelijke voorwaarden, waardoor de privacybescherming door de verantwoordelijken geen lege huls wordt. Bovendien stellen PET de burger en consument in staat om de verwerking van zijn persoonsgegevens te controleren om daardoor zijn vertrouwen in de rechtmatige verwerking te vergroten.[274] Koorn[275] wijst erop dat PET-toepassingen binnen informatiesystemen mogelijk maken, wat anders wettelijk onmogelijk zou zijn. In functionele zin blijkt het toepassen van PET niet problematisch te zijn. PET omvatten alle technische maatregelen om de privacy te waarborgen en risico's op inbreuken op de bescherming van privacy te voorkomen en te managen. Met behulp van PET kan een organisatie al aan de bron technische maatregelen nemen en het aantal identificerende gegevens tot het absolute minimum beperken en de identiteit loskoppelen van de overige persoonsgegevens.

De in dit hoofdstuk besproken research met betrekking tot de conceptuele ontwerpelementen voor privacyveilige informatiesystemen geeft een positief, maar theoretisch antwoord op de vijfde onderzoeksvraag (OV 5): *Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen*?

De mogelijkheden nemen toe om effectief persoonsgegevens met PET te beschermen. Dat is goed nieuws. De afhandeling van steeds meer transacties vindt direct plaats tussen informatiesystemen, software agents, intelligente sensoren en robots, zonder tussenkomst van mensen. In veel van deze systemen is geen rekening gehouden met de informationele privacy en komen privacyincidenten steeds meer voor. Het is een absoluut noodzakelijk dat technologische maatregelen worden ontwikkeld en in informatiesystemen worden ingebouwd om de persoonlijke levenssfeer effectief te beschermen, anders zal onze informationele privacy steeds meer eroderen. In de paragrafen 5.11.2 en 5.11.3 zijn PET besproken die het mogelijk maken de privacyvoorkeuren van het individu aan zijn persoonsgegevens te koppelen en de verspreiding van persoonsgegevens te volgen. Privacymanagementsystemen, toepassing van privacyontologieën en overdrachtregels (paragrafen 5.12 en 5.13) kunnen theoretisch de privacybescherming sluitend maken.

---

274 Klaver, e.a., 2002, p. 100-108.
275 Koorn, e.a., 2004, p. 13-16.

De Commissie van de EU steunt het gebruik van PET en stimuleert in haar onderzoeksprogramma's het fundamenteel onderzoek naar PET. In verschillende lidstaten zijn expliciete PET-maatregelen in de wetgeving opgenomen. Fritsch stelt dat: " (…) tools for unobservability and identity protection have reached a high level of maturity. Some concepts, such as trusted platforms, anonymous credentials or DRM technology application for information tracking have not entered the market yet. However, for the purpose of managing personal data in information systems, many working building blocks are available. They should be taken advantage of."[276]

In hoofdstuk 6 zal de vijfde onderzoeksvraag (OV 5) *Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen*? getoetst worden aan de praktijk.

Het bouwen van privacyveilige systemen met de PET-aanpak van gegevensbescherming vraagt om een innovatieve opstelling van de ontwerpers en 'thinking out of the box'.[277] Bijvoorbeeld: via e-mail worden veel persoonsgegevens verspreid. Zou de verspreiding van persoonsgegevens door middel van e-mail gereduceerd kunnen worden door een systeem te bouwen dat de inhoud van de e-mail niet verzendt maar de e-mail met inhoud vastlegt op de eigen server, terwijl tegelijkertijd naar de bestemming (de ontvanger) een bericht wordt gestuurd met een link naar de server waarop de versleutelde e-mail staat? Om de e-mail te lezen moet de ontvanger een verbinding maken met de server waarop de e-mail staat en het bericht decrypten. De verzender kan op zijn eigen server het e-mailbericht altijd verwijderen en houdt controle op wie toegang heeft tot de e-mail met zijn persoonsgegevens.

Zijn er voorbeelden van goed functionerende privacyveilige (PET inside) informatiesystemen? "The proof of the pudding is in the eating".

276 Fritsch, 2007, p.30.
277 Klaver, e.a., 2002, p. 140.

6. Privacyveilige architecturen

"Denn, wenn du sie anschaust, wirst du zwar nicht etwas sehen, was allen gemeinsam wäre, aber du wirst Ähnlichkeiten, Verwandtschaften, sehen, und zwar eine ganze Reihe. Wie gesagt: Denk nicht, sondern schau!"
L. Wittgenstein - Philosophische Untersuchungen Teil 1, German & English text translated by G. E.M. Anscombe, Oxford 1953, No. 66, p.31.

In dit hoofdstuk wordt de vijfde onderzoeksvraag beantwoord (OV 5): *Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen*?. In paragraaf 6.1 wordt het ontwerpproces toegelicht. In 6.2 komen de ontwerpvereisten voor een privacyveilig informatiesysteem (PRIVIS) aan bod. In paragraaf 6.2.1 is het resultaat van de beantwoording van eerste onderzoeksvraag (OV 1) *Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacy wet- en regelgeving worden afgeleid?* overgenomen, namelijk de lijst van juridische specificaties, waar de ontwerper van PRIVIS niet omheen kan. In 6.2.2 wordt aangehaakt bij het resultaat van de beantwoording van de derde onderzoeksvraag (OV 3)*: Met welke privacybedreigingen en -risico's moeten de burger en de ontwerper van systemen rekening houden*? de privacybedreigingen. In 6.3 wordt gewezen op het belang van een duidelijke scheiding van rollen in PRIVIS, te weten de betrokkene, de verantwoordelijke en bij het gebruik van certificaten met de 'trusted third party' (TTP). In paragraaf 6.4 wordt aangetoond dat er naast privacyrechten ook privacyplichten bestaan. Om de privacyplichten goed te kunnen beheren is het 'Obligation Management System' (OMS) ontworpen.

In de paragrafen 6.5 tot en met 6.9 wordt het antwoord op de vierde onderzoeksvraag (OV 4) *Wat houdt het concept Privacy Enhancing Technologies (PET) in?* toegepast. In 6.5 komen gegevensminimalisatie en de daarbij behorende PET-maatregelen als ontwerpbeginselen voor het voetlicht. Ter adstructie van de in de vorige paragraaf vermelde ontwerpbeginselen volgt in paragraaf 6.5.1 de bespreking van de metazoekmachine Ixquick. De bespreking omvat de architectuur, het zoekproces, de clickfraude en de cookies. Drie juridische vragen doen zich bij de werking van de metazoekmachine Ixquick voor. Deze worden toegelicht in paragrafen 6.6.1 en 6.6.2. De rapportage over Ixquick wordt afgesloten in paragraaf 6.6.3 met het PET-model informatiesysteem 1.

In paragraaf 6.7 wordt het tweede model van een werkend PET-informatiesysteem (model informatiesysteem 2 in figuur 6.8) gepresenteerd, namelijk het

ziekenhuisinformatiesysteem, zoals dat onder meer in het psychiatrisch ziekenhuis Meerkanten wordt gebruikt. In de analyse komen de centrale database, de relationele database, het gebruik van de Identity Protector, en de gegevensdomeinen met pseudo-identiteiten aan de orde. De analyse wordt afgesloten met figuur 6.11 waarin de sequentiële communicatiedialoog binnen het ziekenhuisinformatiesysteem zichtbaar wordt gemaakt. In paragraaf 6.7.3 wordt betoogd dat de kritiek op het veelbecommentarieerde elektronisch patiënten dossier dat het Ministerie van VWS wil invoeren, kan worden gepareerd door op het elektronisch patiëntendossier het model PET-informatiesysteem 2 toe te passen. In paragraaf 6.8 wordt de toepassing van het derde model PET-informatiesysteem in het Victim Tracking and Tracing System (ViTTS) ten tonele gevoerd. Bij de bespreking van dit systeem worden de privacybeschermende maatregelen in kaart gebracht. Ten slotte komt in paragraaf 6.9 de nieuwe loot aan de PET-stam, de privacymanagementarchitectuur aan de orde. Ter adstructie van deze PET-architectuur dient de in 2003 ontwikkelde 'privacy incorporated software agent' (PISA). Deze agent wordt besproken in paragraaf 6.9.1 waarin de consequenties van de privacybedreigingsanalyse, de opsplitsing van de PII, de ingebouwde juridische kennis, de interactieprotocollen, het gebruik van 'onion routing' en de 'audit trail' besproken worden. In paragrafen 6.10 en 6.11 worden de vraagstukken rond de PISA-applicant (een mobiele software agent die voor zijn 'master' een baan zoekt) besproken. Paragraaf 6.12 gaat in op de vraag of er sprake is van mislukte PET-automatisering en het hoofdstuk wordt afgesloten met de samenvattende beantwoording van de vijfde onderzoeksvraag (OV 5) in paragraaf 6.13.

6.1. Het ontwerpproces

Het conventionele denken over het toepassen van PET is dat PET "have not gone mainstream. In other words nullus prettii[1] – no commercial potential".[2] Maar uit mijn vijftien jaar ervaring met PET stel ik vast dat dit een onjuist standpunt is. PET kan voor zowel de overheid als het bedrijfsleven een vitale rol spelen om het vertrouwen van het individu dat zijn persoonsgegevens afstaat, te verkrijgen en te behouden. Canon meent dat "PET can provide the backbone for an ongoing trust relationship with both citizens and customers."[3] Waarom wordt deze 'backbone' dan niet massaal gebruikt? Canon meent dat dit komt omdat de kennis over privacy in organisaties onderontwikkeld is en de technologie, die privacybescherming mogelijk maakt, gebruikersonvriendelijk is.[4] Ik heb daar een andere mening over, die ik in hoofdstuk 7 uiteen zal zetten. Voor bouwers (ontwerpers en codeschrijvers) van privacyveilige informatiesystemen en applicaties geldt dat

1 Het Latijnse woord prettii is onjuist. Het moet zijn pretii. Conform F. Muller, Beknopt Latijns-Nederlands Woordenboek, Groningen 1958, p. 730.
2 Canon, 2004, p. xxvi.
3 Canon, 2004, p. xxvi.
4 Canon, 2004, p. xxvii.

"developing solutions can be very demanding"[5] met veel en diverse inbreng van consumenten, organisaties, partners, analisten, marketeers en de eigen productgroep binnen de onderneming. Een van de belangrijkste vragen die de ontwerper zich moet stellen is volgens Canon[6]: "Will building privacy awareness into my application be enough of a differentiator to offset the time investment?"[7]

Om het ontwerpen en bouwen van privacybeschermende componenten succesvol te laten verlopen, dient het bedrijf een solide infrastructuur te hebben, bestaande uit:

1. Een expert op het gebied van privacybescherming (bijvoorbeeld de 'privacy officer' (de Nederlandse functionaris gegevensbescherming), of een privacycommissie van werknemers.
2. Een klantengroep die zich bezighoudt met privacyproblemen.
3. Eén of meerdere projectmanagers die een goed inzicht hebben in architectuur[8] van de verschillende componenten van het systeem en met name inzicht hebben in de gegevensstromen.
4. Een gespecificeerde privacystandaard (meetlat) die als uitgangspunt kan worden toegepast op elk te bouwen component. Een dergelijke meetlat zal de 'privacy policy' van het bedrijf weerspiegelen.[9]

Zodra besloten is een privacybeschermende component of systeem te bouwen aan de hand van een eerder uitgevoerd ontwerp, moeten de volgende stappen worden genomen:

1. Uitvoeren van een privacybedreigings- en/of privacyimpactanalyse (PIA) met specifieke aandacht voor de gegevensstromen en de data-opslag binnen het te bouwen component of systeem (zie hoofdstuk 4).
2. In kaart brengen van mogelijke uitzonderingen op de privacymeetlat van het component of systeem, dat door de PIA aan het licht is gekomen en de manier waarop dit kan worden opgelost, bijvoorbeeld door PET-maatregelen.
3. Verifiëren op welke manier het individu toegang kan krijgen tot zijn persoonsgegevens in het systeem en zijn rechten kan uitoefenen.
4. Vaststellen of in het ontwerp privacyincidenten kunnen worden gelogd (voor de 'audit trail') en hoe privacyincidenten kunnen worden gecorrigeerd.
5. Op welke wijze, wanneer het systeem eenmaal is geïmplementeerd in de organisatie, de parameters (afstellingen) van het systeem kunnen worden bijgesteld om privacyincidenten te voorkomen.

---

5 Canon, 2005, p. 175.
6 Canon werkt voor Microsoft (USA) als privacystrateeg in de Corporate Privacy Group.
7 Canon, 2005, p. 175.
8 Rijsenbrij, 2002, p. 3: "Architectuur is een (coherente) verzameling van principes, regels, standaarden en richtlijnen. De architectuur wordt aan de ene kant bepaald door de wensen die de organisatie heeft voor een informatiesysteem en aan de andere kant begrensd door de mogelijkheden die de aanwezige technologie biedt."
9 Canon, 2004, p. 126-127: "The privacy policy expresses a certain expected behavior base on the company values, The privacy standard indicates how the privacy policy applies to a specific business practice such as marketing to customer or building products."

Deze procedure leidt tijdens het ontwerp van het privacyveilige systeem, applicatie of component tot het opstellen van een privacyspecificatie per systeem, applicatie en component. In deze specificaties worden alle benodigde persoonsgegevens, de noodzakelijke verspreiding en raadpleging, onderlinge afhankelijkheid van andere componenten en kenmerken vastgelegd.[10] Daarna worden in de privacyspecificatie de te verwerken data, het voorziene gebruik en de getroffen beveiliging nogmaals gecontroleerd.[11] De manier waarop in het systeem de inzage-, wijzigings- en verwijderings- en andere rechten met betrekking tot de persoonsgegevens kunnen worden uitgeoefend, kunnen in de applicatie zelf als mededeling aan de gebruiker in 'firmware' (chips) worden vastgelegd. Het kan natuurlijk ook later gebeuren via de website van de afnemer of een andere instructie aan de gebruiker van het systeem. Dit hangt af van de wensen van de afnemer van het systeem. 'Wired-in' privacyrealisatiebeginselen zijn te preferen, omdat het op die manier voor de eigenaar van het informatiesysteem het veel moeilijker zal zijn die beginselen te ontduiken.

De financiële afweging ontbreekt hierbij natuurlijk niet. Er zal door de ontwerpers een analyse moeten worden gemaakt of het toevoegen van privacybeschermende componenten aan de te ontwerpen applicatie of systeem financiële en marketingvoordelen oplevert. De financiële aspecten komen in hoofdstuk 7 aan de orde. Na de bouwfase komt de testfase waarin opnieuw een aantal cruciale vragen moet worden gesteld over de feitelijke verzameling, verwerking, verspreiding en opslag van de data door het systeem, of het gebruik wordt vastgelegd, of het systeem enige informatie afgeeft aan andere (netwerk)systemen en of een onbedoelde privacyinbreuk ontstaat als het systeem onjuist wordt gebruikt. (zie paragraaf 4.10). Wanneer de 'beta release' plaatsvindt, is gecontroleerd of alle privacybeschermende middelen zijn ingebouwd, is een laatste privacycontrole uitgevoerd en is het systeem klaar voor gebruik.

Een privacyveilig informatiesysteem (PRIVIS) kan in algemene zin drie privacybeschermende opties aanbieden:

1. Anonieme of pseudonieme verwerking van persoonsgegevens al dan niet ten gevolge van het toepassen van het beginsel van gegevensminimalisatie.
2. Verwerking van (klare, niet versleutelde) persoonsgegevens met in achtneming van alle op het informatiesysteem betrekking hebbende rechtsregels die persoonsgegevens beschermen door ingebouwde privacyrealisatiebeginselen (zie hoofdstuk 2).
3. Een mengvorm van de twee voorafgaande opties.

De in hoofdstuk 5 besproken privacyontologieën en andere mechanismen om de privacywetgeving automatisch bij de verwerking toe te passen, zullen afhankelijk van de gekozen beschermingsoplossing medebepalend zijn voor het ontwerp. De juridische knowhow die door middel van de privacyontologieën is ingebouwd,

10 Canon, 2004, p. 178-192.
11 Canon, 2004, p. 194-212.

moet ervoor zorgdragen dat de gehele verwerking plaatsvindt binnen de door de EU-privacyrichtlijnen gestelde grenzen.

6.2. Ontwerpeisen te stellen aan PRIVIS

Het ontwerp van PRIVIS met daarbij behorende programmatuur en componenten, dient zodanig te zijn dat een dergelijk IS de persoonsgegevens verwerkt conform de privacyrealisatiebeginselen. Het ontwerp van een privacymanagementsysteem (PMS) die aan PRIVIS kan worden toegevoegd, zorgt ervoor dat het PMS 'meekijkt' in de PRIVIS- of de interne verwerking en de uitwisseling en verspreiding van persoonsgegevens aan derden in de omgeving (zie paragraaf 5.4.6) van het informatiesysteem juist (conform de Richtlijnen 95/46/EG, 2002/58/EG en 2006/24/EG) verloopt en rekening wordt gehouden met de privacy-voorkeuren van het gegevensverstrekkende individu.[12]

6.2.1. Juridische specificaties

Om een PRIVIS te ontwerpen, dienen de in paragraaf 2.13 vermelde juridische specificaties,[13] in het ontwerp te worden meegenomen:

1. Beginselen die aan de basis van PRIVIS-ontwerp ten grondslag liggen:
   a. Gegevensminimalisatie (maximale anonimiteit, zo min mogelijk gegevens en zo vroeg mogelijke verwijdering van data).
   b. Transparantie of openheid betreffende de verwerking.
   c. Beveiliging conform de privacyrisico-, bedreigings- of impactanalyse.
2. Beginselen met betrekking tot de rechtmatige verwerking. De verwerking in het informatiesysteem dient zodanig te zijn ingericht dat de volgende privacyrealisatiebeginselen worden gerealiseerd:
   a. Rechtmatigheid (bijvoorbeeld toestemming).
   b. Bescherming van speciale categorieën persoonsgegevens.
   c. Finaliteit, doelbinding van de te verwerken persoonsgegevens.
3. Kwaliteit van gegevens. Voor een uitvoerige opsomming van de vereisten onder deze specificatie wordt verwezen naar paragraaf 2.5.8.
4. Rechten van het persoonsgegevens genererende individu. Het systeemontwerp dient twee situaties te onderscheiden:
   a. De persoonsgegevens die worden verkregen van de betrokkene.
   b. De persoonsgegevens worden op een andere manier verkregen.

---

12 Van Blarkom, Borking & Olk, 2003, p. 141.

13 Deze ordening van privacyuitoefeningsbeginselen is door de Landesbeauftragter für den Datenschutz in Schleswig-Holstein (ULD) opgesteld voor het doen van privacyevaluaties in het kader van de programma van de ULD betreffende de "'Gütesiegel' voor IT Producten en Diensten", https://www.datenschutzzentrum.de/guetessiegel/.

De inrichting van het systeem dient zodanig te zijn dat voldaan wordt aan:
- Informatievereisten o.a. over wie de verantwoordelijke is.
- Melding van de verwerking van persoonsgegevens.
- Inzage, correctie, verwijdering, blokkering.
- Verzet tegen verwerking.

5. Gegevensverkeer met landen buiten de EU en EEA. De overdracht van persoonsgegevens aan een derde land (d.w.z. niet een lidstaat van de EU, EEA of land of instantie waarvan de adequate bescherming van persoonsgegevens door de EU-Commissie is vastgesteld) is slechts toegestaan als het land in kwestie een adequate mate van bescherming biedt. Derhalve dient in het systeem de bestemming van de gegevens geverifieerd te worden en wanneer de gegevens niet verzonden mogen worden, dient de verwerking te worden geblokkeerd.
6. Specifieke restricties op bepaalde vormen van gegevensverwerking ex Richtlijn 2002/58/EG[14] en speciale eisen uit de Richtlijn 2006/24/EG.

Van belang is Overweging 46 van Richtlijn 95/46/EC, die benadrukt dat:

> "the protection of the rights and freedoms of the individuals with regard to the processing of personal data requires that appropriate technical and organisational measures be taken, both at the time of the design of the processing system and at the time of the processing itself" en Overweging 30 van Richtlijn 2002/58/EC waarin staat dat:
>
> "systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum".

Paulus[15] wijst erop dat de juridische vereisten evenwel niet direct bruikbaar zijn als technische ontwerpvereisten voor software engineering, als niet vooraf zowel de verantwoordelijkheid als het concrete technische gebruik is vastgesteld. Voor generieke softwarepakketten is dat een probleem. Is de bouwer, de systeemintegrator of degene die het systeem heeft aangeschaft en gebruikt verantwoordelijk (afhankelijke van de gesloten overeenkomst) of zijn zij dat allemaal? Het antwoord op deze vraag heeft gevolgen voor het ontwerp. Bijvoorbeeld: de functie in de applicatie die te maken heeft met het verwijderen van data kan in het ontwerp worden ingebouwd. De systeemintegrator kan het gebruik van deze functie in het systeem configureren, maar de feitelijke beslissing om de data te laten verwijderen, is de verantwoordelijkheid van degene die het systeem gebruikt. Of moet deze functie zo worden gebouwd dat de verwijdering altijd automatisch plaatsvindt?

Een ander voorbeeld: het privacyrealisatiebeginsel, dat gegevens moeten worden opgeslagen conform het doel waarvoor de data zijn verzameld, dient in

14 Artikel 3 (1) van de Richtlijn 2002/58 betreffende de toepasbaarheid. Zie ook artikel 2 van de Richtlijn 2002/21/EG. Uitzonderingsregel over toepasbaarheid zie artikel 5 (3) van de Richtlijn 2002/58/EG.

15 S. Paulus is Senior Vice President Product Security Governance bij SAP.

de programmatuur in functies te worden gedefinieerd. Deze juridische formulering verbiedt bijvoorbeeld niet dat 'data warehousing' na de opslag plaatsvindt. Ten slotte: als de ontwerpspecificatie inhoudt dat door het systeem op het scherm de boodschap moet worden weergegeven "verwijder privacy gerelateerde data", dan moet eerst de verwijderfunctie worden ontwikkeld en vervolgens zal het begrip "privacy gerelateerde data" sluitend moeten worden gedefinieerd zodat iedere ontwerper op dezelfde wijze ermee om kan gaan. Anders bestaat er geen zekerheid dat inderdaad alle "privacy gerelateerde data" zijn verwijderd.[16]

Samenvattend: het ontwerp van PRIVIS dient rekening te houden met de hiervoor vermelde juridische specificaties, de uitkomsten van de privacyrisico-, privacybedreigings- of privacyimpactanalyse, het daarbij noodzakelijke beveiligingsniveau en de in te zetten PET-maatregelen.

6.2.2. Vereisten voor beveiliging

Uit de juridische vereisten kunnen zonder dat er een privacyrisico-, bedreigings- of effect-(impact)-analyse is uitgevoerd, toch gedeeltelijk de bedreigingen worden gedistilleerd. De artikelen 2, 6, 7, 8, 9,10, 11, 12, 13, 17 en 25 van Richtlijn 95/46/EG en de artikelen 4, 5, 6, 7, 8, 9, 11 en 12 van de Richtlijn 2002/58/EG kunnen door de ontwerper van PRIVIS geïnterpreteerd worden als door de wetgever beoogde tegenmaatregelen om een aantal specifieke bedreigingen te pareren. Deze onderliggende bedreigingen zijn evenwel niet als zodanig in de overwegingen of de artikelen van de beide Richtlijnen geformuleerd. Zou dit wel zo zijn, dan zou dat de ontwerpers en verantwoordelijken een aanmerkelijk beter houvast geven voor het nemen van organisatorische en technische beveiligingsmaatregelen. De lijst van primaire bedreigingen en risico's voor PRIVIS zal dan ook de privacyrechtsregels van het rechtssysteem waarin PRIVIS wordt gebruikt, weerspiegelen.[17] Er kan, zoals in hoofdstuk 4 is uiteengezet, een veertiental bedreigingen uit de Europese privacyrechtsregels worden gedistilleerd, die op hun beurt zijn samen te vatten als:

1. Geheim bezit van of controle over persoonsgegevens.
2. Geheime verwerking van persoonsgegevens: er is een gebrek aan transparantie en er is geen vrije, ondubbelzinnige en specifieke toestemming van de betrokkene.
3. De verwerking van persoonsgegevens vindt plaats in strijd met de privacyvoorkeuren van de betrokkene.
4. De verwerking van persoonsgegevens vindt in strijd met de wet plaats en is onrechtmatig.
5. Niet-toegestane verwerking buiten de EU: verspreiding van persoonsgegevens vindt plaats naar een land, dat geen (adequate) bescherming biedt zoals die geldt binnen de EU.

---

16 Paulus, 2008, p.6-7, beschikbaar op http://prise.oeaw.ac.at/conf_contrib.htm.
17 Van Blarkom, Borking & Olk, 2003, p. 26-27.

6. Geen of beperkte reactie van de verantwoordelijke op de aanmaning (bijvoorbeeld: verzoek tot inzage of blokkering) van de betrokkene.
7. Ernstige privacyinbreuken en onzorgvuldig datamanagement. Er zijn geen passende technische en organisatorische maatregelen genomen om persoonsgegevens te beveiligen.

6.3. Scheiding van rollen binnen PRIVIS

In het PRIVIS-ontwerp dient rekening te worden gehouden met de binnen de systeemlogica gescheiden rollen van de betrokkene (het individu dat zijn persoonsgegevens afstaat), de verantwoordelijke (natuurlijke en/of rechtspersonen) en, wanneer zich dit voordoet, de bewerker, zoals gedefinieerd in artikel 2 (a), 2 (d) en 2 (e) van de Richtlijn 95/46/EG. Deze rollen kunnen worden teruggevonden in het privacyomgevingsmodel van PRIVIS waarin de juridische en feitelijke omgeving van het systeem is weergegeven. Mede bepalend voor het ontwerp zijn ook de algemene privacyverwachtingen van de gebruikers van het systeem (bijvoorbeeld de klanten van het bedrijf). Deze verwachtingen worden gevoed door het privacybeleid van de organisatie. Wanneer het ontwerp van het systeem ervoor zorgt, dat de ervaringen van de gebruikers met de verwachtingen overeenkomen, dan heeft dat een positief effect op de reputatie, de merkbekendheid, het vertrouwen en de binding van de klanten. Omdat encryptie[18] bij PRIVIS veelvuldig als PET-maatregel zal worden toegepast, kan het inzetten van een 'Trusted Third Party' (TTP) noodzakelijk zijn voor het beheer en de uitwisseling van de encryptiesleutels die gebruikt worden voor de vercijfering en ontcijfering van de persoonsgegevens.[19]

6.4. Naast privacyrechten: privacyplichten

Zoals uit het bovenstaande blijkt, dient er met zeer veel specificaties bij het ontwerpen van PRIVIS en andere privacyveilige applicaties rekening gehouden te worden. Naast de privacyrechten van degenen die de persoonsgegevens verstrekken, staan de (waar wettelijk vereist) expliciete toestemmingen van de betrokkenen betreffende de verwerking van hun persoonsgegevens en de privacyplichten van de verantwoordelijke. Deze drie elementen dienen uiteindelijk in de architectuur van PRIVIS hun plaats te krijgen. In feite leiden deze drie elementen tot een doelgerichte beperking van de ontwerpvrijheid doordat de beperkingen tot niets anders mogen leiden, dan tot de realisatie van het beoogde privacyveilige informatiesysteem.[20]

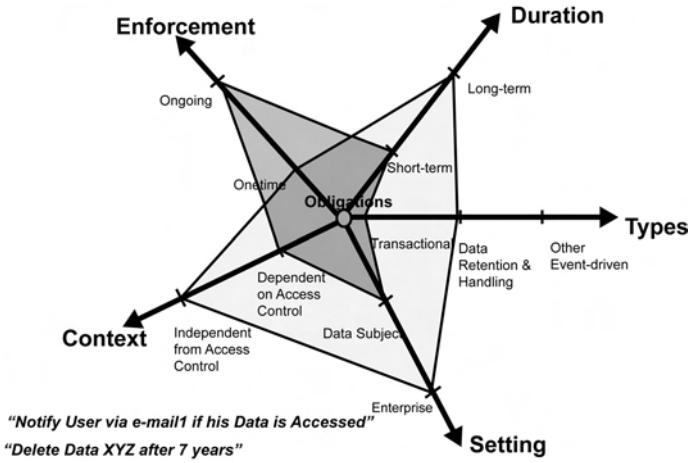
---

18 Kleve, 2004, p. 86-92, voor een verhandeling over single pad en asymmetrische encryptie.
19 Duthler, 1998. Duthler heeft een uitvoerig onderzoek naar juridische modellen voor trusted third parties gedaan. Voor de privacyaspecten van een TTP, zie Versmissen, 2001.
20 Dietz, 2002, p. 3.

Dietz & Mulder merken over dit soort architectuurbeginselen op dat binnen de 'Enterprise Architecture' hiervan veelvuldig gebruik wordt gemaakt. Hun functie is om te dienen als referentiekader voor implementatieprojecten. Een architectuurprincipe heeft een naam, een omschrijving, een reden en beschrijft de implicaties. De doelstelling van het formuleren van architectuurprincipes is om de vrijheidsgraden van de onderliggende niveaus zodanig in te perken dat de ontwerpen voor deze niveaus in lijn zijn met de strategische doelstellingen voor de organisatie als geheel (bijvoorbeeld de borging van cruciale informatiestromen tussen domeinen). Deze inperking kan zowel positief als negatief worden geformuleerd. Positief geformuleerde beginselen geven aan hoe de onderliggende oplossingen eruit moeten zien, bijvoorbeeld alle gegevens zijn via een portaal te benaderen. Negatief geformuleerde beginselen hebben het karakter van verboden, bijvoorbeeld onzichtbare koppelingen zijn verboden. Ter wille van de maximaal mogelijk bereikbare privacybescherming is de standaard uitgangspositie van het ontwerp van PRIVIS dat daar waar dat mogelijk is, alle interacties met en binnen PRIVIS a priori anoniem of onder pseudoniemen geschieden.

De vraag is nu hoe al die (complexe) privacyplichten gekoppeld aan de verwerking van persoonsgegevens in het ontwerp kunnen worden geïncorporeerd zodat een privacyveilige toegangscontrole, een privacyveilige behandeling van de persoonsgegevens en een privacyveilig beheer gedurende de levenscyclus van de verwerkte en opgeslagen persoonsgegevens kan worden gerealiseerd. Hoe complex en multidimensionaal dit vraagstuk is, blijkt uit figuur 6.1. [21]

Figuur 6.1: Voorbeeld privacyverplichtingen, Cassassa Mont, 2006, p. 11.



21 Cassassa Mont, 2006, p. 11.

In deze figuur wordt in twee gedeeltelijk overlappende voorbeelden geïllustreerd met welke factoren rekening gehouden moet worden. In het voorbeeld zijn dat de naleving van de verplichting, de periode waarbinnen de verplichting moet worden uitgevoerd, de aard van de verplichting (bijvoorbeeld wettelijk), de omstandigheden die voor de verplichting van kracht zijn, zoals: geldt er een toegangscontrole voor het individu van wie de persoonsgegevens zijn of het bedrijf dat de gegevens verwerkt, en de context waarbinnen de verplichting valt. Het donkergrijze vlak in de figuur betreft de privacyplicht om de gebruiker via een bepaald type e-mail in te lichten wanneer zijn gegevens zijn ingezien en het lichtgrijze vlak gaat over de privacyplicht om de persoonsgegevens XYZ na zeven jaar volledig uit het informatiesysteem te verwijderen. Om dergelijke en andere privacyplichten goed te beheren is het *Obligation Management System* (OMS) ontworpen**.** Dit systeemcomponent regelt en ondersteunt het beheer, de planning, handhaving en monitoring van de privacyplichten betreffende de persoonsgegevens binnen PRIVIS. De privacyplichten in dit systeem bestaan uit een reeks van beperkingen voortvloeiend uit de privacy- en andere wetgeving die op de verzamelde persoonsgegevens moeten worden toegepast, met daarnaast de wensen van de eindgebruikers en de plichten van de medewerkers die zich met de bescherming van de persoonsgegevens bezighouden.[22] De privacyplichten dwingen softwarematig een privacybewust en privacyveilig levenscyclusbeheer van persoonsgegevens binnen PRIVIS af. In het PRIVIS-systeem zijn privacyplichten geformuleerd als een 'reactive rule' bestaande uit drie kernaspecten:

a. Het doel van de specifieke privacyplicht, te weten hoe het desbetreffende persoonsgegeven moet worden beheerd.
b. De gebeurtenissen en voorwaarden die de specifieke privacyplicht teweegbrengen (met inbegrip van op tijd gebaseerde gebeurtenissen, of de controle van op inzage gebaseerde gebeurtenissen, etc.).
c. De acties die moeten worden genomen zodra de specifieke privacyplicht wordt teweeggebracht (met inbegrip van het verwijderen van gegevens, het berichten van gebruikers, uitvoering van complexe 'workflows', etc.).

Deze privacyplichten kunnen in relatie tot de handhaving van korte en lange termijn van aard zijn, en kunnen óf een eenmalige handhaving vereisen óf, in het geval van lopende verplichtingen, binnen een bepaald tijdsbestek, een repeterende en veelvoudige handhaving vereisen.[23] Bovendien wordt aan een dergelijke privacyverplichting ook gekoppeld wie verantwoordelijk is voor het uitvoeren van de privacyplicht, de mogelijke uitzonderingen en de speciale gevallen.[24] In een meer abstracte zin wordt in het systeem een privacyplicht geconstrueerd als

22 In de Amerikaanse Gramm-Leach-Blileywet van 1999 (Public Law 106-102 106th Congress) staat de algemene en abstracte privacyplicht: "Every financial institution has an affirmative and continuing obligation to respect customer privacy and protect the security and confidentiality of customer information" en dient in specifieke privacyplichten binnen het informatiesysteem te worden omgezet.
23 Casassa Mont, 2006, p. 4.
24 Casassa Mont, 2005, p. 57-60.

een verzameling van alle unieke identificerende gegevens (i), een verzameling van alle mogelijke doelen (t), een verzameling van alle mogelijke gebeurtenissen (e) en een verzameling van alle mogelijk te nemen acties (a) waarbij voor de gebeurtenissen alle logische combinaties (AND, OR, NOT) worden gedefinieerd en voor de acties de operationele combinaties, zoals de volgorde van de te nemen acties, worden vastgesteld.[25] Dit systeem is geen toekomstmuziek. Inmiddels heeft het PRIME-project[26] een werkend OMS-prototype opgeleverd en zijn er commerciële aanbieders (zoals IBM en HP) die dit systeemcomponent hebben geïntegreerd in de door hen aangeboden privacymanagementsysteemprogrammatuur.

6.5. Gegevensminimalisatie als middel voor privacybescherming

In hoofdstuk 5 is aangegeven dat er een aantal technisch realiseerbare mogelijkheden is, die zouden kunnen leiden tot een privacyveilig informatiesysteem.

Een van deze mogelijkheden steunt op het privacyrealisatiebeginsel van de gegevensbeperking met gebruik van de 'Identity Protector'. Het beginsel van dataminimalisatie is een van de hoekstenen van de privacybescherming. Dit beginsel stoelt op artikel 6 (1) b, c en e van Richtlijn 95/46/EG en 14 (3) van Richtlijn 2002/58/EG en betreft zakelijk weergegeven: maximum anonimiteit, zo min mogelijk gegevens verzamelen en zo vroeg mogelijke verwijdering van data. In vervolg op het beweerde in hoofdstuk 2 kan worden vastgesteld, dat het ontwerpvoordeel van dit principe is dat gegevens die niet opgeslagen zijn ook niet behoeven te worden beveiligd en niet beheerd behoeven te worden. Al hoewel de Richtlijn zich richt tot de lidstaten en niet tot individuen, is voor ontwerpers toch het bepaalde in artikel 14 (3) van de Richtlijn 2002/58/EG, van belang. Dit artikel bepaalt dat in het ontwerp van de 'terminals' zodanige voorzieningen moeten worden genomen dat de gebruikers het gebruik van hun persoonsgegevens kunnen beschermen en controleren. Bovendien stelt Overweging 30 van deze Richtlijn uitdrukkelijk dat systemen bestemd om te worden gebruikt voor elektronische communicatienetwerken en dienstverlening zo moeten worden ontworpen, dat het gebruik van persoonsgegevens wordt gelimiteerd tot het strikt noodzakelijke minimum. Dit beginsel houdt tevens in dat waar mogelijk in het ontwerp gestreefd moet worden naar het niet-registreren van (onmiddellijk) identificerende data. Het beginsel regardeert ook de vernietiging van de persoonsgegevens zodra deze data niet langer (dan strikt noodzakelijk voor de verwerking van de data) zijn vereist. Dit laatste stelt aan de ontwerper de eis

25 Casassa Mont, 2006, p 31: "A privacy obligation is <i,t,L(e),C(a)> tuple: <i,t,e,a> € <1,2^T,2^E,2^A>; L: defines a logical combination (AND,OR,NOT) of events; C(a): defines an operational combination of actions, such as a consequence of actions; i: set of all unique identifiers; t: set of all possible targets; E: set of all possible events; A: set of all possible actions." € staat voor: "is lid van".

26 EU research PRIME (Privacy and Identity Management in Europe) project Contract No. 507591(2004-2008).

om de data op een zodanige manier op te slaan dat (automatisch) de identificatie van de personen waarop de persoonsgegevens betrekking hebben niet langer kan plaatsvinden dan nodig is voor het doel waarvoor de gegevens werden verzameld en verwerkt.

Voor verkeersgegevens is dit ontwerpvereiste in artikel 6 van Richtlijn 2002/58/EG vastgelegd waarin wordt bepaald: "Verkeersgegevens van abonnees (...) die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1."

Wanneer wettelijk het geven van toestemming vereist is, dienen gebruikers van het systeem, bijvoorbeeld via een mededeling op het scherm van hun computer of terminal, op de hoogte worden gebracht over de geplande bewaartermijn van hun persoonsgegevens. Het ontwerp dient zo ingericht te zijn, dat deze informatie aan de gebruiker vóór het geven van de toestemming tot verwerking wordt gegeven. De gebruikers moeten er vanuit kunnen gaan dat na de expiratiedatum de persoonsgegevens of verwijderd worden of worden geanonimiseerd. Dat zou bijvoorbeeld in het privacybeleid van de verantwoordelijke op de website kunnen worden vermeld.

Gegevensminimalisatie kan ook inhouden, dat het informatiesysteem zo is ingericht dat wanneer de persoonsgegevens slechts tijdelijk nodig zijn, de gegevens in eerste instantie worden verwerkt en daarna direct worden vernietigd of door middel van cryptografische technieken losgekoppeld worden van de overige gegevens. Het vernietigen en/of loskoppelen van data moet wel onomkeerbaar gebeuren.

In hoofdstuk 5 is uiteengezet dat de 'Identity Protector' een systeemmodule betreft die de uitwisseling van de identiteit van de gebruiker tussen de overige systeemmodules en processen beheerst. Binnen het informatiesysteem kan met PET-maatregelen de 'Identity Protector' zo worden ingesteld, dat bijvoorbeeld de identiteit van de gebruiker bij rechtmatig gebruik niet vrijgegeven wordt. De 'Identity Protector' kan afhankelijk van de applicatie de identiteit van de gebruiker afschermen van zowel medegebruikers als diensten die binnen het informatiesysteem geleverd worden. De koppeling tussen het identiteitsdomein en de pseudo-identiteitsdomeinen kan worden gemaakt indien dit noodzakelijk is voor het verwerkingsproces.

Samenvattend: de ontwerper van PRIVIS zal op grond van artikel 6 en 7 van de Richtlijn 95/46/EG vooraf zich vragen moeten stellen. Het EuroPrise-project heeft een catalogus samengesteld met alle relevante vragen die per juridische specificatie (zie paragraaf 6.2.1) zijn gegroepeerd. Het totaal aantal vragen is 353. Ter illustratie volgen zes vragen met betrekking tot dataminimalisatie hieronder:

1. Is het mogelijk om de verwerking van persoonsgegevens te laten plaatsvinden zonder gebruik van identificerende gegevens?
2. Tot welk minimum kan het aantal identificerende gegevens dat voor het specifieke doel wordt verzameld, worden beperkt?

3. Kunnen de data automatisch worden geanonimiseerd of gepseudonomiseerd? Moet er een voorziening worden getroffen om dit zonodig op verzoek van de betrokkene achteraf te laten gebeuren? Kunnen hiervoor parameters worden ingebouwd? Hoe kunnen de gepseudonimiseerde persoonsgegevens worden beveiligd tegen te gemakkelijke heridentificatie?
4. Welke combinatie van persoonsgegevens is werkelijk noodzakelijk? Welke criteria kunnen hiervoor ingebouwd worden? Tot op welke hoogte is het werkelijk noodzakelijk om bepaalde data te combineren voor het functioneren van het systeem?
5. Is het mogelijk om binnen het systeem onnodige schaduwdossiers ('shadow files') bij het opnieuw inloggen te vermijden? Als de 'shadow files' noodzakelijk zijn, hoe kunnen deze dan optimaal worden beveiligd tegen onrechtmatige toegang van derden?
6. Als data doorgegeven moeten worden naar andere systemen en verantwoordelijken, kunnen dan functionaliteiten worden ingebouwd die gegevens uitfilteren die niet nodig zijn om door te sturen?

Waartoe deze vragen kunnen leiden bij het ontwerp van PRIVIS wordt in de paragrafen 6.5 tot en met 6.11 aangetoond. Er komen drie modellen informatiesystemen met PET-architectuur aan de orde. De eerste is de metazoekmachine Ixquick (6.5.1), de tweede is het ziekenhuisinformatiesysteem (6.7) en het derde is het Victim Tracking and Tracing System (ViTTS) (6.8). Ten slotte volgt de privacymanagementarchitectuur met PET-mengvormen in de bespreking van de privacy incorporated software agent (PISA) in de paragrafen 6.9 tot en met 6.11.

6.5.1. De metazoekmachine Ixquick

Een voorbeeld van de toepassing van privacy verhogende technieken (PET) door middel van dataminimalisatie is Ixquick. Ixquick (www. ixquick.com) is een 'meta-search engine', die door een in Nederland gevestigd bedrijf wordt geëxploiteerd en wereldwijd wordt aangeboden in zeventien talen.[27] Een 'meta-search engine' is een zoekmachine, die de zoekopdracht van een gebruiker tegelijkertijd spreidt over twaalf zoekmachines zoals: All the web, Yahoo, Google, Mozilla, Wikipedia, Ask, etc. De metazoekmachine combineert de resultaten en destilleert daaruit de meest relevante resultaten. Ixquick gebruikt daarvoor een unieke methode. Uit de resultaten die gegenereerd zijn door andere zoekmachines, haalt Ixquick per zoekmachine de eerste tien van de resultaten. Ieder resultaat dat in de top tien voorkomt krijgt een ster. Als een resultaat in vijf zoekmachines in de top tien voorkomt, dan krijgt het gevonden resultaat vijf sterren. Daaruit kan de gebruiker van Ixquick de relevantie van de resultaten afleiden.[28]

---

27 http://ixquick.nl/.
28 Conform de mededelingen op de webpage van Ixquick na geklikt te hebben op Ixquick info.

Ixquick's businessmodel is dat zij geld verdient met het plaatsen van advertenties bij de zoekresultaten. De advertenties worden verzorgd door de advertentie-aanbieder en sluiten nauw aan bij de zoekvraag die een gebruiker heeft gesteld.[29] In 2003 en 2004 nam het internetverkeer ten gevolge van minder zoekopdrachten voor Ixquick met meer dan 20% af, omdat de zoekmachine geen grotere toegevoegde waarde opleverde dan andere zoekmachines. In 2005 zakte het internetverkeer van Ixquick nog eens met 5% en stabiliseerde later dat jaar. De oorzaak voor de stabilisering lag in het feit dat Ixquick de website, de manier van de presentatie en de dienstverlening totaal had vernieuwd. In 2006 en 2007 nam het internetverkeer weer toe, niet zozeer door de vernieuwde website, maar vooral omdat Ixquick de zoeker en de zoekresultaten sinds juni 2006 anonimiseerde. Ten gevolge van een reeks hieronder te behandelen technische maatregelen, waaronder gegevensminimalisatie en encryptie-(hashing)-technieken[30] nam het internetverkeer in 2006 weer met 15% toe en in 2007 met 6%.[31] In 2008 is het gebruik ten gevolge van aanvullende PET-maatregelen verder gestegen. In de eerste helft van dat jaar volgens het management met 18%. In het interview met Dijkman & Borking[32] heeft het management van Ixquick verklaard dat er geen veranderingen in de bedrijfsvoering van Ixquick hadden plaatsgevonden. Het is aannemelijk te veronderstellen dat als Ixquick haar dienstverlening niet had voorzien van PET, dat dan het internetverkeer ten minste met 5% per jaar zou zijn blijven zakken. De reden voor Ixquick om deze privacybeschermende voorzieningen toe te passen, lag in het feit dat een geanonimiseerde zoekmachine die tevens de privacy van de bezoekers beschermt, een 'unique selling point' (USP) oplevert. Ixquick is de eerste geanonimiseerde en privacybeschermende zoekmachine.

Hoe kan nu vastgesteld worden dat de door Ixquick gebruikte techniek van gegevensminimalisatie inderdaad een privacyveilig informatiesysteem oplevert? Het probleem met zoekmachines vanuit een privacyperspectief is dat zoekmachines zowel de IP-adressen (die aan een gebruiker kunnen worden gerelateerd) vastleggen, als ook het gebruikte computersysteem, het besturingssysteem, de browser, de zoektermen, de datum en het tijdstip waarop de zoekterm is ingevoerd.[33] Weichert concludeert dat: "Werden viele solche Anfragen gemeinsam ausgewertet, lassen sich hieraus präzise Interessenprofile erstellen, also mit welchen Themen eine Person sich zu welcher Zeitbeschäftigt hat. Werden diese Angaben einer konkreten Person zugeordnet, so lässt sich aus dem Anfrageprofil

29 Andriessen, 2008 p. 10.

30 Van Vliet, 2008, p. 5: "J.J. Borking performed the legal part of this evaluation, specifically the section "Compliance with data protection and data security regulations" and "Set 2: Legitimacy of Data Processing. The technical part is performed by F. van Vliet".

31 Dijkman &.Borking, 2008, p. 13.

32 Dijkman & Borking, 2008, p. 13.

33 In de film The Net (regie: Irwin Winkler), uitgebracht in 1995,waarvan het scenario volledig op internet is gebaseerd, is goed te zien hoeveel informatie gebruikers van internet achterlaten en wat er kan gebeuren als de beveiliging en de privacy bescherming het laten afweten.

zumindest bei Personen, die regelmäßig Suchmaschinen nutzen, ein langfristiges Interessenprofil erstellen."[34] Weichert stelt voorts dat: "Die Analyse der Datenschutzprobleme bei Internet-Suchmaschinen zeigt, dass hier das Recht auf informationelle Selbstbestimmung derzeit nicht hinreichend gewahrt wird. Die gesetzlichen Regelungen sind völlig unzureichend und teilweise auf die eingesetzte Technik nicht anwendbar; die Vollzugsdefizite sind groß; die Aufsichtsbehörden haben keine praktischen Handhaben zur Durchsetzung des Datenschutzes."[35]

Daarom zijn privacybeschermende maatregelen in een zoekmachine belangrijk, want: "die Löschung bzw. Anonymisierung der Nutzungsdaten erfolgt, kann für die Betroffenen von eminenter Bedeutung sein, da Dritte an einer zweckentfremdenden Nutzung ein großes Interesse haben können und die Internet-Nutzer beeinträchtigt werden können. Selbst staatlicherseits kann an diesen Daten ein – nicht immer legitimes – Interesse bestehen", aldus Weichert.[36]

Tussen 29 februari en 23 juni 2008 hebben Borking en Van Vliet in het kader van het door de EU gesubsidieerde researchproject EuroPrise[37] een onderzoek gedaan[38] naar de juistheid van de door Ixquick geclaimde privacyvriendelijkheid van het systeem. Daarbij is als norm gehanteerd de wettelijke vereisten van de Richtlijnen 95/46/EG en 2002/58/EG. Het onderzoek vond plaats in het kantoor van de directie die belast is met de dagelijkse gang van zaken van Ixquick, de plaats waar de servers van Ixquick waren geplaatst en door middel van directe analyse van de website en de processen. Alle systeemdocumentatie is bestudeerd, alsmede de contracten die ten behoeve van Ixquick waren gesloten, onder andere met betrekking tot het adverteren op de website. Er zijn verschillende interviews gehouden met het management, een system administrator en een programmeur zowel ter voorbereiding van het onderzoek als ten tijde van het onderzoek.

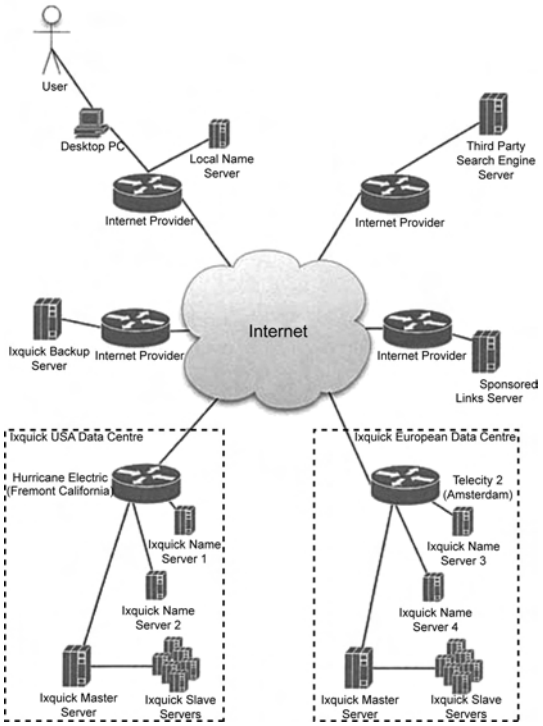
a. De architectuur

Uit de architectuur van Ixquick (zie in figuur 6.2 de twee gestippelde rechthoeken) valt op te maken, dat de servers[39] zowel in Europa (Amsterdam) als in de Verenigde Staten (Fremont, California) staan. Zoals bij de juridische beoordeling in dit hoofdstuk zal blijken is dit juridisch een belangrijk feit.

---

34 Weichert, 2007, p. 188.
35 Weichert, 2007, p. 196.
36 Weichert, 2007, p. 195.
37 Het project wordt gesubsidieerd door de Europese Commissie onder het eTEN Programma. Het EuroPrise project begon op 10 juni 2007 en is op 28 februari 2009 beëindigd. Zie: http://www.european-privacy-seal.eu/about-europrise/fact-sheet.
38 Aan de hand van versie 0.2 van het door EuroPrise in 2007 ontwikkelde Evaluation Manual.
39 De configuratie in Amsterdam (Telecity 2) en Fremont (Hurricane Electric) is Ixquick Name servers, Ixquick Master Server en Ixquick Slave servers.

Figuur 6.2: Architectuur Ixquick, Borking & Van Vliet, 2008, p. 7.

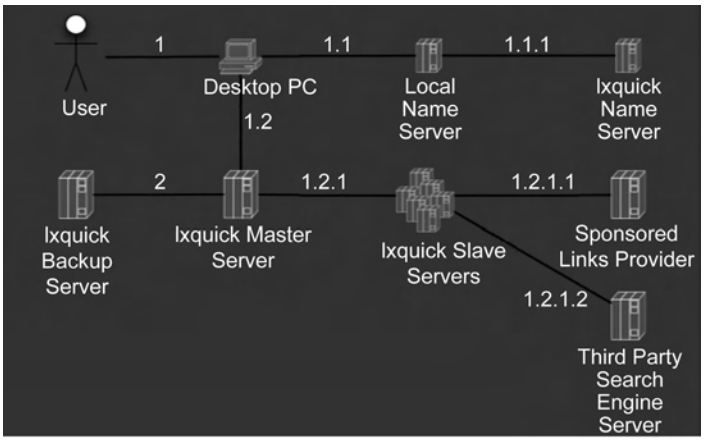


Figuur 6.2 bevat in de linkerbovenhoek de representatie van de gebruiker met zijn zoekvraag, die via internet contact maakt met de server van Ixquick en toont voorts de mogelijke routering van zijn zoekvraag naar de verschillende servers.

b. Het zoekproces

Figuur 6.3 laat de stappen in het zoekproces bij het gebruik van Ixquick zien, beginnend bij de gebruiker van de zoekmachine, waarna de zoekvraag met het IP-adres uitwaaiert over de verschillende servers, die onder meer een rol spelen bij de anonimisering van de zoeker (IP-adres) en de zoekvraag.

Figuur 6.3: Zoekproces binnen Ixquick, Borking & Van Vliet, 2008, p. 10.



Het zoekproces (zie de cijfers in figuur 6.3) verloopt als volgt:

1. De gebruiker achter zijn pc gebruikt een browser (een computerprogramma om webpagina's te kunnen bekijken, bijvoorbeeld Windows Internet Explorer, Mozilla Firefox, Safari of Opera) voor het zoeken naar bepaalde zoektermen.

1.1. DNS ('Domain Name System') is het systeem en het protocol dat op het internet voornamelijk gebruikt wordt om domeinnamen naar IP (Internet Protocol) -adressen te vertalen en omgekeerd.[40] DNS vraagt het IP-adres van www.ixquick.com van de 'Local Name Server' (LNS) van de Internet Service provider (ISP).[41] Het DNS verzoek aan de LNS server is buiten de beoordeling gebleven omdat het voor Ixquick onmogelijk is de communicatie tussen de desktop-pc en LNS te beveiligen.

1.1.1 De LNS zoekt het IP-adres van www.ixquick.com op van de Ixquick Name Server. Het IP-adres dat gevonden wordt is het adres van de dichtst bijzijnde 'master server'.

1.2. De pc van de gebruiker communiceert nu met de 'master server' via het protocol voor de communicatie tussen een webclient (meestal een webbrowser) en een webserver). Twee 'cookies' worden door Ixquick aan de gebruiker gestuurd: de 'Preferences Cookie' en de 'Exclude Repetive Results Cookie' en geplaatst op

40 Het werkt als 'telefoonboek' voor internet. Het vertaalt de leesbare naam van de site (hostname), bijvoorbeeld www.Sgoa.org in een IP-adres, bijvoorbeeld *123.45.678.901*. Het IP-adres is een unieke cijfercode waaraan kan worden herleid vanaf welke computer de zoekvraag is gekomen.

41 Van Ammelrooy, 2008, p.9: "Dan Kaminsky... had een fundamentele weeffout ontdekt in de manier waarop computers elkaar vinden op internet." Kaminsky ontdekte dat cache poisoning (manipuleren van het tijdelijk geheugen voor de opslag van IP-nummers van de DNS-servers) makkelijker was dan tot nu toe werd aangenomen, waardoor hackers in staat zijn het internet grondig te ontregelen. Tegenmaatregelen zijn genomen maar niet duidelijk is het of die afdoende zijn.

de computer van de gebruiker. Cookies zijn kleine stukjes data die gebruikt worden in de communicatie tussen een website en de computer van een gebruiker. In de cookie worden verschillende gebruikersinstellingen opgeslagen (zoals bijvoorbeeld de taal of het computersysteem van de gebruiker). Zo kan een website een terugkerende gebruiker 'herkennen'.

1.2.1. De 'master server' stuurt alle http-communicaties[42] met daarin de zoekvraag door naar een van de 'slave servers' (om de communicaties gelijkelijk te verdelen over de 'slave servers').

1.2.1.1. De 'slave server' vraagt de gesponsorde verbinding voor deze zoektermen van de 'Sponsored Links Server' van de advertentie-aanbieder. Alleen een 'one way' (onomkeerbaar) 'hashed' IP-adres en de zoekvraag gaan naar de advertentie-aanbieder en op basis van de vraag levert de advertentie-aanbieder een advertentie bij de zoekterm. Persoonlijke gegevens worden niet vrijgegeven.[43] Hier wordt voor de eerste keer de 'Identity Protector' ingezet en wordt het IP-adres van de gebruiker omgezet in het IP-adres van Ixquick.

Voor alle duidelijkheid: hashen geschiedt met een algoritme (bijvoorbeeld MAC, MD5, SHA) dat de versleutelde persoonsgegevens omvormt tot een stuk tekst (de hashwaarde) op een zodanige manier dat het onmogelijk is het proces om te draaien (decrypten). Wanneer van grote aantallen personen de identificerende gegevens gehashed moeten worden, neemt de betrouwbaarheid af. Het kan voorkomen dat de hashfunctie tot 'botsingen' leidt. De kans neemt dan toe dat verschillende personen bij toeval dezelfde code krijgen. Bij de Stichting Informatie Voorziening Zorg (IVZ) die onder meer verantwoordelijk is voor de zorg aan verslaafden (LADIS) zijn van 1994 t/m 2000 140.200 hashcodes toegekend, terwijl er 145.579 feitelijke unieke personen in LADIS waren opgenomen. Daaruit valt te concluderen dat er 5.307 personen uit het registratiesysteem door 'collision'[44] zijn 'verdwenen'. Dat kan voorkomen worden door in dat geval tweemaal te hashen, dat wil zeggen de eerste maal met bijvoorbeeld een 140 bits sleutel en het resultaat de tweede maal te versleutelen met een 128 bits sleutel.[45]

1.2.1.2. De slave server vraagt, zonder enige identificatie van de gebruiker, de zoekresultaten op voor de zoekterm van verschillende andere zoekmachineservers en de resultaten gaan naar de gebruiker. Hier wordt voor de tweede keer de Identity Protector ingezet en wordt het IP-adres van de gebruiker omgezet in het IP-adres van Ixquick.

2. Een reservekopie van de master server en het systeem wordt elke dag gemaakt.

Nadat het zoekproces is afgerond wordt het IP-adres van een gebruiker van de zoekmachine binnen 48 uur weer gewist uit de databases van Ixquick. De encryptiesleutel voor het 'one way hashed' IP-adres met toevoeging van een

42 Http staat voor HyperText Transfer Protocol.
43 Andriessen, 2008, p. 10.
44 Collision houdt in dat twee sets van dezelfde tekens uit de hash van bijvoorbeeld een naam worden gegenereerd.
45 Ouwehand, 2002, p. 12-14.

wachtwoord,[46] wordt na enige dagen vervangen door een andere. Cookies zonder persoonlijke informatie worden na veertien en negentig dagen gewist.

Andere zoekmachines slaan de persoonlijke gegevens van de gebruikers een langere tijd op. Zo bewaart Google deze zogenoemde 'server logs' maximaal achttien maanden.[47] De gebruiker kan als hij twijfelt aan de betrouwbaarheid van de infrastructuur van waaruit hij de zoekmachine benadert (bijvoorbeeld een internetcafé) altijd een https- (de s staat voor 'secure') verbinding openen.[48] Overigens als de gebruiker de computer niet vertrouwt, dan heeft het gebruik van https geen zin. De beveiliging van https werkt wel als de gebruiker zijn eigen (te vertrouwen) laptop gebruikt op een onbetrouwbaar netwerk. Bij een publiek 'access point' ('wireless' internet) werkt de beveiliging van https ook.

Tijdens het uitvoeren van de zoekopdracht worden twee typen data gegenereerd. Primaire data,[49] direct gerelateerd aan de geboden dienst, in dit geval de zoektermen, en secundaire data,[50] die ontstaan bij het verwerken van de primaire data. Het gaat hier om data in de 'web server log files', zoals bijvoorbeeld de IP-adressen, tijden van bezoek, in de 'application log files', zoals de IP-adressen, de zoektermen, de tijd waarop de zoekopdracht plaatsvond, de gebruikte taal, cookies, waarin voorkeuren en cookies die bij een nieuwe opdracht de reeds eerder verschafte informatie wegfilteren.

Onderzoekers hebben gegevensstromen onderzocht en voor de Ixquick-zoekmachine kunnen er drie stromen onderscheiden worden:

1. Eerste gegevensstroom: wanneer een gebruiker onderzoekstermen op de website van Ixquick invoert, worden zij door de metazoekmachine van Ixquick overgenomen.
2. Tweede gegevensstroom: deze zoektermen worden vervolgens naar verschillende andere zoekmachines verspreid en het zoekresultaat wordt dan geaggregeerd voor de gebruiker/bezoeker van de website. Persoonsgegevens (IP-adressen) worden binnen 48 uur door Ixquick verwijderd. De werkelijke IP-adressen bijvoorbeeld 11.22.33.44 (zie hieronder), worden allemaal vervangen door 0.0.0.0. [51]

46 Het wachtwoord is nodig omdat er te weinig IP-adressen (ongeveerd 4 miljard) zijn.
47 Fleischer googleblog.blogspot.com 11.06.2007; vgl. www.heise.de, 12 juni 2007.
48 Van Vliet, 2008, p. 12.
49 Korff, 2008, p. 3: "Primary data: data, which the IT-product primarily proceeds (data of the data subject, content data)."
50 Korff, 2008, p. 3:"Secondary data: data which additionally incurred during the processing of (primary) data." "These data might be personal data of data subjects, personal data of people operating the product or service, or privacy-relevant configuration data."
51 Van Vliet, 2008, p. 22.

Figuur 6.4: Webserver log file: IP-adressen opgeslagen wanneer de zoekopdracht wordt geregistreerd.

11.22.33.44 - - [21/Apr/2008:02:00:13 0200] "GET/HTTP/1.1" 200 10270 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14"

22.33.44.55 - - [21/Apr/2008:02:00:13 0200] "GETcss/ixquick_result_page.css HTTP/1.1" 304 - "http://eu2.ixquick.com/do/metasearch.pl?" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)"

Figure 9 33.44.55.66 - - [21/Apr/2008:02:00:14 0200] "POST/do/metasearch.pl? HTTP/1.1"; 200 59049 "http://eu2.ixquick.com/do/metasearch.pl" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

Figuur 6.5: Webserver log file na 48 uur: IP-adressen gewist en vervangen door 0.0.0.0.

Figure 10 0.0.0.0 - - [23/Apr/2008:02:00:13 0200] "GET/HTTP/1.1" 200 10270 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14"
Figure 11

Figure 12 0.0.0.0 - - [23/Apr/2008:02:00:13 0200] "GETcss/ixquick_result_page.css HTTP/1.1" 304 -"http://eu2.ixquick.com/do/metasearch.pl?" "Mozilla/4.0
Figure 13 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)"
Figure 14

Figure 15 0.0.0.0.- - [21/Apr/2008:02:00:14 0200] "POST/do/mtasearch.pl? HTTP/1.1" 200 59049 "http://e2.ixquick.com/do/metasearch.pl" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

De IP-adressen worden maximaal 48 uur bewaard om de 'system administrators' in staat te stellen 'scraping'[52] te detecteren en te blokkeren. Alle niet-identificerende informatie wordt na veertien dagen verwijderd. Behoudens Ixquick ontvangen de andere derde partijen slechts de gegevens die nodig zijn voor de te leveren

52 Scraping houdt hier in dat de resultaten die de zoekmachine levert weer gebruikt worden door anderen, bijvoorbeeld voor marketingdoeleinden. Daardoor wordt de zoekmachine door die verzoeken zwaar belast zonder dat daar revenuen tegenover staan.

zoekresultaten. Deze partijen zijn niet in staat om de gebruikers van de Ixquick-service te identificeren.

3. Derde gegevensstroom: aan de advertentiepartner worden de zoektermen getoond als gesponsorde zoektermen en deze worden samen met de landencode en het 'one way hashed' IP-adres verzonden.[53]

Willen gegevens beschouwd kunnen worden als persoonsgegevens dan dient er sprake te zijn van (in)direct tot een persoon herleidbare gegevens.[54] IP-adressen worden aangemerkt als persoonsgegevens. De eerste gegevensstroom bevat persoonsgegevens. De gebruiker die een bepaalde zoekterm invoerde is identificeerbaar omdat zijn IP-adres bekend is. De tweede en derde gegevensstroom bevatten geen persoonsgegevens omdat het IP-adres van de gebruiker wordt omgezet in het IP-adres van Ixquick en het IP-adres van de gebruiker niet wordt verspreid naar andere zoekmachines. Ixquick handelt in feite als een 'anonymizer'. Een anonymizer is een softwareprogramma dat alle direct identificerende persoonsgegevens filtert uit de gegevens die nodig zijn voor het opbouwen van verbindingen via het netwerk.[55]

c. Clickfraude

Om clickfraude[56] te voorkomen wordt bij iedere zoekterm aan de advertentie-aanbieder (sponsored links server) de zoekterm, de landencode en het 'one way hashed' IP-adres verzonden. Het 'hashed' IP-adres wordt met het volgende algoritme berekend:

1. Het IP-adres is gekoppeld met de geheime sleutel, die na een overeengekomen periode van enkele dagen[57] op een totaal willekeurige wijze[58] wordt veranderd, bijvoorbeeld het IP-adres 11.22.33.44 en de geheime sleutel zabcdefgh, met als resultaat 11.22.33.44 zabcdefgh.
2. Een SHA1-hash[59] wordt berekend over het resultaat (1), en leidt tot een hash van bijvoorbeeld vijftig tekens. In het voorbeeld, resulteert de SHA1-hash van 11.22.33.44 zabcdefgh in de code: 9w45bn%#ad3c533bf61d19559f431c61e7de6c95159b2dfdf2.

---

53 Van Vliet, 2008, p. 3-4.

54 Artikel 2 a van Richtlijn 95/46/EG en Overweging 26; WP 136 Opinion #4 On the concept of personal data, Brussels 2007, p. 16-17: IP-adressen zijn persoonsgegevens. Zie http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

55 Klaver, e.a., 2002, p. 52.

56 Clickfraude wordt veroorzaakt door dat iemand bewust elke keer dezelfde advertentiebanner aanklikt om het bedrijf dat daarmee adverteert te benadelen, doordat elke click inhoudt dat het bedrijf een bepaald bedrag verschuldigd is aan de advertentie-aanbieder.

57 De precieze informatie valt onder de non disclosure agreement.

58 Een van de mogelijke random number generators die hier gebruikt kan worden is de system default Perl (Practical Extraction and Report Language) distribution.

59 Hashen geschiedt met een algoritme (bijvoorbeeld MAC, MD5, SHA) dat de versleutelde persoonsgegevens omvormt tot een stuk tekst (de hash-waarde) op een zodanige manier dat het onmogelijk is het proces om te draaien (decrypten). Cannon, 2004, p. 260-262.

3. Slechts een beperkt aantal tekens van resultaat (2) worden voor patroonherkenning gezonden naar de *Sponsored Links Server* van de advertentieaanbieder. Bijvoorbeeld de laatste twintig tekens. In dit voorbeeld zou dat dan alleen 61e7de6c95159b2dfdf2 zijn.

De geheime sleutel (met een sleutellengte van 2^n)[60] maakt het voor de advertentieaanbieder onmogelijk om de hash van ieder mogelijk IP-adres te berekenen en te vergelijken met de ontvangen IP-adressen. Omdat binnen een vaste periode van enige dagen de hashsleutel wijzigt, is het correleren van de hashes van iedere periode onmogelijk, terwijl de sleutellengte *reverse engineering* voorkomt.[61] Omdat de hashed IP-adressen niet gekoppeld kunnen worden met een gebruiker, is er geen sprake van een persoonsgegeven. Naast de bescherming van persoonsgegevens heeft Ixquick nog een privacyveilige oplossing gevonden. Bij clickfraude zou men verwachten dat bij ontdekking de fraudeur wordt aangepakt. In dit geval wordt niet de fraudeur zelf aangesproken, maar de fraude ongedaan gemaakt door de 'clicks' niet in rekening te brengen.

d. Cookies

Het laatste aspect dat met betrekking tot Ixquick privacyverhogende oplossing wordt besproken is het gebruik van 'cookies'. Een 'cookie' is een stukje informatie dat in de browser van de gebruiker wordt opgeslagen, waardoor voor de website het mogelijk wordt om haar gebruikers te volgen (zgn. tracking cookies). Weichert wijst erop dat cookies wel uitgeschakeld kunnen worden, maar "das allerdings dazu führen könne, dass manche Elemente oder Dienste nicht richtig funktionieren".[62] Volgens de Artikel 29 Werkgroep maakt een 'web cookie' een nauwkeurige identificatie van een persoon mogelijk, want gezien het (semi)permanente karakter van de cookie kunnen zoekresultaten met een persoon in verband worden gebracht.[63]

Volgens Weichert leidt dit tot een ontoelaatbare verpersoonlijking. "Werden nun über die IP-Adresse, über ein Cookie oder über sonstige Identifier die personenbezogenen Daten des Nutzenden mit denen des Suchdienst-Profiles kombiniert."[64]

De Ixquickservice gebruikt geen cookies die gebruikers in de gaten kunnen houden. Ixquick maakt wel gebruik van twee cookies voor servicedoeleinden:

1. Een van de cookies (de voorkeurencookie) wordt gebruikt om de zoekvoorkeuren te bewaren, die worden gebruikt voor het volgend bezoek. Het gaat

60 De sleutellengte is vertrouwelijk.
61 Van Vliet, 2008, p. 25.
62 Weichert, 2007, p. 194.
63 WP 29, Opinion 148 on Data Protection Issues Related to Search Engines, Brussels 2008, p. 7.
64 Weichert, 2007, p. 195.

hier om het voorkeursthema en de voorkeurstaal. De houdbaarheidstermijn van deze cookie is negentig dagen, waarna direct vernietiging plaatsvindt.
2. Het tweede cookie (de exclude repetitive results cookie) voorkomt dat dezelfde zoekresultaten worden getoond als de bezoeker/gebruiker weer opnieuw dezelfde zoekterm gebruikt. Dit cookie bevat voor elke zoeksessie een unieke waarde, maar kan niet worden gebruikt om gebruikers te volgen, omdat het direct na de zoeksessie expireert (hetgeen het moment is waarop de gebruiker zijn browser sluit of wanneer hij een nieuwe zoekterm invoert).[65]

Ixquick informeert overigens op de website de bezoekers en gebruikers van de zoekmachine duidelijk over het gebruik van deze cookies, zoals door de Article 29 Working Party is geadviseerd.[66]

6.6. Juridische beoordeling: drie vragen

Bij de juridische beoordeling naar de privacybescherming van de Ixquick metazoekmachine in het EuroPrise-onderzoek wordt aan de hand van vragen over de privacyrealisatiebeginselen nagegaan of de verwerking van persoonsgegevens niet in strijd is met Richtlijnen 95/46/EG en 2002/58/EG. Drie vragen vroegen speciale aandacht. 1 Zijn de EU-privacyrichtlijnen op zoekmachines van toepassing? 2 Heeft de transnationale verwerking van gegevens in derde landen (buiten de EU en EEA) juridische consequenties voor Ixquick en 3 Is de uitoefening van de inzage, wijzigings- en verwijderingsrechten van betrokkene, i.c. de zoeker niet illusoir, waardoor Ixquick een ernstige privacyinbreuk zou plegen?

6.6.1. Richtlijn 95/46/EG van toepassing?

Voorafgaande aan de twee specifieke vragen over de metazoekmachine van Ixquick, diende eerst de vraag beantwoord te worden: zijn op zoekmachines de nationaal wettelijke vereisten voortvloeiende uit de privacyrichtlijnen 95/46/EG en 2002/58/EG van toepassing?

De Artikel 29 Werkgroep betreffende de gegevensbescherming maakt in zijn Opinie 148 over privacy en zoekmachines[67] duidelijk, dat de toepasselijkheid van de Richtlijn 95/46/EG op grond van de artikelen 4 (1) a en 4 (1) c van de Richtlijn 95/46/EG buiten twijfel staat. Opinie 148 stelt op bladzijde 7:

> "The use of cookies and similar software devices by an online service provider can also be seen as the use of equipment in the Member State's territory, thus invoking that Member State's data

65 VanVliet, 2008, p. 5.
66 WP 29, Opinion 148 on Data Protection Issues Related to Search Engines, Brussels, 2008, p. 22.
67 WP 29, Opinion 148 on Data Protection Issues Related to Search Engines, Brussels, 2008, p. 8-11.

> protection law. This issue was discussed in the above mentioned working document (WP56). It stated that "the user's PC can be viewed as equipment in the sense of Article 4 (1) c of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and, as it has been explained in the previous paragraphs, several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory."

Dezelfde opinion 56 geeft als extra voorbeeld het computersysteem voor het reserveren van een passagiersplaats in een vliegtuig:

> "that when a system can be accessed from the EU, even if the equipment of the system is not located in the EU, EU law automatically applies."[68]

Daarentegen is naar het oordeel van de Artikel 29 Werkgroep, noch de Richtlijn 2002/58/EC ("Search engine services in the strict sense do not in general fall under the scope of the new regulatory framework for electronic communications of which the ePrivacy Directive is part"[69]), noch de Data Retentie Richtlijn (2006/24/EC) op zoekmachines van toepassing. Gezien het feit dat zoekmachines niet voldoen aan de definitie in artikel 2 sub c van de 'framework directive' 2002/21/EG en artikel 1 van de daarmee in verband staande Richtlijn 98/34/EG en artikel 5 (2) van Richtlijn 2006/24/EC:

> "No data revealing the content of the communication may be retained pursuant to this Directive", waarover de Article 29 Working Party stelt dat: "Search queries themselves would be considered content rather than traffic data and the Directive would therefore not justify their retention."[70]

Nu blijkt dat alleen de Richtlijn 95/46/EG van toepassing is op zoekmachines, houdt dit in dat de metazoekmachine Ixquick alleen moet worden getoest aan alle bepalingen van de Richtlijn, die in het nationale recht zijn getransponeerd.

Na vastgesteld te hebben dat de data naar een land buiten de EU (de Verenigde Staten) worden getransfereerd (zie figuur 6.2) en dat land geen passende bescherming van persoonsgegevens biedt, diende de tweede vraag beantwoord te worden: heeft de transnationale verwerking van gegevens in derde landen (buiten de EU en EEA) juridische consequenties voor Ixquick? De feiten zijn, dat de verantwoordelijke (in de zin van de Richtlijn) voor Ixquick is gevestigd in Nederland. De verantwoordelijke maakt gebruikt van in haar eigendom zijnde servers in Europa

68 WP 29, Opinion 56 on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites Brussels, 2002, p. 4.
69 WP 29, Opinion 148 on Data Protection Issues Related to Search Engines, Brussels, 2008, p. 12.
70 WP 29, Opinion 148on Data Protection Issues Related to Search Engines, Brussels, 2008, p. 12.

en de Verenigde Staten. Een deel van het Europese dataverkeer wordt bij overbelasting van de Europese servers 'gererouted' naar servers in de Verenigde Staten en vice versa. Het antwoord op de tweede vraag wordt gegeven in de Opinion 56 on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites. "The place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible. It is the place where it pursues its activity.(...) For example: a direct marketing company is registered in London and develops its European wide campaigns there. The fact that it uses web servers in Berlin and Paris does not change the fact that it is established in London."[71]

Het feit dat de eigenaar van Ixquick een in Nederland gevestigde rechtspersoon is, vanuit Nederland de metazoekmachine aanbiedt, en de servers in de Verenigde Staten haar volledig eigendom zijn, heeft tot gevolg heeft dat er geen sprake is van de in artikel 25 van Richtlijn 95/46/EG beoogde situatie. Derhalve is dit artikel niet van toepassing en de persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na doorgifte te worden verwerkt, naar de server van Ixquick in de Verenigde Staten mogen worden doorgegeven. Derhalve heeft de doorgifte van de data aan de server in Fremont (Ca) geen juridische consequenties voor Ixquick.

6.6.2. Recht op inzage, correctie, verwijdering van toepassing?

Zoals uit het proces blijkt (zie figuur 6.3), worden er persoonsgegevens verwerkt. Uiterlijk na 48 uur zijn er geen persoonsgegevens van de zoeker meer aanwezig, omdat de IP-adressen binnen 48 uur door Ixquick automatisch worden verwijderd. Zoals in paragraaf 6.6.1 vastgesteld is de Richtlijn 95/46/EG op deze verwerking van toepassing. Gezien de zeer korte termijn van het bestaan van persoonsgegevens deed de derde vraag zich voor of de uitoefening van het recht van betrokkene (de steller van de zoekvraag) op inzage, correctie, blokkering en verwijdering van zijn persoonsgegevens niet illusoir was door de korte termijn van het bestaan van deze data, waardoor aan de privacybescherming van de zoeker afbreuk zou worden gedaan. Het antwoord op deze (derde) vraag luidt, dat deze rechten weliswaar uitgeoefend kunnen worden, maar dat deze feitelijk onuitvoerbaar zijn. Immers de termijn waarbinnen de zoeker dit recht kan uitoefenen is te kort om het automatisch wissen van het IP-adres voor te zijn. De betrokkene moet binnen 48 uur onweerlegbaar aantonen dat hij het was die de Ixquick website bezocht vanaf het IP-adres, dat door de Ixquick server is gelogd, in verband met een specifieke

71 WP 29, Opinion 56 on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites, Brussels, 2002, p. 8.

zoektermopdracht. Het leveren van dit onweerlegbare bewijs is vrijwel ondoenlijk en vereist dat een boven elke twijfel verheven betrouwbare partij, bijvoorbeeld een Trusted Third Party (TTP), ten behoeve van de betrokkene een digitaal certificaat afgeeft. Als het al uitvoerbaar zou zijn, dan zal het leveren van een dergelijk bewijs disproportioneel kostbaar zijn.

6.6.3. Dataminimalisatie

Door Borking & Van Vliet is vastgesteld[72] dat de zoekmachines aan wie Ixquick de zoektermen doorgeeft geen identificerende gegevens van de gebruikers van de Ixquick metazoekmachine bevat. De persoonsgegevens van de gebruikers van Ixquick worden afdoende beschermd. Ook bij het voorkomen van 'click fraud' beschermt de hash van de IP-adressen de informationele privacy van de gebruikers optimaal.

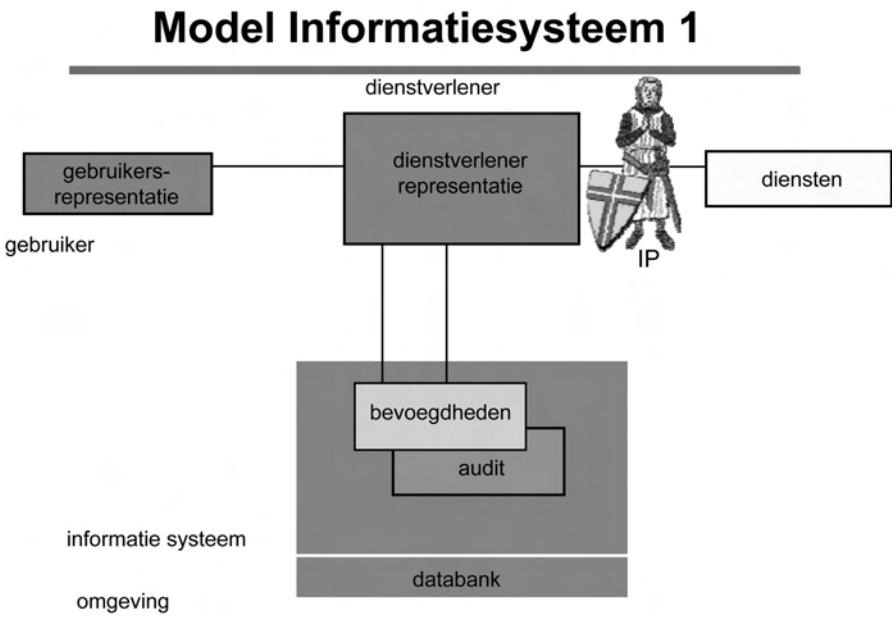
Het Europrise evaluatierapport CS-X-080711-002 ten behoeve van het verlenen van het privacycertificaat concludeert dan ook dat de metazoekmachine Ixquick volledig voldoet aan de EU- en nationale wetgeving betreffende de bescherming van persoonsgegevens en op adequate wijze de privacy van de gebruiker juridisch en vanuit een beveiligingsperspectief beschermt.[73] Het inbouwen van een beperkte houdbaarheid van elektronische data (48 uur maximaal) door Ixquick is een toepassing van PET door middel van anonimisering en hashing.[74]

Zoals uit de modelarchitectuur in figuur 5.5 in hoofdstuk 5 kan worden vastgesteld, bepaalt de positie van de 'Identity Protector' het domein waarin de identificerende gegevens worden afgeschermd. In figuur 6.6 valt het volgende vast te stellen. Bij Ixquick zorgt de 'Identity Protector' ervoor dat er twee domeinen ontstaan:

1. Links van de Identity Protector ontstaat het domein waar de gebruiker identificeerbaar (voor maximaal 48 uur) is binnen het systeem van de Ixquick.
2. Rechts van de Identity Protector ontstaat het domein waar de gebruiker anoniem is, omdat zijn identiteit vervangen is door het IP-adres van Ixquick in het domein waarbinnen de zoekresultaten worden verzameld. De levering van de diensten geschiedt aan Ixquick en de gebruiker is dus anoniem.

72 Borking & Van Vliet, 2008, p. 18.
73 Andriessen, 2008, p. 10.
74 Horlings, e.a., 2003, p. 36.

Figuur 6.6: Model informatiesysteem 1 met Identity Protector; de kruisridder staat symbolisch voor de IP. De dienstverlening is anoniem



6.7. Het ziekenhuisinformatiesysteem

In het dagelijks leven worden regelmatig gegevens van consumenten vastgelegd in databases met behulp van een unieke sleutel, bijvoorbeeld het burgerservicenummer of een patiëntennummer. Het vastleggen van medische gegevens is hier een voorbeeld van. Medische gegevens zijn niet alleen belangrijk en interessant voor de behandelend arts, maar kunnen dat ook voor anderen zijn, zoals bijvoorbeeld: de collega-arts, verplegend personeel, de apotheek, de verzekeraar, de wetenschappelijk onderzoeker, een werkgever en de politie.[75] De medische gegevens in de databases zijn vaak niet omgeven met privacybeschermende maatregelen, zodat in principe iedereen met toegang tot de database met de zoeksleutels alle gegevens van een patiënt kan opvragen, ook als niet alle gegevens uit de databank nodig zijn voor het uitoefenen van hun functie.[76] Niet voor alle betrokken partijen is het noodzakelijk de identiteit van de patiënt te kennen. Bijvoorbeeld: wetenschappers die onderzoek verrichten naar ziektebeelden en -patronen. Het is voor de wetenschappers wel van belang dat ze over alle voor het onderzoek relevante gegevens van een persoon kunnen beschikken. Niet alleen de ziektes en

75 Hes & Borking, 2000, p. 39.
76 Klaver, e.a., 2002, p. 51.

behandelingen die een persoon heeft ondergaan zijn interessant, maar ook bepaalde gewoontes zoals roken, sporten e.d. Te vaak gebruiken wetenschappers de identiteit van patiënten om alle vastgelegde gegevens te kunnen verzamelen.

De vraag is nu hoe de privacy van patiënten kan worden beschermd bij het vastleggen van medische gegevens in een database overeenkomstig de bepalingen in de Richtlijn 95/46/EG en de Nederlandse wetgeving, zonder dat dit verstorend werkt op de processen binnen een ziekenhuis.

Dit vraagstuk speelde bij het ziekenhuis Veldwijk-Meerkanten met 22 vestigingen in de Noordoostpolder, zuidelijk Flevoland en de Veluwe. Uit een diepgaande privacyaudit uitgevoerd door de Registratiekamer in 1995 door Koorn, Borking & Van Rossum bleek dat het psychiatrisch ziekenhuis op bijna alle onderdelen voldeed aan de toen van kracht zijnde privacywetgeving (Wet persoonsregistraties 1989), met uitzondering van de logische toegangsbeveiliging die ruime inzage- en mutatiemogelijkheden bood.[77] Mede ten gevolge van de bevindingen in de privacyaudit gaf de directie van het ziekenhuis Veldwijk-Meerkanten aan ICL/SIAC de opdracht een nieuw privacyveilige ziekenhuisinformatiesysteem te bouwen. Daarbij gold als uitgangspunt dat vanuit medisch gezichtspunt het noodzakelijk werd geacht dat, welke privacybeschermende oplossing ook zou worden gevonden, er een open relatie tussen de geneesheer/zorgverlener en patiënt bleef bestaan. Vastgesteld werd dat voor de behandeling de arts/behandelaar de identiteit van de patiënt dient te kennen, maar dat de overige betrokken partijen binnen het ziekenhuis de identiteit van de patiënt noodzakelijkerwijs niet (altijd) hoeven te weten.

Conform de risicobepalingsmethodiek van de Registratiekamer van 2001 geldt ten gevolge van de hoge complexiteit van de verwerking van medische gegevens voor Veldwijk-Meerkanten een beveiligingsniveau III (hoog risico).[78] Richt bij Ixquick de bescherming van persoonsgegevens zich op het proces van het gegevens verzamelen bij de *intake*, bij het ziekenhuisinformatiesysteem van Veldwijk-Meerkanten gaat het vooral om het daarop volgende proces van de verwerking en opslag van gegevens, waarbij zwaar weegt dat de interne combinatie en verwerking van gegevens kan leiden tot nieuwe aanvullende persoonsgegevens. In hoofdstuk 5 is theoretisch aangetoond, dat het gebruik van de 'Identity Protector' door het toekennen van pseudo-identiteiten in combinatie met scheiding van gegevensstromen en encryptie, het beveiligingsniveau kan verhogen en de bescherming van privacy kan versterken.

Omdat buiten de arts/behandelaar de overige medewerkers niet de identiteit van de patiënt hoeven te kennen, is het mogelijk een scheiding tussen identificerende gegevens en overige gegevens aan te brengen. Bovendien zou de behandelrelatie

77 Koorn, 2004, p. 66.
78 Van Blarkom & Borking, 2001, p. 26-29. Zie ook in dit boek hoofdstuk 4.2. 'Risicoklassen'. Ten tijde van de audit in 1994 gold Exclusiviteitsklasse 3 zoals vermeld in Borking, e.a., 1994, p. 17.

tussen zorgverlener en patiënt door middel van een functionele autorisatie in het ziekenhuisinformatiesysteem kunnen worden afgeschermd. De uitgangspunten leidden ertoe dat vooraf een zorgvuldige afweging plaatsvond ten aanzien van welke gegevens nu precies voor welke doeleinden bestemd zouden zijn. Speciale aandacht in het ontwerp kreeg de centrale database.

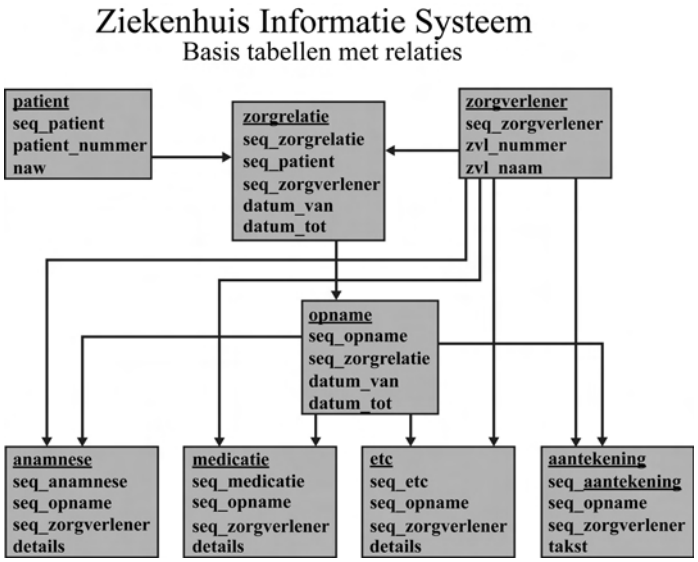
6.7.1. De centrale database

In een centrale database wordt één database gebruikt voor de gegevensverwerking. De centrale database kan door verschillende personen vanaf verschillende locaties worden benaderd, zoals het handelsregister van de Vereniging van Kamers van Koophandel, het Beroepen Individuele Gezondheidszorg-(BIG)-register van het Ministerie van VWS, de registers van de Informatie Beheer Groep (IB-Groep) en de polisadministratie van het UWV.

Lokaal worden er geen gegevens opgeslagen en verwerkt, anders dan direct in de centrale database. De bewerkingen die op de centrale database worden uitgevoerd, worden vanuit één of meer locaties geïnitieerd.[79] In het Ziekenhuis Veldwijk-Meerkanten wordt gewerkt met het ziekenhuisinformatiesysteem, gebaseerd op een client-serverarchitectuur[80] en een centrale database met veel te raadplegen locaties. Van Blarkom[81] wijst erop dat in moderne informatiesystemen de data worden opgeslagen in een 'Relationele Database Management Systeem' (RDBMS) in eenheden, die tabellen ('tables') worden genoemd. De data worden over een aantal tabellen gesplitst, waarbij in elke tabel logisch aan elkaar gerelateerde data-onderdelen zijn opgeslagen. In figuur 6.7 zijn de tabellen patiënt, zorgrelatie, zorgverlener, opname, anamnese, medicatie, etc., en de tabel aantekening opgenomen. Tussen de tabellen lopen de verbindingslijnen, die de logisch aan elkaar gerelateerde data koppelen. In de tabelen staan de sequëntiele databasenummers van de patiënt, de zorgrelatie, de zorgverlener, de opname, de aantekening etc., ten behoeve van het leggen van de relaties in het ziekenhuisinformatiesysteem.

79 Koorn, e.a., 2004, p. 22-23.
80 Van Blarkom, 1997, p. 29-32.
81 Van Blarkom, 1998, p. 30-33.

Figuur 6.7: Relationele database: basistabellen met relaties.



Het ziekenhuisinformatiesysteem bevat veel tabellen. Zo is er een tabel genaamd 'patiënt' met de persoonlijke informatie van de patiënt, een tabel genaamd 'medicatie', waarin de recepten zijn opgeslagen, een tabel 'afspraken' met afspraken en een tabel 'chirurgische behandeling' met de details van de uitgevoerde operaties. Aan iedere naam van de patiënt is in de database een nummer toegekend om hem te onderscheiden van de andere patiënten. Dit nummer is een intern databanknummer en niet het nummer van de ziektekostenverzekering of het burgerservicenummer. Teneinde de medicatie met de chirurgische ingreep van de patiënten met elkaar in verband te brengen, worden de unieke databasenummers van de patiënten in de tabellen medicatie en chirurgische behandeling gekopieerd.

Van Blarkom ziet in deze aanpak twee belangrijke gevaren voor privacyinbreuk: "1. Once the patient's name is located, the database number is found, this value can easily be used to read the table 'medication' or 'surgical treatment' to find the medical record of the patient; and 2. By searching any of the data in the linked tables, with little deduction, the unique database number can easily be used to establish the identity of the patient."[82]

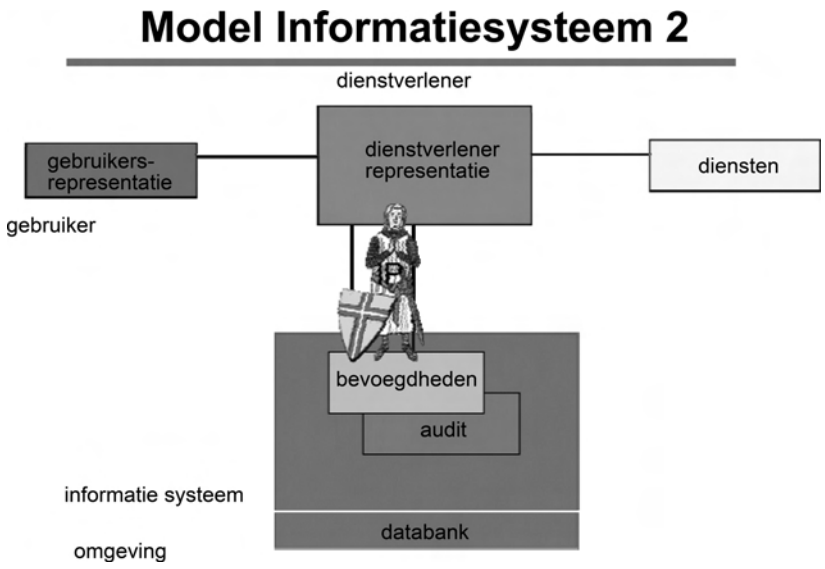
82 Van Blarkom, 1998, p. 32.

6.7.2. De oplossing

Door naast een sterk toegangcontrolemechanisme, gebaseerd op gebruikersgroepen, een mechanisme te introduceren waarbij groepen van persoonsgegevens in de database van elkaar en van direct identificerende gegevens worden losgekoppeld, wordt oneigenlijk gebruik van persoonsgegevens bemoeilijkt.[83] Door middel van de 'Identity Protector' worden domeinen gecreëerd. In het identiteitsdomein (zie paragraaf 5.8) worden de persoonsgegevens inclusief een patiëntnummer opgeslagen. In de pseudo-identiteitsdomeinen worden de diagnostische en behandelgegevens opgeslagen. Hoewel in dit domein een patiëntnummer wordt gebruikt, mogen de patiëntnummers uit het identiteitsdomein en de pseudo-identiteitsdomeinen niet aan elkaar gelijk zijn, omdat iedereen dan de koppeling tussen de identificerende en niet-identificerende gegevens zou kunnen maken. Om de mogelijke koppeling te voorkomen, wordt het patiëntnummer uit het identiteitsdomein versleuteld. Dit versleutelde nummer wordt als patiëntnummer gebruikt in een specifiek pseudo-identiteitsdomein. Met behulp van de 'Identity Protector' kan het versleutelde patiëntnummer worden ontcijferd en wordt de koppeling met het identiteitsdomein gemaakt. Op deze wijze kunnen alleen degenen die de beschikking hebben over de 'Identity Protector', de twee domeinen met elkaar in verband brengen. Er kunnen in de database even zoveel pseudo-identiteiten per patiënt zijn als het aantal tabellen.[84] Deze oplossing wordt in figuur 6.8 in de architectuur van model informatie-systeem 2 (vergelijk figuur 5.5 in hoofdstuk 5) als volgt weergegeven. Er zijn vier modulen, namelijk de gebruikersrepresentatie, de dienstverlenerrepresentatie, de diensten en de databank met de bevoegdheden en de audit. Deze modulen zijn verbonden met een interactielijn waarover het dataverkeer gaat. De 'Identity Protector' is geplaatst op de interactielijnen tussen 1. de combinatie gebruikersrepresentatie – dienstverlener representatie – de diensten en 2. de databank met de bevoegdheden en auditfaciliteiten. De 'Identity Protector' zorgt voor de anonimisering c.q. pseudonimisering. In de relatie tussen de zorgverlener, die de diensten aanbiedt, en de patiënt is de identiteit van de patiënt bekend.

83 Klaver, e.a., 2002, p. 51.
84 Hes & Borking, 2000, p. 40.

Figuur 6.8: Model informatiesysteem 2 met Identity Protector; de kruisridder staat symbolisch voor de Identity Protector. De databank valt binnen het door de Identity Protector gerealiseerde pseudo-identiteits-domein.



Deze aanpak is uitgewerkt door ICL/SIAC in 1996/7[85] en resulteerde in de X/Mcare-database gebaseerd op een Oracle relationele database en client-serverstructuur. Teneinde een privacyveilige oplossing te bereiken diende: "The patient-identifying number has to be removed from all tables forming the medical record", aldus Van Blarkom.[86] Vervolgens is het ziekenhuis informatiesysteem in twee gescheiden verzamelingen opgedeeld.[87] Het ene gedeelte bestaat uit de persoonsgegevens van de ingeschreven patiënten, de zorgrelatie en de vastlegging van de functionele autorisatie. PET steunt namelijk sterk op authenticatie- en autorisatiemanagement. Wanneer het toekennen (autoriseren) en het uitreiken van de authenticatiemiddelen niet zorgvuldig gebeuren, kunnen ongeautoriseerde personen onrechtmatig toegang verkrijgen tot de persoonsgegevens. Hiermee wordt het voordeel van PET geheel tenietgedaan.

Het tweede gedeelte omvat de medische gegevens en de medisch dossiers van de patiënten. Elk dossier bevat onder meer de anamnese, medicatie, behandelplan,

85 Van Blarkom, 1997, p. 29-32.
86 Van Blarkom, 1998, p. 33.
87 Van Blarkom, Patent Application Number 9712459.8 (application date 14th June 1977) "Figure 1: block diagram showing a computer system incorporating a secure database", p. 12.

afspraken met zorgverleners, chirurgische behandeling, laboratoriumuitslagen, en verstrekkingen van gegevens aan derden (huisarts, tandarts, apotheker, laboratorium etc.).[88] Elke tabel in de twee gescheiden verzamelingen is voorzien van een primaire sleutel. Elk onderdeel van het medisch dossier is ondergebracht in een eigen tabel waarbij de waarde van de primaire sleutel per tabel verschilt, ook al heeft zij betrekking op een en dezelfde patiënt, hetzelfde medisch dossier etc.[89] In het X/Mcare-systeem zijn alle logisch bij elkaar horende gegevens opgeslagen in aparte tabellen. De tabel 'patiënt' bevat alle persoonsgegevens, de tabel 'aanmelding' alles wat de aanmelding van de patiënt betreft, de tabel 'agenda_afspraak' bevat de feiten rond het consult en niet meer dan dat. Tussen de tabellen zijn wel logische verbanden maar niet fysiek aanwezig in de database. Binnen dit systeem bestaan geen 'constraints'[90] of andere mechanismen die zulke fysieke verbanden kunnen leggen tussen kenmerkgegevens van zorgverleners en patiënten en de zorggerelateerde gegevens.

Om een koppeling te maken tussen de tabellen, moet eerst vastgesteld worden of er een geldige zorgrelatie met een geselecteerde patiënt is. In dat geval is het unieke kenmerk van de betrokken patiënt bekend. De applicatie versleutelt dit vervolgens tot unieke kenmerkgegevens van de gewenste zorggerelateerde tabel. Deze versleutelde kenmerken stellen de toepassing vervolgens in staat de benodigde gegevens in de database te benaderen. In de X/Mcare-database bestaat voor elke tabel een uniek encryptieprotocol. Daarmee is bereikt dat elke zorggerelateerde tabel voor een en dezelfde patiënt een unieke sleutel bezit. De relaties tussen de tabellen worden onderhouden door middel van beschreven 'constraints' voor het bewaken van de referentiële integriteit[91] van de database om te voorkomen dat gegevens van een bestaande patiënt kunnen worden verwijderd. Het is hierdoor ook niet mogelijk om een behandeling te laten uitvoeren door een niet-geregistreerde zorgverlener.

In figuur 6.9, gebaseerd op figuur 6.7, zijn de relaties tussen de verschillende tabellen vervangen door 'Identity Protectors' (weergegeven door het symbool van de kruisridder), die de pseudo-identiteiten tot stand brengen.[92]

---

88 Van Blarkom, Patent Application Number 9712459.8 (application date 14th June 1977) "Figure 2: shows a skeleton model of the database", p. 13.

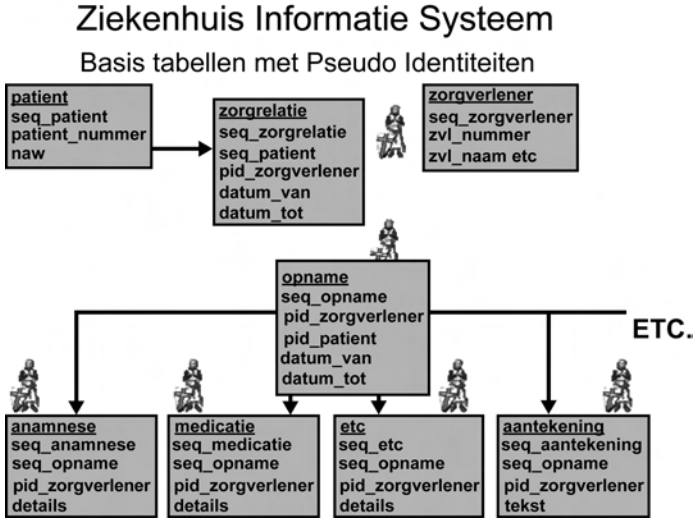
89 Borking, 2005, p. 25: "The aim of the pseudo-identity domain is to make sure the real person involved cannot be traced on the basis of previously obtained personal data, and vice-versa, to make sure the personal data cannot be found on the basis of the obtained identity."

90 Een constraint in een database is een vastgelegde voorwaarde, bedoeld om de integriteit of logica van de opgeslagen gegevens te bewaken. Een constraint zorgt ervoor dat er een foutmelding wordt gegeven als de betreffende regel overtreden dreigt te worden.

91 Referentiële integriteit in een relationele database is het uitgangspunt dat de interne consistentie tussen de verschillende tabellen binnen die database wordt gewaarborgd. Dat betekent dat er altijd een primaire sleutel in een tabel bestaat als er in een sleutelveld in een andere tabel naar wordt verwezen. Het DBMS waarborgt de consistentie en zorgt ervoor dat een transactie die de consistentie doorbreekt niet wordt aangebracht.

92 Voor de functies van de Identity Protector zie hoofdstuk 5 paragraaf 5.9.

Figuur 6.9: Basistabellen waarin de relaties zijn vervangen door Identity Protectors; de kruisridders staan symbolisch voor de Identity Protectors.



Om een hacker het niet mogelijk te maken persoonsgegevens te koppelen aan het medisch dossier, dat in tabellen is opgesplitst, zijn tussen de tabellen geen 'constraints' gedefinieerd. Ook zijn er geen verborgen tabellen aanwezig waarin een relatie wordt gelegd tussen de primaire sleutel die binnen de twee databankdelen in gebruik zijn. Het medisch dossier omvat tabellen die als startpunt worden gebruikt voor een applicatiefunctie nadat de patiënt is geselecteerd. Deze tabellen zijn voorzien van een extra kolom waarin de pseudo-identificatie wordt vastgelegd, die gebruikt wordt als toegangssleutel tot de gewenste informatie in het medisch dossier.[93] Er is hier sprake van de invoering van de 'identity protector', die de identiteit van de zorgverlener en patiënt afschermt.

De client-software biedt de mogelijkheid op basis van de primaire sleutel van een patiënt een pseudo-identificatie samen te stellen met behulp van encryptietechnologie. Het encryptieprotocol kent drie parameters:

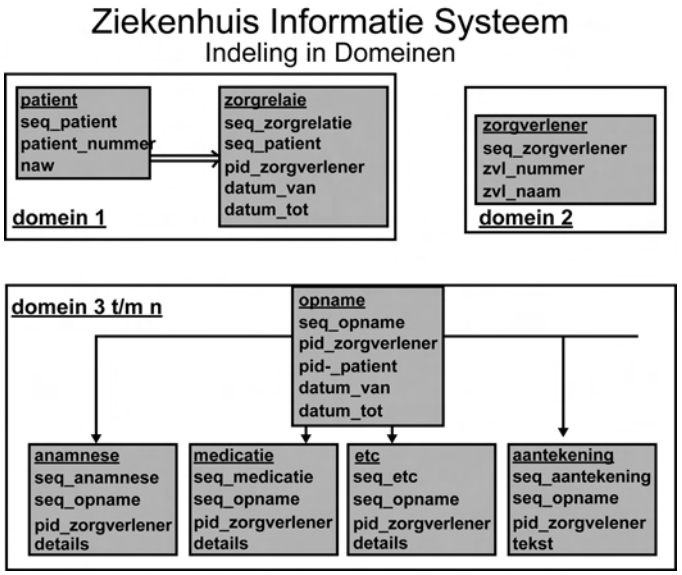
a. de primaire sleutel;
b. de encryptie sleutel van 128 bits of hoger;
c. een unieke tabel 'identifier'.

Het encryptieprotocol gaat bijvoorbeeld als volgt: de seq_patiënt is 34, de unieke 'identifier' voor de tabel 'medicatie' is 47 en de encryptiesleutel is

93 Klaver, e.a., 2002, p. 51.

263447432356645391. De uit deze bewerking resulterende pseudo-identiteit[94] wordt opgenomen in een tabel van het medisch dossier en wordt gebruikt voor de toegang tot die tabel. Van Blarkom stelt: "The illegal user accessing the database can't see a relation between the two values, making the database safe against unauthorized access."[95] Elke tabel binnen het medisch dossier krijgt zijn eigen pseudo-identificatie toegewezen. Om een afspraak met een zorgverlener te kunnen maken uitgaande van een gegeven in het medisch dossier, bestaat ook de mogelijkheid om softwarematig vanuit de pseudo-identificatie de primaire sleutel van de patiënt te produceren. Door het gebruik van de 'Identity Protectors' worden zoveel als nodig identiteits- en pseudo-identiteitsdomeinen gecreëerd. In figuur 6.10 zijn de gecreëerde domeinen aangeven als rechthoeken, waarbinnen zich de specifieke tabellen bevinden.

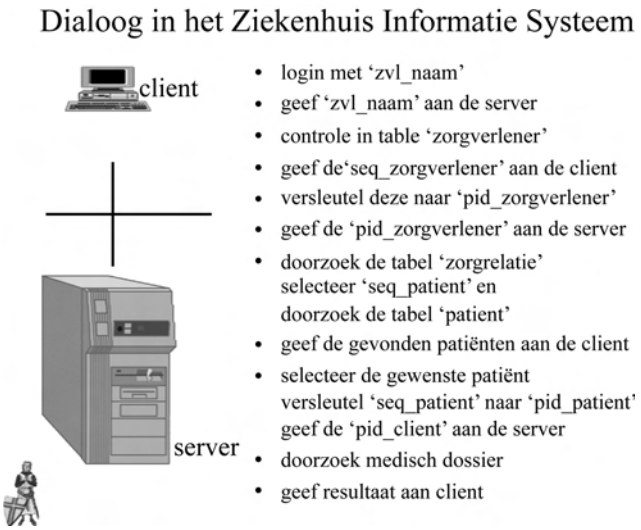
Figuur 6.10: Domeinindeling in het ziekenhuisinformatiesysteem. Domein 3 t/m n kan voor wetenschappelijk onderzoek worden gebruikt en bevat geen identificerende gegevens.



94 ICL, Latest Patent Applications: C1372 Secure Database 14-06-97 in Intellectual Property Department, London, Issue 97/2, 1st August 1997, p. 1-18.
95 Van Blarkom, 1998, p. 33.

De communicatie tussen client en server zorgt voor de geautoriseerde ontsluiting van de tabellen en gegevens. Een client is een applicatie of een computersysteem met toegang tot een ander systeem, de server, via een netwerk. Men spreekt hierbij van een client-servermodel. De client neemt initiatief tot communicatie met de server met als doel bijvoorbeeld het opvragen van gegevens, het overdragen van gegevens of het uitvoeren van een actie op de server. Figuur 6.11 laat de dialoog tussen client (groen) en server (rood) zien:

Figuur 6.11: Dialoog tussen client (groen) en server (rood) Zvl = zorgverlener; seq = sequentie; pid = pseudo-identiteit.



De gekozen oplossing maakt het mogelijk, dat alleen de behandeld arts, zorgverlener of specialist en de patiënt inzage in het hele dossier hebben. De administratie, het laboratorium en de verpleegkundigen hebben slechts inzage in die gegevens uit het patiëntendossier die van belang zijn voor het uitvoeren van hun functies.[96] Deze toepassing is als de 'Privacy Incorporated Database' geoctrooieerd.[97] De in deze toepassing te gebruiken encryptiesleutels dienen te worden beheerd door middel van een TTP (Trusted Third Party), want voorkomen moet

96 Borking, 2003, p. 211-246.
97 European Patent: EP0884670 (G. van Blarkom, inventor, ICL).

worden, dat als een hacker zich toegang zou kunnen verschaffen tot de computers, dat hij de sleutel op de 'client' van de zorgverlener zou kunnen ophalen en dan alsnog het systeem zou kunnen binnendringen.

6.7.3. Elektronisch patiëntendossier

Het is de bedoeling van het door het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) aangeprezen elektronisch patiëntendossier (EPD) dat met het EPD zorgverleners medische gegevens kunnen uitwisselen**.** De wettelijke verplichting voor de zorgaanbieders om zich aan te sluiten op het EPD gaat waarschijnlijk in de loop van 2010 in, afhankelijk van de wetsbehandeling door de Eerste Kamer. Op 19 februari 2009 heeft de Tweede Kamer het voorstel voor de Wet elektronisch patiëntendossier (EPD) aangenomen.[98]

Terecht stelt het Ministerie dat het belangrijk is dat zorgverleners veilig en betrouwbaar relevante medische gegevens met elkaar kunnen delen. Nochtans heeft bijna een derde (31 procent) van de Nederlandse artsen bezwaar gemaakt tegen de uitwisseling van de medische gegevens van zijn patiënten via het elektronisch patiëntendossier (EPD), omdat de beveiliging van de gegevens en de privacy van patiënten onvoldoende is. Dit blijkt uit een enquête in het blad 'Medisch Contact' van 12 mei 2009. Een kwart van de dokters overweegt alsnog bezwaar te maken. Zeven procent vindt het maken van bezwaar te lastig, maar zou dit wel hebben gedaan als het eenvoudiger zou zijn. Kortom erg veel draagvlak is er onder de artsen niet.

De onder paragraaf 6.7.2 besproken oplossing zou heel goed kunnen worden toegepast om het elektronisch patiëntendossier van VWS privacyveilig te maken. De 'Identity Protector' en pseudo-identiteitsdomeinen kunnen de gegevens van patiënten, artsen en andere zorgverleners adequaat beveiligen. Bovendien kan bepaald worden wie en welk gedeelte van het dossier kan worden ingezien. De patiënt en de arts kunnen zeggenschap houden op de toegang tot het dossier. Dat kan bij het voorgestelde elektronisch patiëntendossier niet. Toepassing van de in paragraaf 6.7.2 weergegeven architectuur zal de bezwaren tegen het EPD van de privacybewuste burgers, patiënten en artsen weg kunnen nemen.

6.8. Het Victim Tracking and Tracing System

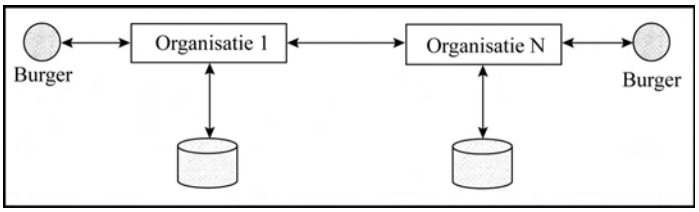
Een aanmerkelijk complexere uitwerking van het hierboven behandelde ziekenhuisinformatiesysteem is het Victim Tracking and Tracing System (ViTTS) dat uit het Nederlands Trauma Informatie Systeem (NTIS) is voortgekomen.

---

98 Tweede Kamerstukken, vergaderjaar 2008-2009, 31 466, nr. 29: "Patiënten kunnen evenwel decentrale brondossiers (de huisartsen- en ziekenhuisdossiers, dus de lokale EPD's) nog niet door middel van deze de EPD inzien. In een aangenomen motie van de Tweede Kamer kan de minister op grond van artikel 13hb Wet EPD ook voor regionale zorginformatiesystemen eisen dat patiënten elektronisch toegang krijgen tot hun medische gegevens en de loggegevens daarin."

In beide informatiesystemen is sprake van een ketenstructuur (zie figuur 6.12).

Figuur 6.12: Vereenvoudigde weergave van een ketenstructuur in Koorn, e.a., 2004, p. 25.



In een keten worden gegevens uitgewisseld of doorgegeven tussen minimaal twee organisaties. Een kenmerk van een keten is dat de ketenorganisaties zelf databases hebben waarin gegevens worden opgeslagen. Voorbeeld van een keten is de Dienst Wegverkeer (RDW)-keten.[99] Hierin communiceren de erkenninghouders (dit zijn vaak garagehouders of Algemene Periodieke Keuring (APK)-keuringsstations) via een communicatie-provider met de RDW. De providers verzamelen een gedeelte van de informatie die de erkenninghouders via hen aan de RDW verstrekken. Andere voorbeelden van ketens met een hoge informatiseringsgraad zijn te vinden in de zorg (bijvoorbeeld CVA Ketenzorg),[100] Verkeer & Waterstaat (bijvoorbeeld de gegevensuitwisseling in de Rotterdamse haven) en bij de relatie politie – justitie (bijvoorbeeld elektronische aangifte, proces-verbaal en dossier).[101]

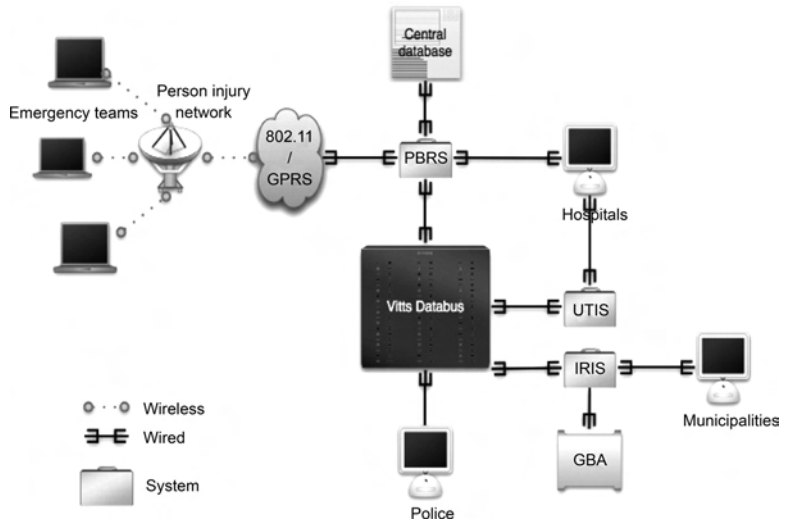
In het ViTTS gaat het om een digitaal registratiesysteem voor traumapatiënten met zwaar acuut letsel die geholpen worden op de afdeling Spoedeisende Hulp.[102] De 'emergency teams' (zie figuur 6.13 hieronder) geven de levende en niet-levende slachtoffers een uniek identificerend ongevalnummer (Unique Identifying Casualty Number: UICN), dat wordt ingevoerd in de ViTTS-databank. Aan dit nummer zijn medische gegevens gekoppeld over het slachtoffer, de plaats en tijdstip waar het ongeluk gebeurde en naar welk ziekenhuis het slachtoffer is gebracht en wordt behandeld. Niet-geïdentificeerde slachtoffers krijgen eveneens een UICN. De gemeente waar dit slachtoffer zich feitelijk bevindt, poogt het slachtoffer te identificeren op basis van ontvangen informatie van familieleden of

99 Voordat de Wegenverkeerwet 1994 in werking trad had deze dienst de naam Rijksdienst voor het wegverkeer. De afkorting RDW was zo ingeburgerd dat die bleef gehandhaafd.
100 De CVA-ketenzorg is gericht op patiënten met een beroerte (Cerebro Vasculair Accident, CVA).
101 Koorn, e.a., 2004, p. 25.
102 De gegevens betreffende ViTTs werden verkregen gedurende de interviews van de onderzoekers Ribbers, Dijkman & Borking in 2007 met drs. Luc Taal, Director Trauma Center UMCU te Utrecht in het kader van een economisch onderzoek voor de EU-Commissie.

anderen die het slachtoffer kennen en die hebben laten registeren dat zij familieleden vermissen. Slachtoffers, die verplaatst worden, kunnen met hun UICN-nummer voortdurend worden gevolgd. Gegevens kunnen later ook gebruikt worden om analyses van rampen uit te voeren.

De sterk vereenvoudigde ViTTS-architectuur ziet er als volgt uit:

Figuur 6.13: ViTTS-architectuur: Ribbers, 2007(A), p.51
802. 11/GPRS betreft een 'blue tooth'-verbinding; PBRS staat voor patiënt barcode registratie systeem. 802.11 of Wi-Fi verwijst naar de gebruikte standaarden voor draadloze netwerken (Wireless LAN) bij ViTTS. GPRS betekent General Packet Radio Service en is een techniek om in het GSM-netwerk berichten sneller te verzenden. UTIS betekent Utrechts Trauma Informatie Systeem. I-RIS staat voor Internet Registratie Systeem. GBA is de gemeentelijke basisadministratie



Het verzamelen van gegevens waaraan een UICN wordt gekoppeld, geschiedt met een mobiele RFID-/barcodelezer: het patiënt barcode registratie systeem (PBRS) (zie figuur 6.13). De gegevens worden direct via een beveiligde lijn verzonden en opgeslagen in de PBRS-databank die gekoppeld is met de ViTTS-databank. Het ziekenhuis waar het slachtoffer verblijft, kan via een internetverbinding contact opnemen met het Utrechts Trauma Informatie Systeem (UTIS) om meer informatie over de ramp te verkrijgen. Omdat bij een ramp de verantwoordelijkheid voor de afwikkeling van de ramp mede wordt gedragen door de gemeente waar de

ramp heeft plaatsgevonden, wordt de verkregen informatie ook naar de desbetreffende gemeente en politie gezonden. De gemeenten gebruiken het Internet Registratie Systeem (I-RIS) om de bevolking te informeren over het aantal gewonde mensen en om de familieleden in te lichten waar het slachtoffer zich bevindt.[103] De gemeenten en de politie krijgen uitsluitend de informatie waartoe zij gerechtigd zijn. De gemeentelijke basisadministratie (GBA) valideert de informatie. De politie ontvangt slechts informatie als een persoon is overleden.[104]

Artsen, verpleegkundigen en assistenten hebben op basis van functionele autorisatie toegang tot dit systeem. Door de elektronische vastlegging en uitwisseling van medische gegevens kan een efficiëntere en effectievere hulpverlening aan de patiënt worden geboden en de ramp beter beheerst worden. Tevens worden de uiterst gevoelige medische patiëntgegevens en behandelmethoden anoniem geanalyseerd zodat men de behandelmethoden kan verbeteren, de patiënten beter kunnen worden geholpen en de kans op overleven groter wordt.[105] Het spreekt vanzelf dat gezien de privacygevoeligheid van de medische gegevens, technische maatregelen zijn genomen om alle gegevens vanaf het moment van verzamelen te versleutelen. De communicatie gaat over beveiligde lijnen en de gegevens worden versleuteld in de database opgeslagen.

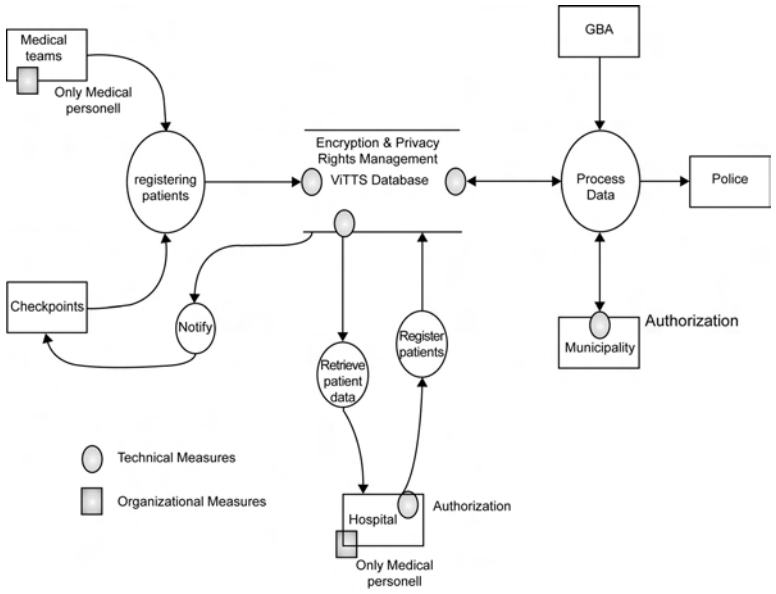
6.8.1. Privacybeschermende maatregelen

Omdat het ViTTS-systeem privacygevoelige informatie over slachtoffers verwerkt en deze gegevens door het ziekenhuispersoneel, de medische staf, de gemeenten en politie geraadpleegd kunnen worden, is het van groot belang de privacybedreigingen het hoofd te bieden, door optimale bescherming aan de persoonsgegevens te verlenen en overtreding van de privacywetgeving te voorkomen. Privacyvraagstukken binnen de gezondheidszorg zijn complex. Hiervoor moeten organisatorische en technische maatregelen worden getroffen. Tijdens de rampenbestrijding is het van het grootste belang dat de netwerkverbinding niet uitvalt. Hier is organisatorisch in voorzien door drie radiografische netwerken te creëren, zodat bij uitval van het ene netwerk het andere netwerk de communicatie kan overnemen.

Figuur 6.14 laat een vereenvoudigd gegevensstroomdiagram zien en geeft aan waar technische (PET-) en/of organisatorische beveiligingsmaatregelen zijn genomen. De cirkels in het diagram verwijzen naar een reeks van PET-maatregelen. De organisatorische maatregelen (in figuur 6.14 de vierkanten) die genomen zijn, betreffen onder meer de functionele authorisatie van het medisch personeel.

103 Ribbers, 2007, p. 46-49.
104 Ribbers, 2007, (A) p. 48-51.
105 Koorn, e.a., 2004, p. 29.

Figuur 6.14: Organisatorische en technische maatregelen in ViTTS gebaseerd op PET-maatregelen, Ribbers, 2007, p. 46



Sterke beveiliging wordt toegepast door een verfijnde functionele autorisatiestructuur, waarbij de rol van de gebruiker bepaalt tot welk deel van het systeem hij toegang heeft. Deze oplossing is ook in het ziekenhuisinformatiesysteem toegepast (zie **paragraaf** 6.7). Alleen het medisch personeel kan inloggen, informatie invoeren over de tirage bij de ramp, gegevens opvragen waarbij encryptie en privacymanagementtechnieken worden gebruikt en versleuteld informatie verzenden.[106] Geautoriseerde zorgverleners maken gebruik van digitale certificaten die op chipkaarten zijn opgeslagen of van chipkaarten met biometrische gegevens om zich uniek te identificeren. Andere gebruikers maken gebruik van softwarecertificaten, maar daarmee krijgt men geen toegang tot de medische gegevens.[107]

Net zoals in het informatiesysteem van het Veldwijk-Meerkantenziekenhuis vindt scheiding van gegevens plaats, waarbij de medische gegevens en NAW-gegevens[108] in verschillende tabellen zijn opgeslagen. De NAW-gegevens zijn versleuteld, zodat de medische gegevens voor ongeautoriseerde personen (bijvoorbeeld systeembeheerders) niet zijn te herleiden tot een natuurlijk persoon. De database met medische

106 Ribbers, 2007 (A), p. 48-49.
107 Ribbers, 2007 (A), p. 46.
108 NAW staat voor naam, adres, woonplaats.

gegevens is opgeslagen bij een vertrouwde derde partij, de 'Trusted Third Party' (TTP), die stringente fysieke[109] en logische beveiligingsmaatregelen heeft getroffen en hierop regelmatig wordt geaudit. Bovendien vindt minimalisatie van gegevens plaats die worden uitgewisseld met andere informatiesystemen. De voorloper van ViTTS was het Nederlands Trauma Informatie Systeem (NTTS). In NTTS[110] wordt een beperkt aantal gegevens verstrekt aan een systeem waarmee de Regionaal Geneeskundig Functionaris (RFG) kan zien welke personen uit zijn gemeente betrokken zijn bij een ramp. Naast de NAW-gegevens wordt uitsluitend een classificatiecode verstrekt. De classificatiecode geeft informatie over de zwaarte van het letsel, maar de RGF krijgt geen inzage in de medische gegevens. Dit systeem bevat een tijdelijke database en de NAW-gegevens blijven hierin niet bewaard. De functionaris kan de gegevens evenwel exporteren naar zijn eigen computer[111] en dat kan bij onzorgvuldig handelen privacyrisico's opleveren.

Om persoonsgegevens te beschermen worden de volgende organisatorische en technische maatregelen ter ondersteuning van de 'Identity Protectors' in ViTTS toegepast:

1. Ten behoeve van de bescherming van persoonsgegevens bij het registeren van slachtoffers op de plaats van de ramp zijn de technische maatregelen:
   a. Het opzetten van drie speciale (slachtoffer)netwerken ingeval er een uitvalt.
   b. Bij het verzenden van informatie naar ViTTS wordt de data over een versleutelde lijn verzonden. De genomen organisatorische maatregel bij het verzamelen van informatie over slachtoffers is dat het alleen aan het medisch personeel is toegestaan (medische) gegevens te verzamelen over slachtoffers van de ramp conform de vereisten ex artikel 8 van de Richtlijn 95/46/EG.
2. Wat betreft het opvragen van informatie over slachtoffers/patiënten zijn de volgende technische maatregelen genomen:
   a. Ziekenhuizen kunnen de webinterface van het Utrechts trauma informatie systeem (UTIS) gebruiken om contact te maken met het ViTTS-systeem. In het UTIS zijn strikte functionele autorisatietechnieken geïmplementeerd, die bij het inloggen door de techniek aan de gebruiker dwingend worden opgelegd.
   b. Encryptie en privacymanagementsystemen zorgen ervoor dat alleen het medisch personeel gegevens kan opvragen.
   c. Encryptietechnieken zorgen ervoor dat alleen het medisch personeel informatie kan toevoegen en terugzenden.
   d. Bij het registeren van de slachtoffers met UICN wanneer zij in het ziekenhuis worden opgenomen, zijn bij het inloggen, het invoeren van

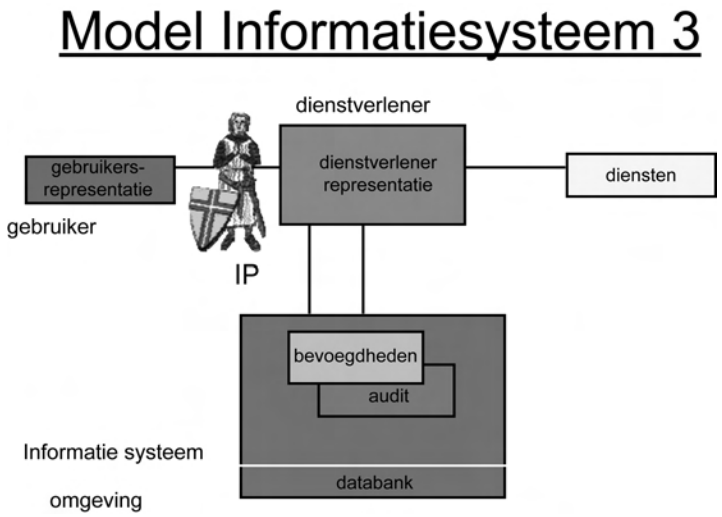
109 Met fysieke beveiligingsmaatregelen wordt bedoeld alle maatregelen die genomen worden om de hulpmiddelen te beveilginge, die gebruikt worden voor het gegevensbeheer.
110 Dit is kennelijk niet het geval bij ViTTS, althans dit kan niet uit de architectuur (zie figuur 6.13.) worden afgelezen.
111 Koorn, e.a., 2004, p. 28-30.

data en het verzenden van informatie dezelfde organisatorische en technische maatregelen genomen, nl. functionele autorisatie en encryptie.

e. Wat betreft het verwerken van data (inloggen in I-RIS om de identiteit van het slachtoffer vast te stellen, het opvragen en verzenden van informatie) zijn eveneens technisch afdwingbare autorisatietechnieken, encryptie en privacymanagement toegepast.

De gekozen oplossing kan in de model architectuur (zie figuur 5.5 van hoofdstuk 5) sterk vereenvoudigd worden weergegeven als model informatiesysteem 3 (zie figuur 6.8 en figuur 6.15).

Figuur 6.15: Model informatiesysteem (IS) 3. De Identity Protector wordt al direct bij de intake van data toegepast en schept hierdoor een groot pseudo-identitydomein binnen het IS. Voor de Identity Protector is de kruisridder als symbool gebruikt.



6.9. Privacymanagementarchitectuur

De meest gecompliceerde mogelijkheid om privacy te beschermen, houdt in, dat daar waar persoonsgegevens niet geanonimiseerd kunnen worden, binnen het informatiesysteem op alle te verwerken en verwerkte persoonsgegevens automatisch de wetgeving betreffende de bescherming van persoonsgegevens en het privacybeleid van de verantwoordelijke worden toegepast. Dit geschiedt op een zodanige wijze dat verwerking in strijd met de wettelijke verplichtingen of de

privacy *policy* leidt c.q. kan leiden tot het af- of onderbreken van de verwerking of het automatisch loggen van de afwijking op het privacybeleid, waarvoor later door het management van de organisatie verantwoording dient te worden genomen. Deze laatste mogelijkheid is met name van belang voor informatieprocessen binnen de overheidsinstanties, banken en verzekeringsbedrijven die over het algemeen zeer identiteitsrijk zijn en ook op grond van wettelijke bepalingen niet zonder identificerende gegevens kunnen. Om persoonsgegevens te beschermen, die niet of in aanmerkelijk mindere mate zijn afgeschermd dan in de hierboven besproken architecturen, dient er een sterk vertrouwen te bestaan tussen de betrokkene die zijn persoonsgegevens afgeeft en de verantwoordelijke die de persoonsgegevens verzamelt, verwerkt en opslaat. In een netwerkomgeving impliceert het vereiste van vertrouwen dat de persoonsgegevens conform de persoonlijke privacyvoorkeuren en de wettelijke vereisten worden behandeld, nog prangender. Want de data van de gebruiker zijn bij alle interacties binnen de hedendaagse communicatienetwerken terug te voeren op de initiator en dat betekent dat de gebruiker bij alle partijen (service providers, zoekmachines, websites etc.) er volledig op zal moeten kunnen vertrouwen dat zijn persoonsgegevens niet in strijd met privacyrealisatiebeginselen worden behandeld en dat verwerkers niet gezamenlijk hun data delen en extensieve profielen van de gebruiker maken.

De vraag is nu hoe kan worden bereikt dat men erop kan vertrouwen dat persoonsgegevens conform de privacyrealisatiebeginselen worden behandeld. De PRIME[112]-architectuur is specifiek ontwikkeld om het vertrouwen te vergroten van de gebruiker/betrokkene in de verwerking van data binnen informatiesystemen. Toepassing van geavanceerde cryptografische technieken lijkt de oplossing voor het versterken van vertrouwen te zijn. Sommer schrijft dat: "a user's privacy can even be protected if service providers and certifiers are dishonest, if business processes are appropriately defined and PRIME technology is used".[113]

In de hieronder te bespreken 'Privacy Incorporated Software Agent' is voornamelijk met PET en privacyontologieën gewerkt om het vertrouwen te versterken en de privacy van de gebruiker te beschermen. 'Obligation Management'-technieken (zie paragraaf 6.4) waren eind 1999 bij de start van het PISA-project nog niet ontwikkeld.

6.9.1. Privacy Incorporated Software Agent (PISA)

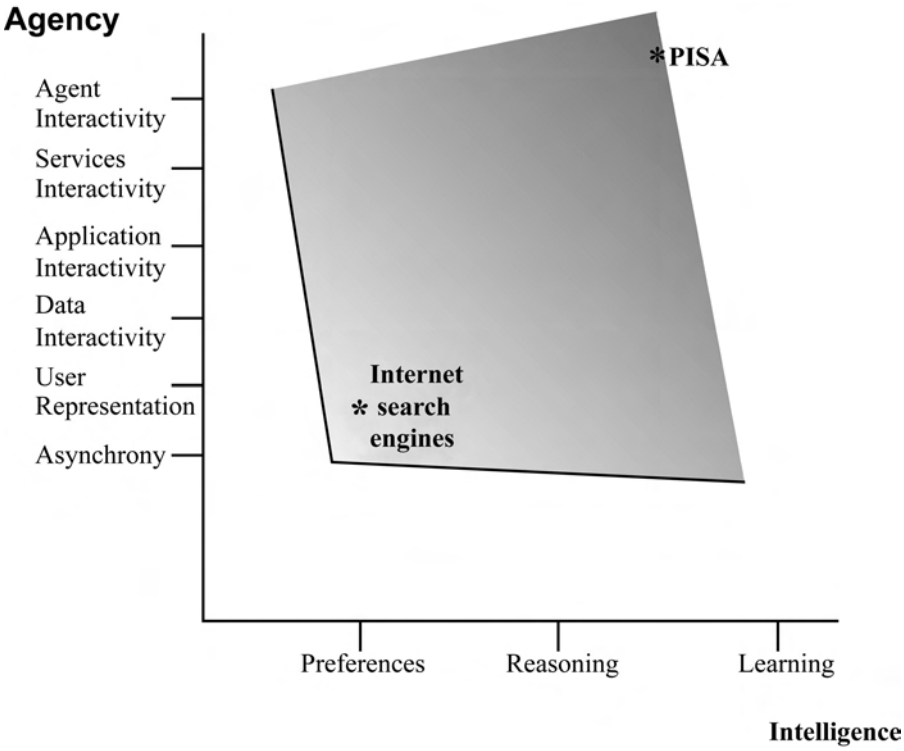
Over Intelligent Software Agents[114] bestaan veel definities[115] zoals "software en/of hardware die in staat is autonoom te handelen teneinde een taak uit te voeren

112 EU research PRIME (Privacy and Identity Management in Europe) project Contract No. 507591(2004-2008).
113 Sommer, 2008, p. 127.
114 Ik heb gekozen voor de meervoudsvorm 'agents' in plaats van 'agenten' om het verschil met menselijke agenten aan te geven.
115 Schermer, 2007, p. 20-21, een aantal definities waarvan een er luidt: "By a software agent we thus mean a computer program that behaves in a manner analogous to a human agent."

voor haar gebruiker in een complexe netwerk omgeving."[116] De Intelligent Software Agent (ISA) kan zonder dat de gebruiker er zich mee bemoeit taken uitvoeren, die, als jezelf tijd genoeg had, zelf zou kunnen doen.[117] ISA's helpen ons nu al met het uitvoeren van eenvoudige routine (repeterende) taken,[118] maar in de nabije toekomst zal een dergelijke software agent zich gaan gedragen als onze digitale butler. Een voorbeeld van deze ontwikkeling is de software agent Phil in de videoclip 'the knowledge navigator' die in 1987 is gemaakt voor Apple Inc.[119] De ISA kan mobiel zijn, deliberatief (overleggend) gedrag en interactie met andere ISAs vertonen en bezit de mogelijkheid om te leren en te identificeren. Volgens Schermer[120] bestaan er drie categorieën software agent architecturen die grosso modo zijn in te delen in: de reactieve agenten, de deliberatieve agenten en de hybride agenten.[121] De hieronder te bespreken privacy incorporated software agent (PISA)[122] moet beschouwd worden als een mobiele deliberatieve agent. Deliberatieve agenten zijn agenten die in staat zijn om hun acties te plannen en 'na te denken' over hun gedrag. Zij gebruiken een model van hun omgeving om hun acties te plannen. De ondernomen actie is dus niet direct gerelateerd aan de waarneming, maar volgt uit het redeneren over het intern in ISA opgebouwde model. Op basis van het model worden mogelijke acties en de resultaten van die acties bepaald. Om een idee te krijgen van de geavanceerdheid van de software agent verwijs ik naar figuur 6.16.

116 Borking, Van Eck & Siepel, 1999, p. 6, 9 en 10.
117 The US Uniform Electronic Transaction act (UETA) defines an electronic agent as: "A computer program or electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual. Deliberative agents can plan their action and 'think' about their behavior."
118 Borking, Van Eck & Siepel, 1999, p. 11. Bijvoorbeeld het Pleiades System van Carnegie Mellon University, maakt afspraken en regelt vergaderingen en verzamelt informatie.
119 Minsky & Riecken, 1994, p. 22-29.
120 Schermer, 2007, p. 22-24.
121 .Luck, Ashri & M. d'Inverno, 2003, p. 12.
122 .Borking, 2001, p. 130-140.

Figuur 6.16: De positie van agents in relatie tot kunstmatige intelligentie; Borking, Van Eck & Siepel, 1999, p. 10.



Het feit dat een mobiele software agent autonoom (los van zijn gebruiker) kan handelen in naam en soms voor rekening en risico van de gebruiker en de mogelijkheid heeft om informatie met andere ISA's uit te wisselen of op en andere manier aan de omgeving bloot te stellen, is belangrijk voor de juridische kwalificatie van een ISA. In de Nederlandse wetgeving bestaat (nog) geen regeling die aan ISA's een juridische status toekent. De ISA moet worden gezien als een instrument dat de gebruiker aanwendt en dat alle handelingen die de ISA verricht moeten worden toegerekend aan de gebruiker of aan de eigenaar van de ISA.[123] Schermer, Durinck & Bijmans gaan er ten onrechte vanuit dat als de agent door de gebruiker wordt ingezet er geen sprake is van verwerking door een verantwoordelijke in de zin van de Richtlijn 95/46/EG.[124] Het stelsel van bescherming van persoonsgegevens is zo ingericht dat er altijd een verantwoordelijke wordt aangenomen, anders dreigt er in sommige gevallen een juridisch vacuüm. Het zal in de toekomst waarschijnlijk

123 Schermer, Durinck & Bijmans, 2005, p. 24.
124 Schermer, Durinck & Bijmans, 2005, p. 28.

gebruikelijk zijn, dat een organisatie (telecommunicatie-aanbieder, internet service provider) software agents ter beschikking van een gebruiker zal stellen bijvoorbeeld door middel van verhuur. Zolang de aanbieder niet via de ter beschikking gestelde software agent ten behoeve van de gebruiker direct of indirect persoonsgegevens van de gebruiker en anderen verwerkt, blijft de gebruiker zelf de verantwoordelijke. Hetzelfde geldt voor de gebruiker die een agent voor eigen gebruik bouwt. In dat geval neemt de gebruiker de rol op zich van betrokkene en verantwoordelijke. Deze opvatting heeft consequenties voor het door een ontwerper op te stellen privacyomgevingsmodel. Dit model beschrijft de juridische en feitelijke omgeving waarin een ISA zijn werk verricht.[125]

De ISA kan zich voordoen als een goedaardige digitale butler of een kwaadaardige digitale misdadiger of als een middel om voortdurend zaken en mensen in de gaten te houden. ISA weerspiegelt in 'cyber space' de rollen en het gedrag van mensen. Software agenten zullen ongetwijfeld een rol gaan spelen in de Ambient Intelligence (AMI)-omgeving. Software Agent-ontwerpers analyseren de manier waarop mensen hun taken met succes trachten af te ronden en nemen die in hun ontwerp over. Dit is goed te zien in de MAS-architectuur.[126] Om goed te kunnen functioneren heeft de ISA van de gebruiker persoonsgegevens of Personal Identifiable Information (PII), de privacyvoor- en afkeuren en andere niet persoonlijke informatie nodig. De ISA verzamelt de relevante informatie voor de uit te voeren taak en persoonsgegevens van zowel de gebruiker als van anderen. De ISA zal die persoonsgegevens bekendmaken conform de door de gebruiker aangegeven privacybeschermingsniveaus. Omdat de ISA automatisch persoonsgegevens verwerkt, zijn de Richtlijnen 95/46/EG en 2002/58/EG en de daarvan afgeleide nationale wetgeving van de EU-lidstaten van toepassing.[127]

De privacyrealisatiebeginselen (zie hoofdstuk 2), dienen in het ontwerp van een privacybeschermende ISA te worden ingebouwd. Omdat de autonome ISA de mogelijkheid bezit om volledig geautomatiseerd beslissingen te nemen, is het noodzakelijk om bij de ISA een volgsysteem in te bouwen om de logica achter de bereikte resultaten van de ISA te kunnen bewijzen en de aansprakelijkheid van de transacties te kunnen dragen.[128] Dit is ook van belang omdat ISA's tijdens hun onderhandelingen met andere ISA's persoonsgegevens van derden verwerken waaraan constraints[129] kunnen zijn gekoppeld. Een ISA mag niet zomaar

125 Van Blarkom,.Borking & Olk, 2003, p. 146.

126 MAS: Multi Agent System. In de MAS zijn beslissingsbomen opgenomen die leren van de representatieve groep van gegevens over de omgeving waarin de agent werkt en van 'constraint satisfaction programming' gebaseerd op een set van constraint rules.

127 Borking & Foukia, 2008, p. 1.

128 Als de ISA door een derde aan een gebruiker ter beschikking wordt gesteld en die derde kwalificeert zich als verantwoordelijke in de zin van artikel 1d van de WBP, dan geldt artikel 35 lid 4 WBP: " Desgevraagd doet de verantwoordelijke mededelingen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens." Zie ook artikel 12 (a) en artikel 15, lid 1 van Richtlijn 95/46/EG.

129 Een constraint in een database is een vastgelegde voorwaarde, bedoeld om de integriteit of logica van de opgeslagen gegevens te bewaken.

persoonsgegevens van derden verwerken als daar geen toestemming voor is of noodzaak voor bestaat.[130]

> De mogelijkheid van ISA's tot het autonoom nemen van beslissingen en het opbouwen van een profiel met voor- en afkeuren van de gebruiker op basis van de aanvaarding en afwijzing van door de agent ten behoeve van de gebruiker uitgevoerde taken, vergroot de privacygevoeligheid van de ISA. Een afwijzing zou in het profiel kunnen worden opgevat als een afkeur en een aanvaarding als een voorkeur. Hoe langer de lijst van voor- en afkeuren des te beter is de basis waarop de agent toekomstige beslissingen kan nemen. In het Privacy Incorporated Software Agent (PISA) project is als 'demonstrator'[131] een structuur van mobiele privacybeschermende software agents gebouwd die als taak kregen een vaste baan voor de gebruiker van de ISA (hierna: 'applicant') via het internet te vinden. De research werd gesubsidieerd door de EU onder het 5th EU Framework for Technology Research.

a. Consequenties van de privacybedreigingsanalyse

De PISA-privacybedreigingsanalyse, die in paragraaf 4.10 is behandeld, maakte duidelijk dat:

1. Privacyinbreuken kunnen door andere 'vermomde' software agents worden veroorzaakt.[132]
2. Privacybedreigingen kunnen ontstaan door onzorgvuldig beheer van de eigen persoonlijke agent en daaraan gekoppelde taak agents.
3. Onzorgvuldige communicatie met agents van andere gebruikers kan privacy-risico's veroorzaken.
4. De agent kan worden overmeesterd door andere agenten, die vervolgens persoonsgegevens van de overmeesterde agent stelen.[133]
5. 'Web data mining' kan een serieuze bedreiging voor de agent zijn.[134]

De ontwerpers concludeerden uit de privacybedreigingsanalyse dat de PISA-agent te kwetsbaar was om in zijn geheel binnen internet mobiel te opereren. De veiligste aanpak is de persoonlijke agent de mogelijkheid te geven om per uit te voeren taak (bijvoorbeeld: regel voor mij een vliegticket van A naar B) een 'task agent' in het leven te roepen. De 'task agent' krijgt niet meer persoonlijke informatie (een zeer klein deel van het volledige curriculum vitae van de gebruiker) mee, dan strikt noodzakelijk is voor de te vervullen taak. Daarmee kan naast het verminderen van het privacyrisico ook tegelijkertijd aan het beginsel van gegevensminimalisatie worden voldaan. Naast de generieke persoonlijke agent en de specifieke taak agents komen in het researchproject met betrekking

130 Schermer, Durrinck & Bijmans, 2005, p. 28.
131 De Europese Commissie vereiste bij de subsidiering van het PISA-project dat er een werkend bewijs (demonstrator) zou worden getoond van de privacybeschermende kwaliteiten van de ISA.
132 Borking, Van Eck & Siepel, 1999, p. 29.
133 Borking, Van Eck & Siepel, 1999, p. 30-31.
134 Vlachakis, Eirinaki & Anand, 2004.

tot PISA ook service agenten voor "to segment responsibility with regard to the protection of personal data."[135]

Om de software agents te beveiligen tegen privacybedreigingen zijn er twee mogelijkheden om PET in te zetten. PET wordt als een beschermingsschil om de agent gelegd, dus tussen de agent en zijn omgeving geplaatst of PET wordt in de verschillende componenten van de software agent geïntegreerd. Borking, Van Eck & Siepel wijzen erop dat een PET-schil rond de agent als nadeel heeft: "A disadventage of wrapping is that only external activities of the agent can be logged and audited."[136] In PISA is gekozen voor een combinatie van een PET-beschermingsschil rond de ISA en een geïntegreerde PET-bescherming in de verschillende componenten binnen de agent. In paragraaf 6.18 wordt ingegaan op de architectuur van PISA. Om aan de privacybedreigingen het hoofd te kunnen bieden is het ook noodzakelijk de persoonsgegevens van de gebruiker van ISA in vier niveaus[137] te splitsen, namelijk:

Niveau 1 PII:

Niveau 1 PII omvat onder meer de naam en het adres, telefoonnummer en e-mailadres van de gebruiker van PISA. Deze verzameling van persoonlijke informatie (PII) wordt door PISA overgedragen wanneer de directe communicatie tussen gebruiker en het kandidaatbedrijf voor het vervullen van de vacature dat vereist. Men kan deze gegevens alleen gebruiken, wanneer de stroom van uitgewisselde gegevens tussen PISA en de agent van de organisatie tot het gewenste resultaat heeft geleid en daardoor direct menselijke contact tussen de gebruiker (bijvoorbeeld de zoeker naar de baan) en de directie van de organisatie nodig is. Het is onbelangrijk of men een echte identiteit of een pseudo-identiteit gebruikt. Niveau 1 PII kan ook het creditcardnummer van de gebruiker zijn, waarmee hij wil betalen voor het downloaden van het iTunes-nummer. Om deze reden wordt dit niveau PII als contactgegevens (om de transactie af te ronden) aangeduid.

Niveau 2 PII:

Dit betreft alle andere onderdelen van de (beperkte) persoonsgegevens van de gebruiker behalve de gegevens die tot niveau 1 PII, Niveau 3 PII en Niveau 4 PII behoren.

Niveau 3 PII:

Het gaat hier om persoonsgegevens die als speciale categorieën van persoonsgegevens in artikel 8 (1) van Richtlijn 96/46/EG zijn vermeld. Niveau 3 persoonsgegevens mogen slechts in die omstandigheden worden verwerkt, die overeenkomen met de manier zoals in artikel 8 (2) t/m (7) is aangegeven.

Niveau 4 PII:

Deze gegevens betreffen de verkeersgegevens die een agent creëert wanneer die zich door het internet van website naar website verplaatst. Zolang deze

135 Van Blarkom, Borking & Olk, 2003, p. 147.
136 Borking, Van Eck & Siepel, 1999, p. 39.
137 Borking, 2003, p. 238: "Eerst in drie niveaus. Pas in een laat stadium zijn de verkeersgegevens erbij gekomen."

gegevens direct of indirect informatie over de gebruiker van de agent produceren, moeten deze gegevens worden beschouwd als persoonsgegevens. In het PISA-ontwerp worden deze gegevens door middel van beveiligde communicatie zo behandeld dat die niet aan de gebruiker zijn toe te schrijven.

Het is niet uit te sluiten dat de identiteit van de gebruiker toch uit niveau 2 PII en 3 PII afleidbaar is. Bij de bouw van LADIS (Landelijk Alcohol en Drug Informatiesysteem) is onderzoek gedaan hoe de identificatie van de gebruiker zou kunnen worden verhinderd. Door middel van dubbele 'hashing' van naam, geslacht en geboortedatum kan het identificatieprobleem worden opgelost, maar bij de uitwisseling van gegevens tijdens de onderhandelingen van agents is deze aanpak te complex en daardoor contraproductief gebleken. Koorn e.a. wijzen erop dat deze vorm van anonimisering alleen in identiteitsarme of identiteitloze processen kan worden toegepast.[138] Een belangrijk verschil tussen niveau 2 PII en niveau 3 PII is dat niveau 3 PII sterkere (technische en organisatorische) beveiligingsmaatregelen vereist om deze categorie van persoonsgegevens te beschermen.[139] PET-maatregelen, (zie paragraaf 5.7.3), beschermen Niveau 1 PII door deze gegevens binnen PISA op het tijdstip van verkrijging direct in te kapselen. Slechts de partij die het recht heeft om niveau 1 PII te ontvangen, krijgt toegang tot de middelen om de met PET ingekapselde niveau 1 PII te openen. De algehele privacybescherming en beveiliging binnen de PISA-'applicant' wordt gerealiseerd door een combinatie van 'Identity Protectors' in de vorm van:

1. Anonimisering en pseudo-identiteiten.
2. Certificaten van een TTP om de agent (met een eigen pseudo-identiteit) in staat te stellen zich te kunnen authenticeren in het contact met andere agenten.
3. Privacymanagementtechnieken zoals 'transfer rules', paragraaf 5.13.
4. Een beveiligde omgeving (door authenticatie) van de met elkaar communicerende agents, waarin vaststelling van de integriteit van de gecommuniceerde boodschappen en de confidentialiteit van de uitgewisselde mededelingen plaatsvindt.

Alle gegevens die de agent bij zich draagt, zijn ter wille van de beveiliging en privacybescherming versleuteld.

b. Ingebouwde juridische kennis

In de PISA-'applicant' is rudimentaire juridische kennis (de privacyrealisatiebeginselen) als norm voor het handelen ingebouwd om er zeker van te zijn dat de verwerking van persoonsgegevens tijdens de werkzaamheden en onderhandelingen van de software agent geschiedt overeenkomstig de Richtlijn 95/46/EG (zie figuur 6.18). De PISA-'applicant' draagt daarnaast met zich mee de

138 Koorn, e.a., 2004, p. 39.
139 Van Blarkom, Borking & Olk, 2003, p. 148. Zie ook hoofdstuk 2.2.3.

privacyvoorkeuren (zie hoofdstuk 2) van de gebruiker en de privacy policy van de verantwoordelijke. In de PISA-'applicant' zijn de privacyvoorkeuren en de privacy policy in overeenstemming met de EU-richtlijnen 95/46/EG en 2002/58/EG. De privacy policy van de verantwoordelijke is opgenomen in de 'Agent Practices Statement' (APS) die de agent bij zich draagt. Tijdens het zich verplaatsen van de PISA-'applicant' door het internet is deze agent zo geprogrammeerd dat onderhandelingen over de overdracht van PII pas plaatsvindt als de APS van de agent waarmee onderhandeld wordt, ten minste gelijkwaardig is aan het beschermingsniveau dat de Richtlijn 95/46/EG biedt.[140]

c. Interactieprotocollen

De interactieprotocollen tonen aan hoe de communicatie in het multi-agentensysteem wordt georganiseerd, waar veel agents elkaar op 'agents platforms' (virtuele marktplaatsen) binnen internet tegenkomen. De interactieprotocollen specificeren op welk moment welk patroon van communicatie door de PISA-'applicant' moet worden gevolgd betreffende de uitwisseling van de niveaus PII in de communicatie tussen agenten en PISA-'applicant'. De protocollen refereren aan de in de agent geïmplementeerde transfer rules, want de PISA-'applicant' moet in staat zijn om vast te stellen of de PII wel of niet kan worden verzonden. In paragraaf 5.13 is een dergelijke ingebouwde instructie van de agent weergegeven als "if APS-(1) matches privacy-preference-(2) and APS-(2) matches privacy-preference-(1) and PII level 2-(1) matches PII level 2-(2) then allow disclosure/exchange PII level 1-1."[141] Voor dit doel zijn zowel informatie over de agent die PII ontvangt als de metagegevens van PII nodig. De metagegevens van PII zijn belangrijk omdat het de privacyvoorkeuren van de gebruiker bevat. De PISA-'applicant' moet de privacyvoorkeuren vergelijken met de privacy policy van de ontvanger door middel van zijn ingebouwde 'transfer rules' (de regels die gaan over de overdracht van de PII). De 'transfer rules' bestaan uit één of meerdere regels per privacyrealisatieprincipe. Als de 'transfer rules' positief worden beoordeeld en PII wordt verzonden naar de ontvanger, dan moeten de metagegevens over de PII die de privacyvoorkeuren van de gebruiker bevatten samen met PII worden verzonden. Op deze manier kan de ontvangende agent weer als afzender van PII conform de privacyvoorkeuren van de gebruiker handelen als deze agent weer een andere agent ontmoet.

Bij de PISA-'applicant' is er vanuit gegaan dat er zich een keten van agenten vormt voordat de juiste baan gevonden is.[142] Die keten bestaat ten minste uit de volgende 'task agents' (van verschillende gebruikers):

---

140 Borking, 2003, p. 243.

141 APS staat voor Agent Practices Statement (de privacy policy) waaronder de software agent opereert. De cijfers tussen haakjes betreffen de elkaar ontmoetende agenten (1) en (2). PII (2) gaat over een set persoonsgegevens met een laag identificerend gehalte (er zijn vier niveaus).

142 Van Breukelen, Ricchi & Bison, 2003, p. 305-315.

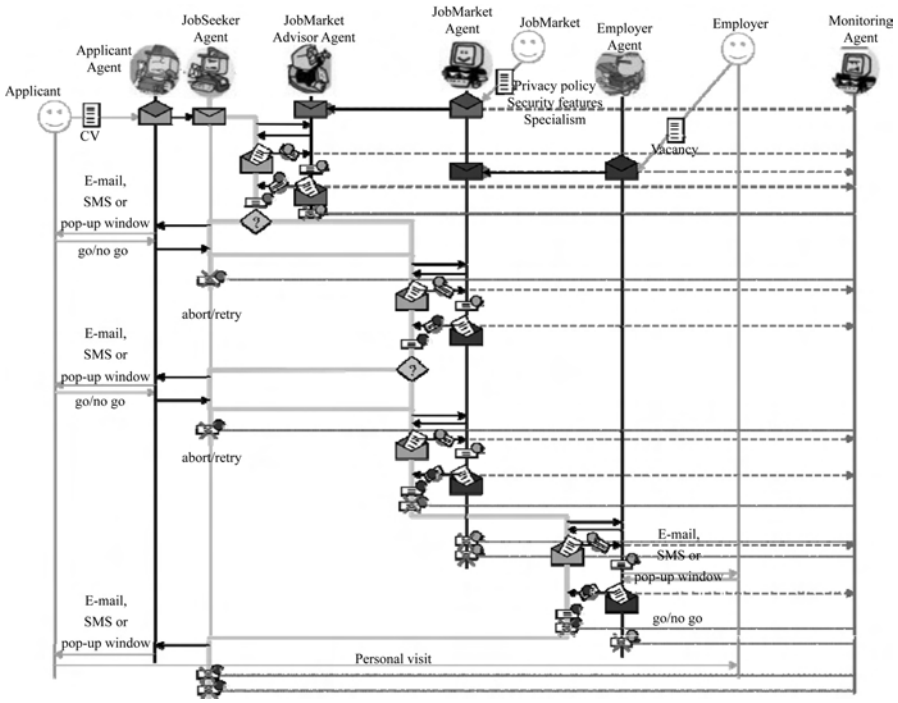
1. De persoonlijke agent van de gebruiker, die permanent op de pc van de gebruiker blijft.
2. De task agent, die de gebruiker 'vertegenwoordigt' (dat wil zeggen dat de acties van de agent aan de gebruiker worden toegerekend) tijdens het zoeken naar een baan en zorgt voor de communicatie met de gebruiker en de andere agents.
3. De solicitatie agent, die mobiel is en zich verplaatst van het ene naar het andere 'agentsplatform' waar arbeidsmarktagents resideren.
4. De arbeidsmarktadviseuragent, die de sollicitatie agent op de hoogte stelt van de betrouwbare en passende arbeidsmarkt agents.
5. De arbeidsmarktagent die voor een gespecialiseerde arbeidsmarkt als een 'matchmaker' fungeert en de sollicitatie agents in contact brengt met de verschillende werkgevers agents.
6. De werkgeversagent, die het bedrijf of een 'headhunter' representeert.
7. De 'monitor'agent, die alle communicatie logt en overziet, zoals wie met wie communiceert en welke metadata over de inhoud (dus niet de inhoud zelf) hierbij meespelen. Daarbij geldt als uitdrukkelijke voorwaarde, dat de een agent niet met een ander kan communiceren als niet de monitoragent beschikbaar is om de communicatie te loggen.[143]

De gegevensstromen tussen de sollicitant en de potentiële werkgever zijn:
1. Vanuit de gebruiker de niveau PII 2 gegevens via de 'task agent' en de wensen met betrekking tot de baan naar de 'job market' agent en vanuit de werkgever via de organisatie agent naar de 'job market' agent het profiel van de baan en beperkt identificerende gegevens over de organisatie zelf.
2. Vanuit de gebruiker de niveau PII 2 gegevens via de 'task agent' en het profiel van de sollicitant naar de 'job seek' agent en vanuit de werkgever via de organisatie agent naar de 'vacancy agent' met de door de sollicitant te vervullen vereisten en beperkt identificerende gegevens over de organisatie zelf.
3. Wanneer beide partijen via hun task agents een 'match' hebben, dan gaan er niveau PII 1 gegevens van de gebruiker via de task agent naar de organisatie agent naar de werkgever en omgekeerd de contactinformatie van de werkgever.[144]

Figuur 6.17 laat de eerste bladzijde van de tachtig bladzijden tellende communicatie- en onderhandelingensequentie tussen de agenten zien bij het vinden van een baan voor de gebruiker van de PISA-'applicant'.

143 Van Breukelen, 2003, p. 1-80.
144 Van Breukelen & Meyer, 2003, p. 316.

Figuur 6.17: Eerste bladzijde van de communicatie tussen PISA en andere mobile software agents. De kleur van de envelop geeft de herkomst van het verzonden bericht aan. In deze figuur worden enveloppen gestuurd door drie verschillende agents, nl. de applicant agent, de job market agent en de employer agent. De vraagtekens betekenen dat met de gebruiker van de agent dient te worden overlegd voordat de agent zijn taak verder kan uitvoeren.



De vraagtekens in de figuur 6.17 betreffen de in een 'pop-up window' gestelde consultatievragen van de agent aan de gebruiker over hoe te handelen met betrekking tot afgifte van PII. Hieronder volgen drie voorbeelden.

1. User Applicant receives message from applicant agent about vacancy that is potentially interesting, but for which the employer agent needs more private information. Please make a choice. Choose scenario: Do not continue negotiations or Hand over extra private information and continue negotiations.
2. Job seeker agent has finished task sequence. Based on input from applicant agent the job seeker agent continues search or not. Please choose scenario: Abort search or Continue search.

3. Applicant receives message from applicant agent about job market that doesn't offer the desired privacy policy and/or security features, or isn't specialized in the job market you are interested in. Please make a choice: Do not trust job market agent or Trust job market agent.[145]

d. Anonimiteit en pseudo-identiteit

In PISA wordt een onderscheid gemaakt tussen persoonlijke en (afgesplitste) task agents. De persoonlijke agents zijn permanent en bevatten alle niveaus PII. De persoonlijke agent delegeert beperkte PII aan de taak agents, die een beperkte dimensie en slechts één leven hebben (na de uitvoering van de taak wordt hij en zijn klonen[146] direct uitgeschakeld ('killed'), want bij hergebruik kan tracering van de gebruiker plaatsvinden). De taak agent bevat slechts de relevante informatie voor één bepaalde taak. Vandaar dat alle persoonlijke informatie vercijferd is afgeschermd zolang die informatie niet uitdrukkelijk wordt opgevraagd en vrijgegeven. De 'task agent' die een specifieke taak voor een gebruiker uitvoert, is niet anoniem aangezien de agent overeenkomstig de specificaties van FIPA[147] gebouwd moet zijn en derhalve een naam moet hebben, waardoor deze kan worden geïdentificeerd. De identiteit van de gebruiker kan niet uit de naam van de agent worden afgeleid en kan derhalve als pseudo-identiteiten van de gebruiker worden gezien. Slechts de persoonlijke agent van de gebruiker weet welke agent als task agent optreedt.

Een aanvaller (hacker) zou een communicatie-analyse van het 'agents platform' kunnen uitvoeren en dat zou de relatie tussen de persoonlijke agent en de task agent kunnen openbaren. Toepassing van 'onion routing'[148] met encryptielagen kan dit probleem oplossen, want een alternerende 'onion routing' maakt anonieme communicatie tussen agenten mogelijk, waardoor de uitgewisselde mededelingen worden beschermd tegen verkeersanalyse. Deze benadering verbergt informatie die zou kunnen duidelijk maken welke agent met welke agent voor welk doel wordt verbonden (zie figuur 6.18). De 'sender' bepaalt de route van het bericht. Hij zendt het bericht met encryptielagen naar een 'mix'. Een 'mix' is een computer die tussen zenders en ontvangers 'bemiddelt'. De 'mix' slaat berichten op, past daarop cryptografische berekeningen toe en zendt deze weer verder naar het volgende 'mix'station. De verzending van ontvangen berichten geschiedt totaal willekeurig, dat wil zeggen op een manier die door anderen niet te voorspellen is.

---

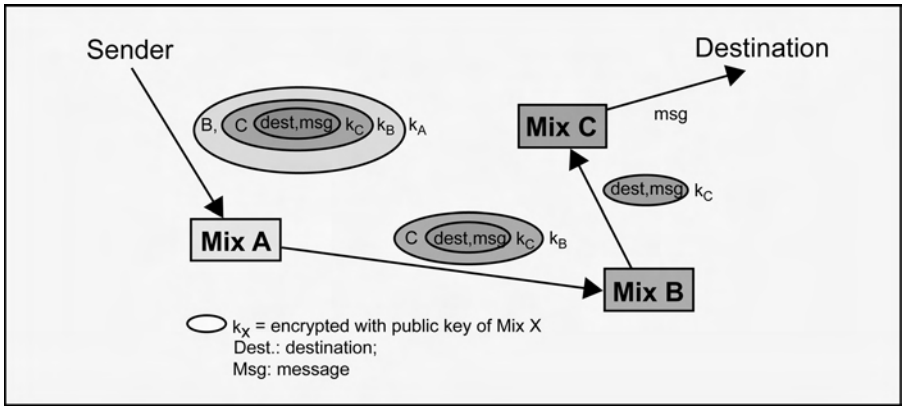
145 Er zijn er nog veel meer van deze pop-upberichten.

146 Om het zoekproces te versnellen kan de task agent zichzelf klonen in zo veel kopieën als door de agent nodig wordt geacht bijvoorbeeld als er duizenden aanbiedingen voor het gewenste werk wordt gedaan.

147 Foundation for Intelligent Physical Agents, die de standaarden voor agents vaststelt.

148 Canon, 2004, p. 21: "Onion routing is an adaptation of a mix network to facilitate online applications. The packets with layered encryption are referred to as onions." De toepassing kan gevonden worden bij http://www.onion-router.net/.

Figuur 6.18: Mixes: de basis van union routing. De gekleurde schijven zijn de 'af te pellen' encryptieringen, te vergelijken met enveloppen waarin weer enveloppen zich bevinden. In dit voorbeeld zendt A de mededeling naar de gekozen bestemming met de publieke sleutels Ka, Kb, Kc naar de bestemming (de uiteindelijke ontvanger) via Mix A; Mix A analyseert de encryptie en herkent de publieke sleutel Kb en stuurt de mededeling door naar Mix B; Mix B volgt dezelfde procedure en zendt door naar Mix C etc.



Zoals als eerder betoogd neemt een 'taskagent' slechts die PII mee, die voor de taak is vereist. Alvorens persoonlijke informatie naar een andere agent te verzenden, zal de 'taskagent' ervoor zorgdragen dat de ontvanger met de privacyrealisatiebeginselen en de privacyvoorkeuren van zijn meester (de gebruiker) instemt. Bijvoorbeeld: een 'service agent' ontvangt slechts Niveau 2 PII en pas na toestemming van de persoonlijke agent of de gebruiker zelf kan gevoeligere persoonlijke informatie worden overgedragen. Zelfs wanneer de 'taskagent' de contactinformatie onthult, dan nog zou deze informatie de echte identiteit van de gebruiker kunnen verbergen. De contactinformatie zou slechts een e-mailadres kunnen bevatten waardoor de gebruiker niet of met veel moeite identificeerbaar is. Overeenkomstig de EU-privacyrichtlijnen moet de agent in staat zijn om de PII van de gebruiker op zijn verzoek te kunnen verwijderen en/of bij te werken. Om dit doel te bereiken, ondersteunt de PISA-'applicant' in de interactieprotocollen de privacyrealisatierechten van de gebruiker (inzage, verwijdering, correctie, blokkering) en zal de agent de PII overeenkomstig het verzoek van de gebruiker op elk gewenst moment bijwerken. Behalve het verwijderen van de PII zal het ook voor de gebruiker mogelijk zijn om een 'taskagent' samen met zijn PII te 'killen' en zelfs zijn persoonlijke agent en alle taakagenten die daaruit zijn ontstaan te annihileren.[149]

149 Van Breukelen & Meyer, 2003, p. 315-320.

e. Audit trail

De gebruikers van de PISA-'applicant' dienen te weten welke berichten tussen agents worden verzonden, zowel ter wille van de transparantie, de controle (monitoring) op het handelen van de 'task agent', als de aansprakelijkheid die uit handelingen van hun '(task) agents' zouden kunnen voortvloeien. Voor de verwezenlijking van de transparantie, wordt voor elke gebruiker een 'log agent' aangemaakt. De 'log agent' is een specifieke 'task agent', die met de gebruiker is geassocieerd. Als dusdanig, heeft de agent toegang tot de persoonsgegevens van de gebruiker en zijn hoofddoel is om vast te leggen wat er gebeurt tijdens de onderhandelingen tussen agents met de PII van de gebruiker en de daaruit voortvloeiende transacties. In deze context krijgt de log agent automatisch terugkoppeling over alle berichten waarin de persoonsgegevens zijn opgenomen. Het gaat niet zozeer om de inhoud van de persoonsgegevens, maar door het oormerken van gegevens de gebruiker genoeg terugkoppeling te geven om te kunnen nagaan waar zijn persoonsgegevens naartoe zijn gegaan.[150] Deze loggingfunctionaliteit bevat ook een 'audit agent' die de agents zal controleren op hun handelen en die slechts door een van tevoren geautoriseerde RA- of RE-accountant of door een daartoe aangewezen medewerker (auditor) van de Data Protection Authority (in Nederland het College bescherming persoonsgegevens) kan worden geraadpleegd. De combinatie van log agent en audit agent is de monitor agent in figuur 6.17.

6.10. De structuur van de PISA-applicant

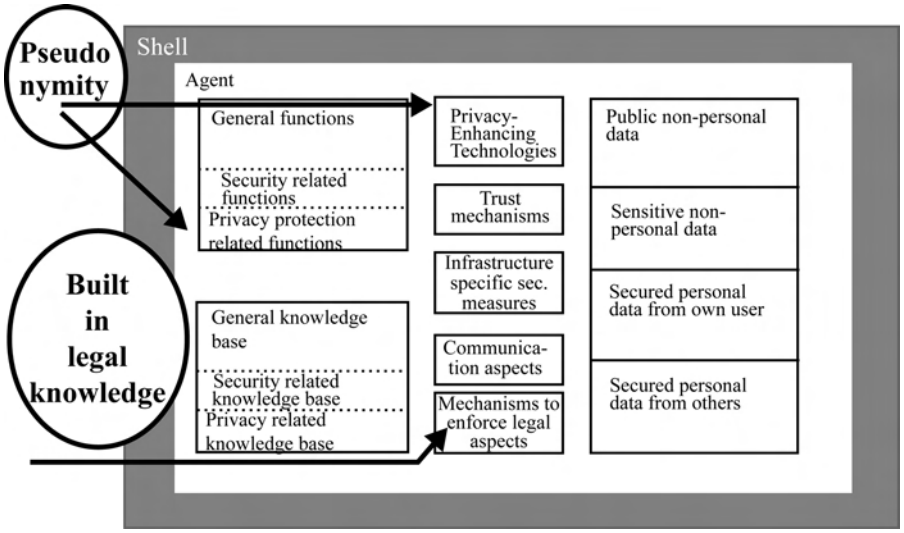
Zoals hierboven is aangegeven dient de PISA-'applicant' zich tegen aanvallen, beveiligingsrisico's en privacyinbreuken te beschermen.[151] Deze agent heeft daarom een anonimiteitsschil en ingebouwde privacybeschermende functies, privacy enhancing technologies (PET) voor pseudo-identiteiten, ingebouwde juridische knowhow, en mechanismen om de privacyrealisatiebeginselen af te dwingen. De 'Identity Protectors' worden aangestuurd door de componenten privacy related function en PET. De trust mechanisms worden beveiligd met geavanceerde encryptie.[152] Figuur 6.19 geeft een vereenvoudigd overzicht van deze componenten. De 'shell' is de beschermende schil rond de software agent, te vergelijken met een 'Identity Protector' tussen de agent en zijn omgeving.[153] Ingebouwd zijn PET-maatregelen die bij bepaalde uitwisseling van informatie extra bescherming behoeven. In de agent zijn drie lagen aangebracht, bestaande uit algemene kennis van omgeving waarbinnen de agent moet werken, kennis

150 Dit datataggingmechanisme is ontwikkeld in het PRIME-project zoals aangegeven in hoofdstuk 5 van dit boek.
151 Borking, 2003, p. 86-91.
152 Cartrysse, 2005: "Dit afdwingen gebeurt met behulp van geavanceerde cryptografische technieken."
153 Borking, van Eck & Siepel, 1999, p. 39.

over informatiebeveiliging en kennis over de privacybescherming. Deze drie lagen bepalen de acties van de agent. De agent kan op basis van de informatie die hij tijdens zijn acties tegenkomt, besluiten tot het coöperatief gedrag, planmatig gedrag of een beslissing nemen. De modules binnen de schil geven aan uit welke domeinen de agent kan putten voor zijn gedrag. Belangrijk is dat in de PISA-agent de privacyrealisatiebeginselen zijn ingebouwd. op grond waarvan de agent mede een beslissing kan nemen over het beschermen van de persoonsgegevens van de gebruiker ('master').

In de PISA-agent (zie figuur 6.19) zijn de privacyrealisatiebeginselen (ingebouwde juridische kennis, aangegeven als 'legal knowledge'), de scheiding van de verschillende soorten persoonsgegevens (o.a. 'secured personal data from own user', 'secured personal data from others', 'public-non-personal data' en de overdrachtsregels dominant in de afweging in het beslissingsmodel). Het component 'trust mechanisms' kan bestaan uit middelen ten behoeve van beveiligde identificatie, authenticatie, integriteit, logging en auditing, een en ander afhankelijk van de infrastructuur waarbinnen de agent moet werken. Het kan zijn dat specifieke certificaten worden meegedragen om binnen een 'trusted environment' te kunnen opereren.

Figuur 6.19: Structuur van PISA-agent met PET-schil en ingebouwde PET-functionaliteiten.



6.11. De toestemming

Er blijven in deze context nog twee belangrijk privacyrechtelijke vraagstukken over. 1. Hoe moet de voorgeschreven toestemming in het agentensysteem worden

omgegaan c.q. worden ingebouwd, 2. hoe moet worden gehandeld wanneer persoons- en transactiegegevens moeten worden overgedragen aan agenten die opereren onder andere rechtssystemen, dan die van de EU en EEA.

Los van het feit dat het eerste uitgangspunt voor het ontwerp van een privacyveilige agent anonimiteit en pseudo-identiteit is, blijft direct daarna het meest belangrijke ontwerpbeginsel het managen van de toestemming van de gebruiker/betrokkene, voor zover toestemming wettelijk vereist is. Immers, de Richtlijn 95/46/EG vereist in artikel 7 (a) dat de persoonsgegevens slechts kunnen worden verwerkt als de betrokkene zijn of haar ondubbelzinnige toestemming heeft gegeven. Volgens de Richtlijn, betekent de toestemming van de betrokkene 'any freely given specific and informed indication by which the data subject signifies his agreement to personal data relating to him being processed'. Zoals in hoofdstuk 2 is aangegeven, betekent dit dat de betrokkene zonder dwang precies aangeeft wat zijn wensen zijn met betrekking tot de te verwerken persoonsgegevens.[154] Het is daarom essentieel dat gebruikers begrijpen wanneer en wat voor een verplichting zij aangaan en wat de gevolgen daarvan zijn. Zij dienen zich dan ook bewust te zijn van de bijzondere omstandigheden wanneer hun persoonsgegevens zonder hun toestemming of zonder dat er sprake is van een overeenkomst worden verwerkt. Vandaar dat in de interface tussen gebruiker en de agent dit prominent en duidelijk dient te zijn, bijvoorbeeld door in een 'pop-up window' consultatievragen van de agent aan de gebruiker te stellen over hoe te handelen met betrekking tot het geven van toestemming. Dat betekent dat bij de testen van de ISA moet worden nagegaan of voldaan wordt aan de vier 'human computer interfaces' (HCI) (de 4 C's) vereisten[155], te weten:

1. 'Comprehension' – Begrijpt of weet de gebruiker wat van hem wordt verwacht?
2. 'Consciousness' – Is de gebruiker zich bewust of geïnformeerd wanneer de opties van het agentsysteem door hem kunnen c.q. moeten worden gebruikt?
3. 'Control' – Is de gebruiker in staat om wat hij doet en heeft gedaan binnen het systeem te controleren en te corrigeren? En
4. 'Consent' – Is de gebruiker in staat ondubbelzinnig en vrij toestemming te verlenen en met de resultaten van de onderhandelingen in te stemmen?[156]

De PISA-'demonstrator' is in Ottawa door het National Research Center onder 200 studenten op de 4 C's getest. De resultaten waren dat:

> "The prototype worked fairly well (72%) and was easy to navigate (76%), but it had poor visual appeal (42%); The Users understood the concept of a personal assistant (digital butler) who could

154 Korff, 2007, p. 13: "According to article 2 (f) of the Directive 2002/58/EC 'consent' by the user or subscriber corresponds to the data subject's consent in the Directive 95/46/EC. Recital 17 adds that 'consent' may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting a Internet website."

155 Van Blarkom, Borking, & Olk, 2003, p. 260-265 voor een uitvoerige beschrijving van de beginselen van HCI.

156 Mulder & Borking, 2006, p. 256.

provide services (92%); Users understood (>90%) the major functions (create, modify, track, results)."[157]

Terecht merkt Bygrave[158] op dat als de toestemming via elektronische agents wordt uitgevoerd dat een dergelijke toestemming slechts geldig zal zijn wanneer dit conform de wettelijke vereisten conform de Richtlijn 95/46/EG geschiedt. Juridische analyse van dit vraagstuk in de context van agents leidt tot de conclusie dat het toestemmingsvereiste alleen wordt vervuld als er sprake is van het telkens per transactie of taak creëren van één specifieke eenmalige en tijdgebonden 'task agent'. Zoals uit het vorenstaande blijkt voldoet het PISA-ontwerp van de 'task agents' hieraan. De specifieke PISA-'task agent' (die door de monitor agent wordt gelogd) levert het bewijs van de vereiste ondubbelzinnige toestemming voor de verwerking van persoonsgegevens voor de transactie of opgelegde taak. Ingewikkelder is het feit dat de Richtlijn de verwerking van gevoelige of speciale categorieën van gegevens verbiedt dan wel aan strikte voorwaarden bindt, zoals gegevens over ras of etnische oorsprong, politieke standpunten, godsdienstige of filosofische opvattingen, vakbondslidmaatschap, de gezondheid of de seksuele geaardheid. Dit verbod bij de verwerking van deze gegevens kan worden opgeheven wanneer verwerking plaatsvindt na expliciete toestemming van de betrokkene. De vereiste toestemming kan tezamen met een biometrisch kenmerk van de gebruiker in een zodanige elektronische vorm worden verstrekt dat de onherroepelijkheid van die toestemming boven elke twijfel verheven is. Bovendien geldt als voorwaarde dat uit een begeleidende tijdsstempel die aan de expliciete toestemming van de gebruiker is gehecht, moet blijken dat de toestemming recent is, bijvoorbeeld niet ouder dan 24 uur.

Artikel 8 lid 2 van de Richtlijn 95/46/EG geeft aan wanneer het verbod vervat in lid 1 niet toepassing is, bijvoorbeeld als gegevens moeten worden verwerkt in het kader van de medische zorg. Voor het ontwerp van de PISA-applicant is het bepaalde in artikel 8 lid 2b van belang. Dit lid bepaalt dat lid 1 niet van toepassing is wanneer: "de verwerking noodzakelijk is met het oog op de uitvoering van de verplichtingen en de rechten van de voor de verwerking verantwoordelijke inzake arbeidsrecht, voor zover zulks is toegestaan bij de nationale wetgeving en deze adequate garanties biedt."

Opinion 114 van de Article 29 Working Party over de toestemming in een arbeidscontext stelt dat:

"Specific difficulties might occur to qualify a data subject's consent as freely given in an employer context, due to the relationship of subordination between de employer and employee.

157 Huizenga, 2006, p. 18.
158 Bygrave, 2001, p. 288.

> Valid consent in such a context means that the employee must have a real opportunity to withhold his consent without suffering any harm, or to withdraw it subsequently if he changes his mind."[159]

Per lidstaat kunnen er nog wel eens verschillen optreden. Het vereiste in de Franse wet op de gegevensbescherming[160] met betrekking tot de 'uitdrukkelijke toestemming' voor de verwerking van gevoelige gegevens, is dat de toestemming schriftelijk dient te worden gegeven.[161] Dat kan natuurlijk met software agents niet. De Franse 'Commission nationale de l'Informatique et des Libertés' (CNIL) heeft bepaald dat met betrekking tot verwerking van gevoelige gegevens via het internet, de betrokkene met een 'tweemaal klikken' van de muis aangeeft uitdrukkelijk toe te stemmen (d.w.z. de eerste 'klik' bevestigt dat men bewust is van de voorgestelde verwerking en de tweede klik geeft aan dat men uitdrukkelijk toestemt).[162] Verschillende DPA's binnen de EU hebben voorgesteld als blijk van toestemming een vierkantje aan te klikken of aan te kruisen.[163] In privacyveilige agents wordt het toestemmingsmechanisme ondervangen door strikte 'transfer rules' in de agent in te bouwen en door met 'Just-In-Time-Click-Through Agreements' (JITCA's) te werken. JITCA's zijn gebaseerd op de observatie dat de meest voorkomende manier om toestemming in computer-applicaties te krijgen, plaatsvindt door middel van een gebruikersovereenkomst. Na installatie van bijvoorbeeld software op een pc wordt op het scherm vaak een interfacevlak getoond met een virtuele knop met de woorden 'I agree'. Bij afronding van de installatie van software, moet de gebruiker als bewijs van instemming met de voorwaarden op deze knop klikken.[164] Patrick en Kenny wijzen erop dat: "The main feature of a JITCA is not to provide a large, complete list of service terms but instead to confirm the understanding or consent on an as-needed basis. These small agreements are easier for the user to read and process and facilitate a better understanding of the decision being made in-context."[165]

Een JITCA is geen standaard contract vergelijkbaar met algemene voorwaarden, maar een korte omschrijving van de beslissing die genomen moet worden. In de loop van de onderhandelingen met de agents kunnen zeer veel JITCA's

159 WP 29, Working document 114 on a Common Interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, Brussels, 2005, p. 11.
160 La loi n 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978/modification la loi du 6 aout 2004.
161 Ook in de Bondsrepubliek Duitsland bevat de Federale Wet op de gegevensbescherming in artikel 4 a lid 1 de bepaling dat de toestemming schriftelijk moet geschieden. Maar in artikel 2 lid 3 van de Duitse handtekeningenwet mag er ook sprake zijn van een elektronische handtekening, tenzij specifieke omstandigheden een andere vorm toestaan.
162 Borking, 2005.
163 Camenish, Leenes & Sommer, 2008, p. 368.
164 Patrick, 2002, p. 1. Over de juridische haalbaarheid is net als over de shrink wrap agreement veel gediscussieerd. The Cyberspace Law Committee of the American Bar Association heeft zes richtlijnen voor JITCA's gepubliceerd.
165 Patrick & Kenny, 2003, p. 107-124.

voorkomen. De EU Article 29 Working Party heeft in haar 'Opinion On More Harmonized Information Provisions' van 25 november 2004 een mededeling met een drie lagenstructuur voorgesteld waarin de informatie, die in artikel 10 van de Richtlijn 95/46/EG is voorgeschreven, is opgenomen.[166] JITCA's voldoen aan de vereisten van de hierboven vermelde Opinion en kunnen dus beschouwd worden als te voldoen aan de toestemming vereisten ex artikel 7 (a) van de Richtlijn 95/46/EG.

6.12. Agenten in niet-EU-rechtssystemen

Binnen cyberspace zijn er geen landsgrenzen. Software agents verplaatsen zich binnen internet van website en agentsplatform tot website. Dit houdt in dat zowel ten aanzien van de verwerking als de openbaarmaking van PII agents met andere rechtsstelsels en met agents uit andere rechtstelsels dan het EU-privacyrechtssysteem geconfronteerd zullen worden. Vandaar dat de openbaarmaking van de PII door de verzendende PISA-agent (met de normen van de Richtlijn 95/46/EG als minimum standaard ingebouwd) aan de ontvangende agent alleen is toegestaan als de APS (privacy policy) van de ontvangende agent past binnen de privacyvoorkeuren van de verzendende PISA-agent. De verzendende agent dient zich, in welk rechtstelsel deze zich ook bevindt, ervan te vergewissen dat de APS van de ontvangende agent voldoet aan de wettelijke vereisten zoals vastgelegd in de Richtlijn 95/46/EG. Wanneer aan de ontvangende agent persoonsgegevens worden overgedragen, dan zal de task agent ook moeten verifiëren dat de ontvangende agent, wanneer deze de van hem ontvangen gegevens moet doorzenden, dezelfde procedure volgt bij het overdragen van gegevens aan de volgende ontvangende agent door in zijn rol van verzendende agent de APS van de ontvangende agent op dezelfde manier te verifieren. Wanneer het gaat om een gegevensuitwisseling tussen een Amerikaanse en Europese software agent zal (zie paragraaf 2.4.2), het regime van de Safe Harbor Agreement kunnen gelden.[167] Dat betekent dat de agent in staat zal moeten zijn om zijn ingebouwde (rudimentaire juridische) kennis te toetsen aan de Safe Harbor Agreement regels. In het PISA-project is uitsluitend gewerkt met de privacyrealisatiebeginselen, die in de logica van de transfer rules zijn ingebouwd. Als de APS van een Amerikaanse agent niet met de PISA-agent overeenkomt, dan vindt de overdracht van persoonsgegevens niet plaats. De agent zal dan zijn gebruiker om een specifieke toestemming moeten vragen of de onderhandelingen en de uitvoering van de taak afbreken. Landen zoals bijvoorbeeld Canada[168] worden door de EU-Commissie beschouwd als een

166 http//: ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.
167 Safe Harbour Principles, US Department of Commerce, 21 July 2000.
168 EU Commission Decision 2002/2/EC of 20 December 2001 concerning the Canadian Personal Information Protection and Electronic Documents Act.

land met een adequaat niveau van bescherming van persoonsgegevens. Aan Canadese agents, mits hun APS klopt, kunnen de gegevens zonder problemen worden overgedragen. Mocht er geen uitwisseling van gegevens plaats kunnen vinden, dan kan altijd nog naar andere mogelijkheden worden gezocht, bijvoorbeeld zoals vermeld in artikel 26 lid 1 van de Richtlijn 95/46/EG. Er kan ook vooraf over een contract betreffende de uitwisseling van persoonsgegevens worden onderhandeld.[169] Dit is tijdrovend en niet erg praktisch.

Ten gevolge van het feit dat de PISA-agent zo is ingericht dat de privacy policy van de ontvangende agent bij een uitwisseling van PII buiten de EU moeten voldoen aan de Europese vereisten, kan geconcludeerd worden dat in welk rechtsstelsel de agent zich ook bevindt, er sprake is van een adequate bescherming van persoonsgegevens zelfs als de Europese Commissie dat rechtsgebied niet heeft gekwalificeerd als een regime met een adequate bescherming. In feite worden via het ontwerp van PISA de Europese normen op het gebied van bescherming van persoonsgegevens opgelegd. Of dat feitelijk ook economisch haalbaar is, zal nog moeten blijken. Omdat de verantwoordelijke voor privacyinbreuken aansprakelijk gehouden kan worden, zal de verantwoordelijke ernaar streven aan de gebruikers van zijn agents een agent te verstrekken, die privacyzaken conform de wet kan afhandelen. Deze situatie is vergelijkbaar met het kopen van een auto. Niemand wil een auto die de bestaande wetgeving voor auto's overtreedt. Daarom zal geen enkele autofabrikant auto's willen bouwen die in strijd zijn met de bestaande wetgeving. Met name wanneer het gaat om massaproductie van agents zal de ontwikkelaar gedwongen worden om privacybescherming in zijn agents in te bouwen. De economische machtsverhoudingen zullen dan een woordje gaan meespreken, waardoor de EU-privacyregels wel eens onder druk zouden kunnen komen te staan.

6.13. Mislukte PET-automatisering?

Als ict-arbiter en -mediator weet ik uit ervaring maar al te goed dat er heel wat automatiseringsprojecten mislukken en informatiesystemen niet voldoen aan de tussen partijen afgesproken specificaties. Er zijn slechts enkele publicaties te vinden waarin het falen van automatiseringsprojecten in algemene zin aan de orde komt. Borking & Mulder hebben de arbitrale vonnissen[170] en mediationafspraken van de Stichting Geschillen Oplossing Automatisering[171] in 1999 en in 2004

169 Er zijn standaard contractbepalingen voor dergelijke transfers beschikbaar. See http://europa.eu.int/commm/internal_market/en/dataprot/modelcontracts/index.htm.

170 Franken, Borking & Van Schelven, 12 over de SGOA, Den Haag, 1999, p. 109-123; Computerrecht1996/3 p. 107; 1999/1 p. 40, 2001/6 p. 315.

171 Voor meer informatie zie: www.sgoa.org.

bestudeerd en stellen vast dat in de voorgelegde mediation- en arbitragezaken vier missers dominant voorkomen:

1. De directie stuurt het contract aan in plaats van het project.
2. De gewenste functionaliteit is renovatie derhalve bouwen bovenop het 'oude systeem'.
3. Keuze voor 'state of the art' of 'bewezen' technologie is afhankelijk van de toepassing.
4. Kleine aanpassingen in het project stellen de klant tevreden.[172]

Warmerdam e.a. geven in hun onderzoek aan dat bij automatisering in eigen beheer vooral de specificatieproblemen het meest zwaarwegend zijn.[173] Zij stellen vijftien problematische aspecten bij automatiseringsprojecten vast, die in vijf tot tien procent van de gevallen door de betrokkenen als zeer problematisch worden ervaren. Het gaat dan met name om de problemen met de projectbewaking, doorlooptijd, de planning van de kosten, communicatie tussen (externe) automatiseerders en gebruikers en de inzet en bereikbaarheid van interne en externe deskundigen.[174] De respondenten in het onderzoek van Warmerdam e.a. stellen dat vijf procent van de automatiseringsprojecten duidelijk is mislukt.[175]

Koorn e.a.[176] rapporteert over veertien casussen waarin PET is toegepast. Over een van de casussen is in paragraaf 6.7 geschreven, namelijk over het ziekenhuis Veldwijk-Meerkanten. Bij vrijwel al deze casussen ben ik als vicevoorzitter van de Registratiekamer intensief betrokken geweest. In geen van deze casussen is sprake van een mislukte PET-toepassing. Het gunstige resultaat is het gevolg van een goed automatiseringsplan, een gedegen projectorganisatie en adequate invloed van het management en de eindgebruikers in de betrokken organisaties. De toepassing van de PET-maatregelen (met name encryptie en domeinscheiding) in het informatiesysteem heeft geleid tot advisering van de Registratiekamer. Dit heeft er mede toe bijgedragen dat de klassieke oorzaken van mislukking van automatiseringsprojecten niet konden optreden. Bovendien werd bij de betrokken Nederlandse organisaties een gebalanceerd stappenplan uitgevoerd, waarover in hoofdstuk 8 meer. Ook elders in de wereld (o.a. Canada, Duitsland en Frankrijk) heeft het experimentele en innovatieve karakter van PET geleid tot zorgvuldige begeleiding van (sporadische) PET-projecten, waardoor mislukking is voorkomen.

Nochtans, als er geen goede PET-kennis gecombineerd met juridische kennis op het gebied van privacybescherming beschikbaar is, dan is mislukking van zo'n PET-project te voorspellen. In een nog niet gepubliceerd onderzoek van Godel & Conlon (oktober 2009) over 'the economic benefits of privacy enhancing technologies' blijkt nochtans een groot misverstand. Uit de casestudies in

172 Borking & Mulder, 1999, p. 81-90; Borking & Mulder, 1999 (A).
173 Warmerdam, e.a., 1988, p. 26.
174 Warmerdam, e.a., 1988, p. 38-39.
175 Warmerdam, e.a., 1988, p. 40.
176 Koorn, e.a., 2004, p. 92.

verschillende Europese landen kan men vaststellen dat de stakeholders denken met PET te maken te hebben. Het gaat evenwel slechts om algemene PET-maatregelen (zie paragraaf 5.7.3) die vrijwel uitsluitend als middel voor informatiebeveiliging worden ingezet en niet voor gerichte privacybescherming.[177]

6.14. Samenvatting

Met gebruikmaking van de input uit de beantwoording van de eerste onderzoeksvraag (OV 1) (juridische specificaties), de derde onderzoeksvraag (OV 3) (lijst van privacybereigingen) en de vierde onderzoeksvraag (OV 4) (de PET-maatregelen) is in dit hoofdstuk de vijfde onderzoeksvraag (OV 5): *Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen?* beantwoord. In dit hoofdstuk zijn vier voorbeelden uitgewerkt, waarin de in hoofdstuk 5 besproken ontwerpbeginselen en technieken zijn toegepast. Deze vier voorbeelden tonen aan dat persoonsgegevens van individuen op een privacyveilige manier goed zijn te beschermen en geen afbreuk doen aan de functionaliteit van de informatiesystemen. Het concept 'privacy enhancing technologies' (PET) speelt als onderdeel van de informatiearchitectuur hierbij een belangrijke rol. Opname van PET als onderdeel van de informatiearchitectuur om persoonsgegevens en de informationele privacy van het individu te beschermen, betekent in het algemeen een fundamentele herziening van de architectuur vooral met betrekking tot de onderlinge relaties van de onderdelen en de relaties met de omgeving van het systeem.[178]

Vijftien jaar PET-onderzoek en ervaring met de bouw van informatiesystemen hebben geleerd dat integratie van PET in nieuw te ontwikkelen systemen een reële optie is. Vooral in het proces van het gegevens verzamelen is de potentiële effectiviteit van PET het grootst, omdat hier privacybescherming van de persoonsgegevens aan de bron plaatsvindt. De besproken metazoekmachine Ixquick geeft daar blijk van. Zoals uit het voorbeeld van het ziekenhuis Veldwijk-Meerkanten blijkt, kan ook tijdens de verwerking en opslag van gegevens PET uitstekende dienst bewijzen voor de bescherming van de persoonsgegevens. Complexere systemen als NTIS[179] en ViTTS met hun grote hoeveelheid medische gegevens zouden zonder PET niet kunnen bestaan. De privacy van de patiënt en zorgverlener kan in het door VWS voorgestelde elektronisch patiëntendossier met PET-maatregelen uitstekend worden beschermd. Bij toepassing van PET-maatregelen kan weerstand bij de stakeholders voorkomen worden. Ook bij de verspreiding van gegevens biedt PET goede mogelijkheden, vooral om ontoelaatbare koppelingen van gegevens te voorkomen.[180] 'Sticky policies' en 'data track'

177 Godel & Conlon, 2009, p. 122-199.
178 Klaver, e.a., 2002, p. 4.
179 Wijskamp, Ter Hart & Koorn, 2004.
180 Klaver, e.a., 2002, p. 6-11.

(zie paragrafen 5.11.2 en 5.11.3) kunnen de privacybescherming volledig maken. Het PISA-project toont aan dat ondanks de complexiteit om privacyrecht in systemen in te bouwen en te handhaven, PET-persoonsgegevens ook wanneer zij in klare (niet versleutelde) taal verwerkt worden, afdoende kunnen worden beschermd.

Voor bestaande systemen is de implementatie van PET in de praktijk een lastige opgave omdat, wanneer er wordt overgegaan naar de vastlegging van gegevens verdeeld over verschillende gegevensdomeinen, het gegevensmodel moet worden aangepast aan de domeinen en de nieuwe gegevensstromen. Dit betekent veelal een fundamentele systeemaanpassing en dat zal tijdrovend en kostbaar zijn. Anonimiseren kan bij bestaande systemen makkelijker worden toegepast omdat het als een 'accessoire' kan worden toegevoegd aan het informatiesysteem.[181] Het introduceren van geanonimiseerde gegevens in informatiesystemen heeft wel effect op de uit te voeren processen en het businessmodel van de organisatie.

Het gebruik van privacymanagementsystemen (PMS) die het naleven van privacyregels afdwingt, staat nog in de kinderschoenen. Het PISA-project is een geavanceerde toepassing daarvan en levert kennis op die gebruikt kan worden in een ambient intelligence (AMI) omgeving. De meest veelbelovende toepassingen (o.a. het obligation management system) hebben nog maar net de onderzoekslaboratoria verlaten, maar er zijn al commerciële producten van grote internationale ictbedrijven, waarmee een effectief privacy- en identiteitsmanagement in de organisatie kan worden gevoerd. Zorgvuldige begeleiding door teams bestaande uit, privacytoezichthouders, gespecialiseerde juristen en informatici, bij de wereldwijd en nationaal gezien geringe aantallen PET-projecten, hebben de klassieke oorzaken van mislukking van automatiseringsprojecten in deze projecten voorkomen.

Sommer signaleert nochtans een duidelijke aarzeling om PET toe te passen:

> "We still face major obstacles towards a deployment of such technology in the field at a large scale (…) the part of convincing business to design their business processes in a way such that data minimization can be implemented as envisioned in PRIME will even be harder than has been the technological part".[182]

Met de beantwoording van zesde onderzoeksvraag (OV 6) *Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?* zal in het volgende hoofdstuk op de door Sommer gesignaleerde aarzeling in worden gegaan.

---

181 Koorn, e.a., 2004, p. 67.
182 Sommer, 2008, p. 127.

7. Belemmeringen voor privacy enhancing technologies

"Uncertainty motivates individuals to seek information, as it is an uncomfortable state."
E.M. Rogers, Diffusion of Innovations, New York 2003, p. xx

In het vorige hoofdstuk heb ik aangetoond dat informationele privacytechnisch goed kan worden beschermd en dat 'privacy enhancing technologies' (PET) als onderdeel van de informatiearchitectuur een belangrijke rol hierbij kunnen spelen.[1] In dit hoofdstuk zal de beantwoording van de zesde onderzoeksvraag aan de orde komen:

Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren? (OV 6).

In paragraaf 7.1 wordt gerefereerd aan de motie Nicolaï, waarin de overheid wordt opgeroepen PET bij de eigen verwerking van persoonsgegevens in te zetten. Paragraaf 7.2 onderzoekt de toepassing van PET bij overheidsinstanties. Vastgesteld wordt dat de Nederlandse overheid in een vicieuze cirkel zit bij de toepassing van PET: zolang PET zich niet hebben bewezen, acht men het risico van mislukking te groot; zolang men het risico te groot vindt, worden PET niet toegepast en kunnen PET zich niet bewijzen. Paragraaf 7.3 stelt de vraag of het niet-inzetten van PET berust op het feit dat organisaties huiverig zouden kunnen zijn voor de mogelijke veranderingen in het arbeidsproces of in de structuur van het bedrijf die PET zouden kunnen veroorzaken. Is er sprake van een weerstand tegen verandering? In de paragrafen 7.4 tot en met 7.8 is naar de oorzaken gezocht die acceptatie van PET kunnen beïnvloeden. In paragraaf 7.4 wordt aan de hand van criteria getoetst of PET een innovatie is. In paragraaf 7.5 zal PET vanuit dit gezichtspunt worden benaderd. Rogers heeft voor innovaties, een adoptietheorie ('diffusion of innovation theory'(DOI)) ontwikkeld. In paragraaf 7.6 komen de stadia in het adoptieproces aan de orde en in paragraaf 7.7 de rol van organisaties bij adoptie. Paragraaf 7.8 behandelt de uit onderzoek gebleken adoptiefactoren voor innovatieve technologie, de interne aspecten van de adopterende organisatie

1 Horlings, e.a., 2003, p. 3.

en de externe omgevingsaspecten die van toepassing zijn op de adopterende organisatie. Dit leidt tot een tabel met een opsomming en waardering van de adoptiefactoren.

In paragraaf 7.9 wordt onderzocht of de maturiteit van een organisatie invloed heeft op het accepteren en toepassen van PET. Het toepassen van identiteits- en toegangsbeheer binnen een organisatie blijkt indicatief te zijn voor het adopteren van PET. In deze paragraaf wordt een aantal maturiteitsmodellen besproken en aan de hand van de reikwijdtematrix van Porter & Millar aangegeven in welke typen organisaties de potentiële vraag van PET kan optreden. In paragraaf 7.10 wordt nagegaan of voor informationele privacybescherming ook een maturiteitsmodel van toepassing is. Het vermijden van reputatieschade blijkt een 'driver' te zijn voor het nemen van PET-maatregelen. In paragraaf 7.11 wordt vastgesteld dat er drie Nolan Norton S-curven zijn te onderscheiden, die een indicatie kunnen geven wanneer een beslissing om in PET te investeren in een organisatie wordt genomen. In paragraaf 7.12 wordt als implementatiestrategie voor PET de multi-actoranalyse toegelicht. Gezien het feit dat de kosten voor innovaties een negatieve adoptiefactor zijn, wordt in paragraaf 7.13 betoogd dat de economische onderbouwing van de PET-investering van groot belang is voor het nemen van een positieve beslissing. Paragraaf 7.14 bespreekt de 'return on security investment' (ROSI) formule, die mutatis mutandis ook voor PET-investeringen toegepast kan worden. In paragraaf 6.5 is juridisch en technisch onderzocht of de metazoekmachine Ixquick privacyveilig is. Dat bleek het geval te zijn. In paragraaf 7.15 wordt aan de hand van de ROI-PI-formule nagegaan of de PET-investering voor Ixquick ook economisch verantwoord is. Paragraaf 7.16 bespreekt de netto contante waarde ('net present value') formule als verfijning van de ROI-PI-formule. Paragraaf 7.17 sluit het hoofdstuk af met de beantwoording van de zesde onderzoeksvraag.

7.1. De motie Nicolaï

In de motie Nicolaï e.a. van 18 november 1999 wordt de overheid zoals rijk, provincie, gemeente, zelfstandige bestuursorganen (ZBO's) en andere overheidsinstanties verzocht:

1. te bevorderen dat de ontwikkeling en het gebruik van PET krachtig ter hand wordt genomen;
2. te bevorderen dat de overheid als innovatieve aanbesteder ('launching customer') het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens.[2]

2 Tweede Kamerstukken 1999-2000, 25 892, nr. 31.

In 2004 zijn door Koorn e.a. echter binnen de Nederlandse overheid en semi-overheid slechts twaalf casussen gevonden waarin PET structureel in informatiesystemen is toegepast.[3] Cas & Hafskjold stellen: "So far PETs have not contributed as much as would be possible to the protection of privacy; partly because of a lack of availability of PETs, partly because of a lack of user friendliness."[4] Leisner & Cas wijzen er bovendien op dat: "PETs are insufficiently supported by current regulations; in particular it is not compulsory to provide the option of anonymous access to services or infrastructures."[5]

Sommer constateerde in 2008, dat ondanks het feit dat PET goed persoonsgegevens kunnen beschermen, er een duidelijke aarzeling binnen het bedrijfsleven is om PET toe te passen. Dit komt niet zozeer omdat de technologie niet zou werken, maar het is moeilijk organisaties ervan te overtuigen dat zij hun bedrijfsprocessen zo moeten inrichten dat zo min mogelijk persoonsgegevens worden opgeslagen.[6]

De hierboven vermelde constateringen roepen de vraag op wat de oorzaak is dat organisaties PET op zulke kleine schaal toepassen en waarom de verantwoordelijken (in zin van 95/46/EG) zo terughoudend zijn PET toe te passen om persoonsgegevens te beschermen. Aan gebrek aan aandacht die besteed wordt aan PET zal het niet liggen.[7] Volgens Bos echter zijn de voordelen die PET te bieden hebben, kennelijk niet voldoende om het gebruik ervan als privacybeschermende maatregel ter hand te nemen.[8] Hierdoor benutten organisaties het potentieel van PET niet.[9] Een onderzoek dat het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in 2003 heeft laten uitvoeren werpt enig licht op de redenen om PET niet toe te passen.[10]

7.2. Onderzoek naar de toepassing van PET bij overheidsinstanties

Als gevolg van de motie Nicolaï e.a.[11] staat in de nota 'Contract met de Toekomst' van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) (directie Informatiebeleid Openbare Sector) van mei 2000 in paragraaf 5.3: "Het kabinet zal nagaan op welke wijze invulling kan worden gegeven aan een recht op regie over eigen persoonsgegevens. Bekeken zal worden wat de gevolgen

3 Koorn, e.a., 2004, p. 92.
4 Cas & Hafskjold, 2006, p. 41.
5 Leisner & Cas, 2006, p. 50.
6 Sommer, 2008, p. 127.
7 De Leeuw, e.a., 2008, p. 51-102.
8 Bos, 2006, p. 2.
9 De Rooij, 2004, p. 22.
10 Horlings, e.a., 2003.
11 Bij de behandeling in de Tweede Kamer is kamerbreed de motie Nicolaï (Tweede Kamerstukken 1999-2000, 25 892, nr. 31) aangenomen waarin de regering wordt opgeroepen in haar eigen systemen PET voor de verwerking van persoonsgegevens toe te passen.

zijn voor de bedrijfsvoering van de overheid. (...) Het kabinet zal in kaart brengen wat de mogelijkheden zijn om de privacy te garanderen met behulp van PET."[12]

Dit heeft vervolgens in 2003 geleid tot een onderzoek dat RAND Europe heeft uitgevoerd in opdracht van BZK. Daarbij is onderzocht of het mogelijk is proefprojecten op te zetten om de overheid bij de verwerking van persoonsgegevens PET te laten toepassen. In het kader van dit onderzoek zijn bij zeventien overheidsinstanties[13] en een commerciële organisatie[14] interviews afgenomen.

Van de zeventien overheidsinstanties bleven er zeven over, die genoeg aanknopingspunten hadden om een succesvol pilotproject op te starten. In deze groep van zeven[15] bleken er plannen te zijn om PET in de 'frontoffice' of de 'backoffice' te introduceren. Slechts enkele instanties beheren echter een scherp afgebakend proces, waarin de behandeling van privacygevoelige gegevens met PET beschermd zouden kunnen worden.[16] Dat was onder meer het geval bij de IB-Groep met een basisadministratie en een eigen domein voor studenten en Prismant met diverse discrete processen, zoals het routeringsinstituut en plannen ten aanzien van het gebruik van biometrie in de methadonverstrekking.

Toen BZK echter bij de zeven geselecteerde overheidsorganisaties aanklopte om de proefprojecten op te zetten, werd door de geïnterviewde instanties aangegeven dat zij het nog niet opportuun achtten om PET in te voeren.[17] XS4ALL, de enige commerciële organisatie in de groep van zeven, dacht daar anders over. Bij XS4ALL was men juist erg geïnteresseerd om een beperkte houdbaarheid van elektronische data in hun gegevensbestanden in te bouwen, zodat persoonsgegevens minder zouden kunnen worden verspreid via koppelingen met databanken van instanties.[18] Omdat XS4ALL echter geen overheidsinstantie is en geen werkzaamheden direct voor overheden uitvoert, werd het bedrijf van deelname aan het proefproject van BZK uitgesloten.

In het onderzoek constateerde RAND Europe dat de overheidsinstanties in de ontwikkeling van en het denken over PET de nadruk sterk leggen op de interactie via internet tussen burgers en bedrijfsleven en tussen overheid en burgers. De meeste aandacht besteden zij daarbij aan identificatie en autorisatie van de gebruikers terwijl processen in de 'backoffice' van de overheid nauwelijks aandacht krijgen. Bovendien wordt er bij de geïnterviewde instanties voornamelijk gewerkt aan de ontwikkeling van technologieën die specifieke functionaliteiten kunnen vervullen (bijvoorbeeld:

12 www.e-overheid.nl/achtergrond/geschiedenis/contracttoekomst/contracttoekomst.xml.
13 Informatie Beheer Groep (IBG), Belastingdienst, Douane, Prismant, Centraal Bureau Rijvaardigheidsbewijzen, Bureau Informatisering Amsterdam (BIA), ICTU, Nederlandse Mededingingssautoriteit (NMa), Basisadministratie Persoonsgegevens en reisdocumenten, Meld Misdaad Anoniem, Sociale Verzekeringsbank (SVB), Politie Kennemerland, Coöperatie Informatiemanagement Politie, Vereniging van Kamers van Koophandel, Leids Universitair Medisch Centrum (LUMC), Senter, Immigratie-en Naturalisatiedienst (IND).
14 De internetprovider XS4ALL.
15 BIA, IBG, IND, Prismant, LUMC, SVB en NMa.
16 Horlings, e.a., 2003, p. 37.
17 Horlings, e.a., 2003, p. 39.
18 Horlings, e.a., 2003, p. 36.

'anonymizers') en veel minder aan de ontwikkeling van complete ict-architecturen, waarin een of meerdere PET-functionaliteiten geïntegreerd zijn.[19] RAND Europe geeft in de analyse van de interviews aan dat de ondervraagde organisaties een aantal opvallende parallellen vertonen qua onderliggende argumenten waarom een geavanceerde vorm van PET op korte termijn nog niet kan worden ingevoerd. Daarbij zijn vijf argumenten te onderscheiden:

1. De bestaande methoden van privacybescherming voldoen.
2. Privacybescherming is niet nodig.
3. Experimenten met PET zijn een gevaar voor de betrouwbaarheid, kwaliteit van de dienstverlening en het imago van de instantie.
4. PET zijn nog niet volwassen.
5. Er is geen tijd, geld of mankracht om de invoering van PET te realiseren.[20]

De onderzoekers constateerden dat de Nederlandse overheid op het moment van het onderzoek (2003) in een vicieuze cirkel verkeerde bij de toepassing van PET: zolang PET zich niet hebben bewezen, acht men het risico van mislukking te groot; zolang men het risico te groot vindt, worden PET niet toegepast en kunnen PET zich niet bewijzen.[21] Uit de ervaringen van de Registratiekamer naar de toepassing van PET, is echter gebleken, dat wanneer PET goed wordt toegepast, deze technologieën de betrouwbaarheid en het imago van de betrokken organisaties vergroten, zoals bijvoorbeeld het routeringsinstituut RINIS.[22] In de conclusies van het rapport[23] wordt een aantal redenen gegeven voor het geringe gebruik van PET. Die wijzen naar een dieperliggend probleem bij het gebruik van PET.

1. Zo geven verschillende overheidsinstanties aan dat zij het te risicovol vinden om te experimenteren met PET zolang niet is bewezen dat PET afdoende functioneren. De Belastingdienst bevestigt op bladzijde 21 van het RAND Europe rapport dat zij er niet op uit is om als technologische koploper gezien te worden. Zij straalt liever naar de burgers uit dat haar systemen betrouwbaar zijn en goed functioneren.
2. Andere ondervraagden voeren aan dat de beleidsmakers (en beslissers) gebrek aan kennis hebben over de voor- en nadelen van PET.
3. Bovendien menen zij dat PET nog niet volwassen (dus geen 'mainstream' toepassing) zijn, hoewel er niet aan wordt getwijfeld dat er in hun bedrijfsvoering PET-oplossingen mogelijk zijn.
4. Voorts hebben de ondervraagden behoefte aan standaardisatie en duidelijke (wettelijke) criteria voor technologische privacybescherming.
5. De ondervraagden hebben geen behoefte aan privacybescherming ondanks het groeiend aantal koppelingen tussen bestanden en de sterk toegenomen uitwisseling van persoonsgegevens. De ondervraagden (CBR, VVK en

19 Horlings, e.a., 2003, p. 55-56.
20 Horlings, e.a., 2003, p. 59-63.
21 Horlings, e.a., 2003, p. 64.
22 Koorn, e.a., 2004, p. 15 (LCMR), p. 18 (RINIS), p. 29 (NTIS), p. 39 (LADIS).
23 Horlings, e.a., 2003, p. 63-64.

NMa) werken (deels) met een openbaar register en zien ondanks de risico's geen noodzaak PET te gebruiken om persoonsgegevens te beschermen.
6. Zelfs al zou PET goed functioneren, dan houden instanties zoals CBR, Belastingdienst en IND liever vast aan de bestaande methoden met het adagium: 'if it ain't broke, don't fix it'.
7. De perceptie van verschillende organisaties is dat intern alle gegevens beschikbaar moeten zijn en dit moeilijker zal worden met PET. Dit wordt bevestigd in het in 2007 uitgebrachte rapport 'Eerste fase evaluatie – Wet bescherming persoonsgegevens'. De toepassing van PET stuit op praktische bezwaren bij de verantwoordelijken.[24]
8. De hoge uitvoeringskosten en de relatief grote inspanningen die nodig zijn om veranderingen in een informatiehuishouding te implementeren wegen zwaar.
9. Bij de verantwoordelijken is onduidelijk wat als passend beveiligingsniveau ex artikel 13 Wbp moet worden beschouwd ondanks de uitleg hiervan die het College bescherming persoonsgegevens in 2001 heeft gepubliceerd. Deze onduidelijkheid blijkt eveneens de invoering van PET-maatregelen af te remmen.[25]

7.3. Weerstand tegen verandering?

Hoe komt het dat bedrijven de ene technologische vernieuwing veel sneller omarmen dan de andere? Het internet en de mobiele telefoon bijvoorbeeld zijn in relatief korte tijd een onmisbaar middel geworden in de bedrijfsvoering. PET daarentegen, is nog nauwelijks in het bedrijfsleven geaccepteerd, terwijl empirisch is aangetoond dat het een effectieve methode is om persoonsgegevens te beschermen. Zijn er mogelijk dieperliggende redenen om PET al dan niet toe te passen naast de redenen die uit het onderzoek van RAND Europe naar voren komen? Als dat zo is, hoe beïnvloeden deze redenen dan de besluitvorming over PET? Een van de dieperliggende oorzaken zou kunnen zijn dat organisaties huiverig zijn voor de mogelijke veranderingen in het arbeidsproces of in de structuur van het bedrijf die PET zouden kunnen veroorzaken.[26] Wellicht ligt de oorzaak in het individu en bestaat er bij de beslissers zelf binnen organisaties weerstand tegen de verandering, die toepassing van (hen onbekende) PET met zich mee brengen. Te denken valt aan verlies van macht of invloed of het duidelijk worden van gebrek aan specifieke kennis. Warmerdam e.a. merken op dat: "(...) automatiseringsprocessen geen geïsoleerd verlopende technische veranderingsprocessen zijn, maar dat ze zich voltrekken in een context van machts- en

24 Zwenne, e.a., 2007, p. 144 en 155.
25 Zwenne, e.a., 2007, p. 144, en 155.
26 Warmerdam, e.a., 1988, p. 66-74.

beïnvloedings- processen waarin diverse partijen onderscheiden belangen trachten te realiseren."[27]

Psychologen hebben de sociaalpsychologische processen die in individuen plaatsvinden bij de weerstand tegen veranderingen onderzocht. Zo stelden Katz & Lazarsfeld al in 1955 vast dat bij verkiezingscampagnes in de Verenigde Staten (waarvan de uitslag kan leiden tot veranderingen) mensen zich selectief blootstellen aan informatie. Dit verschijnsel treedt ook op wanneer de zender en de ontvanger van informatie in nauw contact met elkaar staan "as every college professor knows through his classroom experience with students!"[28] Het is evenwel zeer moeilijk te bewijzen dat individuen opzettelijk zich onttrekken aan argumenten waarin zij niet geïnteresseerd zijn of die hun eigen waardepatroon verstoren. Bij het analyseren van de Nixon-Kennedy televisiedebatten in 1960 stelden onderzoekers vast dat er "surprisingly little avoidance of opposing arguments" optrad.[29] Ook is onderzocht of mensen zich verzetten tegen verandering vanwege externe stimuli die bij hen angst teweegbrengen. Zij gaan dan bepaalde informatie onderdrukken, of zoeken onbewust een cognitieve balans, want er is "the necessity of the organism to retain a state of consonance, cognitive balance, congruity or consistency."[30] Doordat mensen zoeken naar een cognitieve balans, reageren zij defensief wanneer de informatie dissonant is met bestaande interne waarden. Die defensieve reacties resulteren in ontkenning of in een versterking van de aangevallen waarde of in een 'opsplitsing' van het storende element.[31] Secord & Backman geven als voorbeeld uit de begin zestiger jaren van de vorige eeuw: "Hydrogen bomb testing is positively valued for many people as necessary for defense, but poisoning of the atmosphere is negatively valued. For a person with these values, there is imbalance in the belief in bomb testing. This can be resolved by differentiating the attitude object into two parts: testing 'dirty' bombs that poison the atmosphere and 'clean' bombs that do not."[32]

Een ander voorbeeld van dit psychologische mechanisme is de opvatting dat het roken van 'gewone' sigaretten kanker veroorzaakt en filtersigaretten niet. Voor deze sociaalpsychologische aanpak is wat betreft het niet toepassen van PET geen empirische steun gevonden. De reden hiervoor ligt in het feit dat PET-toepassingen niet in informatiesystemen worden geïmplementeerd vanwege de beleving van een enkel individu, maar pas nadat er een haalbaarheidsonderzoek heeft plaatsgevonden waarbij verschillende partners betrokken zijn. Individuele sociaalpsychologische processen tegen verandering spelen daarbij geen (zichtbare) rol. Een vruchtbaardere benadering blijkt de implementatie van PET

27 Warmerdam, e.a., 1988, p. 3.
28 Secord & Backman, 1964, p. 177.
29 Secord & Backman, 1964, p. 176.
30 Secord & Backman, p. 182.
31 Secord & Backman, p. 182-186: "cognitive balacing as a defensive process in a resistance to attitude change (...) states of imbalance are regarded as disturbing and are resolved by 1. Denial (...), 2. Bolstering (...) and 3. Differentiation (...) it restores balance by splitting an element into two parts (...)".
32 Secord & Backman, p. 183-184.

vanuit de organisatie te benaderen. De centrale vraag is dan hoe en onder welke voorwaarden organisaties een nieuwe toepassing zoals PET in hun bedrijfsprocessen zullen adopteren. Daarmee hangt samen dat moet worden nagegaan wat het effect van privacybescherming is op de bedrijfsprocessen.

7.4. PET, een innovatie

Nieuwe ideeën worden niet zomaar aanvaard en raken niet zomaar verspreid in de samenleving, zelfs als ze aantoonbare voordelen hebben. Dit geldt met name bij innovaties. Volgens Rogers is innovatie:"an idea, practice, or object that is perceived as new by an individual or other unit of adoption."[33] Ribbers stelt dat of iets als een innovatie wordt gezien relatief is.[34] Dat wil zeggen dat iets als een innovatie kan worden beschouwd wanneer het in een bepaalde omgeving of door bepaalde personen als nieuw wordt ervaren. Bos schrijft dat vele zaken een innovatie kunnen zijn, zoals een idee, een methode, een technologie of een product. Bij de bestudering van een bepaalde innovatie moet er rekening mee gehouden worden dat elke innovatie haar eigen kenmerken bezit, die een rol spelen bij de toepassing daarvan.[35] De Organization for Economic Co-operation and Development (OECD) omschrijft technologische innovatie als: "A technological new product or process that includes a significant improvement and has been actually put into use. The technological new product or process consists of a variety of scientific, technical, organizational, financial and commercial aspects."[36] PET vallen binnen deze definitie. Zij kunnen als een innovatie worden beschouwd vanwege:

1. hun relatief korte (1995) bestaan;
2. de voortgang die zij boeken op het gebied van privacybescherming;
3. de nieuwe perspectieven die zij bieden voor de bescherming van persoonsgegevens.

7.5. Verspreiding en toepassing van technologische innovaties

Nu PET als innovatie kan worden gekwalificeerd, is de vraag hoe technologische innovaties in het algemeen en PET in het bijzonder zich binnen een bepaalde omgeving verspreiden en hoe deze innovaties vervolgens worden aanvaard en toegepast door die omgeving.[37] Rogers definieert verspreiding ('diffusion') als: "the process by which an innovation is communicated through certain channels

33 Rogers, 2003, p. 12.
34 Ribbers, 2007, p. 11.
35 Bos, 2006, p. 9.
36 Organization for Economic Co-operation and Development (OECD), Oslo Manual, Guidelines for Collecting and Interpreting Innovation Data, 3rd edition 2005, beschikbaar op http://www.oecd.org/.
37 Fairchild & Ribbers, 2008, p. 82.

over time among the members of a social system".[38] Naast de innovatie zijn dan ook van belang:
1. de communicatiekanalen (de manier waarop een bericht van het ene naar het andere individu wordt overgebracht);
2. de tijdsduur die gemoeid is met de toepassing;
3. het sociale systeem binnen een bepaalde samenleving of tak van industrie waarbinnen de innovatie wordt verspreid.

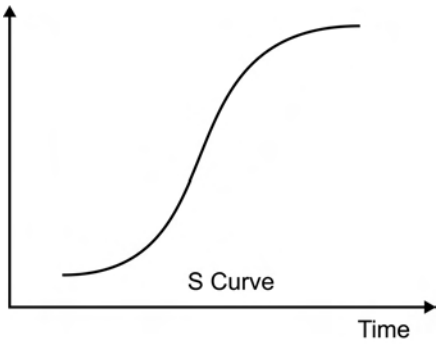
Zoals in hoofdstuk 1 is aangegeven, is adoptie het ontwikkelingsproces van een persoon of organisatie vanaf een eerste kennismaking met de innovatie tot het uiteindelijke gebruik daarvan: "Adoption refers to the stage in which a technology is selected for use by an individual or an organization."[39] Bij de verspreiding van een innovatie is bepalend hoe de direct betrokkenen binnen de omgeving, waarin de innovatie wordt geïntroduceerd, de innovatie beoordelen. Rogers noemt vijf attributen die de mate van adoptie bepalen:
1. het relatieve voordeel;
2. de compatibiliteit;
3. de complexiteit;
4. de testbaarheid;
5. de zichtbaarheid.[40]

Om te voorspellen of de samenleving een innovatie zoals PET zal aanvaarden en zich zal gaan verspreiden moet gekeken worden naar de snelheid waarmee en de vorm en mate waarin een specifieke innovatie wordt toegepast.[41] Bovendien moet geanalyseerd worden welke factoren ervoor zorgen dat een organisatie geschikt is om een specifieke innovatie toe te passen. Op basis van het resultaat van beide onderzoeken kan worden vastgesteld welke factoren bepalend zijn voor de toepassing van een innovatie in een specifieke omgeving.[42] Volgens Rogers kent het proces waarmee innovaties worden verspreid en toepast een relatief voorspelbaar en constant ontwikkelingspatroon.[43] Hij beschrijft het toepassingsproces als een S-vormige curve. (figuur 7.1). Op de X-as staat de tijdsduur en op Y-as het aantal 'adopters', degenen die de innovatie toepassen.[44]

---

38 Rogers, 2003, p. 35.
39 Carr, 1996, p. 1.
40 Rogers, 2003, p. 36.
41 Ribbers, 2007, p. 13.
42 Bos, 2006, p. 10.
43 Borking & Vriethoff, 1995, p. 14. De S-curve is ook toepasbaar op de groei van organisaties, zoals de Registratiekamer (nu CBP).
44 Rogers, 2003, p. 262 voor een voorbeeld van de S-curve betreffende de adoptie van mobiele telefoons in Finland (1981-2002) of p. 273 voor een voorbeeld van de S-curve over de periode 1927-1943 van adopters van hybride maïszaad.

Figuur 7.1: Mate van adoptie volgens Rogers, 2003, p. 11.



De S-vormige curve geeft weer de aanvankelijk beperkte belangstelling van de doelgroep voor de innovatie, gevolgd door een toenemende belangstelling, resulterend in een intensieve toepassing die daarna weer afvlakt. Hoewel dit concept geldt voor alle adoptievormen, kan de gradiënt (hellingshoek) van de curve per innovatie verschillen.[45] Hoe steiler, hoe sneller het grote publiek met de innovatie in aanraking komt of er meer gebruik van maakt. Andere economen ondersteunen de theorie van Rogers. Zij stellen dat er ook sprake is van deze curve wanneer een innovatieve technologie gedeeltelijk wordt toegepast als middenweg tussen aanvaarding en niet-aanvaarding. Gedeeltelijke toepassing van een innovatie kan de keuze tussen toepassen of niet-toepassen makkelijker maken.[46] Gezien de beperkte verspreiding van PET kan vooralsnog geconcludeerd worden dat, óf PET aan het begin van de S-curve staat, óf dat de S-curve zeer vlak verloopt en dat PET dus zeer langzaam ingeburgerd raakt.

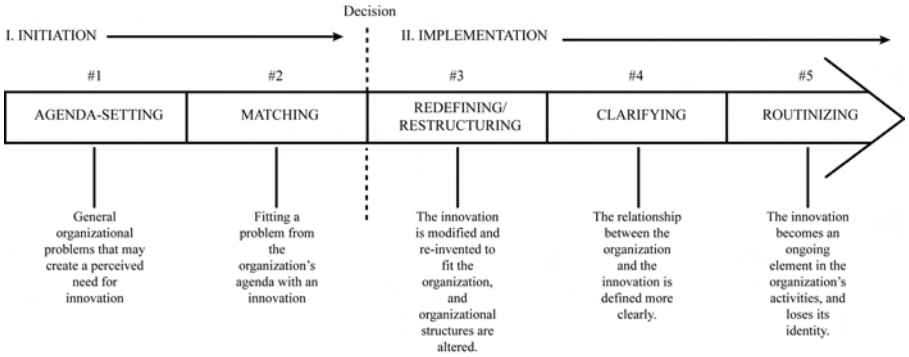
7.6. Stadia in het adoptieproces

Sinds de industriële revolutie volgden innovaties het traditionele model. Dit model wordt ook wel het 'top-down'-model genoemd omdat het management van bovenaf de innovatieve technologie in de organisatie introduceerde. De daarmee samenhangende besluiten en strategieën zorgden ervoor dat de organisatie de innovatie verder adopteerde en intern verspreidde. Een succesvolle adoptie was sterk afhankelijk van de mate van de ondersteuning en de deskundigheid van het management. Het kwam bijna niet voor dat de innovatie 'bottum-up' werd geïntroduceerd, dat wil zeggen doordat individuen de innovatie via laterale

45 Ribbers, 2007, p. 13.
46 Bayer & Melone, 1989, p. 161-166.

communicatie stimuleerden. Deze zogeheten 'grass roots'-adoptiecyclus is pas mogelijk geworden door de pc, het internet en het World Wide Web.[47] Om inzicht te krijgen in dit toepassingsproces is een aantal gedragsmodellen ontwikkeld die verenigd zijn in de 'Unified Theory of Acceptance and Use of Technology' (UTAUT).[48] Personen worden in deze modellen niet als volledig rationeel beschouwd, omdat er ook subjectieve gronden meespelen wanneer zij besluiten de innovatie toe te passen.[49] Doordat organisaties op een andere manier besluiten nemen dan individuen, verloopt het adoptieproces over het algemeen bij organisaties gestructureerder. Organisaties lijken over het algemeen rationeler te werk te gaan en beschikken doorgaans over betere informatie dan individuele personen.[50] Of de innovatie ook werkelijk wordt gebruikt, hangt uiteindelijk af van de individuele werknemer.[51] Voordat organisaties een innovatie kunnen toepassen, moeten zij volgens Rogers een vijftal fasen doorlopen. Deze fasen zijn agendering, passend maken, herstructurering, afbakening en trajectbepaling. De eerste twee stappen (agendering en passend maken) vormen de initiële fase, die voorafgaat aan het formele besluit en uiteindelijk leidt tot het besluit de innovatie al dan niet toe te passen. De laatste drie fasen (herstructurering, afbakening en trajectbepaling) vormen tezamen de implementatiefase waarbinnen alle activiteiten plaatsvinden die leiden tot de uiteindelijke keuze om gebruik te maken van de innovatie (zie figuur 7.2). Als de laatste fase (trajectbepaling) ingaat is de innovatie strikt genomen al geen innovatie meer.

Figuur 7.2: Stadia in het adoptieproces, Rogers, 2003, p. 420-435.



47 Carr, 1996, p. 2.
48 Venkatesh, e.a., 2003, p. 425-478.
49 Bos, 2006, p. 11.
50 Bos, 2006, p. 11.
51 Ribbers, 2007, p. 13.

Hoewel er geen alom geldende theorie bestaat over de toepassing van innovaties door organisaties, wordt de theorie van Rogers als zeer gezaghebbend beschouwd.[52] Carr wijst er evenwel op dat de adoptie van interactieve communicatie tussen gebruikers van internet en het Wereld Wijde Web als innovatie op drie belangrijke punten afwijkt van de voorafgaande innovaties:

1. A critical mass of adopters is needed to convince the "mainstream" teachers (professionals)[53] of the technology's efficacy.
2. Regular and frequent use is necessary to ensure success of the diffusion effort.
3. Internet technology is a tool that can be applied in different ways and for different purposes and is part of a dynamic process that may involve change, modification and reinvention by individual adopters."[54]

De innovatieve en de pragmatische toepassing van internettechnologieën, zoals e-mail, 'chat rooms' en het gebruik van zoekmachines, begon met de 'grass root' enthousiastelingen ('innovators' en 'early adopters') die een nieuwe cultuur schiepen waar anderen zich bij aansloten om tot de incrowd te behoren. Individuen die graag risico's nemen of een positieve grondhouding ten aanzien van innovaties hebben, zullen vaak de early adopters zijn. Internettoepassingen kunnen echter door de gevestigde orde binnen een cultuur of gemeenschap als een bedreigende concurrent worden gezien. Een voorbeeld hiervan is geschillenoplossing via internet binnen de juridische wereld.[55] Rogers wijst erop dat een innovatie veel sneller kan ingeburgerd raken wanneer zij via internet wordt verspreid. De factor tijdsduur voor de innovatie wordt door internet verkort.[56]

7.7. De invloed van organisaties op technologische innovaties

Zoals eerder opgemerkt onderscheidt Rogers[57] in zijn 'perceived attributes theory' verschillende variabelen aan de hand waarvan innovaties worden beoordeeld. Deze zijn:

1. Het belang de testbaarheid ('trialability'). De vraag hierbij is: kan de innovatie op beperkte schaal worden uitgeprobeerd?
2. Een tweede criterium is de zichtbaarheid ('observability') van de innovatie: kunnen de resultaten worden waargenomen?
3. Ten derde levert de innovatie een voordeel ('relative advantage') ten opzichte van andere innovaties of over de bestaande situatie op.

---

52 Fairchild & Ribbers, 2008, p. 82.
53 Het woord 'professionals' is door mij toegevoegd. Carr is onderzoeker/docent verbonden aan de Muir S. Fairchild Research Information Center van de Militaire Academie van de US Air Force. Zijn paper behandelde het gebruik van internettechnologie in een onderwijsomgeving.
54 Carr, 1996, p. 2.
55 Borking, 2008, p. 149-161.
56 Rogers, 2003, p. 215-216.
57 Rogers, 2003, p. 36.

4. Het vierde attribuut betreft de mate van complexiteit ('complexity'): is het niet te ingewikkeld om de innovatie te gebruiken?
5. In de vijfde plaats komt in de toetsing aan de orde de compatibiliteit ('compatibility'): past de innovatie in de omstandigheden waarin zij zal worden toegepast of is zij daar compatibel mee?

Perceptie van deze factoren door de persoon of organisatie die de innovatie eventueel zal gaan toepassen is bepalend en niet zozeer hoe deze factoren objectief in werkelijkheid scoren. Uit onderzoek is gebleken dat individuen die graag risico nemen of een voorliefde voor innovatie hebben sneller een innovatie gaan uitproberen dan voorzichtige mensen. Daarbij geldt volgens Rogers dat: "An individual is more likely to adopt an innovation if more of the other individuals in his or her personal network have adopted previously."[58]

In het communicatieproces rond innovatie speelt de geloofwaardigheid van de 'communicator' een belangrijke rol spelen. Secord & Backman rapporteren dat experimenten van Asch al in 1952 aantoonden dat: "the meaning of the communication is partially determined by the reputation of the person who makes the statement."[59]

Rogers bevestigt dat: "Opinion leaders are more innovative than their followers."[60] Bij internetinnovaties is mede bepalend of de innovatie vanuit een ontwerpersperspectief ('developer-based') wordt gezien of vanuit de gebruiker van de innovatie ('adopter-based'). Bij de developer-based visie is technologische superioriteit van de innovatie ten opzichte van de bestaande situatie bepalend, terwijl het bij de adopter-based benadering gaat om de gebruiker van de innovatieve technologie en het voordeel dat het biedt om de gewenste verandering tot stand te brengen. Carr schrijft daarover: "Human control over the innovation is a key issue, and it is considered essential to understand the social context in which it will be used and the function it will serve."[61] Rogers[62] wijst in zijn 'innovation decision process theory' erop dat er vijf fasen zijn die een potentiële 'adopter' van een innovatief technologisch proces doorloopt:

1. Eerst moet hij kennis verwerven over de innovatie ('knowledge').
2. Dan moet hij overtuigd raken van het nut van de innovatie ('persuasion').
3. Vervolgens moet hij de beslissing nemen de innovatie toe te passen (adopteren) ('decision').
4. Daarna moet de gebruiker of de adopter innovatie implementeren ('implementation').
5. Ten slotte moet hij de juistheid van de beslissing herbevestigen of verwerpen ('confirmation').

---

58 Rogers, 2003, p. 359
59 Secord & Backman, 1964, p. 130.
60 Rogers, 2003, p. 318.
61 Carr, 1996, p. 3.
62 Rogers, 2003, p. 168-218.

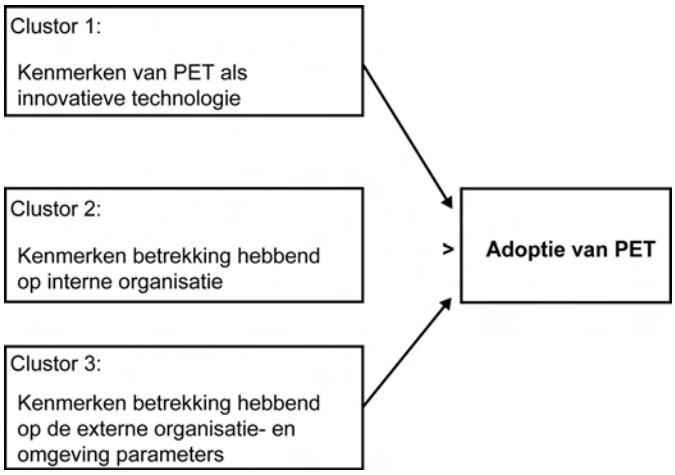
Voor organisaties, die openstaan voor innovaties onderscheiden Fairchild & Ribbers als bepalende factoren voor adoptie:

1. De algemene houding van het topmanagement ten opzichte van verandering die door de innovatie kan plaatsvinden (openstaand of afwijzend).
2. Is er sprake van centralisatie van macht en management binnen de organisatie?
3. Is complexiteit beheersbaar doordat er voldoende kennis en expertise in de organisatie aanwezig is?
4. Bestaat er de interne cohesie van de medewerkers in de organisatie?
5. Is er voldoende elasticiteit in mensen, middelen en omvang van de organisatie?
6. Hoe bureaucratisch is de organisatie?
7. Hoe open is de organisatie in haar contacten met andere organisaties?[63]

Rogers' theorie over hoe innovaties zich verspreiden binnen de samenleving (bekend als de 'Diffusion of Innovation' (DOI)-theorie) heeft algemene erkenning gekregen. De variabelen zijn in meerdere studies getest en relevant bevonden. De onderzoekers analyseerden en beoordeelden in verschillende studies ruim honderd variabelen.[64] Ook hebben zij empirisch onderzocht wat de meest voorspelbare factoren waren waardoor organisaties informatietechnologische innovaties invoeren.[65] Uit de bevindingen van Jeyarai, Fichman en Rogers kan geconcludeerd worden dat er voor PET drie clusters van factoren voor adoptie kunnen worden onderscheiden.[66] De eerste cluster betreft de kenmerken van PET als innovatieve technologie en bevat de variabelen die betrekking hebben op de technische innovatie op zich. De tweede cluster regardeert de kenmerken die betrekking hebben op interne organisatie en bevat de variabelen die bepalend zijn op de omgeving waarbinnen de technologische innovatie verspreid wordt. Het gaat om de interne kenmerken van de organisatie die de innovatie invoert, hetgeen inhoudt dat er inzicht dient te zijn in de organisatie- of bedrijfskenmerken en de factoren die een organisatie in staat stellen de innovatie te implementeren.[67] De derde cluster bevat de factoren die betrekking hebben op de externe organisatie- en omgevingsparameters die van toepassing zijn op innovaties: dit zijn factoren die bepalend zijn voor de organisatie die de innovatie toepast en de omgeving waarbinnen dit gebeurt. Het betreft daarom de kenmerken van de organisatie of het bedrijf enerzijds en de kenmerken van de omgeving en de bedrijfstak anderzijds.[68] Het conceptuele model ziet er als volgt uit:

63 Fairchild & Ribbers, 2008, p. 82.
64 Fichman & Cincinnati, 2000; Jeyaraj, Rottman & Lacity, 2006, p. 1-23.
65 Bos, 2006, p. 15.
66 Bos, 2006, p. 14.
67 Rogers, 2003, p. 225-226.
68 Ribbers, 2007, p. 13.

Figuur 7.3: Adoptiemodel van PET als innovatie, Bos, 2006, p. 59.



7.8. Adoptiefactoren

Bos[69] (in Nederland) en Hosein[70] (in het Verenigd Koninkrijk) hebben kwalitatief onderzoek gedaan om het adoptiemodel te toetsen. Hun onderzoek bestond uit casestudies, 'workshops' en interviews[71] met experts uit de centrale overheid en bedrijfsleven. Verdeeld over de hierboven vermelde drie clusters werden vijftien adoptiefactoren vastgesteld.

7.8.1. Het eerste cluster: PET zelf

a. Relatief voordeel

In de 'workshops' in het Verenigd Koninkrijk met experts uit het bedrijfsleven was opvallend weinig discussie over de specifieke kenmerken van de mogelijke PET-oplossingen. De experts betwijfelden of het wel een goede aanpak was om te zoeken naar technologische oplossingen voor het oplossen van het privacyvraagstuk, want organisaties geven al erg weinig geld aan privacymanagement uit, laat staan aan technologische oplossingen. Hosein concludeerde uit de discussies op dit punt dat:

---

69 Bos, 2006, p. 33, 38-60: Drie casestudies: Digitaal Klantendossier, Elektronisch patiëntendossier, Algemene Periodieke Keuring van de RDW en interviews met vijf experts.

70 Ribbers, 2007, p. 29-33. Hosein van de London School of Economics heeft in het kader van het PRIME onderzoek in Londen in mei 2007 een workshop gehouden met participanten uit de overheid en het bedrijfsleven om de resultaten van Bos te toetsen aan de in het Verenigd Koninkrijk levende opvattingen.

71 Yin, 2003: Casestudies zijn niet minder betrouwbaar dan een experimenten die harde kwantitatieve resultaten leveren.

> "This certainly validates the view that relative benefit and advantages of a technological solution is an issue, though the level of doubt is not promising."[72]

b. Compatibiliteit

Met compatibiliteit wordt enerzijds bedoeld de mate waarin PET aansluit bij andere, oudere, methoden die privacy beschermen en anderzijds de mate waarin PET aansluit bij andere concepten binnen de organisatie, zoals de cultuur. In Nederland wordt de compatibiliteit van PET matig geacht, want als technische beschermingsmaatregel verschillen PET aanzienlijk van bijvoorbeeld de gangbare procedurele maatregelen. Op grond van de interviews in Nederland concludeert Bos dat de gebrekkige compatibiliteit van PET de adoptie van PET negatief beïnvloedt.[73]

c. Complexiteit van bedrijfsprocessen

Privacyverhogende technologieën moeten doorgaans worden aangepast aan een specifieke organisatie of een bepaald proces. Hoe complexer deze technologieën, des te moeilijker deze zijn te implementeren. Dit heeft een negatieve invloed op de adoptie van PET.[74]

d. Kosten

Organisaties ervaren PET als een kostbare vorm van innovatie (met onduidelijke voordelen).[75] Veel hangt echter af van het moment waarop deze technologieën binnen een organisatie worden geïntroduceerd. Als dit geschiedt bij de ontwikkeling van een nieuw systeem dan zijn de kosten over het algemeen aanvaardbaar. De extra kosten bedragen dan tussen de 1 en 10% van de totale projectkosten.[76] In principe is het inbouwen van PET in een nieuw informatiesysteem ook de enige realistische optie. PET zijn te complex om achteraf op bestaande systemen toe te passen.[77] De kosten blijken dan veelal hoger uit te vallen dan die van traditionele maatregelen. De kosten zijn een negatieve factor voor de adoptie van PET.

e. Integratie van privacyverhogende technologieën

Een belangrijk kenmerk van privacyverhogende technologieën is dat deze al bij de implementatie moeten worden geïntegreerd in informatiesystemen. Daarvoor is een gecombineerde juridische en informatietechnologische expertise vereist. Die

---

72 Ribbers, 2007, p. 31.
73 Bos, 2006, p. 62.
74 Fairchild & Ribbers, 2008, p. 84.
75 Bos, 2006, p. 57.
76 Koorn, e.a., 2004, p. 50.
77 Koorn, e.a., 2004, p. 69.

expertise is schaars.[78] Uit het eerder genoemde onderzoek van Hosein in het Verenigd Koninkrijk bleek dat er volgens de ondervraagden een verband bestond tussen privacyoplossingen en informatiemanagement.[79] Als organisaties geen animo konden opbrengen voor privacyverhogende technieken, dan zouden deze technieken beter kunnen worden gebruikt om de informatiemanagementmethoden van organisaties op orde te brengen, bijvoorbeeld door databases op te schonen, aldus de ondervraagden. Uit het feit dat de ondervraagde experts dit soort verbanden leggen, concludeerde Hosein dat de bepaalde eigenschappen van PET investeringsbevorderend werken: "it must be able to not just limit data but also adequately manage data flows", niet alleen binnen organisaties maar ook voor organisaties in hun onderlinge relaties. "That is, privacy is increasingly being seen as the management of information across the 'supply chain' or with third party organizations. A technological solution would have to cater for this broader goal."[80]

De ondervraagden hadden duidelijk het gevoel dat de aard van de bedrijfsprocessen veel gewicht in de schaal legt bij de toepassing van PET.

f. Zichtbaarheid en testbaarheid

Er is tot nu toe geen breed maatschappelijk draagvlak voor het gebruik van privacyverhogende technologieën in de samenleving. Dit komt doordat PET-maatregelen als onderdeel verwerkt worden in informatiesystemen. Daardoor onttrekken zij zich grotendeels aan de waarneming van het grote publiek. Als het bestaan van PET meer maatschappelijke bekendheid zouden genieten, dan zou dit waarschijnlijk ervoor zorgen dat organisaties PET sneller zouden invoeren.[81] Het EuroPrise-onderzoek bevestigt dit.[82] Zoals hiervoor betoogd is testbaarheid van de innovatie volgens de Diffusion of Innovation theorie van Rogers een factor die de adoptie van innovaties beinvloedt. Eenvoudige PET zijn vrij makkelijk te testen. Complexe PET-vragen echter om een omvangrijke infrastructuur en testomgeving. Ribbers constateert nochtans dat: "The testability of PET seems to have no influence on the adoption."[83]

7.8.2. Het tweede cluster: interne organisatie

Cluster twee van het conceptmodel is gericht op de interne aspecten van de adopterende organisaties. Bos heeft daarbij het gehele samenwerkingsverband binnen de organisatie onder de loep genomen.[84]

---

78 Schmidt, 2004.
79 Hosein, 2007, p. 27.
80 Hosein, 2007, p. 31.
81 Ribbers, 2007, p. 84.
82 Bock, 2009.
83 Ribbers, 2007, p. 66.
84 Bos, 2006, p. 36.

a. Managementsteun en sleutelfiguren

Of PET gebruikt worden, blijkt dikwijls af te hangen van specifieke personen op sleutelposities die met de materie vertrouwd zijn en een voortrekkersrol vervullen bij de toepassing van dit type technologieën. Deze personen kunnen daarbij dan ook sterke positieve invloed uitoefenen.[85] Volgens Fairchild & Ribbers is primair bepalend "How open is top management to accept changes that accompany innovation."[86]

b. Individuele banden met voorlichtende organisaties

Een belangrijke rol bij de adoptie van PET lijkt voor adviserende instellingen, zoals accountants, advocaten, en rechtsbijstandverzekeringen te zijn weggelegd. Bos signaleert dat de voorgangster van het College Bescherming Persoonsgegevens (CBP), de Registratiekamer, een belangrijke rol heeft gespeeld bij de acceptatie van PET. Tot 2001 heeft de Registratiekamer een actieve adviserende rol gespeeld om het gebruik van privacyverhogende technologieën binnen organisaties te stimuleren, met name bij grootschalige projecten. Doordat het gebruik van PET meer aandacht kreeg zijn ze ook vaker toegepast. Momenteel worden deze technologieën door het CBP niet meer proactief als oplossingsrichting geadviseerd, waardoor de toepassing daarvan achterblijft. Ook blijkt uit het onderzoek van Bos dat de relaties die organisaties onderhouden met adviserende instellingen (zoals het CBP) van invloed zijn op het al dan niet gebruikmaken van privacyverhogende technologieën. Organisaties die geen relaties onderhouden met dergelijke instellingen blijken deze technologieën vrijwel niet in praktijk te brengen.[87] In het onderzoek van Hosein in het Verenigd Koninkrijk[88] kwam evenwel het tegendeel naar voren. Organisaties zien de toezichthoudende instellingen niet als een belangrijke factor voor de toepassing van privacyverhogende technologieën in hun informatiesystemen. Dat zou een gevolg kunnen zijn van het feit dat de Britse privacytoezichthouder volgens de participanten aan de 'workshop' vrij onbekend is in het Verenigd Koninkrijk. Discussianten vonden de rol en invloed van bedrijfsverenigingen en industriële normen belangrijker. Volgens Hosein: "This may change as privacy breaches come to dominate business privacy concerns as regulators may choose to re-open dialogue about the role of encryption and other such technologies to minimize damages, but this was not seen as an immediate or pressing component."[89]

---

85 Bos, 2006, p. 53.
86 Fairchild & Ribbers, 2008, p. 83.
87 Bos, 2006, p. 52.
88 Ribbers, 2007, p. 29-33. G. Hosein van de London School of Economics heeft in het kader van het PRIME-onderzoek in Londen in mei 2007 een workshop gehouden met participanten uit de overheid en het bedrijfsleven om de resultaten van Bos te toetsen aan de in het Verenigd Koninkrijk levende opvattingen.
89 Ribbers, 2007, p. 31.

Participanten meenden echter dat organisaties privacy wellicht meer prioriteit zouden geven als gegevensbescherming onderdeel zou zijn van wetgeving die het management verplicht is privacybescherming organisatorisch in te bedden. Dit is bijvoorbeeld het geval bij wetgeving op financieel/boekhoudkundig gebied waar een accountantscontrole verplicht is.

c. Omvang, structuur en cultuur van de organisatie

Rogers geeft aan: "the size of the organization has consistently been found to be positively related to its innovativeness. Large organizations are more innovative".[90]

Uit het onderzoek van Bos blijkt dat de innovatie dient aan te sluiten bij de structuur en de cultuur van een organisatie. Uit de door hem uitgevoerde drie casestudies valt op te maken, dat de grootte en structuur van de organisatie soms wel en soms niet een positieve bijdrage aan de adoptie van PET leveren. Bos merkt op dat tevens meespeelt of de (keten)organisatie relatief eenvoudig en klein is.[91] Hosein rapporteerde over het belang van de bedrijfscultuur, dat het vooral van de interne cultuur van de organisatie afhangt of privacybescherming een prioriteit heeft binnen het bedrijf en of erin wordt geïnvesteerd. De ondervraagden tijdens de workshop in Londen zagen de bereidheid van organisaties om de privacy te beschermen als een recent verschijnsel. De bedrijfscultuur dient zodanig te zijn dat het management bij afwijkingen van het vastgestelde privacybeleid krachtig daartegen optreedt. Als er een dergelijke bedrijfscultuur is, dan blijkt dat de sterkste drijfveer te zijn voor het investeringen in PET-maatregelen. "For instance, if a PET was adopted to manage access controls, this could be simply circumvented through staff abusing their roles or privileges — and this is a problem that only a strong privacy culture could manage."[92]

Wat betreft de omvang van de organisatie concluderen Fairchild & Ribbers in tegenstelling tot Rogers dat een grotere omvang van een organisatie juist een negatieve invloed heeft op de adoptie van PET.[93]

d. Opvatting over privacynormen

In twee van de drie casestudies rapporteert Bos dat de privacywetgeving een positieve invloed heeft op de toepassing van PET.[94] Het onderzoek van Ribbers bevestigt dat naleving van de wet een positieve invloed op de adoptie heeft, maar: "The law imposes in particular general and abstract standards. E.g. article 13 of the Dutch Law on Privacy protection states that 'effective measures' are necessary, which is quite subjective, and provides little direction."[95]

---

90 Rogers, 2003, p. 409.
91 Bos, 2006, p. 53 en 59.
92 Hosein, 2007, p. 32
93 Fairchild & Ribbers, 2008, p. 84.
94 Bos, 2006, p. 54.
95 Ribbers, 2007, p. 74 en 85.

Praktijkdeskundigen tijdens de workshop in Londen meenden dat: “organizations were not overly concerned about compliance with legal requirements. In fact, there was a feeling that organizations aren’t overly concerned about privacy altogether”.[96] Deze houding heeft een remmend effect op de toepassing van privacyverhogende technologieën.

e. Diversiteit in informatiesystemen

De aard van de verwerkte gegevens en de gebruikte informatiesystemen blijkt geen positieve invloed te hebben op de adoptie van PET. Evenwel wanneer het risico op privacyinbreuk hoog is, bestaat er meer animo om gebruik te maken van privacyverhogende technologieën.[97]

7.8.3. De derde cluster: omgevingsfactoren

De derde cluster bestaat uit factoren die samenhangen met de externe aspecten dan wel de omgeving van de adopterende organisatie. Deze kunnen worden onderverdeeld in regelgevende, maatschappelijke en marktgerelateerde factoren.

a. Druk van de privacywetgeving en het toezicht

Uit de drie casestudies die Bos onderzocht heeft blijkt dat organisaties PET sneller toepassen als er door toezichthouders druk op hen wordt uitgeoefend om de wetgeving voor de bescherming van persoonsgegevens na te leven.[98] De toezichthouders voor de bescherming van persoonsgegevens (bijvoorbeeld het CBP) oefenen echter weinig proactieve druk uit op organisaties om PET in praktijk te brengen. Omdat er weinig controle op de privacybescherming is, hebben organisaties geen behoefte om privacybevorderende technologieën te implementeren. Het onderzoek van Ribbers bevestigt dat organisaties zich nauwelijks realiseren wat de gevolgen zijn als zij niet voldoen aan de wettelijke vereisten. “As a result the adoption of PET is not high on the management agenda.”[99] Als in de privacywetgeving het management uitdrukkelijk zou worden verplicht de gegevensbescherming organisatorisch en technisch in de organisatie in te bedden, dan zal privacybescherming een vast onderdeel worden van de managementagenda. De uitkomsten van de discussie in de workshop in Londen bevestigen dit. Deskundigen in de workshop waren van mening dat de privacywetgeving slecht werd uitgevoerd. Er werden volgens hen te weinig boetes opgelegd en deze waren dan ook nog minimaal: “Stronger regulators could play a larger role in privacy protection, and in turn they could promote

96 Ribbers, 2007, p. 32.
97 Ribbers, 2007, p. 67.
98 Bos, 2006, p. 42-48.
99 Ribbers, 2007, p. 18.

privacy enhancing technologies. But the general consensus was that the current situation was unlikely to promote PET adoption."[100]

b. Complexiteit van de wetgeving

Organisaties weten of begrijpen vaak niet waartoe de privacywetgeving hen verplicht. Omdat de privacywetgeving vaak te ingewikkeld is en voor meerdere uitleg vatbaar lijkt, gebruiken zij niet de juiste beschermingsmaatregelen.[101] Dat laatste is volgens Ribbers weer een negatieve factor in de adoptie van PET.[102]

c. Verschillen tussen publieke en private organisaties in een keten

In de publiekprivate samenwerking kunnen de machtsverhoudingen tussen de publieke en private partijen verschillend liggen. In zo'n situatie stelt Ribbers dat: "The structure of the chain seems to have a negative influence in the adoption of PET. A consequence of this is that it is hard to make decisions that all parties can agree to. Since the PET measures needs uniform agreement, this has a negative influence on the adoption of PET."[103]

d. Beschikbaarheid van PET-producten of -maatregelen

PET-applicaties zijn niet voldoende beschikbaar. Volgens Bos wordt de adoptie van PET hierdoor negatief beïnvloed.[104] Het omgekeerde geldt ook: voldoende aanbod van PET-producten heeft een positieve invloed op de adoptie van PET. Zijn er wel zo weinig PET-applicaties? Goldberg stelde al in 1997 dat er veel code is ontwikkeld om de privacy te beschermen (conform de Amerikaanse privacy-normen). Vandaar dat: "The cypherpunks credo can roughly paraphrazed as "privacy through technology, not through legislation."[105] Koorn & Ter Hart[106] zijn van mening dat de inzet van geautomatiseerde PET-producten op de lange termijn kosten kan besparen. De ontwikkeling van PET kan weliswaar kostbaarder zijn dan de ontwikkeling van een organisatorische procedure, maar de kosten vallen mee wanneer de PET-maatregel tegelijkertijd wordt ontwikkeld met het onderliggende informatiesysteem.

---

100 Hosein, 2007, p. 33.
101 Bos, 2006, p. 55.
102 Ribbers, 2007, p. 20.
103 Ribbers, 2007, p. 84.
104 Bos, 2006, p. 58.
105 Goldberg, Wagner, & Brewer, 1997.
106 Koorn & Ter Hart, 2004, nr. 3, p. 15-22.

De onderzoeken van Bos en Ribbers leiden tot het volgende schematische model:

Figuur 7.4: Clusterkenmerken en het effect op adoptie, Bos, 2006, p. 62; Ribbers, 2007, p. 20.

Kenmerken Cluster 1, 2, 3	Effect op adoptie
Compatibiliteit	–
Complexiteit	–
Kosten	–
Verwevenheid innovatie met proces	–
Zichtbaarheid	+
Testbaarheid	0/+
Managementsteun en sleutelfiguren	+
Rol voorlichtende instituties en individuele banden daarmee	+
Omvang en structuur van de organisatie	–
Opvatting over privacynormen	+
Diversiteit in informatiesystemen	–
Druk van de privacywetgeving en het toezicht mits consequent en frequent uitgevoerd[107]	+
Complexiteit van de wetgeving	–
Verschillen tussen publieke/private organisaties	–
Beschikbaarheid van PET-producten of -maatregelen	+

Uit bovenstaand schema kan geconcludeerd worden dat de toepassing van PET niet van zelfsprekend is en weinig positieve stimulatoren kent. Tot nu toe wordt PET slechts beperkt gebruikt. Als er echter voldoende druk vanuit de wet- en regelgeving is en als de advisering en informatievoorziening over PET beter zouden zijn, dan zou PET meer worden toegepast. Fairchild & Ribbers constateren: "we found that only the legal and regulatory pressure (and the promotion by such advisory or supervisory bodies as data protection authorities) with regard to privacy protection is perceived to-date as having an undivided positive impact on the adoption process. It must be noted, however, that current legislation contains too little explicit reference to the concept of privacy enhancing technologies, which is a weakening factor in the adoption process".[108]

7.9. Maturiteitsmodel voor PET

Tijdens het laatste decennium van de vorige eeuw zijn verscheidene maturiteitsmodellen door Nolan Norton, CMMi, en INK ontwikkeld voor specifieke onderzoekgebieden zoals onder meer het gebruik van IT binnen organisaties,

107 Uit de interviews blijkt dat de 'pakkans' bij privacyinbreuken als minimaal wordt beschouwd. De 'pakkans' moet drastisch omhoog.
108 Fairchild & Ribbers, 2008, p. 84.

softwareontwikkeling en informatiebeveiliging. Elk van deze modellen hebben één ding gemeenschappelijk; allemaal beschrijven zij de maturiteit van één of meerdere processen binnen een organisatie. In de volgende paragrafen wordt onderzocht of dit ook voor PET zou kunnen gelden.

7.9.1. Identiteits- en toegangsmanagement, een aanleiding voor PET?

Zoals in paragraaf 7.3 (PET-trap) is weergegeven, bestaan PET in vele vormen. PET passen in en zijn vaak een extensie van algemene beveiligingsmaatregelen, zoals versleuteling, logische toegangsbeveiliging, gebruikersidentiteiten, autorisatie en toegangsbeheer bij het raadplegen van gevoelige gegevens. Zelfs al is er geen sprake van privacygevoelige gegevens, dan is een elektronische identiteit noodzakelijk, bijvoorbeeld om e-mail te lezen of om thuis of op kantoor op een pc te kunnen werken. Sinds informatietechnologie en computers hun intrede hebben gedaan in de werkomgeving, kost het steeds meer werk om gebruikersidentiteiten tijdens hun levenscyclus te beheren.[109] Al deze processen om e-identiteiten te controleren en te beheren kunnen worden gekwalificeerd als 'Identity and Access Management' (IAM).[110] Afgezien van de positieve en negatieve factoren voor adoptie van PET is het tevens belangrijk te onderzoeken of er een positieve correlatie bestaat tussen IAM en de bescherming van persoonsgegevens. Als die er is, zou dat dan kunnen betekenen dat organisaties daardoor ook vaker PET gaan gebruiken?

Om onjuiste of onbevoegde toegang tot informatiesystemen te verhinderen en bescherming van (persoons)gegevens te verbeteren, troffen organisaties beveiligingsmaatregelen en voerden zij het IAM als bedrijfsproces in. Gebruikers kregen meerdere gebruikersnamen en wachtwoorden voor verschillende applicaties toegewezen of ontvingen specifieke informatie voor identificatie en autorisatie. Omdat het aantal gebruikers bleef groeien, nam ook het aantal elektronische identiteiten toe. Organisaties ervoeren het beheer hiervan als kostbaar en tijdrovend omdat deze identiteiten en de daarbij behorende gebruikersprofielen tijdens hun levenscyclus moesten worden onderhouden.[111] Dat leidde ertoe dat organisaties meer aandacht gingen besteden aan IAM. De ontwikkeling van IAM binnen organisaties heeft ertoe geleid dat sinds de laatste tien jaar organisatiedeskundigen via de ontwikkeling van IAM de fasen en de kenmerken van de maturiteit van een organisatie kunnen vaststellen.[112] Organisaties kunnen op hun beurt aan de hand van een dergelijke classificatie het maturiteitsniveau van hun

---

109 Van Gestel, 2007, p. 11.

110 Baladi, e.a., 2006. Dit document definieert IAM als: "Identity and Access Management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources."

111 Van Gestel, 2007, p. 11: "Because of the multitude of applications and user accounts the maintenance of these accounts is time consuming and thus costly."

112 Van Gestel, 2007, p. 30-36.

eigen processen vaststellen en kunnen bepalen welke opvolgende logische maatregelen zij zouden moeten treffen om op het daarop volgende, gewenste of logische maturiteitsniveau te komen. Daarnaast kan een organisatie met behulp van deze classificatie vaststellen welke PET-vorm bij het gewenste maturiteitsniveau hoort en welk onderdeel van het IAM-bedrijfsproces zij zou moeten aanpassen of verbeteren om PET makkelijker te introduceren.[113]

7.9.2. Maturiteitsmodellen

De afgelopen tien jaar zijn er verschillende maturiteitsmodellen van bedrijfsprocessen ontwikkeld door o.a. de Carnegie Mellon University (CCMi Capability Maturity Model), het Instituut Nederlandse Kwaliteit (INK), en KPMG. Volgens Smit is een maturiteitsmodel: "a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached."[114]

Het afgelopen decennium zijn er binnen het bedrijfsleven ook maturiteitsmodellen ontwikkeld op specifieke onderzoeksgebieden, zoals voor de onderlinge afstemming van verschillende informatietechnologieën van ondernemingen, softwareontwikkeling en beveiliging van informatie. Al deze modellen hebben één ding gemeen: ze beschrijven alle de maturiteit van een of meer processen binnen een organisatie. De beschrijvingen van deze maturiteitsniveaus zijn per model verschillend, maar komen in grote lijnen met elkaar overeen. In ieder model wordt de eerste maturiteitsfase ('immature') gekenschetst als chaotisch, en hebben deelprocessen van IAM (1 monitoring; 2 provisioning; 3 authorization management; 4 user management; 5 authentication management) een ad hoc karakter. Het CCMi maturity model dat het Software Engineering Institute (SEI) in 2000 heeft ontwikkeld beschrijft voor bedrijfsprocessen binnen organisaties de volgende maturiteitsfasen:[115]

Fase 1:	Alleen nieuwe processen zijn gedefinieerd, en deze worden uitgevoerd op ad hoc-basis. (Fase: 'immature'.)
Fase 2:	Processen die lijken te werken en in orde zijn, worden herhaald. De planning van specifieke IAM-deelprocessen staat centraal. (Fase: 'starting up'.)
Fase 3:	Processen worden regelmatig uitgevoerd, gestandaardiseerd en gedocumenteerd om vast te stellen of ze dienovereenkomstig worden uitgevoerd. Op dit punt in de ontwikkeling van de organisatie heeft zij de ad hoc-fase definitief achter zich gelaten. (Fase: 'active'.)
Fase 4:	Het welslagen van processen wordt organisatiebreed gemeten, processen en kwaliteit worden bewaakt op basis van kwantitatieve procedures. Het periodiek actualiseren

113 Van Gestel, 2007, p. 2.
114 Smit, Rotterdam, 2005, p. 2.
115 Peekel, 2006, p. 23.

	van de authenticatie vereisten geschiedt op basis van continue risicoanalyses. Het gebruikersbeheer is nog steeds handmatig, maar wel gecentraliseerd en betreft nu alle gebruikersregistraties. (Fase: 'pro active'.)
Fase 5:	Processen worden systematisch verbeterd aan de hand van kwantitatieve terugkoppeling van (test)resultaten en innovatieve ideeën. IAM is een belangrijk onderdeel van de ondernemingsdoelstellingen.[116] (Fase: 'top class'.)

De combinatie van de procesbeschrijvingen en de beschrijvingen van de maturiteitsfasen resulteren in het volgende IAM-maturiteitsmodel.[117]

Figuur 7.5: Identiteit en toegangsprocessen en daarbij behorende technologieën, Van Gestel, 2007, p. 34. Op de X-as staan de maturiteitsfasen en op de Y-as de IAM-processen, die toenemen in complexiteit.

Authentication Managment	No authentication means	Arbitranily formulated authentication requirements (authentication mens are provided, adjusted and deleted on user request)	Authentication Requirements based on a one time survey	Authentication Requirements based on continuous risk analyis	Authentication requirements based on continuous risk analyis and are continuously adjusted
User Managment	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, Limited user group, manual procedures	Central registration, controlled authorization processes, manual procedures	Central real-time controlled authorizatione sourses automated procedures
Authorisation Managment	No authorization matrixes authorization is defined ad hoc	Authorization matrizes defined but are not updated	Authorization matrizes are updated periodically	Role Based Access Control used for critical applications	Role Based Assess Control for all applications and continuous updated authorizations
Provisioning	Manual process locally	Limited automated unreliable processes locally	Limited automated reliable processes locally	Limited automated reliable for multiple sources	Automated and reliable for multiple sources
Monitoring(Audit)	No respousibility delegated into AO/IC organisation	Sporadically delegated responsibility of AO/IC	Putial delegation of responsibility to AO/IC	Full responsibilty to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	Starting-up	Active	Pro-Active	Top Class

Een organisatie zal zich steeds bewuster worden van het belang van IAM-processen naarmate zij de vijf maturiteitsfasen doorloopt. De organisatie moet hierdoor niet alleen haar IAM-processen bijstellen, maar ook haar eigen organisatiestructuur en bedrijfsbeleid. Het privacybeleid kan hierbij niet achterblijven. IAM-processen blijken ook conform de S-curve van Rogers (zie paragraaf 7.5) te verlopen.[118]

116 Ribbers, 2007, p. 23.
117 Van Gestel, 2007, p. 25-34.
118 Ribbers, 2007, p. 29.

7.9.3. PET in het maturiteitsmodel

Nu de maturiteitsfasen in kaart zijn gebracht, is de vraag of vastgesteld kan worden in welke maturiteitsfase organisaties besluiten PET toe te passen en zo ja, om wat voor soort organisaties het dan gaat. Om die vraag te kunnen beantwoorden, heeft Van Gestel gezocht naar een geschikt maturiteitsmodel dat laat zien hoe het toepassingsproces van PET binnen organisaties verloopt.[119]

Fairchild & Ribbers[120] hebben dit onderzoek naar een gezamenlijk maturiteitsmodel voor 'Identity & Access Management' (IAM) en PET voortgezet en ook het maturity model van Nolan Norton hierbij betrokken. Volgens Koorn e.a.[121] bestaat PET uit een aantal verschillende technologieën die weer zijn onderverdeeld in een viertal verschillende componenten (zie paragraaf 5.7.3). Fairchild & Ribbers: "Obviously these technologies require a certain level of IT infrastructure."[122]

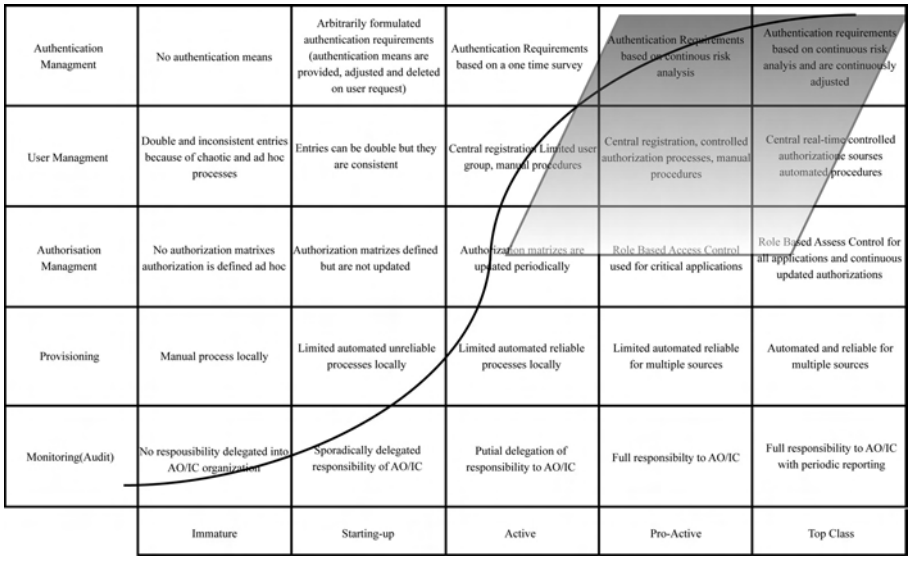
Om privacyverhogende technologieën in een organisatie te implementeren is het noodzakelijk dat binnen de organisatie structureel IAM wordt toegepast. Immers, zonder IAM-processen is het niet mogelijk het gebruik van en de toegang tot (gevoelige) persoonsgegevens te controleren. Volgens de PET-trap (zie figuur 5.2) behoort IAM tot de categorie: algemene PET-maatregelen. Beveiligde toegang is echter niet meer dan een eerste stap in privacyverhogende maatregelen. Zoals uit paragraaf 5.7 blijkt, hebben de PET-maatregelen onder meer ook tot doel de identiteit van een persoon veilig te stellen door persoonlijke informatie van overige informatie te scheiden. Afhankelijk van de eisen die de organisatie stelt om PET te implementeren, is een bepaald maturiteitsniveau van de betreffende IAM-processen noodzakelijk. Het is zeer onwaarschijnlijk dat onvolgroeide organisaties overgaan tot implementatie van PET, laat staan dat deze organisaties voldoende beseffen wat er nodig is voor een optimale privacybescherming. Organisaties kunnen aan de hand van het IAM-maturiteitsmodel vaststellen in welke maturiteitsfase zij zich bevinden, waardoor zij na een privacybedreigingsanalyse de voor hen geëigende PET kunnen inzetten. Fairchild & Ribbers hebben vergeleken hoe het maturiteitsmodel zich verhoudt tot het gebruik van PET-technologieën en voorspellen voor organisaties dat: "PET will be applied by organizations in the Top-Class and Pro-Active maturity level, with the exception for organizations that update authorization matrixes periodically (organization level: active)."[123]

Dat wil dus zeggen dat bij organisaties die zich in de vierde of vijfde fase van het maturiteitsmodel bevinden, de kans het grootst is dat zij PET-maatregelen

119 Van Gestel, 2007, p. 37-39.
120 Fairchild & Ribbers, 2008, p. 84.
121 Koorn, e.a., 2004, p. 40.
122 Fairchild & Ribbers, 2008, p. 87.
123 Fairchild & Ribbers, 2008, p. 88.

zullen toepassen. Voor IAM is de S-curve van Rogers eveneens van toepassing. De niveaus 3 (gedeeltelijk), 4 en 5 liggen rond deze S-curve. Figuur 7.6 geeft aan dat bij organisaties op het niveau 'active', die de 'authorization matrices' periodiek actualiseren, rijp zijn voor het implementeren van PET-maatregelen.

figuur 7.6: Potentiële toepassing van privacybescherming en PET (rood paralellogram) in IAM-maturiteitsmodel. Op de X-as staan de maturiteits-fasen en op de Y-as de IAM processen, die toenemen in complexiteit.



Uitzondering hierop zijn (micro-)organisaties die behoren tot de categorie kleine en middelgrote ondernemingen waar vertrouwen een cruciale succesfactor is, hetgeen het geval is voor beroepsgroepen zoals artsen, advocaten, notarissen, accountants, belastingadviseurs etc. De in paragraaf 6.5.1 beschreven casus van Ixquick is daar een bewijs van. Er mag van worden uitgegaan dat deze kleine en middelgrote ondernemingen en beroepsgroepen de persoonlijke informatie van hun klanten goed beschermen, al dan niet door gebruik te maken van encryptie of een rudimentaire vorm van PET. Over het algemeen zullen deze organisaties evenwel niet blijken te voldoen aan de processen uit het maturiteitsmodel in vergelijking met het niveau van de toegepaste IAM- en PET-maatregelen.

7.9.4. PET-gevoelige organisaties

De premisse is dat een organisatie die gevoelige informatie beheert en verwerkt waardoor persoonsgegevens moeten worden beschermd, potentieel PET zou kunnen

gebruiken. Porter & Millar[124] hebben een reikwijdtematrix ontwikkeld die de intensiteit van de informatie in bedrijfsprocessen kwantificeert. Met het reikwijdtemodel is te zien hoe informatie ontwikkeld en gebruikt kan worden om concurrentievoordeel te behalen.[125] Met deze matrix zou ook de groep van organisaties in kaart kunnen worden gebracht die PET potentieel zou kunnen toepassen.[126] De verticale (Y-)as in figuur 7.7 meet de informatieintensiteit van de 'value chain' (de technologische en economische activiteiten van een bedrijf). Bijvoorbeeld: de informatieintensiteit in de cementindustrie is laag, terwijl die van een uitgever hoog is. De horizontale (X-)as geeft de mate van de informatieinhoud van het product of dienst. De informatieinhoud van aardolieproducten is laag, terwijl die voor bancaire producten hoog is.[127]

Een hoge informatie-intensiteit in de waardeketen treedt op bij:

1. een bedrijf dat direct handelt met een grote groep aanbieders;
2. een product dat een grote hoeveelheid informatie vereist om te kunnen worden verkocht;
3. een productlijn met veel onderscheidende productvariëteiten;
4. een product dat uit veel onderdelen bestaat;
5. een product dat in een groot aantal stappen gefabriceerd wordt;
6. een product dat een lange verkoopcyclus heeft variërend van de initiële order tot de aflevering van het product.[128]

Zoals hierboven is uiteengezet, bepaalt de IAM-maturiteit van de organisatie mede de potentiële PET-vraag om aan de wettelijke eisen voor privacybescherming te voldoen.

Figuur 7.7: PET-vraagindicatie, Borking, 2002, p. 197. De Y-as meet de informatie-intensiteit van de 'value chain'. De X-as geeft de mate van de informatie-inhoud van het product of dienst.

Zoals is te zien in figuur 7.7 komen in het bovenste rechterkwadrant organisaties voor die met een hoge informatie-intensiteit (en verwerking van persoonsgegevens) te maken hebben en die dus het meest in aanmerking komen om PET toe te passen. Het onderzoek van Ribbers bevestigt dit en voegt toe dat die organisaties ook de beste financiële en technische mogelijkheden hebben om een dergelijke bescherming in hun bedrijfsprocessen te incorporeren.[129]

---

124 Porter & Millar, 1985, p. 149-160.
125 Earl, 1989, p. 62.
126 Borking, 2002, p. 196-202.
127 Bedrijfseconomisch begrip: een opeenvolging van elkaar afhankelijke activiteiten waarbij in elke schakel van het proces een waardetoevoegende activiteit plaatsvindt. Hierbij wordt onderscheid gemaakt tussen de zogenaamde primaire activiteiten en de ondersteunende activiteiten.
128 Porter & Millar, 1985, p. 150-151.
129 Ribbers, 2007 (A), p. 26.

7.10. Validiteit van de maturiteitsmodellen

De hiervoor gepresenteerde maturiteitsmodellen moeten aan de praktijk getoetst worden. Voordat een organisatie PET kan adopteren moet zij eerst beslissen of zij de persoonsgegevens ook langs technische weg wil beschermen. Het is belangrijk te weten welke gevolgen zo'n beslissing heeft op de bedrijfsvoering. Daarom zijn in het kader van dit proefschrift[130] vier workshops en zes gerichte interviews gehouden met experts van middelgrote en grote organisaties in de sectoren: overheid (belastingen en defensie) telecommunicatie, delfstoffen, banken en verzekeringen, elektronica, gezondheiszorg en entertainment (casino). De interviews vonden in 2007 plaats in Londen, Den Haag, Tilburg, Utrecht en Hoofddorp en in 2008 in Stockholm, Bristol, Zurich en Eindhoven. De interviews vonden plaats onder het regime van de 'Chatham House Rule'. Dit houdt in dat zowel de persoon als de organisatie die geïnterviewd is anoniem blijft. Het bleek niet zo makkelijk te zijn om op de modellen (figuren 7.3, 7.6 en 7.7), die tijdens een presentatie werden getoond, een reactie te krijgen. Toen deze begripsmodellen werden gepresenteerd, waren er maar weinig discussianten die het interessant genoeg vonden als leidraad voor de discussie. Het bleek echter dat het maturiteitsmodel (figuur 7.6) als analytisch instrument kan dienen om de feedback van de discussianten te verifieren. De deelnemers ontvingen van tevoren een vragenlijst. De vragenlijst (protocol) is opgenomen als bijlage in dit boek.

7.10.1. Bedrijfsstrategie en privacybescherming

Bij de meeste ondervraagde bedrijven blijkt privacybescherming geen bewust onderdeel te zijn van de bedrijfsstrategie. De bewustwording op dit gebied lijkt echter wel toe te nemen, in ieder geval als het om de persoonlijke informatie van klanten gaat. Deelnemers aan de workshop in Bristol deelden onder meer mee:

> "I think there can be a big mismatch between employer perception and the perception of the general public. There have been some surveys over the past year that show that certainly in the UK the public regard privacy as a very important issue, one of the most important issues, but employers don't seem to have taken that on board."
> "I think it's almost broken down into two parts. I think the companies recognize privacy for external facing people, but internally it's very poorly recognized. So are their own employees."[131]

Natuurlijk kunnen deze opvattingen niet gegeneraliseerd worden omdat in elke organisatie weer specifieke omstandigheden gelden en de privacycultuur van land tot land kan verschillen. Onderzoekers stelden vast dat bij de elf participerende bedrijven in de workshop in Bristol het niveau van de IAM-processen varieerde

130 De interviews werden mede uitgevoerd in het kader van het PRIME onderzoeksproject. PRIME (Privacy and Identity Management for Europe) Contract No. 507591 Research periode 2004-2008.
131 Ribbers, Fairchild & Tseng, 2008, p. 11.

van 'starting-up' tot 'top class'. In Stockholm stelden de representanten van de telecommunicatie-industrie (top class maturiteit) dat:

"Sweden is probably the most high-trust society in the world; this imposes a responsibility for XYZ to respect that trust and with that the privacy of the customers....(..) The relationship in Finland is mainly based on trust, the damage in a privacyincident is much higher….because it effects the core of trust."[132]

Klanten van deze industrie verwachten dat hun persoonsgegevens goed beschermd zijn. Slechts een klein privacyincident haalt met gemak de voorpagina van de kranten. Dat neemt echter niet weg dat privacy niet erg hoog op de managementagenda van Zweedse bedrijven staat: "Unless privacy becomes an (business) opportunity, it will not be high on the management agenda. (...) [The] Main vision is to offer so much privacy to meet customer demand (…) that is different in Kazachstan[133] than in Sweden."[134]

Met andere woorden de geboden privacybescherming in Kazachstan lag vele niveaus lager dan in Zweden. De deelnemers aan de workshop in Zurich zagen privacy als een synoniem voor confidentialiteit[135] voor alle zaken waarbij cliënten betrokken waren:

> "Client confidentiality is very important for us and our customers (…) it is vital for ABC to prevent its products and services from being abused, while still respecting the privacy of its clients. In addition to adhering to local legislation, the bank applies strict Swiss regulations for the prevention of money laundering and terrorist financing in its international locations."[136]

Voor de meeste bedrijven blijkt privacy een synoniem voor informatiebeveiliging te zijn. In de workshop in Nederland bleek echter dat bedrijf PQR (top class maturity) in zijn benadering van privacy zich totaal anders opstelde dan organisaties in de andere workshops. Binnen PQR is privacybescherming onderdeel van de bedrijfscultuur. PQR beschouwt privacy als een fundamenteel middel om het vertrouwen dat cliënten hebben in het bedrijf en de goede reputatie van het merk te bevorderen. Als enige organisatie die participeerde in de workshops heeft PQR een:

> "corporate privacy infrastructure in place: a chief privacy officer plus network of privacy officers throughout the worldwide company (...) We have also a privacy group in division XYZ and privacy security research group."[137] Binnen PQR gelden verschillende privacyprocedures voor de gegevens van cliënten en werknemers: "We have a strategy on privacy for employee data; we have implemented binding corporate rules for employee data, it is part of our ethics code (...) For the consumer data there is a global privacy policy for these data (...) we have an extremely global centralized database on consumer data. Security is very strict and as well the access policy. (...)

---

132 Ribbers, Fairchild & Tseng, 2008, p. 15.
133 Een van de gebieden waar XYZ een dochteronderneming heeft.
134 Ribbers, Fairchild, & Tseng, 2008, p. 16.
135 In figuur 2.2 zijn de verschillen tussen privacy, confidentialiteit en informatiebeveiliging gevisualiseerd.
136 Ribbers, Fairchild, & Tseng, 2008, p. 24.
137 Borking, 2008, p.7.

> There are very strict procedures and data are only available on a very limited basis. For outsiders if they want to use data, there are many elaborate privacy clauses in the contracts. (...) if the database would have a problem, the problem would be very big. Employees have to load consumer data in this database and aren't allowed to keep it."[138]

Tijdens de discussie over het IAM-maturiteitmodel en het moment waarop een bedrijf PET-applicaties overweegt deelde de 'chief privacy officer'(CPO) van een bedrijf in Nederland mee dat:

> "To align the different interests within our organization (several divisions) you look at the privacy maturity levels. For comparison we use the standard of the GAP Institute of Internal Auditors (GAP schema GTAG 5.)[139] We are for the whole of our organization at level X (confidential). (…) There seems to be in the GAP privacy level scheme a S-curve as well."[140]

Het schema (figuur 7.8) waar de CPO aan refereert, ziet er als volgt uit:

Figuur 7.8: Privacymaturiteitmodel volgens GAP.

Initial	Activities are ad hoc, with: • No defined policies, rules, or procedures. • Eventually lower-level activities, not coordinated. • Redundancies and lack of teamwork and commitment
Repeatable	The privacy policy is defined, with: • Some senior management commitment. • General awareness and commitment. • Specific plans in high-risk areas.
Defined	The privacy policy and organization are in place, with: • Risk assessments performed. • Priorities established and resources allocated accordingly. • Activities to coordinate and deploy effective privacy controls.
Managed	A consistently effective level of managing privacy, privacy requirements, and considrations ia reflected in organization, with: • Early consideration of privacy in systems and process development. • Privacy integrated in functions and performance objectives. • Monitoring on an organizational and functional level. • Periodic risk-based reviews.
Optimizing	Continual improvement of privacy policies, practices, and controls, with: • Changes systematically scrutinized for pricacy impact. • Dedicated resources allocated to achieve privacy objectives. • A high level of cross-functional integration and teamwork to meet privacy objectives.

Source: Hargraves et al 2003

De resultaten van de workshops en interviews geven aan dat de participerende organisaties uiteenlopende ideeën hebben over de strategische relevantie van privacy. Het is daarom te verwachten dat daardoor de toegepaste bedrijfsprocessen en structuren om privacy te beschermen per bedrijf net zoveel van elkaar verschillen.

---

138 Borking, 2008, p.8.
139 Hahn, Askelson & Stiles, 2008.
140 Borking, 2008, p. 8.

7.10.2. PET-toepassing

De algemene opvatting in de workshops was dat vanuit de informatiebeveiliging de middelen worden ontwikkeld om (persoonlijke) informatie te beschermen. Tijdens een workshop in Nederland deelde een 'chief privacy officer' mee dat: "The tools that are in use are security driven. The IT dept identifies risks and how to mitigate it. Where there is a privacy/security risk there is special software to protect it. (…) There will be security tools whether that is a PET tool, or something else. (...) there are going to be more security tools, not primarily to protect privacy."[141]

In het algemeen gebruikt dit bedrijf geen PET, behalve de standaardbeveiliging door middel van encryptie:

> "We took the decision to encrypt all hard discs of our computers and laptops mandatory, because we don't want to be forced to identify that we fulfill all US security requirements for personal data later. We took the decision to do it everywhere not for the sake of privacy but to avoid to give information about what security we use later.[142]

Het bankbedrijf ABC gebruikt geen PET, hoewel ABC in termen van beveiligings- en IAM-architectuur zich op het hoogste niveau van maturiteit bevindt.[143] Tijdens de workshop in Zurich gaven de vertegenwoordigers uit de bancaire sector aan:

"PET should enable us to do some kind of business. Of course it is interesting, it would remove the need for registration processes, it could be used in business relationship processes. But it is a long way, it is not just a technical issue, it is also a legal issue, regulatory issue. It is also a project feasibility issue, whether it can be made user friendly for the customer. (...) The privacy enhancing features should also be easy to use and it's benefits well understood. If you introduce too complicated features on Internet banking, such as hardware tokens, it is questionable how much the customer understands these features, so you would expect some customers to leave rather than be pleased."[144]

7.10.3. Reputatieschade

Afgezien van de wettelijke verplichtingen waaraan bedrijven moeten voldoen, lijken zij vooral in PET te willen investeren om reputatieschade te vermijden.[145] . Alle workshopdeelnemers zien omzetverlies en potentiële reputatieschade als de

---

141 Borking, 2008, p. 7.
142 Borking, 2008, p. 7.
143 Ribbers, Fairchild & Tseng, 2008, p. 22.
144 Ribbers, Fairchild & Tseng, 2008, p. 23.
145 L. Gaines-Loss van het consultancybureau Weber Shandick deelt in het Financiele Dagblad van 6 augustus 2009 mee dat kans op reputatieschade door internet steeds groter wordt.

grootste risico's van een privacyinbreuk. Een dergelijke reputatieschade vermijden is zelfs één van hun grootste zorgen. In Bristol deelde een participant mee:

> "I know a few incidents where there was a privacy violation where the application developers fixed the privacy violation themselves rather that reporting it, because the implications of reporting it would have been a rather big audit, which they didn't want."[146]

Of dit ook geldt voor monopolistische overheidsdiensten is de vraag, zo vertelde een andere deelnemer:

> "There is no reputation impact because you don't have an alternative supplier, as someone who wants to take a driving test I only have one supplier, as someone who doesn't what to pay his taxes, I only have one supplier, so it doesn't make any difference in that respect, it has a reputation impact on the government of the day, but given that the general election is two and a half years down the line, the impact is zero."[147]

De representanten van de telecommunicatie-industrie in Stockholm stelden, dat "XYZ is in a very sensitive market; reputation damage has big consequences (...) if a privacy breach would come on top of that would be very damaging to the company (...) It all relates to the reputation of the company (...) The damage in reputation from incidents tends to add up, damaging the brand and customer loyalty."[148]

In de discussie in Stockholm kwam een nieuwe variabele aan het licht: de invloed van de ethische analisten en ethische investeerders. "We (XYZ) conduct privacy risk reporting every quarter, such reporting is useful for ethical investors (Calvert Group, F&C, Dow Jones) and can be benchmarked against the Dow Jones Sustainability Index, which now includes an additional variable for minimizing reputational risk. Last year they included a number of questions on privacy and how we manage privacy. Inclusion in such indices reduces our cost of capital. This is the result of an increase flow of money that has been raised around ethical business. It minimizes the reputational risks and investors like that. They don't like to be mentioned in the newspapers with some bad news."[149]

Het oordeel van de markt- en ethische analisten over het economisch risico dat een bedrijf loopt (het vraagstuk van de 'sustainability') blijkt effect te hebben op bijvoorbeeld het rentepercentage van de aan het betrokken bedrijf te verstrekken lening. PQR wil niet bij een privacyincident betrokken raken omdat het tot grote reputatieschade leidt: "(...) it will backfire. PQR will not do a quick win and by that jeopardizing its brand image over the last 100 years." Ook het bedrijf PQR werkt met sustainability reports.[150]

---

146 Crane, 2008, p. 18.
147 Crane, 2008, p. 19.
148 Tseng, 2008, p. 3.
149 Crane, 2008, p. 19.
150 Borking, 2008, p. 7.

Bij bank ABC zou reputatieschade ertoe kunnen leiden dat de licentie om als bank te mogen opereren zou kunnen worden ingetrokken, waardoor het bedrijf geen bestaansrecht meer zou hebben en failliet gaat. Daarom is confidentialiteit een van de belangrijkste ethische waarden binnen het bedrijf.

> "(…) it is easier to talk about confidentiality than privacy. We have a better understanding of what needs to be done with a confidentiality breach than with privacy. Such a breach would be dramatic, from legal, reputation damage, we may even go out of business if the banking license is revoked."[151]

De vrees voor reputatieschade kan voor bedrijven een sterke stimulans zijn om PET-maatregelen te nemen. Toch zijn de meeste terughoudend om te investeren in PET. De reden voor deze weerstand is onder meer het gebrek aan vertrouwen dat de investering in PET zich terugbetaalt. In Rogers' termen: de voordelen zijn niet duidelijk. Het probleem met het investeren in PET is dat de kosten bekend zijn, maar dat de voordelen nochtans onzeker zijn, of zoals een deelnemer in Bristol het formuleerde:

> "Don't take this wrongly, but in many ways if you are a provider of PET it's like trying to sell insurance. Everyone knows they need it, but equally from a business point of view there is nothing worse than an undefined cost."[152]

In termen van informatiebeveiligingsarchitectuur, bevindt ABC zich op het hoogste niveau van IAM-maturiteit. Jaarlijks investeert het bedrijf ten minste vijftien procent van het IT-budget in beveiligingstechnologieën om in het top segment van de markt te blijven. Daarbij wordt goed gelet op wat directe concurrenten doen. Toch overweegt ABC momenteel niet om PET in hun de productenaanbod aan te bieden. Er is wel belangstelling voor PET, maar de beslissing voor het invoeren van PET (ano- en pseudonimisering) is gebaseerd op de overweging:

> "PETs should enable us to do some kind of business. Of course it is interesting, it would remove the need for registration processes, it could be used in business relationship processes. But it is a long way, it is not just a technical issue, it is also a legal issue, a regulatory issue. It is also a project feasibility issue, whether it can be made user friendly for the customer."[153]

151 Tseng, 2008, p. 3.
152 Crane, 2008, p. 30.
153 Tseng, 2008, p. 5.

7.11. Drie S-curven

Uit de interviews en de workshops valt op te maken dat als bedrijven PET al toepassen, zij dit in eerste instantie niet doen om de persoonsgegevens te beschermen, maar om informatie te beveiligen.[154] Zij laten zich daarbij leiden door standaard calculatiemodellen zoals 'Return On Security Investment' (ROSI).[155] Toch blijkt dat bedrijven ook steeds vaker PET toepassen om de privacy te beschermen. Je zou kunnen zeggen dat zij op dit gebied steeds meer bewustwording krijgen en zich steeds 'volwassener' ('mature') gaan gedragen. Dit maturiteitsproces voor privacybescherming ontwikkelt zich ook langs een S-curve. Op grond van eerdere waarnemingen in dit hoofdstuk kan geconstateerd worden dat er drie S-curves met betrekking tot de toepassing van PET te onderkennen zijn:

1. Een om PET te adopteren; de wetgeving op het gebied van privacybescherming en de rol van de adviserende privacytoezichthouders zijn hierbij de belangrijkste positieve stimulerende factor.
2. Een om IAM-processen toe te passen; de maturiteit van de IAM-processen moet hierbij hoog zijn. En
3. Een om de bescherming van privacy met de bedrijfsprocessen te integreren, zoals weergegeven in het 'GAP privacy level'-model. (zie figuur 7.8).

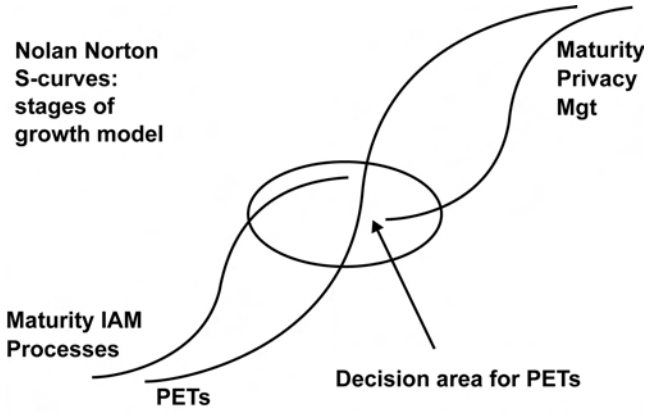
Zoals uit figuur 7.9 blijkt, zal een organisatie besluiten om PET in te zetten als de IAM-maturiteit hoog is en de privacymaturiteit laag is. Voor organisaties waar de bescherming van privacy een kritische succesfactor is, zal het management al in een veel vroegere fase van ontwikkeling van de organisatie ervoor kiezen om PET toe te passen. Een voorbeeld hiervan is Ixquick (zie paragraaf 6.5.1). Zoals bleek in dit hoofdstuk uit de interviews van RAND Europe, zullen overheidsinstanties doorgaans niet snel beslissen om PET in te voeren, omdat zij niet het risico willen nemen dat PET-maatregelen wel eens niet zouden kunnen werken. Zij behoren daardoor tot de groep van de 'late majority'.[156] Zo heeft de Nederlandse Belastingdienst in het RAND Europe onderzoek verklaard dat zij niet het imago wil hebben van een technologische koploper te zijn. Essentieel voor het functioneren van de Belastingdienst is dat klanten de instantie betrouwbaar vinden. Horlings e.a. "de Belastingdienst zal PET pas willen invoeren als PET 'mainstream' is geworden en er geen (...) risico's meer aan verbonden zijn".[157]

Deze observaties leiden tot het volgende model:

---

154 Borking, 2008, p. 8.
155 Tseng, 2008, p. 5.
156 Rogers, 2003, p. 212. Rogers onderscheidt vijf groepen bij innovatiebeslissingsproces: 1 Innovators; 2 Early adopters; 3 Early majority; 4 Late majority; 5 Laggards.
157 Horlings, e.a., 2003, p. 21.

Figuur 7.9: Nolan Norton groei S-curves voor IAM, privacy en PET, Borking, 2008.



Met deze S-curves kan bij benadering worden bepaald op welk moment een organisatie voor het eerst zal overwegen om PET te gaan gebruiken (scheiding van gegevens, privacymanagementsystemen, anonimisering) als middel om persoonsgegevens te beschermen.

7.12. De multi-actoranalyse

Op basis van het onderzoek naar het gebruik van PET binnen de Nederlandse overheid, constateert RAND Europe dat invoering van PET een multi-actorprobleem is: "een probleem waarbij de besluitvorming over de invoering, de uitvoering en de beschikbare middelen over de betrokken belanghebbenden (centrale overheid, afzonderlijke instanties en afdelingen, data-eigenaren en klanten) is verdeeld."[158] Omdat PET moeten voldoen aan een aantal fundamentele functionaliteiten en de 'stakeholders' (veel) specifieke eisen kunnen hebben, is het noodzakelijk hen actief bij het besluitvormingsproces te betrekken. Dit zal een breed draagvlak scheppen en de adoptie van PET vergemakkelijken. Als er geen draagvlak is en alle partijen zich niet voor de volle honderd procent inzetten zal de adoptie mislukken. Sterker nog: de betrokken partijen zullen de adoptie tegenwerken als er geen rekening wordt gehouden met hun eisen en wensen en hun belangen als die door de invoering van PET worden geschaad.[159]

158 Horlings, e.a., 2003, p. 65.
159 Riesewijk & Warmerdam, 1988, p. 15. Bij informatisering zijn machtsaspecten in het geding. Zie ook Franken, Borking & Van Schelven, 1999, p. 37-48.

7.13. Economische rechtvaardiging van PET-investeringen

Als medebestuurder van het College bescherming persoonsgegevens heb ik ervaren dat het uiterst moeilijk is organisaties ervan te overtuigen dat de bescherming van persoonsgegevens door middel van PET noodzakelijk is en voordelen oplevert. Dit proces verloopt allereerst moeizaam omdat veel informatici nog nooit over minimalisatie van persoonsgegevens hebben nagedacht, maar ook omdat bedrijfs- of economische modellen ontbreken waaruit blijkt dat een PET-investering financiële voordelen kan opleveren. Voordat een bedrijf besluit om PET toe te passen is het essentieel dat het begrijpt hoeveel een dergelijk proces gaat kosten en wat voor financiële en andere kwantitatieve en kwalitatieve baten het oplevert.[160] Bovendien zijn de kosten een negatieve adoptiefactor voor PET.

Om te onderzoeken of er een positieve business case is voor de toepassing van PET binnen een organisatie, moeten drie kernvragen worden beantwoord. Deze vragen zijn:

1. Draagt PET in belangrijke mate bij aan de beleidsdoelstellingen van de organisatie? Als dat zo is dan dient de bijdrage op te wegen tegen de kosten die ermee gemoeid zijn. Zo niet, dan is er geen business case.
2. Welke kosten brengt PET eenmalig en structureel met zich mee? Het antwoord op deze vraag blijkt voor het management de meest belangrijke beweegreden om PET al dat niet toe te passen in de organisatie.
3. Welke kwalitatieve en kwantitatieve baten kan PET in onze organisatie realiseren? Als het bedrijf minder kwijt is aan operationele kosten wanneer het PET toepast, zal de businesscase dat eenvoudig kunnen aantonen. Niet kwantificeerbare voordelen zoals toegenomen klanttevredenheid, versterking van het (innovatieve) imago van de organisatie naar burgers e.d., zijn echter een stuk lastiger in kaart te brengen.[161]

Er is sprake van een positieve businesscase als de beantwoording van bovenstaande vragen leidt tot de conclusie dat de toepassing van PET in de betrokken organisatie wenselijk en financieel haalbaar is en voordelen oplevert. De positieve businesscase is dan de zakelijke rechtvaardiging van de toepassing van PET.[162] Het niet kunnen kwantificeren van de voordelen behoeft geen belemmering te zijn voor een positieve business case. Voor de besluitvorming is nochtans vooral van belang dat de organisatie een goed inzicht heeft in de 'Return On Investment' (ROI). ROI is door Purser gedefinieerd als: "It is a measure of a company's ability to use its assets effectively to generate additional value."[163]

---

160 Koorn, e.a., 2004, p. 47-56.
161 Koorn, e.a., 2004, p. 47.
162 Koorn, e.a., 2004, p. 47-48.
163 Purser, 2004, p. 542.

Cardholm merkt hierover op dat:

> "Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It is also known as return on capital employed. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options."[164]

Er zijn verschillende versies van de ROI-formule en dat leidt tot verschillende interpretaties van de verkregen resultaten. De meest gangbare formule is:

$$ROI = \frac{nettoopbrengsten}{totale\_kosten} \bullet 100\%$$

Netto-opbrengsten staat voor opbrengsten verminderd met kosten, terwijl onder totale kosten wordt verstaan de initiële, lopende en de terugkerende kosten. ROI wordt doorgaans over het eerste jaar van de investering berekend, omdat in het bedrijfsleven als standaard geldt dat ondernemingen investeringen in het eerste jaar proberen terug te verdienen.[165] Zelfs bij een positieve business case, zullen PET-investeringen met andere bedrijfsprojecten moeten concurreren. Als geen financiële middelen of personeel beschikbaar zijn of als het management geen tijd kan vrijmaken om in PET te investeren, kan dit remmend werken. Of een PET-project hoog op de lijst van prioriteiten eindigt, hangt af van het relatieve belang dat het management aan het PET-project hecht. Het management zal daarbij een kosten-batenafweging moeten maken, want: "To maximize the expected benefit from investment to protect information, a firm should spend only a small fraction of the expected loss due to a security breach."[166]

7.14. Return On Security Investment (ROSI)

De beslissing om middelen te besteden aan privacybescherming dient financieel onderbouwd te zijn. Het heeft geen zin om een kostbare oplossing in de organisatie in te voeren, als een minder dure oplossing net zo'n goede privacy-bescherming biedt. De kosten dienen ook niet hoger te zijn dan de opbrengsten van de investering. Volgens Lucas zijn er vele verschillende methoden om de economische waarde van informatie beveiligingsuitgaven te berekenen, maar: "For the most part ROI (Return on Investment), NPV (Net Present Value), and IRR (Internal Rate of Return) are the standards."[167] De ROI-berekening geniet een hoge populariteit onder economen. Perks stelt dat:

---

164 Cardholm, 2006, p. 20.
165 Cardholm, 2006, p. 21.
166 Gordon & Loeb, 2004, p.105.
167 Lucas, 2005, p. 2.

> "Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options."[168]

Bij gebrek aan empirische gegevens over investeringen in privacybescherming, moet naar een analoge situatie in de informatiebeveiliging gekeken worden. Een gangbare economische formule om de waarde van een investering in informatiebeveiliging te evalueren is Return On Security Investment (ROSI). De ROSI-berekening is ontwikkeld door een groep onderzoekers van de Universiteit van Idaho onder leiding van Hua Qiang Wei.[169] ROSI is een benadering om het effect van de IT-investeringskosten op het verminderen van het beveiligingsrisico te beoordelen. Cardholm stelt: "it is basically a 'savings' in Value-at-Risk; it comes by reducing the risk associated with losing some financial value".[170]

Drie kernelementen zijn bepalend voor de rendementsberekening van de investering, te weten kosten, opbrengsten en niet-financieel meetbare elementen.[171] Een organisatie kan met ROSI de beveiligingsrisico's en de kosten die verbonden zijn aan het oplossen van de risico's analyseren. Wanneer ROSI aangeeft dat de investering lonend is, kan de organisatie besluiten de investering uit te voeren.

De ROSI-formule is als volgt:

$$Rosi = \frac{(RiskExposure * RiskMitigated) - SolutionCosts)}{SolutionCost}$$[172]

Met 'Risk Exposure' (blootstelling aan risico)[173] wordt bedoeld het bedrag dat een organisatie kwijt is (schade) wanneer het te maken krijgt met een beveiligingsrisico (zoals bijvoorbeeld een computervirus). Dit bedrag wordt vermenigvuldigd met het percentage waarmee het risico afneemt met behulp van de investering, die daarvoor een oplossing biedt. De kosten van de investering die de oplossing voor de risicovermindering bewerkstelligt, worden vervolgens van het verkregen resultaat afgetrokken.[174] Anderson merkt op dat "Security ROI may be about 20% per annum."[175] In paragraaf 4.7 is risico al in technische zin aan de orde geweest. Hier gaat het erom risico te kwantificeren. Daar zou de volgende formule voor gebruikt kunnen worden. Het risico dat een organisatie loopt (r) is de waarschijnlijkheid van een gebeurtenis (in casu het beveiligingsincident) (p) vermenigvuldigd met de

168 R.Perks, 2004, p. 381-384.
169 L. Cardholm, 2006, p. 26.
170 L. Cardholm, 2006, p. 26.
171 K. Matthijssen, 2006, p. 14.
172 W. Sonnenreich, 2006, p. 1. De punt staat voor vermenigvuldiging.
173 P.A. Strassmann, 1990, p. 217: " (...) risk analysis is the correct analytic technique with which one can examine the uncertainty of information technology investment prior to implementation."
174 Peekel, 2006, p. 28.
175 Anderson, 2004, p. 19.

schade (e), dus: r = p × e. Zuccato wijst erop dat "we cannot assume that the probability of the risk is simply the product of probabilities: we need a Bayesean probability function."[176] Het is praktisch gezien niet mogelijk om in deze wiskundige formule de inputwaarden van het aantal waarschijnlijkheden te geven, omdat de waarschijnlijkheden exponentieel toenemen met het groot aantal scenario's in de actuele omstandigheden. Met één mogelijke gebeurtenis met waarschijnlijkheid (p) is er nog wel een berekening te maken, maar dat is een verregaande vereenvoudiging, die de berekening onbetrouwbaar maakt.

'Risk Exposure' kan als synoniem van het begrip 'Annual Loss Expectancy' (ALE), het verwachte jaarlijkse verlies, gezien worden.[177] Het is volgens Fairchild & Ribbers: "One of the most common measures for assessing the risk of a harmful event."[178] ALE kan weer uitgesplitst worden in SLE vermenigvuldigd met ARO, zodat voor 'Risk Exposure' geschreven kan worden:

Risk Exposure = ALE = SLE × ARO[179]

SLE staat voor 'Single Loss Exposure': de werkelijke kosten van een beveiligingsincident per voorval. ARO (Annual Rate of Occurrence) betreft de frequentie van een beveiligingsincident per jaar. Het bepalen van de werkelijke kosten van een beveiligingsincident is erg moeilijk, temeer daar maar erg weinig organisaties zulke incidenten rapporteren. Cardholm merkt op, dat:

> "A security investment is judged to be profitable, if the risk mitigation effect is greater than the expected costs. The formula helps for decisions about one investment, not setting priorities in more alternatives, because it lacks the relation to the capital employed. As a result, the marginal cost of security is in the hand of the decision maker."[180]

De ROSI-formule zou in beginsel 'mutatis mutandis' ook gebruikt kunnen worden voor investeringen in PET-applicaties. Er zijn wel een aantal voorwaarden. De organisatie moet op de hoogte zijn van de (frequentie van de) privacyincidenten, waarbij zij betrokken was. Ook moet de organisatie een privacybedreigings- of risicoanalyse (PIA) (zie paragraaf 4.8) hebben uitgevoerd om de privacyrisico's vast te stellen. Bovendien moet de organisatie kunnen inschatten wat de kosten kunnen zijn als de risico's niet worden afgedekt en hoeveel de investering zal bedragen om het risico te verminderen. Het probleem met het begrip SLE is dat er weinig (gestandaardiseerde) empirische gegevens over de kosten van privacyincidenten bekend zijn. Datzelfde geldt overigens ook voor beveiligingsincidenten. Sonnenreich schrijft daarover: "there is no 'standard' model for determining the financial risk associated with security incidents.

176 Zuccato, 2004, p. 229.
177 Lucas, 2005, p. 8.
178 Fairchild & Ribbers, 2008, p. 92.
179 Dijkman, 2008, p. 32.
180 Cardholm, 2006, p. 27.

Likewise, there are also no standardized methods for determining the risk mitigating effectiveness of security solutions. Even methods for figuring out the cost of solutions can vary greatly. Some only include hardware, software and service costs, while others factor in internal costs, including indirect overhead, and long-term impacts on productivity".[181]

Daar komt nog bij dat de schade (materieel en immaterieel) die door een privacyincident ontstaat, zowel voor een individu als voor een organisatie (op de korte termijn) moeilijk is vast te stellen.[182] Boer & Grimmius menen, dat:

> "Burgers kunnen op verschillende manieren schade lijden: Financiële schade door verlies van creditcard- of pinpasgegevens, wachtwoorden en toegangscodes voor internetbankieren; Imagoschade of chantage door het bekend worden van gevoelige informatie over bijvoorbeeld religieuze, politieke of seksuele voorkeur; Fysieke schade, bijvoorbeeld diefstal of molest; en Identiteitsfraude, wanneer iemand anders zich voor de benadeelde burger uitgeeft. De fraudeur heeft niet alleen toegang tot diens gegevens maar kan ook op diens kosten goederen en diensten afnemen of zelfs criminele activiteiten ondernemen onder zijn slachtoffers naam. Identiteitsfraude 'kan overal en op velerlei manier plaatsvinden en is niet beperkt tot specifieke situaties procedures of documenten."[183]

De kosten van PET-maatregelen zijn wel te kwantificeren, maar over het algemeen zal het niet direct duidelijk zijn hoe de PET-investering bijdraagt aan een vermindering van de bedrijfskosten door een verbeterde 'workflow', bedrijfsprocessen of verbetering van de reputatie. Doordat ervaringsfeiten ontbreken is het ook moeilijk te bepalen met hoeveel procent PET-maatregelen het privacyrisico verminderen. Het is mogelijk dat er niet-financieel meetbare baten en kosten zijn. Dat zou een probleem binnen de analyse van het rendement van investeringen in PET kunnen opleveren. Andere gangbare formules die gebruikt worden om het rendement van een investering in informatiebeveiliging te berekenen, kampen met het probleem van de niet-financieel meetbare opbrengsten en kosten.[184] Om een investering in PET te analyseren is het daarom belangrijk om zoveel mogelijk opbrengsten en kosten financieel meetbaar te maken.

In hoofdstuk 2 heb ik al aangegeven, dat het een goede zaak zou zijn, als organisaties wettelijk verplicht worden privacyincidenten en daarbij behorende schadeclaims te rapporteren aan de nationale toezichthouder voor de bescherming van persoonsgegevens. Verplichte rapportage en registratie zorgt ervoor dat de privacyinbreuken worden gemeld. Een dergelijk register maakt het mogelijk dat bekend wordt welke bedrijven privacyonveilig werken. Ook zullen hierdoor de schadecijfers betrouwbaarder worden waardoor privacyrisico's in het vervolg

181 Sonnenreich, 2006, p. 2.
182 Sonnenreich, Albanese & Stout, 2006, p. 45-56.
183 Boer & Grimmius, 2009, p. 26.
184 Matthijssen, 2006, p. 25-32.

beter kunnen worden ingeschat door degenen, die verantwoordelijk zijn voor de gegevensverwerking.[185]

Omdat gegevens over Europese privacyincidenten ontbreken, zijn in het kader van deze dissertatie in 2007 en 2008 interviews gehouden met verschillende Europese organisaties. Op basis van deze interviews konden cijfers worden verzameld over privacyincidenten en over de investeringen die deze organisaties hadden gedaan in privacybescherming. De bedoeling van de interviews was onder meer om na te gaan of het voor andere organisaties financieel zinvol zou kunnen zijn om in PET te investeren. In de Verenigde Staten worden inmiddels dergelijke gegevens sinds 2003 bij de 25 grootste bedrijven verzameld. Het onderzoeksbureau van Ponemon[186] doet jaarlijks onderzoek naar de werkelijke kosten van privacyincidenten in de Verenigde Staten. Het onderzoek wijst uit dat de gemiddelde kosten van een privacyinbreuk $ 6,3 miljoen bedragen, met als laagste bedrag $ 225.000 en als hoogste $ 35 miljoen.

7.15. De PET Business Case van Ixquick

Doordat Ixquick besloot onder meer te investeren in de PET-maatregel 'anonimiseren van IP-adressen' (zie paragraaf 6.5.1), gingen aanzienlijk meer mensen gebruikmaken van de zoekmachine met als gevolg dat de omzet van het bedrijf navenant steeg.[187] De reden van het management om PET te gebruiken was dat privacybescherming een zeer sterk marketingargument is ('Unique Selling Point'). Door deze PET-maatregelen werd Ixquick de eerste volledig geanonimiseerde metazoekmachine. Er waren geen andere redenen voor de eigenaren van Ixquick om PET te gebruiken.[188] Volgens Ixquick leverde anonimisering verder geen extra zakelijke voordelen op. Integendeel, de beslissing om PET in te zetten, maakte daarop volgende bedrijfsbeslissingen alleen maar ingewikkelder, omdat het management van Ixquick bij elk nieuw besluit rekening moest houden met de eerdere anonimiseringsbeslissing.[189] In de periode december 2005 tot juni 2006 bedroegen de investeringskosten in PET voor Ixquick € 45.300. In 2007 deed het bedrijf aanvullende investeringen van € 39.500 om het anonimiseringsproces te verbeteren.[190] In 2008 waren extra investeringen nodig om de privacybescherming en daarbij behorende beveiliging te optimaliseren en te voldoen aan de eisen van het EuroPrise-certificaat voor privacybescherming.[191] De uitgaven hiervoor

185 Wright, 2008, p. 218.
186 Ponemon, 2007.
187 Van Eesteren & Borking, 2008, p. 5.
188 Het EuroPrise evaluatie-onderzoek maakte voor het eerst de omvang van de privacyrisico's duidelijk (zie hoofdstuk 6).
189 Dijkman & Borking, 2008, p. 13.
190 Dijkman & Borking, 2008, p. 13.
191 Het project wordt gesubsidieerd door de Europese Commissie onder het eTEN Programma. Het EuroPrise-project begon op 10 juni 2007 en is 28 februari 2009 beeindigd. Zie: http://www.european-privacy-seal.eu/about-europrise/fact-sheet.

bedroegen € 37.000 inclusief de kosten voor technisch en juridisch advies. Voor de gemaakte pers- en communicatiekosten in verband met het verkrijgen van de Europrise certificaat werd € 8.000 uitgegeven.[192] Al deze kosten waren eenmalig en exclusief btw. Daarnaast zijn er echter ook terugkerende kosten voor het onderhoud van de meta zoekmachine. Deze bedragen € 16.500 per jaar. De totale investeringskosten voor PET bedroegen van 2005 tot 2008: € 179.300. [193] Als Ixquick niet in de PET-maatregelen had geïnvesteerd, dan zou volgens het management de opbrengsten jaarlijks ten minste met 5% lager zijn.[194] De genomen PET-maatregelen bij Ixquick hebben ook geleid tot een aanzienlijke vermindering van het risico op privacyincidenten. Om het verminderde risico te berekenen, is gebruikgemaakt van de calculator van Darwin (2008).[195] Daarbij is ervan uitgegaan dat als gevolg van een privacyinbreuk bij Ixquick 10.000 persoonsgegevens (IP-adressen, tijdstippen en zoekvragen e.d.) gestolen zouden kunnen worden.[196] In een vergelijkbaar geval werden bij AOL in 2006 de IP-adressen en zoekvragen van 650.000 personen gestolen. In sommige van die zoekopdrachten kwamen het 'social security'-nummer en het creditcardnummer voor.[197] De schade die AOL door deze privacyinbreuk heeft opgelopen is nog niet bekend, maar volgens de informatie op de website van de Darwin-calculator bedraagt de geëiste schade per persoon $ 1.000. De juridische en andere kosten zijn daarin niet begrepen.

Voor Ixquick ben ik op grond van de parameters (verlies van 10.000 bestanden) in de 'Darwin-calculator voor e-commerce business' uitgegaan van € 1.050.300 als verminderd risico. Hierbij heb ik rekening gehouden met de wisselkoers van de Amerikaanse dollar ten opzichte van de euro (november 2008). Het hiervoor vermelde bedrag wordt vermeld bij het minus 20% niveau van de calculator van Darwin. Op de website staat over de calculator vermeld: "Darwin created the Tech//404® data loss cost calculator as a tool to demonstrate the scope of negative financial impact an organization may face as a result of a data breach or identity theft data loss scenario. The calculator will automatically generate an average cost, and a plus/minus 20% range, for expenses associated with internal investigation, notification/crisis management and regulatory/compliance if the incident were to give rise to a class action claim."

Er is van een potentiele schade van 80% uitgegaan, omdat Ixquick kleiner is dan AOL, waardoor de potentiële reputatieschade ook kleiner is. Met deze gegevens kan een rendementsberekening gemaakt worden. Voor de rendementsberekening van de investering voor privacybescherming (Return On Investment of

192 Andriessen, 2008, p. 10.
193 Borking, 2008, p.1.
194 Dijkman & Borking, 2008, p. 13.
195 De calculator van Darwin kan gevonden kan worden op www.tech-404.com/calculator.html.
196 Het aantal dagelijkse gebruikers van de Ixquick meta search engine is vertrouwelijk.
197 Leyden, 2006. Zie ook http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/ met een overzicht van de zoekgegevens.

Privacy Investments, hierna te noemen ROI-PI,[198] is door mij gebruikgemaakt van een van berekeningsmethode, die is afgeleid van de ROI-dashboardformule van Pisello.[199] Deze formule maakt gebruik van een risico-aangepast ROI, dit wil zeggen dat het rendement van een investering wordt aangepast naarmate het risico van een project hoger ligt.[200] Volgens Matthijsen, die alle bekende rendements-modellen voor informatiebeveiliging heeft onderzocht, is het ROI-dashboard van Pisello (2001) een betrouwbaar model. Bij dit model wordt samen met een risicoanalyse aangegeven hoe het rendement van een investering bepaald zou kunnen worden met behulp van financieel meetbare (V_q) en niet-financieel meetbare voordelen (V_nq), de waarde van het vermeden risico (R), en de totale kosten van de investering (T).[201]

De ROI-PI-formule is als volgt: $ROIPI = \frac{V_q + V_n q + R - T}{T} \bullet 100\%$

Gezien de hiervoor gesignaleerde moeilijkheden met de niet-financieel meetbare kosten en opbrengsten zijn bij de ROI-PI-berekening voor Ixquick deze kosten in onderstaande ROI-PI-formule buiten beschouwing (€ 0) gelaten.

Dit leidt tot de volgende rendementsberekening voor de PET-investeringen:

Financieel meetbare voordelen: € 340.800
Niet-financieel meetbare voordelen: € 0
Totale kosten van PET-investering: € 179.300
Waarde van het vermeden risico: € 1.050.300

Bij gebruik van deze getallen in de ROI-PI-formule leidt dit tot:

$$ROIPI = \frac{340.800 + 0 + 1.050.300 - 179.300}{179.300} \bullet 100\% = 675,85\%$$

Dit betekent dat het meetbare voordeel bijna zeven keer groter is dan de PET-investeringen. De niet-financieel meetbare kosten en opbrengsten zijn PM gewaardeerd, maar als die berekenbaar zouden zijn, dan is het resultaat nog gunstiger. De ROI-PI-waarde is hier significant genoeg om de PET-investering uit te voeren c.q. bedrijfseconomisch te rechtvaardigen. Tegengeworpen kan worden dat de ROI-PI-waarde zo hoog is, omdat de waarde van het vermeden risico hoog is.[202] In de ROI-PI-berekening is het risico gezien de hoeveelheid dagelijkse bezoekers (het werkelijke aantal is vertrouwelijk) van Ixquick zeer laag ingeschat. Zelfs als de waarde van het vermeden risico € 0 is, dan blijkt de

198 Fritsch & Dijkman waren de eersten die in 2007 de afkorting ROPI gebruikten. Accountants vonden ROPI te verwarrend en adviseerden mij een andere afkorting.
199 Pisello, 2001. De formule is beschikbaar via: http://searchcio.techtarget.com/searchEBusiness/downloads/ROIforITFirstEd.pdf.
200 Matthijssen, 2006, p. 29.
201 Matthijssen, 2006, p. 31-32.
202 Dijkman, 2008, p. 52.

investering reeds de moeite waard, omdat de investeringen die noodzakelijkzijn voor het pakket aan PET-maatregelen in de periode 2005-2008 voor 90,07% al zijn terugverdiend en het voorzienbaar is dat in de loop van de komende jaren de opbrengsten de investering zullen overtreffen. Gezien het feit dat financiële overwegingen een belangrijke rol spelen in de aanschaf van PET zou een gestandaardiseerde ROI-PI-formule door accountants bij een rendementsberekening van PET als een 'quick and dirty' schatting voor organisaties die investeringen in privacybescherming overwegen, kunnen worden toegepast. Onderzoekers in het PRIME-project menen nochtans, dat:

> "organizations should discard the above equations and instead use discounted cash flow methods for investments that have different costs and benefits in different years. The theoretical flaw in ROI (and so in ROSI and related approaches) is that it processes financial figures irrespective of the dates they will be received or paid. The value of 1 euro today is not the same as of 1 euro in two years time."[203]

Een 'discounted cash flow'-methode, zoals 'Net Present Value', leidt tot meer nauwkeurige uitkomsten.[204]

7.16. Net Present Value

De 'Net Present Value' of netto contante waarde (NPV) van een project of een investering wordt gedefinieerd als de som van de verdisconteerde contante waarden van de jaarlijkse cashflows (kasstromen) verminderd met het bedrag dat aanvankelijk wordt geïnvesteerd. De jaarlijkse kasstroom bestaat uit de nettobaten (opbrengsten minus kosten) die tijdens de duur door de investering worden voortgebracht. In de cashflow worden de contante waarde van geld en het risico verdisconteerd. NPV is één van de meest robuuste financiële evaluatiehulpmiddelen om de waarde van een investering te schatten.[205]

De berekening van de netto contante waarde gaat als volgt:

1. Bereken de verwachte vrije cashflows per jaar, die uit de investering resulteren.
2. Trek af/verdisconteer de kosten van het kapitaal (een rentepercentage op basis van tijd en risico).
3. Trek de aanvankelijke investeringen af.

De berekening van 1 en 2 leidt tot de contante waarde.

In de berekening leidt (1-2) – 3 tot de NPV. NPV wordt in de volgende formules uitgedrukt:

---

203 Ribbers, e.a., 2008, p. 28.
204 Cardholm, 2006, p. 20.
205 Cardholm, 2006, p. 20.

NPV = Initiële investering + (cashflow jaar 1 / (gedeeld door (1+r)1) + … (cashflow jaar **n** / (gedeeld door) (1+r)n), of:

$$NPV = i + \Sigma_{t=1}^{t=eindevanhetproject} \frac{cf_t}{(1+r)^t}$$

1. Initiële investering (*i*): Dit is de investering die aan het begin van het project wordt gemaakt. De waarde is gewoonlijk negatief, aangezien de meeste projecten vereisen dat er eerst geld uitgegeven wordt. De aanvankelijke investering kan hardware, softwarelicentie bedragen, en startkosten omvatten.
2. Cashflow (*cf*n): De netto cashflow voor het jaar **n** van het project: dat wil zeggen de baten minus de kosten.
3. Rate of Return (r): Het 'winst'percentage wordt berekend door de investering te vergelijken met alternatieven die dezelfde risico's dragen. Het winstpercentage wordt vaak aangeduid als 'discount', rente, 'hurdle rate', of kapitaalskosten. Bedrijven gebruiken vaak een standaardtarief voor een investeringsproject, dat overeenkomt met het gemiddeld risico dat het bedrijf loopt.
4. Tijd (*t*): Dit is het aantal jaren dat het project gaat duren.

Als de NPV resulteert in een getal groter dan of gelijk aan nul, dan is de investering vanuit financieel perspectief gerechtvaardigd. Cardholm stelt dat:

> "If the NPV is less than zero, the project will not provide enough financial benefits to justify the investment, since there are alternative investments that will earn at least the rate of return of the investment".[206]

Fairchild & Ribbers[207] hebben voor de rendementsberekeningen van PET-investeringen aan de gangbare NPV-formule een aantal componenten toegevoegd. Naast de gebruikelijke elementen als Initiële investering (I(p)), en de jaarlijks terugkerende cashflow zijn dat: Annual Loss Exposure (ALE), Reputation Recovering Costs (RRC), Expected Revenue Accrual (ERA) en Recurring Privacy Costs (RPC). Bij initiële investering [I(p)] gaat het om bedragen die betaald moeten worden voor de privacybedreigings- of risicoanalyse (PIA), het analyseren en modelleren van de bedrijfsprocessen, de aankoop en implementatie van PET-applicaties, productiviteitsverlies, en 'change management'.

De jaarlijks terugkerende 'cashflow', bevat alle financiële effecten van het voorstel die jaarlijks optreden. In deze berekening wordt tevens gekeken naar het verschil in de 'cashflow'-patronen die optreden wanneer de investering wordt gedaan en wanneer deze niet plaatsvindt. Bij het laatste gaat het dan om het handhaven van de bestaande situatie. ALE is al in paragraaf 7.14 aan de orde

206 Cardholm, 2006, p. 21.
207 Fairchild & Ribbers, 2008, p. 92.

geweest. Het betreft de verwachte kosten van een privacyincident en de frequentie van zulke incidenten binnen een jaar. De veroorzaakte kosten zijn omzetverliezen, productiviteitsverlies door privacyinbreuken, reparatiekosten, gemiste orders en schadeclaims. Als voorbeeld kan dienen de toegekende schadevergoeding wegens geleden immateriële schade van 150 gulden per persoon, die door het Ambtenarengerecht in de Ohra-zaak[208] werd vastgesteld. Maar dat is niet de enige schade die door een organisatie geleden kan worden. Zo kunnen privacyinbreuken na een rechterlijke uitspraak leiden tot de geforceerde aanpassing van (de programmatuur van) het informatiesysteem, bijvoorbeeld als het informatiesysteem niet voorziet in de mogelijkheid om inzage te krijgen in de eigen persoonsgegevens. De kosten hiervan moeten niet onderschat worden en kunnen in de honderdduizenden euro's lopen. RCC zijn de uitgaven die gemaakt moeten worden om de reputatie van de organisatie te herstellen, die door een privacyinbreuk is ontstaan. Het betreffen doorgaans PR- en marketinguitgaven. Uit de Double Click Inc.-zaak in de Verenigde Staten (2000-2001) kan worden vastgesteld welke reputatieschade een bedrijf kan oplopen, waaronder een lagere aandelenkoers, die zich overigens gedeeltelijk herstelde toen de FTC (US Federal Trade Commission) haar onderzoek staakte naar de manier waarop het bedrijf persoonsgegevens verzamelde.[209] Op de dag dat publiek werd dat persoonsgegevens gestolen waren, kelderden ChoicePoint's koersen van $ 47,95 naar $ 36,35 (de koers op de dag dat de eerste rechtszaak begon).[210] Een lagere aandelenkoers van een bedrijf kan banken doen besluiten van het bedrijf additionele financiële zekerheden te eisen. ERA geeft de gevolgen weer op het marktaandeel en omzet als gevolg van het publiek maken van het feit dat het bedrijf in PET-maatregelen heeft geïnvesteerd. RPC bevat de jaarlijkse (additionele) privacyuitgaven, die door de PET-investering worden veroorzaakt, zoals de privacybedreigings- of risicoanalyse, privacyaudits, de kosten voor een functionaris gegevensbescherming etc.[211] Dit leidt tot de volgende NPV-formule[212] voor PET-investeringen:

$$NPV = -I(p) + \Sigma_{j=1}^{n} \frac{(ALE + RRC)RM + ERA - RPC}{(1+i)^j}$$

Ribbers merkt hierbij op, dat:

> "the analysis compares the project situation with the situation without the project. Basically this comes down to analyze the cashflow differences between the two situations. This can be done either by applying a factor RM (Risk Mitigated) to the situation without the investment or by subtracting the full-expected cash flow of the two situations from one another. The RM factor for the applied privacy risk reducing/protection solution indicates what part of ALE and RRC has

208 Ambtenarengerecht Amsterdam, 4 februari 1992, TAR 1992, 83 en CRvB 21 oktober 1993, TAR 1993, 249.
209 www.news.com/DoubleClick-climbs-after-privacy-probe-ends/2100-1023_3- 251364.html?tag=st.rn.
210 www.nyse.com onder double click.
211 Buitelaar & Borking, 2005, nr. 1.
212 Ribbers, 2008, p. 33.

been compensated by the solution. Mitigated Risk is expressed as a reduction of the expected number of privacy breaches per year."[213]

De bovenstaande NPV-formule voor PET-investeringen is toegepast op in paragraaf 6.8 besproken 'Victim Tracking and Tracing System' (ViTTS)-casus. De PET-investeringen waren € 1.800.000. De voordelen voortvloeiende uit de risicovermindering werden geschat op € 2.277.000. Uitgegaan werd van een periode van zes jaar, een privacyincident dat elke twee jaar plaatsvindt en kapitaalkosten van 5%. De NPV-berekening gaf als resultaat een ROI van 143,53%.[214] Daarmee stond de positieve business case voor de PET-investeringen in ViTTS vast.

7.17. Samenvatting

Ondanks de aantoonbare technische haalbaarheid van PET-maatregelen zoals in hoofdstuk 6 besproken, maken organisaties nog vrijwel geen gebruik van PET, maar vertrouwen zij voornamelijk op klassieke organisatorische en technische informatiebeveiligingsmaatregelen. In dit hoofdstuk is zesde onderzoeksvraag onderzocht (OV 6): *Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?*

Het blijkt dat een groot aantal factoren organisaties beïnvloeden bij hun beslissing om wel of niet PET toe te passen. Positieve factoren stimuleren de toepassing van PET en negatieve factoren zijn duidelijke belemmeringen om PET te implementeren. De overheid, die zich in de motie Nicolaï verplicht wordt om het voortouw te nemen bij het inzetten van PET in hun eigen gegevensverwerkende en gegevensdragende systemen, zoals bijvoorbeeld het elektronisch patiëntendossier, biometrie in het paspoort, het kinddossier, de ov-chipkaart en de kilometerheffing, past PET structureel niet toe. Dit is het gevolg van het gebrek aan politieke wil en gebrek aan voldoende kennis over de voordelen die PET bij privacybescherming kan bieden. Volgens het Rand Europe onderzoek (zie paragraaf 7.2) is er sprake van een vicieuze cirkel ten gevolge van de opvatting: zolang PET zich niet hebben bewezen, acht de overheid het risico van mislukking te groot; zolang men het risico te groot vindt, worden PET niet toegepast en kunnen PET zich niet bewijzen. Hoofdstuk 6 heeft nochtans aangetoond dat PET zich in vele systemen als betrouwbaar hebben bewezen. Uit het onderzoek naar de adoptiefactoren voor PET blijkt, dat de druk van de wet- en regelgeving en met name van de toezichthouders belast met de bescherming van persoonsgegevens ('data protection authorities') een positieve invloed hebben op de beslissing van organisaties om PET-maatregelen te nemen.

---

213 Ribbers, 2008, p. 34.
214 Ribbers, 2008, p. 35-37.

Aangetoond is dat om PET in een organisatie te kunnen implementeren het noodzakelijk is dat binnen de organisatie structureel 'identity and access management' (IAM) wordt toegepast. Immers, zonder IAM-processen is het niet mogelijk het gebruik van en de toegang tot (gevoelige) persoonsgegevens te controleren. Bovendien is een bepaald maturiteitsniveau van de betreffende IAM-processen noodzakelijk. Het is zeer onwaarschijnlijk dat onvolgroeide organisaties overgaan tot implementatie van PET. De S-curven voor IAM, de maturiteit van organisaties, privacybescherming en voor PET zelf, geven een indicatie waarom de meeste organisaties pas in een relatief laat stadium besluiten om PET-maatregelen toe te passen om persoonsgegevens adequaat te beschermen. Het vermijden van reputatieschade is een stimulans om PET-maatregelen te nemen.

Nochtans zijn de kosten een belangrijke negatieve factor voor de adoptie van PET. Goede businessmodellen met betrekking tot PET-investeringen kunnen een positieve invloed hebben om in PET te investeren. Dergelijke modellen ontbreken. In dit hoofdstuk is een aantal methoden voor investeringsberekeningen besproken. De 'return on investment-formules' voor PET-investeringen (o.a. ROI-PI) en net present value (NPV) -berekening ondersteunen de economische rechtvaardiging om in PET te investeren en doen voor een belangrijk deel de negatieve adoptiefactor 'kosten' teniet. De kwantificeerbare gegevens kunnen de managementbeslissing ondersteunen om PET-maatregelen te nemen. Empirische gegevens over privacyincidenten zijn in de Europese Unie niet beschikbaar, waardoor de consequenties van dergelijke incidenten niet accuraat kunnen worden ingeschat en de rendementsberekeningen van PET-investeringen onvolledig of onnauwkeurig kunnen zijn. Een verplichte bekendmaking en registratie van verlies of diefstal van persoonlijke informatie, zoals voorzien in het wijzigingsvoorstel van de Richtlijn 2002/58/EG, zal ervoor zorgen dat dergelijke gegevens wel beschikbaar worden.[215]

Samenvattend: uit het onderzoek waarover in dit hoofdstuk is gerapporteerd kan als antwoord op de zesde onderzoeksvraag (OV 6) gegeven worden, dat er belangrijke belemmeringen bestaan om PET grootschalig te implementeren, maar het onderzoek geeft ook aan dat er positieve adoptiefactoren zijn die de belemmeringen kunnen opheffen en de implementatie van PET zelfs kunnen stimuleren. Daar dient gebruik van te worden gemaakt. In het volgende hoofdstuk zullen aanbevelingen voor het invoeren van privacyveilige informatiesystemen worden gedaan.

215 www.europarl.europa.eu/sides/get Doc.do?pubRef_//EP//TEXT + TA + P6_TA_2008_0452 + 0 + Doc + xml + Vo//En & Language_ En.

8. Slotbeschouwingen en aanbevelingen

"Gutta cavat lapidem, consumitur anulus usu",[1]
P. Ovidius Naso, Epistulae Ex Ponto, Liber 4, 10, 5.

De probleemstelling van dit proefschrift luidt: *Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker?*[2]

Om de probleemstelling te beantwoorden zijn zes onderzoeksvragen gesteld. Deze luiden:

OV 1: Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacywet- en regelgeving worden afgeleid?

OV 2: Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding?

OV 3: Met welke privacybedreigingen en -risico's moeten de burger en de ontwerper van systemen rekening houden?

OV 4: Wat houdt het concept Privacy Enhancing Technologies (PET) in?

OV 5: Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen?

OV 6: Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?

In de voorafgaande hoofdstukken heb ik geprobeerd een antwoord te geven op deze onderzoeksvragen. De samenvattende beantwoording van onderzoeksvragen OV 1 tot en met OV 6, geschiedt in de paragrafen 8.1 tot en met 8.3. Een antwoord op de probleemstelling wordt in paragraaf 8.4 gegeven. In de paragrafen

---

1 De druppel holt de steen uit, een ring verslijt door het gebruik. De meer bekende variatie hiervan afgeleid is: Gútta cavát lapidém non ví, sed sáepe cadéndo: de druppel holt de steen uit, niet door zijn kracht maar door gestadig te vallen.

2 Verantwoordelijke en bewerker zijn in artikel 1 onder d, respectievelijk onder e gedefinieerd. Zie voor nadere uileg hoofdstuk 2.6 en 2.7 van dit boek.

8.5 tot en met 8.8 volgen acht aanbevelingen gericht aan de overheid (het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Ministerie van Justitie), de Data Protection Authorities (het College bescherming persoonsgegevens) en de verantwoordelijken (zoals gedefinieerd in 95/46/EG), en de Europese wetgever.

Op grond van de vaststelling van de positieve adoptiefactoren worden in paragraaf 8.5 vier aanbevelingen gedaan met betrekking tot de voorlichting, de rol van de toezichthouder, de oprichting van een PET-expertisecentrum en de multi-actoranalyse. In paragraaf 8.6 volgt het stappenplan om een privacyveilig informatiesysteem in een organisatie te implementeren. In paragraaf 8.7 wordt het belang van een positieve business case voor het invoeren van PET-maatregelen benadrukt. Hierna volgen in paragraaf 8.8 aanbevelingen aan de wetgever om de EU-privacyrichtlijnen in verband met de technologische ontwikkelingen aan te passen. In paragraaf 8.8.1 zijn vier algemene aanbevelingen gedaan om de Richtlijn 95/46/EG te actualiseren. In paragraaf 8.8.2 wordt voorgesteld de verantwoordelijke manager voor de gegevensverwerking binnen de organisatie persoonlijk aansprakelijk te stellen bij privacyinbreuken. In paragraaf 8.8.3 volgen vier voorstellen voor wetsaanpassingen om in aanvulling op het beveilingsvereiste in arikel 17 'privacy by design'[3] als verplichting in de Richtlijn 95/46/EG op te nemen, te weten:

1. De privacybedreigingsanalyse en/of de privacy impact analyse (PIA) moet voor de verantwoordelijke verplichtend worden.
2. Het gebruik van PET moet worden voorgeschreven ('by default');
3. Burgers moeten standaard de optie krijgen om diensten en infrastructuren anoniem te kunnen gebruiken.
4. Als ontwerpvereiste dient door de wet voorgeschreven te worden dat in het informatiesysteem controlemogelijkheden en terugkoppeling voor de burgers zijn ingebouwd. Op die manier kan net zoals met een veilige auto aan het verkeer worden deelgenomen, de burger veilig zijn persoonsgegevens aan de verantwoordelijke overdragen en veilig deelnemen aan het interactieve verkeer op onze informatiesnelwegen.

In paragraaf 8.9 wordt het boek afgesloten door terug te keren naar het beginpunt van deze dissertatie, namelijk de titel van dit boek, 'Privacyrecht is code', die gebaseerd is op Lessig's uitspraak 'law is code'. Ik bepleit hierin om de stelling van Lessig voor het privacyrecht om te draaien en de juridische specificaties onderdeel te laten zijn van de programmacode van het gegevensverwerkend informatiesysteem. Daardoor wordt 'privacy law is code', opdat de burger erop

3 De term 'privacy by design' is vaag en open voor interpretaties omdat het niet gedefinieerd is. Er wordt mee bedoeld dat privacybescherming als onderdeel in ict-applicaties dient te worden ingebouwd. Het conceptontwerp WP168 over 'the future of privacy' formuleert het als: "Privacy by design should call for the implementation of data protection in ICT designated or used for the processing of personal data. It should convey the requirement that ICT should not only maintain security but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed."

kan (blijven) vertrouwen dat bij verwerking door informatiesystemen zijn persoonsgegevens optimaal beschermd zijn en privacyinbreuken worden voorkomen.

8.1. Ingebouwde wetgeving om het vertrouwen van de burger te bevorderen

Zoals uit de omgevingsanalyse in hoofdstuk 1 blijkt, is de noodzaak om persoonsgegevens te beschermen groot. Technologische ontwikkelingen maken het praktisch onmogelijk om aan het moderne leven deel te nemen zonder elektronische sporen achter te laten en daarmee mogelijk de eigen privacy in gevaar te brengen. Dergelijke elektronische sporen kunnen zonder enig technisch probleem door de overheid en het bedrijfsleven worden opgeslagen, gekopieerd en geanalyseerd. Door de constante verbeteringen van de ict zal de opgeslagen informatie steeds nieuwe en meer diepgaande informatie opleveren. Wat opgeslagen is, blijft voor altijd beschikbaar. Informatiesystemen vergeten niets.

Bovendien gaat het bij de opslag van deze sporen tevens om een grote hoeveelheid gegevens waar de burger geen weet van heeft, zoals bijvoorbeeld opgeslagen camerabeelden. Doordat de informatiesystemen die ons omringen veelvuldig gegevens registreren en opslaan kan het individu onmogelijk bijhouden welke sporen hij achterlaat.[4]

In de probleemstelling: *hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker*? komt het begrip 'vertrouwen' voor.

Vertrouwen kan worden omschreven als de gedachten, de gevoelens, de emoties, of de gedragingen van het individu, die bij hem optreden, op basis van de algemene verwachting van het individu dat hij op de belofte, de mondelinge of schriftelijke mededeling van een ander individu of groep kan afgaan. Schilfgaarde & Nooteboom[5] geven twee definities van vertrouwen, namelijk:

1. Men is kwetsbaar voor het handelen van een ander maar verwacht dat niettemin, om welke reden dan ook, het 'wel goed zal gaan' (geen grote schade op zal leveren).
2. Men is kwetsbaar voor het handelen van een ander maar verwacht niettemin dat 'het wel goed zal gaan', ook al heeft de ander zowel de mogelijkheid als het belang om niet aan afspraken/verwachtingen te voldoen. Deze toevoeging is cruciaal, omdat beheersing er dan buiten valt, en het alleen nog maar gaat

4 Klüver, Peissl & Tennøe, 2006 p. 83.
5 Schilfgaarde & Nooteboom, Amsterdam 2009, p. 40-41.

om de redenen die verder gaan, zoals normen/waarden, empathie, identificatie, vriendschap, liefde.

Bij vertrouwen geeft het individu zijn directe controle over de omgeving en situatie op. Zo ook moet de gebruiker er op kunnen vertrouwen dat het informatiesysteem doet wat door de verantwoordelijke van het informatiesysteem wordt beloofd. In feite maakt het individu dat zijn persoonsgegevens afstaat, zich kwetsbaar om een bepaald doel te bereiken, bijvoorbeeld gebruik te maken van de aangeboden dienstverlening. Zoals in paragraaf 1.1.7 betoogd, doen wij dat dagelijks met een gerust hart, omdat wij ervan uitgaan dat anderen met wie wij een transactie doen in hun handelingen ons geen nadeel of schade zullen toebrengen. Omvangrijke Europese en nationale privacywetgeving moet er voor zorgen dat het vertrouwen van de burger niet wordt misbruikt. Het zijn deze rechtsregels die bepalen of de persoonsgegevens privacyveilig worden verwerkt. Het is belangrijk dat door middel van de privacywetten de rechtsorde effectief kan worden gehandhaafd. Het wettelijk kader zorgt er tevens voor dat de geleden schade kan worden verhaald en conflicten kunnen worden opgelost en beslecht.[6] Klüver, Peissl en Tennøe merken echter op:

> "Although privacy is highly appreciated in legal terms there seems to be little awareness of it among users, politicians and economical actors. (...) There is a great divide between the individuals and the professional parties on knowledge about possible usage and economical value of personal data."[7]

Het is voor het vertrouwen van het individu dus van het grootste belang dat privacywetgeving direct bij de overhandiging en verwerking van zijn persoonsgegevens een effectieve (dus niet alleen een theoretische) bescherming biedt. Rechtsregels zijn evenwel niet ter plekke 'self-executing'. Daarom is een eerste voorwaarde voor het bestendigen van het vertrouwen van de burger in de rechtmatige verwerking van zijn persoonsgegevens, dat de privacyrechtsregels het uitgangspunt van de ontwerper van het informatiesysteem zijn en dat deze rechtsnormen in het systeem worden ingebouwd. De rechtsnormen zijn dus een onderdeel van de ontwerpspecificaties van een informatiesysteem en na realisatie van het systeem in de programmacode opgenomen.

Het antwoord op de eerste onderzoeksvraag: *Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacy wet- en regelgeving worden afgeleid?* (OV 1) heeft na analyse van de privacy wetgeving zeven algemene juridische specificaties opgeleverd (zie paragraaf 6.2.1).

---

6 Klüver, Peissl & Tennøe, 2006, p. 84.
7

Deze zijn:

1. Beginselen die aan de basis van een privacyveilig systeem ontwerp ten grondslag liggen:
   a. gegevensminimalisatie (waar mogelijk streven naar maximale anonimiteit, zo min mogelijk gegevens en zo vroeg mogelijke verwijdering van data);
   b. transparantie of Openheid betreffende de verwerking;
   c. beveiliging aan de hand van en privacy risico, bedreiging of effect analyse.
2. Beginselen betreffende de rechtmatige verwerking:
   a. rechtmatigheid (bijvoorbeeld: toestemming);
   b. speciale categorieën persoonsgegevens;
   c. finaliteit, doelbinding en de te verwerken persoonsgegevens.
3. Kwaliteit van gegevens.
4. Rechten van het persoonsgegevens genererende individu:
   a. informatie vereisten o.a. over de verantwoordelijke;
   b. melding van de verwerking van persoonsgegevens;
   c. inzage, correctie, verwijdering, blokkering;
   d. verzet tegen verwerking.
5. gegevensverkeer met landen buiten de EU en EEA.
6. Specifieke restricties op bepaalde vormen van gegevens verwerking ex Richtlijn 2002/58/EG en speciale eisen uit de Richtlijn 2006/24/EG.

In paragraaf 6.9.1 is bij de bespreking van PISA aangetoond dat de juridische specificaties in de architectuur van PISA niet alleen kunnen, maar ook zijn geimplementeerd. PISA heeft gediend als voorbeeld voor privacy management-systemen, waar 'rule'systemen en privacy ontologieën ervoor zorgen dat in de software componenten de juridische specificaties geconverteerd zijn naar programmacode. De persoonsgegevens worden hierdoor (los van de bedreigingen) automatisch beschermd. Volgens Van Rooy en Bus[8] is er evenwel een belangrijke complicerende factor, namelijk dat informatiesystemen wereldwijd via netwerken met elkaar zijn verbonden en de gebruiker bij digitale communicatie en transacties die daaruit voortvloeien, te maken kan krijgen met een veelheid aan informatiesystemen. Hij kent hun eigenschappen (is het systeem privacybeschermend of privacybedreigend?), systeemcomponenten, toegepaste technologieën en 'last but not least' de rechtssystemen waarbinnen deze opereren, niet. Het is hierdoor haast een onbegonnen werk om bij de gebruiker zo veel vertrouwen op te wekken dat hij ervan overtuigd is dat zijn privacyvoorkeuren wereldwijd worden gerespecteerd en waardoor hij bereid is zijn (persoons)gegevens door derden te laten verwerken. Dit geldt a fortiori wanneer de verwerking uitbesteed wordt aan andere

8 Van Rooy & Bus, 2009, p. 2.

bedrijven in landen waar geen privacywetgeving bestaat, die aan die van de EU gelijkwaardig is.[9]

In paragraaf 2.11 is uiteengezet dat informatiesystemen uniform voor wereldwijd gebruik (kunnen) worden ontworpen, wanneer de privacyrealisatieprincipes i.c. de juridische specificaties zijn gestandaardiseerd. Dit zou het probleem van de veelheid aan rechtssystemen met een verschillende waardering voor privacybescherming kunnen oplossen. Dergelijke standaards (vergelijkbaar met de ISO-standaard 15408)[10] kunnen dan wereldwijd gebruikt worden als bouwstenen voor het ontwerp van informatiesystemen.

Het zal nog wel vijf tot tien jaren duren voordat de alle privacy realisatieprincipes in ISO-standaarden zijn opgenomen.

8.2. De privacybedreigingen, revisited

In hoofdstuk 3 is de tweede onderzoeksvraag beantwoord. De vraag luidde:

Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding? (OV 2).

Geconstateerd is, dat de overheid voor de terrorisme-, fraude- en misdrijfbestrijding dankbaar gebruik maakt van de stroom locatie- en verkeersgegevens die de telecommunicatie genereert. Bovendien zet de overheid geavanceerde toezichts- en recherchetechnologieën in. Besproken zijn het gebruik van databanken en data warehousing, telecommunicatie, videotoezicht, biometrie en localiseringstechnieken. Individuen en groepen kunnen slechts zeer beperkt zelf bepalen hoeveel zij blootgesteld willen worden aan toezicht en hoe zij de persoonlijke informatie kunnen beperken die over hen wordt verzameld en gebruikt. Toezichtsystemen zijn voor een leek vaak te technisch om te begrijpen en gaan onzichtbaar en daardoor ongemerkt op in de alledaagse structuren en systemen van de maatschappij: op het werk, thuis, op school, op reis en bij communicatie en het gebruik van openbare diensten.[11] Het is natuurlijk lovenswaardig dat de overheid haar burgers een hoog niveau van veiligheid wil verschaffen, maar Nath & Peissl merken op dat "the drive for improved security is often attributed to an ulterior motive of increasing surveillance."[12]

Naast de terrorisme-, fraude- en misdaadbestrijding is het streven naar steeds betere efficiency een belangrijke reden dat de risicotoezichtmaatschappij zich

9 Overigens veel (jonge) gebruikers hebben bij gebrek aan inzicht in de bedreigingen een niet te stoppen verlangen om in het digitale leven (Hyves, Youtube, etc.) te participeren.

10 De standaard betreft Anonimiteit, Pseudonimiteit, Niet-relateerbaarheid en Niet-observeerbaarheid, vastgelegd in 1999 in hoofdstuk 9 van de Common Criteria Technology Security Evaluation standaard ISO 15408 van de *International Organization for Standardization*, en is gericht op het terugdringen van persoonsgegevens in informatiesystemen.

11 Weiser, 1991, p. 94-104.

12 Nath & Peissl, 2006, p. 29-37.

ontwikkelt. Efficiëntieverbetering leidt tot meer persoonsgegevens in de commerciële dienstverlening als gevolg van de één-op-éénbenadering en tot meer elektronische patiëntendossiers in de gezondheidssector. Ook de éénloketgedachte bij de overheid leidt ertoe, dat databanken vaker aan elkaar gekoppeld worden en de behoefte aan identificatie toeneemt.[13] Adequate risicobeheersing in de moderne samenleving brengt met zich mee dat zo veel mogelijk kennis van de te analyseren situatie voorhanden is. Toegang tot persoonlijke gegevens wordt gezien als een voorwaarde is om te weten waar de overheid de preventieve of curatieve middelen moet inzetten.[14] Risico profielen zijn snel te maken dankzij de grote interconnectiviteit van toezichtnetwerken. Sociale sortering zorgt ervoor dat de politie haar aandacht meer richt op overwegend niet-blanke of sociaal lager gekwalificeerde wijken. De risicotoezichtsamenleving, die gestructureerd gebruik maakt van *connection technologies, disconnecting technologies* en *processing technologies*[15] met een complexe infrastructuur die veel persoonsgegevens verwerkt, zal niet meer verdwijnen.

Het antwoord op de tweede onderzoeksvraag is dat de risicosurveillancemaatschappij de privacy van de burger ondermijnt en dat onze informationele privacy in gevaar wordt gebracht door de privacyonveilige risicosurveillance systemen. Om te voorkomen dat de surveillancesystemen van de overheid uit de hand lopen, moeten er, voordat zo'n systeem operationeel wordt, juridische en ingebouwde technische waarborgen zijn geschapen. Het antwoord op de tweede onderzoeksvraag zou ontkennend kunnen luiden als de burger directe terugkoppeling krijgt over en controle (toezicht) kan uitoefenen op zijn verzamelde persoonsgegevens. Dat is nochtans niet het geval.

De ontwikkeling van de ict is in velerlei opzichten ook een niet-omkeerbaar fenomeen. Wanneer in het huidige ontwerp van ict-systemen de bescherming van persoonsgegevens wordt genegeerd om wille van het toezicht of om andere (commerciële) redenen, dan zal de informationele privacy in de komende tien of twintig jaar steeds meer eroderen. Om te bereiken dat informatiesystemen worden gebouwd die onze privacy adequaat beschermen, het vertrouwen in de verwerking onze persoonsgegevens bevorderen en ons tegen de kwalijke gevolgen van de risicotoezichtmaatschappij beschermen, zullen technologieën die de informationele privacy bevorderen (PET) in gezet moeten worden. PET zijn geen panacee om alle privacyproblemen op te lossen, maar kunnen, wanneer PET systematisch zijn geïntegreerd in de systeemontwikkeling, bijdragen aan een gebalanceerde relatie tussen toezicht en privacybescherming.[16]

---

13 Van Rooy & Bus, 2009, p. 2.
14 Ball, e.a., A Report on the Surveillance Society, Manchester 2006, p. 47.
15 Gilbert, 2007.
16 Ball, e.a., 2006, p. 83-84.

In hoofdstuk 3 is vastgesteld dat er een algemene bedreiging van de risicosurveillance systemen voor de privacy uitgaat. In hoofdstuk 4 is naar aanleiding van de derde onderzoeksvraag*: Met welke privacybedreigingen en -risico's moeten de burger en de ontwerper van systemen rekening houden?* (OV 3), uiteengezet welke privacybedreigingen en -risico's burgers en consumenten kunnen tegenkomen. De meeste burgers en consumenten zijn zich daar niet van bewust en nemen dan ook geen adequate beveiligingsmaatregelen tegen de vaak ongewilde registratie, verwerking en opslag van de gegevens.[17] Bovendien kiezen de burger en consument voor het korte termijnvoordeel dat de elektronische dienstverlening binnen de gezondheidszorg, handel en overheid biedt en stappen zij over de mogelijke risico's heen. Tegenover de korte termijnvoordelen staat nochtans dat zij veel persoonsgegevens moeten prijsgeven. Als informatiesystemen hun persoonsgegevens niet privacyveilig verwerken, kan hun privacy op korte of langere termijn ernstig in gevaar komen.

Uit de in hoofdstuk 2 besproken privacyrealisatiebeginselen kunnen ten minste de volgende algemene privacybedreigingen afgeleid worden:[18]

- Bedreiging 1:
  Geheim bezit van of controle over persoonsgegevens: de verantwoordelijke en/of de bewerker hebben controle over persoonsgegevens en verwerken deze ook. Zij hebben dit echter niet gemeld bij de nationale commissie voor de bescherming van de persoonlijke levenssfeer (*Data Protection Authority* (DPA))[19] van de lidstaat van de EU waarbinnen de gegevens worden verwerkt of bij een functionaris gegevensbescherming.
- Bedreiging 2:
  Geheime verwerking van persoonsgegevens: er is een gebrek aan transparantie. De verantwoordelijke of de bewerker heeft de persoonsgegevens rechtmatig onder zich maar verwerkt ze vervolgens zonder dat de betrokkene daarvoor zijn toestemming heeft gegeven.
- Bedreiging 3:
  Geheime verwerking van persoonsgegevens: het individu van wie de persoonsgegevens zijn (hierna: de betrokkene), is niet op de hoogte van het bestaan van persoonsgegevens en van de controle die een onbekende verzamelaar over de persoonsgegevens heeft.
- Bedreiging 4:
  Verwerking van persoonsgegevens in strijd met de wet: de betrokkene heeft niet ondubbelzinnig, specifiek en uit vrije wil toestemming gegeven aan derden om zijn persoonlijke informatie te verzamelen, te gebruiken, te verwerken, openbaar te maken en te verspreiden.[20]

17 Klüver, Peissl & Tennøe, 2006, p. 83.
18 Borking, e.a., 2001, p. 24.
19 In Nederland het College bescherming persoonsgegevens in Den Haag.
20 Artikel 13 van 95/46/EG bevat uitzonderingen en beperkingen op dit verwerkingsbeginsel.

- Bedreiging 5:
  Verwerking in strijd met de doelbinding: de persoonsgegevens worden verwerkt in strijd met de privacyvoorkeuren van de betrokkene of de verantwoordelijke beperkt zich bij de verwerking niet tot het opgegeven doel (doelbinding).
- Bedreiging 6:
  Onrechtmatige verwerking van persoonsgegevens: de verwerking van persoonsgegevens vindt in strijd met de wet plaats.
- Bedreiging 7:
  Gebrek aan gegevensminimalisatie: er worden meer gegevens verzameld en verwerkt dan strikt noodzakelijk om het doel te realiseren waarvoor de persoonsgegevens zijn bestemd. Dit is in strijd met het beginsel van gegevensminimalisatie en het finaliteitsbeginsel.
- Bedreiging 8:
  Excessieve identificatie van het individu: de identiteitsgegevens zijn disproportioneel en blijven langer bewaard dan de doeleinden van de verwerking rechtvaardigen. De informatiesystemen zijn zodanig ingericht dat het desbetreffende individu onbeperkt kan worden geïdentificeerd, geobserveerd en getraceerd.
- Bedreiging 9:
  Verouderde gegevens: de verantwoordelijke neemt verkeerde beslissingen op basis van onjuiste of verouderde gegevens. De persoonsgegevens worden niet correct, niet accuraat, ontoereikend, en niet terzake dienend verzameld en verwerkt.
- Bedreiging 10:
  Verantwoordelijke is onvindbaar of weigert transparantie: er is geen of een beperkte reactie van de verantwoordelijke wanneer de betrokkene hem aanmaant. Personen van wie gegevens worden verwerkt, krijgen niet de mogelijkheid om hun persoonsgegevens in te zien, te verbeteren, aan te vullen, te verwijderen of af te schermen of bezwaar te maken tegen de verzameling en verwerking van hun persoonsgegevens. De verantwoordelijke is onbekend, onvindbaar of heeft zijn identiteit tenonrechte afgeschermd.
- Bedreiging 11:
  Onbeveiligd data management:[21] er zijn geen passende technische en organisatorische maatregelen genomen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking of om te voorkomen dat persoonsgegevens onnodig verzameld en verwerkt worden.

---

21 ISO/IEC 15408-1: 1999; *Evaluation Criteria for IT Security* (ook bekend onder de naam *Common Criteria for Information Technology Security Evaluation*), International Organization for Standardization, 1999, csrc.nist.gov/cc/ccv20/ccv2list.htm. Voor deze bedreigingscategorie dienen de security objectives van ISO/IEC 15408 toegepast te worden.

- Bedreiging 12:
  Niet-vertrouwelijk en onzorgvuldig data management: gebrek aan vertrouwelijkheid van de communicatie.[22] De communicatie en de verkeersgegevens van openbare communicatienetwerken en openbare elektronische communicatiediensten vindt niet op een vertrouwelijke manier plaats.
- Bedreiging 13:
  Verkeersgegevens worden te lang opgeslagen: belpatronen van de abonnees en gebruikers kunnen langdurig worden geanalyseerd. De aanbieder van een openbaar elektronisch communicatienetwerk of -dienst die de verkeersgegevens van abonnees en gebruikers verwerkt en opslaat, wist of anonimiseert deze gegevens niet wanneer hij deze niet langer nodig heeft voor de communicatietransmissie en/of voor de finale afwikkeling van de facturering van abonnees. De verantwoordelijke interpreteert de bepalingen van de data retentie Richtlijn 2006/24/EG te ruim en slaat meer op en langer dan is toegestaan.
- Bedreiging 14:
  Niet toegestane verwerking buiten de EU en EEA: de verantwoordelijke verspreidt de persoonsgegevens en/of geeft ze door aan een land dat geen adequate bescherming biedt zoals die geldt binnen de EU en EEA.

Daarnaast zijn er per applicatie specifieke bedreigingen. In hoofdstuk 4 zijn de bedreigingen voor software agents en biometrische toepassingen bij wijze van voorbeeld opgesomd. Als deze bedreigingen zich materialiseren, dan kan er door de betrokkenen materiële en immateriële schade geleden worden. Boer & Grimmius vermelden in hun rapport[23] dat burgers op verschillende manieren schade kunnen lijden:

1. Financiële schade door verlies van creditcard- of pinpasgegevens, wachtwoorden en toegangscodes voor internetbankieren.
2. Imagoschade of chantage door het bekend worden van gevoelige informatie over bijvoorbeeld religieuze, politieke of seksuele voorkeur.
3. Fysieke schade, bijvoorbeeld diefstal of molest.
4. Identiteitsfraude, wanneer iemand anders zich voor de benadeelde burger uitgeeft. De fraudeur heeft niet alleen toegang tot diens gegevens maar kan ook op diens kosten goederen en diensten afnemen of zelfs criminele activiteiten ondernemen onder de naam van zijn slachtoffer. Identiteitsfraude 'kan overal en op velerlei manier plaatsvinden en is niet beperkt tot specifieke situaties, procedures of documenten.

22 Driml, 2003, *http://www.isaca.org/Template.cfm?Section=Home&Template=/Search/SearchDisplay.cfm.* Voor deze bedreigingscategorie dienen de security objectives van ISO/IEC 15408 toegepast te worden.
23 Boer & Grimmius, 2009, p. 26.

In paragraaf 8.3 wordt op het belang van identiteitsmanagement ingegaan. Wanneer burgers en consumenten zich wel bewust zijn van de privacyrisico's, dan is uit gedragsonderzoek (zie paragraaf 4.15) op te maken, dat: "consumers engage in a privacy calculus where they trade off their privacy costs from sharing information against their value from personalization".[24]

Omdat de verwerking en de aard van de gegevens die beschermd moeten worden risico's met zich meebrengen, schrijven de Europese privacyrichtlijnen en de daarop geënte nationale wetgevingen van de EU-lidstaten een passend beveiligingsniveau van persoonsgegevens voor. Om dergelijke data adequaat te beschermen, moet duidelijk zijn welke privacyrisico's er ontstaan wanneer persoonsgegevens worden verwerkt en nieuwe informatiesystemen worden geïntroduceerd. De interpretatie van artikel 17 van Richtlijn 95/46/EG en artikel 4 van Richtlijn 2002/58/EG, leidt tot de conclusie dat een objectieve methodologische privacybedreigingsanalyse of een privacy impact analyse een *sine qua non* is. In hoofdstuk 4 zijn verschillende methoden om privacybedreigingen en -risico's te analyseren onder de loep genomen.

Fritsch[25] stelt dat de beveiligingsdeskundigen de classificatie van privacyrisico's in de verschillende risicoanalysemethoden en de hieraan gerelateerde kosten niet op een overtuigende manier hebben uitgevoerd en verkeerde beslissingen nemen op grond van onjuiste gegevens. Bovendien zijn de privacyrisico's in de bestaande literatuur niet goed gedefinieerd.[26] Het is belangrijk om een privacyrisico- of bedreigingsanalyse uit te voeren die zo veel mogelijk met de omstandigheden rekening houdt. Daarom verdient een ontologische beschrijving van de bedreigingen, zoals die van Little & Rogova,[27] de voorkeur boven een niet-limitatieve opsomming van privacyinbreuken met daarmee verbonden bedreigingen en risico's die beveiligingsdeskundigen vanuit de praktijk hebben opgesteld.[28] In paragraaf 4.11 is de aanpak van Little & Rogava toegelicht. Het innovatieve van hun aanpak is dat zij in de door hun ontwikkelde bedreigingsontologieen een drie dimensionaal matrixmodel gebruiken, om duidelijk te maken aan welke noodzakelijke aan elkaar gerelateerde attributen[29] een bedreiging en degene die de bedreiging uitvoert dienen te voldoen om de potentie te hebben een zwakke plek in het systeem te kunnen uitbuiten.[30]

Omdat deze attributen binnen een bedreiging zo met elkaar verbonden en van elkaar afhankelijk zijn, is het gevolg van de verstoring of uitschakeling van één van deze elementen dat de bedreiging verdwijnt of zodanig wordt verstoord, dat

---

24 Chellappa & Shivenda, 2008, p. 1.
25 Fritsch, 2007, p. 8.
26 Gellman, 2002.
27 Little & Rogova, 2006, p. 8: "Threat is a very complex ontological item, and therefore a proper threat ontology must be constructed in accordance with formal metaphysical principles that can speak to the complexities of the objects, object attributes, processes, events, and relations that make up these states of affairs".
28 B. Schneier, 2000, p. 225.
29 Little & Rogova, 2006, p. 4.
30 Little richt zich meer op de omgevingsfactoren, terwijl Vidalis zich bezig houdt met de instelling van de agressor zelf.

de bedreiging niet meer effectief kan zijn. Daarom is het van belang om de rol van elk van deze attributen: intenties of motivatie, capaciteiten en (gunstige) omstandigheden binnen een bepaalde dreiging goed te onderkennen. De hiervoor vermelde elementen van een bedreiging kunnen als extern-, intra- of interngerelateerde delen van het geheel van een bedreiging bestaan. Het verdient aanbeveling een wetenschappelijk vervolgonderzoek te doen naar de toepasselijkheid van het bedreigingsmodel van Little & Rogova. Het inzetten van PET-maatregelen verstoren de bedreigingsattributen.

Een van de privacybedreigingen die individuen lopen bij het gebruik van informatiesystemen, is identiteitsfraude. Om ongewenste identificatie van personen te voorkomen en waarborgen tegen onrechtmatige verwerking van persoonsgegevens te scheppen, passen organisaties versleuteling en logische toegangsbeveiliging breed toe. Binnen de logische toegangsbeveiliging is het met name belangrijk dat uniek identificerende persoonsgegevens en bijbehorende autorisatiegegevens goed beheerd worden. Bovendien blijkt het veelal effectiever en efficiënter om privacymaatregelen te automatiseren dan louter te steunen op organisatorische procedures en handmatige activiteiten.[31] Aan de vooraf geconstateerde privacybedreigingen en risico's moet in het ontwerp van informatiesystemen het hoofd worden geboden.

Het antwoord op de tweede onderzoeksvraag dat onze privacy gevaar loopt in de risicotoezichtsmaatschappij leidt tot de constatering dat dit gevaar slechts gekeerd kan worden als er informatiesystemen worden ingezet voorzien van PET-maatregelen met terugkoppeling en controlemogelijkheden voor burger. De in hoofdstuk 4 behandelde methoden van privacyimpact-, privacyrisico- c.q. bedreigingsanalyse, zowel die van de Registratiekamer (classificatie van risico's in klassen), als die van de Canadese PIA, het EU PISA research project en het Noorse PETWEB project, leiden bij toepassing op in dit boek besproken informatiesystemen tot de bevinding dat een keur van PET maatregelen onvermijdelijk zijn om de geconstateerde risico's te voorkomen.

In hoofdstuk 5 is de vierde onderzoeksvraag: *Wat houdt het concept Privacy Enhancing Technologies (PET) in*? (OV 4) behandeld. PET is een technologisch concept en kan theoretisch gezien worden als een belangrijke aanvulling op het bestaande juridisch kader en de organisatorische uitwerking daarvan. PET kan het gebruik van persoonsgegevens elimineren, aanmerkelijk verminderen of de verwerking dwingend binden aan de wettelijke voorwaarden, waardoor de privacy bescherming door de verantwoordelijken geen lege huls wordt. Bovendien stelt PET de burger en consument in staat om de verwerking van zijn persoonsgegevens te controleren en daardoor zijn vertrouwen in de rechtmatige verwerking vergroten.[32] Koorn[33] wijst erop dat PET bepaalde toepassingen binnen informatiesystemen mogelijk maakt, die anders wettelijk onmogelijk zouden zijn. In

31 Koorn, e.a., 2004, p. 5-8.
32 Klaver, e.a., 2002, p. 100-108.
33 Koorn, e.a., 2004, p. 13-16.

functionele zin is het toepassen van PET niet problematisch. PET omvat alle technische maatregelen om de privacy te waarborgen en om risico's op inbreuken op de bescherming van privacy te voorkomen en te managen. Met behulp van PET kan een organisatie al aan de bron technische maatregelen nemen en het aantal identificerende gegevens tot het absolute minimum beperken en de identiteit loskoppelen van de overige persoonsgegevens. De in hoofdstuk 5 besproken research toont aan dat de mogelijkheden toenemen om effectief en automatisch de informationele privacy te beschermen. Omdat er steeds meer transacties niet direct tussen mensen alleen gebeuren, maar in toenemende mate het contact en de afhandeling van de transactie direct tussen informatiesystemen, software agents, intelligente sensoren en robots plaatsvinden, is dit een gunstige ontwikkeling. Het is tegelijkertijd dringend noodzakelijk dat technologische oplossingen worden ontwikkeld om de persoonlijke levenssfeer effectief te beschermen, bij gebreke waarvan de informationele privacy steeds meer zal eroderen.

De Commissie van de EU steunt het gebruik van PET en stimuleert in haar onderzoeksprogramma's het fundamenteel onderzoek naar PET. In verschillende lidstaten zijn expliciete PET maatregelen in de wetgeving opgenomen. Van Rooy en Bus[34] wijzen erop dat niet alleen PET maatregelen moeten worden toegepast om ervoor te zorgen dat de burger en consument vertrouwen krijgen en houden in de gegevensverwerking van hun persoonsgegevens, maar dat het informatiesysteem, het proces en de toegepaste applicatie(s) robuust dienen te zijn.

De kern van PET is de 'Identity protector'. Deze systeemmodule kan samen met de gegenereerde pseudo-identiteiten persoonlijke informatie op een gecontroleerde manier met toestemming van de betrokkene vrijgeven. De 'Identity protector' zorgt ervoor dat de pseudo-identiteiten niet met elkaar zijn te verbinden en dat de doelbinding van persoonsgegevens afdwingbaar is. Wanneer iemand meerdere pseudo-identiteiten (zie figuur 5.6: digitale (deel)identiteiten) heeft, dan is identiteitsmanagement noodzakelijk. In paragraaf 8.3 kom ik hierop terug. De 'Identity protector' draagt verder bij aan de adequate beveiliging van de PII,[35] zorgt voor een beveiliging die de privacy niet corrumpeert en bevordert dat de verantwoordelijken en bewerkers van data de noodzakelijke verantwoording kunnen afleggen.[36] PET-maatregelen ondersteunen de juridische specificaties in de architectuur. Aangezien privacyvraagstukken te vaak worden verwaarloosd bij de ontwikkeling van informatiesystemen, dringen Klüver, Peissl en Tennøe erop aan dat "Privacy Enhancing Technologies (PETs) should be systematically integrated in systems development. Such technologies are not a panacea to solve all privacy issues, but they can significantly contribute to minimizing data collection and analysis."[37]

---

34 Van Rooy & Bus, 2009, p. 2.
35 PII staat voor Personal Identifiable Information.
36 Gürses, 2009.
37 Klüver, Peissl & Tennøe, 2006, p. 87.

In hoofdstuk 4 is tevens de vijfde onderzoeksvraag: *Is het mogelijk privacy-veilige architecturen en systemen te ontwerpen en te bouwen?* (OV 5) theoretisch positief beantwoord, maar in dit hoofdstuk is niet beantwoord of PET en de daarbij behorende ontwerpelementen inderdaad in de praktijk in de architectuur van informatiesystemen kan worden aangewend waardoor er privacyveilige systemen ontstaan. *The proof of the pudding is in the eating*. Dat is gebeurd in hoofdstuk 6, waarover hieronder.

8.3. De rol van identiteit en identiteitsmanagement

In paragraaf 5.10 is uiteengezet dat bij het ontwerp van privacyveilige informatiesystemen een robuust identiteitsbeheersysteem mede in de architectuur dient te worden geincorporeerd. Het gebruik van ict en met name van internet vraagt om systemen waarbij het individu controle heeft over zijn eigen pseudo-identiteiten. Hansen bepleit dat het identiteitsbeheersysteem zo moet zijn ingericht dat het de gebruiker in staat stelt om zijn recht op informationele zelfbeschikking te realiseren.[38] Van belang is dat 'credentials' die de identiteit van een persoon kunnen bewijzen in de context van de privacybescherming voldoen aan het proportionaliteitsbeginsel,[39] zodat dergelijke 'credentials' niet voortdurend moeten worden gecontroleerd, gevolgd en geregistreerd. Door een dergelijk toezicht zou namelijk niet alleen de privacybescherming illusoir worden, maar ook de vrije en democratische samenleving onder druk komen te staan. De door Brands ontwikkelde credentialtechnieken demonstreren dat: "these goals can be achieved through the use of privacy-enhancing technologies that are entirely feasible and secure."[40]

Het probleem is dat er nog geen gestandaardiseerde identificatie-infrastructuur en identiteitsbeheer bestaan. Dat leidt in de praktijk tot grote verschillen. Soms is alleen een paspoortnummer nodig om vast te stellen dat de persoon inderdaad is wie hij beweert te zijn en soms moet de betrokkene om onduidelijke redenen zeer veel persoonlijke informatie prijsgeven. Ook blijken soms de gevraagde identificatiegegevens niet toereikend te zijn om met zekerheid te kunnen vaststellen dat in een transactie de participerende partijen zijn wie zij zeggen te zijn. Dergelijke situaties leiden niet tot meer vertrouwen, geven ruimte tot misbruik en zullen uiteindelijk een negatief effect hebben op de ontwikkeling van de informatiesamenleving. Van Rooy en Bus pleiten dan ook voor een gestandaardiseerde en betrouwbare IDM-infrastructuur (identity management), die noodzakelijk is: "for trustworthy services in domains such as e-government, e-health, e-commerce, finances, web 2.0 communities and the forthcoming Internet of things."[41]

---

38 Hansen, 2003, p. 2.
39 Er moet een evenwicht bestaan tussen nut en last voor de individuele of groepsprivacy.
40 Brands, 2000, p. 266.
41 Van Rooy & Bus, 2009, p. 2.

Zoals eerder in dit hoofdstuk opgemerkt, zijn er dringende redenen om te werken aan een wereldwijde standaard voor de juridische specificaties, maar er is ook dringend behoefte aan standaarden voor de noodzakelijke privacyveilige infrastructuur en het beheer van multi-identiteiten per persoon. De standaard dient als uitgangspunt te nemen dat het individu zijn multi-identiteiten zelf beheert en hij controlemogelijkheden krijgt zodat er geen onoorbare dingen met zijn persoonsgegevens gebeuren. Camenish ondersteunt deze gedachte: "each single user is put into control with regard to his/her PII as much as possible. This is surely better than letting other entities like other users or organizations decide about and being in control of users Personal Identifiable Information (PII)."[42]

De vijfde onderzoeksvraag betreffende het ontwerpen en het bouwen van privacyveilige informatiesystemen is in hoofdstuk 5 vanuit het PET concept positief beantwoord. In hoofdstuk 6 is naar de praktijk gekeken, omdat dan pas blijkt of de theorie kan worden toegepast en goedwerkende privacyveilige informatiesystemen geen luchtkastelen zijn. Uit de praktijk zijn vier informatiesystemen als voorbeelden opgevoerd. Het betreft de metazoekmachine Ixquick (paragraaf 6.5.1), het ziekenhuisinformatiesysteem van het psychiatrisch ziekenhuis Meerkanten in Ermelo (paragraaf 6.7), het Victim Tracking and Tracing System (ViTTS) (paragraaf 6.8) en de privacy incorporated software agent (PISA), waaruit de research naar het privacy managementsysteem is voortgevloeid.

Uit onderzoek is gebleken dat deze informatiesystemen volledig door de gebruiker worden vertrouwd. Ixquick heeft in 2008 van EuroPrise een Europees privacycertificaat gekregen. De privacyaudit van de Registratiekamer heeft aangetoond dat het ziekenhuisinformatiesysteem privacyveilig is. ViTTS is door researchers van PRIME op de privacybescherming getoetst en de PET maatregelen zijn adequaat beschouwd. Uit een enquête van het National Research Center of Canada onder vijftig studenten van de Carleton University naar het vertrouwen in PISA bleek, dat tussen de 90 en 96% van de studenten de geboden functionaliteiten begreep en tussen de 70 en 80% de privacybeschermende functionaliteit zo goed vond dat zij verklaarden, dat zij hun salariswensen, naam, adres en telefoonnummer aan PISA zouden toevertrouwen.[43] De vijfde onderzoeksvraag kan dus zowel vanuit een theoretisch als praktisch oogpunt bevestigd beantwoord worden.

Klüver, Peissl en Tennøe wijzen erop dat "poorly designed ICT products may affect privacy in 10 or 20 years time."[44] Dat wil zeggen dat als wij nu niet privacyveilige informatiesystemen op grote schaal ontwerpen en deze systemen de verwerking van onze persoonsgegevens toevertrouwen, onze samenleving de

---

42 Camenish, Leenes & Sommer Brussels, 2008, p. 515.
43 Van Blarkom, Borking & Olk, 2003, p. 260-288.
44 Klüver, Peissl & Tennøe, 2006, p. 87; Brandon & Segelstein 1976, p. 17 menen dat ten minste van een termijn van 5 tot 8 jaar moet worden uitgegaan.

komende jaren met grote privacy problemen zal worden geconfronteerd. In een lijst van zeven 'challenges' bepleiten Klüver, Peissl en Tennøe de noodzaak om de in paragraaf 4.8 besproken Privacy Impact Assessment wettelijk verplicht te stellen. Dit voorkomt dat systemen de informationele privacy niet of slecht beschermen. Ook pleiten zij voor een structurele gegevensminimalisatie (zie paragraaf 2.5.6) en een systematische integratie van PET in de systeemontwikkeling.[45]

8.4. Beantwoording van de probleemstelling

Met de beantwoording van de eerste vijf onderzoeksvragen staat vast dat persoonsgegevens van burgers effectief kunnen worden beschermd bij het verzamelen, verwerken, opslaan binnen informatiesystemen en het verspreiden over de elektronische infrastructuur. Voorwaarde is dan wel dat informatiesystemen moeten zijn ontworpen met inachtneming van de juridische specificaties, de vastgestelde privacy bedreigingen en noodzakelijke PET-maatregelen. Dergelijke privacyveilige informatiesystemen dienen bovendien zo te zijn ingericht dat de privacypreferenties van het individu dat zijn persoonsgegevens afstaat, automatisch wordt afgedwongen, zoals bijvoorbeeld bij privacy managementsystemen. Daarmee is het *hoe* van de probleemstelling (PBS): *"Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker?"* beantwoord.

De PBS spreekt ook over het *vertrouwen* van de burger. Leiden privacyveilige systemen bij de burger en consument tot het *vertrouwen* dat hun persoonsgegevens rechtmatig zullen worden verwerkt? Leiden deze systemen tevens tot het *vertrouwen* in de verantwoordelijke dat hij de verwerking van hun persoonsgegevens overeenkomstig de Richtlijn 95/46/EG en zijn openbaargemaakte privacybeleid uitvoert? Het vertrouwen van een persoon is gebaseerd op de aanname dat iets of iemand zich zal gedragen met inachtneming van zijn belangen om hem geen leed of schade te berokkenen. De burger c.q. consument kan de betrouwbaarheid vaak niet beoordelen. Schilfgaarde & Nootenboom stellen, dat dit gegeven openheid van de vertrouwde tegen over de vertrouwer vergt en het vermogen van de vertrouwer om de vertrouwde het voordeel van de twijfel te geven.[46] Het vertrouwen kan ondermeer gebaseerd zijn op reputatie van de vertrouwde of verklaringen van personen of organisaties die door de vertrouwer worden vertrouwd.

45 Klüver, Peissl & Tennøe, 2006, p. 84 en 87.
46 Schilgaarde & Nooteboom, 2009, p. 50.

Bij informatiesystemen bestaat er een indirecte relatie tussen de vertrouwer (de burger) en de vertrouwde (de verantwoordelijke). Onderzoek heeft aangetoond dat het vertrouwen drastisch verminderd bij een indirecte relatie, te meer als de communicatie via computers gaat.[47] Om het informatiesysteem te kunnen vertrouwen zal een betrouwbare derde moeten verklaren dat het informatiesysteem voor wat betreft de rechtmatige verwerking van persoonsgegevens betrouwbaar is. Dergelijke verklaringen (bijvoorbeeld in de vorm van certificaten) kunnen door geaccrediteerde derden worden verstrekt. Als zo'n certificaat de privacyveiligheid van het systeem garandeert, zoals de EuroPrise 'privacy seal' bijvoorbeeld doet,[48] dan komt dat de transparantie ten goede. Daarmee krijgen gebruikers van informatiesystemen, die doorgaans niets van privacyveilige systemen, laat staan van PET-maatregelen afweten, ook meer vertrouwen in het desbetreffende systeem en het proces dat hun gegevens verwerkt.[49] Voor een algemeen maatschappelijk vertrouwen in de rechtmatige verwerking van persoonsgegevens is het noodzakelijk dat gecertificeerde privacyveilige systemen grootschalig worden toegepast.

Daarmee zou de probleemstelling afdoende beantwoord kunnen zijn, maar, hoewel vaststaat dat privacyveilige systemen met gebruikmaking van PET gebouwd kunnen worden en het vertrouwen van de burger bevorderen, blijkt uit hoofdstuk 7 dat PET nauwelijks wordt toegepast bij het ontwerp van systemen die persoonsgegevens verwerken. In een nog niet gepubliceerd interimonderzoek van Godel & Conlon (oktober 2009) wordt dit bevestigd:

> "(...) privacy enhancing technologies were not widely deployed and the rate at which deployment has grown over the last few years has not been substantial (…). This is surprising given the belief that privacy risks have been growing and that PETs are effective at reducing privacy risks (...)"[50]

Als in de praktijk geen privacyveilige systemen worden gebouwd, kan de burger geen vertrouwen opbouwen over de verwerking van zijn persoonsgegevens. Het is dus van het grootste belang na te gaan wat de oorzaken hiervan zijn.

Ik vroeg me af of ik iets essentieels over het hoofd had gezien. Vandaar de zesde onderzoeksvraag: *Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?* (OV 6).

De in hoofdstuk 7 geconstateerde positieve en negatieve adoptiefactoren voor PET geven aan dat er inderdaad belangrijke belemmeringen bestaan om PET toe te passen en privacyveilige systemen grootschalig te ontwikkelen. De trage

---

47 Van Blarkom, Borking & Olk, 2003, p. 154.
48 Het EU gesubsidieerde EuroPrise research project begon op 10 juni 2007 en is 28 februari 2009 geëindigd. http://www.european-privacy-seal.eu/about-europrise/fact-sheet.
49 Van Rooy & Bus, 2009, p. 1.
50 Godel & Conlon, 2009, p. 64.

adoptie van PET zorgt voor het voortduren van privacy onveilige situaties voor de burger en de consument, de erosie van privacy en het afnemen van het vertrouwen in de rechtmatige verwerking van persoonsgegevens. Het hierboven gegeven antwoord op de zesde onderzoeksvraag impliceert dat de belemmeringen moeten worden overwonnen om privacyveilige systemen grootschalig te kunnen inzetten. Die belemmeringen kunnen uit de weg geruimd worden als gebruik wordt gemaakt van de positieve adoptiefactoren. Hieronder volgen de daarop gebaseerde aanbevelingen.

8.5. Aanbevelingen voor privacyveilige informatiesystemen

In de paragrafen 8.5 tot en met 8.8 worden tien aanbevelingen gegeven, die het gebruik van privacyveilige informatiesystemen zullen bevorderen. Wanneer de positieve adoptiefactoren (zie paragraaf 7.8) worden benut, zouden organisaties PET-maatregelen sneller op grote schaal in hun informatiesystemen kunnen invoeren. Het gaat hierbij vooral om overheids- en commerciële organisaties die een grote informatieverwerkingsdichtheid kennen. Zij kennen vanuit hun organisatiestrategie een grote behoefte om de privacy van hun cliënten te beschermen en zij hebben de financiële en operationele middelen daartoe.[51] In hoofdstuk 7 werden maturiteitsmodellen en de daarmee samenhangende groeikrommen van identiteit- en toegangsbeheer, PET en privacybescherming beschreven. Hieronder worden mogelijke oplossingen genoemd die de invoering van PET bevorderen en daarmee het vertrouwen van de burger en consument in de verwerking van hun PII vergroten.

8.5.1. Voorlichting

Empirisch onderzoek leidt tot de conclusie dat PET vaker zou kunnen worden geïmplementeerd als gebruik gemaakt worden van de volgende positieve adoptie factoren (zie figuur 7.4): de zichtbaarheid en testbaarheid, de steun van het management en sleutelfiguren, de stimulerende rol van voorlichtende instanties en individuele contacten daarmee, de druk van de privacywetgeving en het toezicht ('data protection authorities') en de beschikbaarheid van PET-producten of –maatregelen. In de voorlichting over privacybescherming en PET kan de overheid deze positieve adoptiefactoren gebruiken[52] temeer daar uit de interviews naar voren is gekomen dat: "Organizations often do not know/understand what privacy laws require them to do. Because privacy laws are overly complex and ambiguous, they do not use the right set of protective measures."[53]

51 Ribbers, 2007(A), p. 11.
52 Bos, 2006.
53 Ribbers, 2007, p. 18.

Horlings e.a.[54] bevestigen dat PET alleen in informatieprocessen van de overheid zal worden ingevoerd wanneer er een gerichte voorlichting over PET komt en de beleidsbeslissers zich bewust worden van de voordelen die PET voor het beheer van persoonsgegevens kan bieden.[55]

Het maturiteitsmodel voor PET (zie figuur 7.6) en het typologieschema van organisaties met een PET-vraagindicatie (zie figuur 7.7) maken het mogelijk dat de toezichthouders de voorlichting over PET-bescherming specifiek kunnen richten op organisaties die zich in potentiële PET-segmenten bevinden. Omdat deze organisaties tot de top 5000 van grote organisaties binnen de EU behoren, zou daarmee al een groot deel van de verwerking van persoonsgegevens afgedekt zijn. Wanneer grote overheids- en bedrijfsorganisaties PET publiekelijk zouden adopteren, zou daarvan leiderschap op het gebied van privacybescherming uitgaan. Dit zou een stimulerend effect hebben op het midden- en kleinbedrijf, zodat men daar uiteindelijk ook PET op grote schaal zou adopteren.

Aanbeveling I aan het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en het Ministerie van Justitie en de Data Protection Authorities (College bescherming Persoonsgegevens):

Maak bij de voorlichting over 'privacy enhancing technologies' gebruik van de positieve adoptiefatoren voor PET. Voer op basis van het maturiteitsniveau van de overheidsorganisaties PET standaard in alle informatiesystemen in, conform de motie Nicolaï.

8.5.2. De cruciale rol van de toezichthouder

Bos signaleert dat het College Bescherming Persoonsgegevens (CBP) een belangrijke rol kan spelen bij de acceptatie van PET. Tot 2002 hebben het CBP en haar voorgangster de Registratiekamer proactief het gebruik van privacyverbeterende technologieën gestimuleerd, met name bij de introductie van grootschalige projecten. De Registratiekamer en het CBP hebben daarmee in belangrijke mate ervoor gezorgd dat twaalf overheidsorganisaties in Nederland PET hebben toegepast. Momenteel bevordert het CBP deze technologieën niet meer actief adviserend, waardoor de toepassing van PET achterblijft, of zelfs stil valt.[56] Uit onderzoek naar de adoptiefactoren van PET blijkt dat de toezichthouders die de bescherming van persoonsgegevens bewaken en bevorderen in belangrijke mate de toepassing van PET actief kunnen bevorderen.[57] Zij kunnen

54 Horlings, e.a., 2003, p. 68.
55 Horlings, e.a., 2003, p. 68.
56 Bos, 2006, p. 52.
57 Borking & Vriethoff, 1995, p. 11-12, visie: "De Registratiekamer wil in het denken over, het ontwikkelen van en het communiceren over relevante normen ten aanzien van de informationele privacybescherming een voor de samenleving herkenbare en onbetwiste leider zijn. Zij bewaakt en bevordert de toepassing van deze normen en bepaalt daardoor mede het humane gezicht van de 21ste eeuw."

een klankbord zijn voor de betrokken partijen die PET maatregelen in hun informatiesystemen willen implementeren. Deze toezichthouders zouden om privacyveilige informatiesystemen te bevorderen zich dan ook niet *ex post* door klachtenbehandeling en controles achteraf, maar juist *ex ante* preventief adviserend moeten opstellen. Het heeft geen zin als toezichthouder informatiesystemen, zoals bijvoorbeeld het electronisch patiëntendossier, af te keuren, als niet tegelijkertijd oplossingen worden aandragen. De data protection authorities (DPA's) zouden hun technologische experts als PET-consulenten kunnen inzetten. Die kunnen bij het in de wet voorziene vooronderzoek en aan de hand van de voorgelegde privacyrisicoanalyses (of PIA's als die wettelijk verplicht worden) kunnen adviseren om PET toe te passen. Daarmee zou de positieve adoptie factor voor PET optimaal worden benut.

Ik realiseer me dat er dan binnen de DPA's een oplossing moet worden gevonden voor de scheiding tussen preventief adviseren en achteraf controleren. Als die niet gevonden kan worden, dan moet deze specifieke voorlichtende en adviserende functie over PET van de DPA's worden afgesplitst (zie paragraaf 8.5.3).

Godel & Conlon rapporteren dat er een fundamenteel verschil van inzicht bestaat onder de DPA's over de manier hoe PET ingezet moet worden. De Information Commissioner in het Verenigd Koninkrijk meent dat bij het inzetten van PET niet moet worden uitgegaan van altruïsme van de organisaties. De toezichthouder is Estland stelde dat "including PETs in applications by default is the way forward". Het College bescherming persoonsgegevens ziet nochtans:

> "(...) consumer concern as the driving force for PETs deployment. It argues that businesses (especially financial institutions) should take active steps to address consumer concerns and mentions examples of measures that are already being taken (e.g. campaigns to inform customers about the threat of phishing attacks and the use of secure connections)".[58]

Deze aanpak zal niet leiden tot structurele privacyveilige oplossingen. Als er geen unanimiteit onder de DPAs is over de inzet van PET, dan werkt dat contraproductief. Multinationals en grote gegevensverwerkers begrijpen dit verschil van inzicht niet. DPA's zijn bij uitstek de gidsen op het gebied van privacybescherming en daar mag juist ten aanzien van het stimuleren van PET één lijn worden verwacht. Gebrek aan unanimiteit is een negatieve adoptiefactor voor PET.

Aanbeveling II aan de Data Protection Authorities (College Bescherming Persoonsgegevens):

Zorg voor unanimiteit in de EU wat betreft het gebruik van PET. Draag dezelfde boodschap over PET EU-breed uit. Bevorder dat PET-standaard (by default) wordt toegepast teneinde de privacyveiligheid van informatiesysteem

58 Godel & Conlon, 2009, p. 66.

te stimuleren. Adviseer en bevorder de opneming van een bepaling in de Wbp die PET gebruik in informatiesystemen verplicht stelt.

8.5.3. Het PET Expertisecentrum

Uit Rogers' Difussion of Innovation (DOI)-theorie[59] blijkt dat organisaties een innovatieve technologie, product, systeem of proces sneller zullen invoeren als de innovatie van tevoren getest kan worden. De expertise over PET-toepassingen is nochtans schaars. Het zou daarom wenselijk zijn een PET Expertisecentrum in het leven te roepen. Gezien de taak van het College bescherming persoonsgegevens (CBP) en haar zusterorganisaties in de EU-lidstaten zou het initiatief in de eerste plaats van hen moeten komen. Vanwege de functiescheiding (controlerend handhaven versus preventief adviseren) zou het CBP een stichting kunnen oprichten aan wie de PET voorlichting en advisering wordt toevertrouwd. Deze stichting zou op 'arm's length' van het CBP moeten opereren, maar wel met het gezag van het CBP.

Wat betreft de overheid zelf, zou 'Het Expertise Centrum' (HEC) dat door het Ministerie van Binnenlandse Zaken en Koninkrijksaangelegenheden is opgericht, de PET voorlichting en advisering als proactieve taak opgedragen kunnen krijgen. Het HEC staat overheidsorganisaties bij en adviseert hen over oplossingen op het snijvlak van bestuur en ict.

Het PET Expertisecentrum zou ook onderdeel van TNO kunnen zijn. Dit centrum zou aangeboden PET applicaties kunnen testen, de overheid en het bedrijfsleven hierover kunnen adviseren en advies kunnen uitbrengen over de integratie van PET in bedrijfsprocessen en over het managen van informatie binnen de keten. Wanneer de toepassing van een innovatie in de dienstverlening voor gebruikers, burgers, consumenten of afnemers zichtbaar wordt gemaakt, bijvoorbeeld door aandacht van de media, dan blijkt dat eveneens een positieve adoptiefactor te zijn. De organisatie zal dan sneller besluiten de innovatie in te voeren. Het PET Expertisecentrum zou door het afgeven van een keurmerk voor de geteste PET-applicatie, de zichtbaarheid bevorderen en de toepassing van PET bekend kunnen maken bij het management van organisaties en het grote publiek. Bijvoorbeeld door de mededeling bij het informatiesysteem: 'PET inside!'.

Daardoor zou de PET-bescherming een onderscheidende rol kunnen gaan spelen in de keuze van de afnemers en consumenten voor privacyveilige producten en diensten. Een dergelijk keurmerk (te vergelijken met de E-nummers die gelden voor levensmiddelen) kan de 'lemons market' bestrijden, waar het volkomen onduidelijk is welk product of welke dienst privacyveilig is.[60] Het zou de door Horlings e.a. gesignaleerde vicieuze cirkel rond PET doorbreken.[61] Het gebrek aan transparantie in de markt leidt er namelijk op termijn toe dat

59 Rogers, 2003, p. 120-122.
60 Vila, Greenstadt & Molnar, 2004, p. 140-153.
61 Horlings, e.a., 2003, p. 71.

organisaties die eerst in PET maatregelen investeerden, bij gebrek aan onderscheid en concurrentie na enige jaren wegzakken tot het niveau van de organisaties die nog nooit in PET hadden geïnvesteerd.

De CEN (Comité Européen de Normalisation) bestudeert of het mogelijk is een Privacy Technology Assessment Committee (PRITAC) in het leven te roepen. De bedoeling van PRITAC is nog vóór of in de eerste testfase te beoordelen in hoeverre nieuwe ict-ontwerpen de privacy bevorderen of bedreigen:

> "(…) the assessment may well be carried out well before the new technology (product, service or system)[62] is actually ready for marketing. It is important that the assessment should be conducted in the phase of development that integrates privacy into the new technology, (product, service or system) (which would preferably be earlier than the test phase)."

Daarnaast zou PRITAC in een vroegtijdig stadium organisaties kunnen adviseren over mogelijke PET oplossingen, "as feedback from the PRITAC (assessment) process may impact design decisions."[63] PRITAC heeft ook nog andere taken. Het kan een kennisbank over PET en 'best practices' opzetten en gerichte voorlichting aan organisaties geven. Het kan ook een functie vervullen in het openbaarmaken van de functionaliteit van informatiesystemen om aan de burgers transparant te maken wat een bepaald systeem met de gegevens doet. De gegevens zelf worden hiermee niet openbaargemaakt. Het is de bedoeling dat PRITAC ook de nationale toezichthouders op het gebied van privacybescherming op de hoogte zal houden van de laatste ontwikkelingen van technologieën en applicaties die de privacy bevorderen of bedreigen. Op die manier kunnen de toezichthouders tijdig de wetgever verzoeken wettelijke maatregelen te nemen als de privacybescherming in gevaar dreigt te komen ten gevolge van nieuwe technologieën. In de loop van 2011 zal duidelijk worden of de Europese Commissie dit voorstel zal aanvaarden en implementeren.

Aanbeveling III aan de Data Protection authorities en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties:

Richt een Europees of landelijk PET Expertisecentrum op en/of bevorder de oprichting van PRITAC op EU-niveau.

8.5.4. De multi-actoranalyse

RAND Europe heeft in 2003 de problemen met het gebruik van PET binnen de Nederlandse overheid geïnventariseerd. Op basis van die inventarisatie constateert RAND dat de invoering van PET ondermeer een 'multi-actor'probleem is. Dat wil

---

62 De tekst tussen de haken was de eerdere concept tekst. De definitie van new technology is "A technological new product, service, system or process, including those with significant improvement or change. The technological new product, service, system or process could consist of a variety of scientific, technical, organizational, financial and commercial attributes".

63 Borking, Bourka & Whelan, 2009, p. 15.

zeggen: "een probleem waarbij de besluitvorming over de invoering, de uitvoering zelf en de beschikbare middelen over de betrokken belanghebbenden (centrale overheid, afzonderlijke instanties en afdelingen, data-eigenaren en klanten) is verdeeld."[64]

In hoofdstuk 5 is gebleken dat PET-functionaliteiten, zoals 'Identity protectors' en scheiding van gegevensdomeinen, in de architectuur van het privacyveilig informatisysteem moeten worden ingebouwd Daarnaast kunnen de belanghebbenden specifieke eisen en wensen hebben. Het is daarom noodzakelijk om hen actief te betrekken bij het besluitvormingsproces. Zo kan een breed draagvlak worden gecreëerd waardoor PET makkelijker als oplossing geaccepteerd wordt. Een activistische toezichthouder voor de bescherming van de persoonlijke levenssfeer kan daarbij een belangrijke rol spelen. Zonder een breed draagvlak van alle betrokken partijen zullen organisaties PET niet toepassen en de invoering ook tegenwerken, met name wanneer hun eisen en wensen worden genegeerd en de belangen van betrokkenen worden geschaad.[65] Een voorbeeld van een overheidsinstantie die een privacybeschermende architectuur heeft toegepast is de Canadese provincie Alberta. Deze architectuur is een uitbreiding op de reeds bestaande ict-infrastructuur en de Government of Alberta Enterprise Architecture (GAEA). Dankzij de voorgestelde privacymanagementsysteemarchitectuur kan de overheid van Alberta haar privacybeleid met gebruikmaking van ict realiseren. In oktober 2002 legden beleidsambtenaren samen met ambtenaren die verantwoordelijk waren voor de ict-infrastructuur en vertegenwoordigers van het bedrijfsleven in detail de vereisten voor de privacyarchitectuur vast. Dit deden zij in overheidsbreed georganiseerde werkvergaderingen. In deze workshops gaven PET-deskundigen uitgebreide voorlichting over de organisatorische en technische kanten van PET en privacy- en identiteitsmanagementsystemen en over de mogelijke voor- en nadelen. Het resultaat van deze workshops leidde tot een multi-actoranalyse.[66] Die bevatte oplossingen waarin de belangen van alle betrokkenen werden meegewogen en die alle betrokkenen (als compromis) konden aanvaarden. Hieruit kwam een lijst van drieënveertig kernvereisten voort.[67] Deze vereisten werden gedetailleerd vastgelegd in het beleidsstuk *GAEA Privacy Architecture Requirements*.[68] Hierin werden onder meer afspraken gemaakt over:

1. de taxonomie van gemeenschappelijk te gebruiken privacyterminologie;
2. de noodzakelijke gebruikersinterfaces;
3. het gebruik van specifieke PET-maatregelen om het privacybeleid af te dwingen;

64 Horlings, e.a., 2003, p. 65.
65 Riesewijk & Warmerdam, 1988, p. 15. Bij informatisering zijn machtsaspecten in het geding. Zie ook Franken, Borking & van Schelven, 1999, p. 37-48.
66 Van de Riet, 2003, p. 25-33.
67 Rockley, 2004.
68 http://domino.watson.ibm.com/odis/odis.nsf/pages/case.16.html.

4. de invoering van een identiteitssysteem gebaseerd op betekenisloze maar unieke nummers (MBUNs).[69] Deze nummers refereren aan domeinen van persoonsgegevens die bewust gefragmenteerd zijn en zo slechts per deel te benaderen zijn. Het concept van identificatiesleutelnummers is gebaseerd op het inzetten van 'Identity protectors' en gelaagde en gescheiden identiteitsdomeinen zoals uiteengezet in hoofdstuk 5.

Nadat de provinciale overheid van Alberta de vereisten voor de privacyarchitectuur in kaart had gebracht, heeft zij een testmodel ontwikkeld. De deelnemers aan dezelfde werkgroepen voorzagen dit vervolgens van commentaar. Met de verkregen informatie werd ten slotte het privacymanagementsysteem gerealiseerd.[70] Vanwege de complexiteit zou de verantwoordelijke van het informatiesysteem standaard bij invoering van PET altijd een multi-actoranalyse moeten uitvoeren. Hij zou de partijen die een belang hebben bij de gegevensverwerking ook moeten betrekken bij de besluitvorming over de invoering, de uitvoering en de beschikbare middelen.

Aanbeveling IV aan de verantwoordelijken:

Voer voordat een opdracht wordt gegeven voor de ontwikkeling van een informatiesysteem of programmatuur waarmee persoonsgegevens worden verwerkt een multi-actoranalyse uit. Daarmee worden mede automatiseringsdebacles voorkomen.

8.6. Stappenplan voor succesvolle implementatie

Intern moet er binnen de organisatie ook veel gebeuren wil een privacyveilig systeem goed functioneren. Een organisatie moet PET doelgericht toepassen. Dat vereist dat de organisatie zich bewust is van de noodzaak van persoonsgegevensbescherming en PET.[71] Dit houdt in dat bij het opstellen van de ontwerpeisen altijd rekening gehouden moet worden met de juridische specificaties (OV 1). Covers en Schmidt noemen deze combinatie van vereisten 'legal requirements engineering'.[72] Om PET in te voeren zal de organisatie de eerder getroffen maatregelen, procedures voor het beheer, beveiliging en de verwerking van gegevens moeten toetsen aan de doelstellingen. Bij afwijking van de doelstellingen zal de organisatie het eerdere stelsel van maatregelen en procedures dat binnen de organisatie geldt moeten heroverwegen. De implementatie van PET gaat gepaard met technische maar ook met organisatorische problemen. Het

69 De MBUNs zijn niet gebaseerd op reeds bestaande identificerende nummers.
70 Koorn, e.a., 2004, p. 66. Het privacy management systeem is gebaseerd op een door IBM ontwikkelde Enterprise Privacy Architecture. Zie: http://www.gov.ab.ca/home/NewsFrame.cfm?ReleaseID=/acn/200311/15428.html.
71 Koorn, e.a., 2004, p. 70.
72 Curvers & Schmidt, 2008, p. 129.

management van een organisatie is hiervoor primair verantwoordelijk. Om PET succesvol in nieuwe informatiesystemen te implementeren raadt Koorn e.a. organisaties het volgende specifieke PET stappenplan aan:[73]

1. In de eerste plaats moet de noodzaak en de diepgang van gegevensbescherming binnen de organisatie worden geanalyseerd.[74] Deze fase levert een overzicht op waaruit vast te stellen is welke persoonsgegevens om welke redenen moeten worden verwerkt.[75]
2. Vervolgens dient de organisatie een PIA of privacybedreigingsanalyse, zoals beschreven in hoofdstuk 4, uit te voeren om de bedreigingen en risico's die optreden bij de verwerking van persoonsgegevens in kaart te brengen. Op grond van de resultaten van de privacyimpact(risico)analyse kan de organisatie bepalen welke vorm van bescherming gewenst is voor de persoonsgegevens die moeten worden verwerkt.
3. Daarna stelt de organisatie vast of het noodzakelijk is PET toe te passen en hoe PET aan de gegevensbescherming kan bijdragen.[76] De organisatie zal een balans moeten vinden tussen enerzijds de organisatorische en procedurele maatregelen en anderzijds de technische maatregelen waaronder PET-maatregelen. Uit de bevindingen van de PIA zal blijken of er sprake is van identiteitsrijke (identificerende persoonsgegevens vereist), identiteitsarme (identiteit eenmalig nodig, maar één persoonskenmerk zoals leeftijd of beroep volstaat) of identiteitsloze processen (geen identiteit nodig).

   Bij identiteitsrijke processen zijn met name de algemene PET-maatregelen toepasbaar: encryptie, toegangsbeveiliging, functionele autorisatie, biometrie en privacymanagementsystemen, zoals besproken in de paragrafen 5.7.2 en 5.12. Bij identiteitsarme processen zijn scheiding van gegevens in identiteit- en pseudo-identiteitdomeinen, zoals besproken in hoofdstuk 5, algemene PET-maatregelen en privacymanagementsystemen goed toe te passen.

   Bij identiteitsloze processen zijn scheiding van gegevens in (pseudo) identiteitsdomeinen en het anonimiseren de aangewezen PET vormen[77].
   In deze fase zal de organisatie ook moeten vaststellen of er sprake is van een positieve businesscase, daarover in de paragraaf 8.6 meer.
4. Vervolgens maakt de systeemontwerper onder meer een procesmodel van de gegevensstromen binnen het informatiesysteem. Koppelingen en uitwisselingen met andere organisaties worden hier ook bij betrokken.
5. De systeemontwerper geeft daarnaast in datamodellen voor iedere gegevensstroom het verwerkingsproces weer van het verzamelen, opslaan, bewaren tot

---

73 Bij legal Engineering zijn nog veel meer vragen te stellen, zie Curvers & Schmidt, 2008, p. 137-141; Holvast, 2002.

74 De precieze uitwerking van de privacymaatregelen in de programmatuur en technische infrastructuur komt uiteindelijk naar voren in de fasen functioneel en technisch ontwerp.

75 Koorn, e.a., 2004, p. 65.

76 Borking, 1990, p. 98-99.

77 Koorn, e.a., 2004, p. 40 (PET vormentrap), p. 70-72.

aan het vernietigen van gegevens. De volgende factoren zijn mede bepalend voor het ontwerp:
- de herkomst van de persoonsgegevens (eventueel gebruik van authentieke registraties en koppelingen met andere gegevensbestanden);
- het type persoonsgegevens (eventuele bijzondere gegevens);
- het type verwerkingsprocessen (eventuele geautomatiseerde beslissingen);
- de gebruikers(groepen) aan wie de organisatie de gegevens verstrekt (eventuele ontvangers buiten de organisatie of zelfs buiten de EU);
- het vereiste niveau van zelfbeschikking van de burger en de informatieplicht aan de burger;
- de privacypreferenties, de beheerder en verantwoordelijke van de gegevens (eventuele uitbesteding);
- de bewaartermijnen (eventuele verplichte vernietiging);
- de betrokkenen bij de gegevensverwerking (eventuele gemachtigden en bewindvoerders).[78]

Het geheel eindigt in het functionele ontwerp waarin de benodigde functies van het informatiesysteem in hun onderlinge verband worden beschreven. Koorn e.a. waarschuwt dat de PET oplossing die een organisatie kiest, grote invloed heeft op het ontwerp. De scheiding van identiteit- en pseudo-identiteitdomeinen heeft directe gevolgen voor het gegevensmodel en voor de koppelingen tussen de (pseudo)identiteitsdomeinen en tussen eventuele andere informatiesystemen die gegevens onttrekken aan de gegevens van de organisatie.[79]

6. De geselecteerde PET vorm wordt vervolgens geïntegreerd in het technisch ontwerp van het informatiesysteem. De PET-vorm is immers geen los toe te voegen component en daarom kan het technisch ontwerp van PET niet los worden gezien van het technisch ontwerp van het gehele informatiesysteem.
7. Cruciaal is de testfase.[80] De opdrachtgevers en de ontwerpers moeten vaststellen of het systeem functioneel conform de specificaties[81] voldoet en of de gebruikers het nieuwe systeem accepteren.[82] In de tests komt dan ook de functionaliteit en de gebruikersvriendelijkheid van PET aan de orde. Gezien de adoptiefactor omtrent de testbaarheid is het raadzaam om eerst een kleinschalige pilot te starten net zoals in de eerder in dit hoofdstuk besproken casestudy 'Province of Alberta'. De resultaten van de pilot kunnen leiden tot nadere aanpassingen van het *PET-proof* informatiesysteem. Het is raadzaam om bij het testen rekening te houden met de schaalbaarheid van het systeem. Dit geldt te meer als gekozen is voor een privacymanagementsysteem is. Dan

78 Koorn, e.a., 2004, p. 72-73.
79 Koorn, e.a., 2004, p. 73.
80 Borking, 1990.
81 Berkvens, e.a., 1989, p. 245-246.
82 Brandon & Segelstein, 1976, p. 136 en 368.

is tijdens het testen gerichte aandacht nodig voor de feitelijke handhaving van de privacyregels die in dit systeem zijn geprogrammeerd.[83]

8. Nadat de organisatie de testfase heeft afgerond, kan het systeem worden uitgerold. Na verloop van tijd beoordeelt de organisatie of het systeem en de PET-maatregelen effectief zijn. Dit gebeurt aan de hand van een evaluatieplan en evaluatiecriteria, vergelijkbaar met het evaluatieonderzoek van de metazoekmachine Ixquick dat in de paragafen 6.5.1 tot en met 6.5.4 is beschreven.
9. Om ervoor te zorgen dat de gebruiker/burger/consument meer vertrouwen krijgt in het informatiesysteem, verdient het aanbeveling om het informatiesysteem te laten certificeren wat betreft de bescherming van de persoonsgegevens.[84]

Het blijkt in de praktijk overigens niet zo gemakkelijk PET in bestaande systemen te implementeren. Koorn e.a. stelt dat PET geen *black box* is die men koopt en achteraf aan een bestaand informatiesysteem toevoegt. Bij bestaande systemen zal door de gekozen PET-oplossing het datamodel moeten worden aangepast. Deze aanpassingen behelzen het bestaande informatiesysteem, de applicatie programmatuur en de databasearchitectuur. PET leidt vaak ook tot aanpassingen van de autorisatiestructuur, vooral als de PET oplossing inhoudt dat gegevens over identiteitsdomeinen gescheiden moeten worden. Een dergelijke ingrijpende systeemaanpassing is kostbaar.[85]

Aanbeveling V aan de verantwoordelijken:

Volg het in deze paragraaf uiteengezette stappenplan om privacyveilige systemen te verwezenlijken.

8.7. Positieve businesscase

Er wordt door de overheid en het bedrijfsleven nauwelijks geinvesteerd in privacyveilige systemen. Kosten zijn een negatieve adoptie factor voor het gebruiken van PET. Businessmodellen om de investering in privacybescherming te onderbouwen, ontbreken vrijwel geheel. In hoofdstuk 7 heb ik aangetoond dat een organisatie PET-maatregelen niet zal invoeren zonder een positieve businesscase. Volgens het PRIME-onderzoek naar het 'Business Model and Economic Drivers for Privacy Enhancement' is de maturiteit van de organisaties op het gebied van IAM en privacybescherming een indicatie wanneer PET binnen een

---

83 Koorn, e.a., 2004, p. 73.

84 Détraigne & Escoffier, Paris, 2009, p. 73-74: "Il s'agit là d'une condition essentielle pour préserver le **climat de confiance** entre les nouvelles technologies et les utilisateurs.(…) Concrètement, un tel label pourrait récompenser des protocoles,standards et outils **limitant, voire supprimant, la collecte des données à caractère personnel**, ce que les Américains appellent les « *PrivacyEnhancing Technologies* » (ou « PET »), c'est-à-dire les technologies renforçant le droit à la vie privée."

85 Koorn, e.a., 2004, p. 66-69.

organisatie kan worden toegepast.[86] De S-curves die bij IAM, privacybescherming en PET horen maken het mogelijk te voorspellen wanneer organisaties zouden kunnen overstappen op PET-maatregelen. Het management van kleine en middelgrote organisaties zal meestal besluiten in PET te investeren als de businesscase een positief rendement oplevert. Helaas is het zo dat het MKB veelal niet beschikt over de informatie en kennis om een goede businesscase op te stellen. Grote bedrijven hebben vaak zo hun eigen redenen om in PET te investeren. Rendementsberekeningen spelen daarbij niet per se een rol. Wel is het zo dat de voorgenomen PET-investeringen met andere investeringen zullen moeten concurreren. De noodzakelijke andere verplichtingen van de organisatie en de beschikbaarheid van financiële en andere middelen (bijvoorbeeld personeel, managementinzet) zullen beperkingen vormen die de organisatie in acht moet nemen. Of een project een hoge prioriteit heeft, hangt af van het belang dat het management eraan hecht.

Door drie kernvragen te beantwoorden wordt duidelijk of een organisatie PET kan toepassen.

a. Draagt PET in belangrijke mate bij aan de beleidsdoelstellingen van de organisatie?
b. Welke kosten brengt PET eenmalig en structureel met zich mee?
c. Wat is het kwalitatieve (positief imago, verbeterde dienstverlening) en kwantitatieve (aantoonbare kostenreducties) voordeel van PET voor de organisatie?[87]

Als uit het antwoord op deze vragen blijkt dat de toepassing van PET wenselijk én vanuit een kosten-batenperspectief rationeel is, dan is er sprake van een positieve businesscase voor de toepassing van PET. Daarvoor zal een organisatie ook een kosten-batenanalyse moeten maken. De in hoofdstuk 7 uiteengezette ROIPI-methode kan daarbij als een ‘quick and dirty’analyse een goed hulpmiddel zijn, maar een Net Present Value cash flowberekening is nauwkeuriger. Er zijn echter geen betrouwbare empirische gegevens over privacyincidenten binnen de Europese Unie beschikbaar. Daardoor kunnen de consequenties van dergelijke incidenten niet accuraat worden ingeschat en de rendementsberekeningen onnauwkeurig zijn. Dat hiaat in empirische gegevens zou kunnen worden opgevuld door een Europees instituut op te richten dat de inbreukgegevens binnen de EU verzamelt, analyseert en publiceert, net zoals Ponemon[88] dat in de Verenigde Staten doet.

86 Fairchild & Ribbers, 2008, p. 82-100.
87 Koorn, e.a., 2004, p. 47-56.
88 Ponemon, 2007, http://download.pgp.com/pdfs/Ponemon_COB-2007_US_071127_F.pdf.

Wanneer organisaties verplicht worden om verlies en diefstal van persoonlijke informatie bekend te maken en te laten registreren (zoals het wijzigingsvoorstel van de e-privacyrichtijn 2002/58/EG[89] beoogt), zullen burgers het vertrouwen terugkrijgen in organisaties, mits deze organisaties de burgers op de hoogte te stellen van de maatregelen die de organisatie neemt om schade en toekomstige inbreuken te voorkomen.[90] De melding zal ongetwijfeld leiden tot reputatieschade voor de betrokken organisatie. Dat kan voor bona fide organisaties een sterke aansporing zijn om de beveiliging van persoonsgegevens te optimaliseren.[91] Organisaties die al onzorgvuldig zijn wat betreft hun informatiebeveiliging, zullen vermoedelijk de beveiligingsbreuk niet rappor-teren.[92] De Branchevereniging van IT-, telecom-, internet- en officebedrijven laat in haar nieuwsbrief ICT ~ Office Online van 25 juni 2009 naar aanleiding van het rapport 'Melding maken?' van het Ministerie van Economische Zaken[93] weten dat een meldplicht niet tot betere beveiliging leidt als er geen sanctie staat op het niet-aanmelden van het privacyincident. De bescherming van privacygevoelige gegevens staat niet hoog op de prioriteitenlijst van organisaties. Volgens Koorn en Ter Hart (KPMG)[94] beschermt slechts 5% van alle Nederlandse bedrijven zijn privacygevoelige gegevens conform de vereisten van de Wet bescherming persoonsgegevens.[95] Hetzelfde verschijnsel doet zich voor in de Verenigde Staten. Baker concludeert dat: "In 59% of breaches, security policies were established but not enacted through actual process; 83% of attacks were not considered to be highly difficult and 85% were opportunistic; 39% of breaches involved business partners and 66% of breaches involved data not known to be on the system. Efforts to locate, catalogue and track sensitive data and assess risk are highly beneficial."[96]

De meeste bedrijven denken pas echt na over de bescherming van de aan hun toevertrouwde persoonsgegevens als er weer een privacyinbreuk in het nieuws komt. Een voorbeeld daarvan is het in hoofdstuk 4 vermelde privacyincident waar de British Revenue and Customs Office 25 miljoen gedetailleerde persoonsgegevens van burgers die in aanmerking kwamen voor sociale voorzieningen, kwijtraakte.[97]

---

89 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

90 Boer & Grimmius, 2009, p. 10.

91 Détraigne & Escoffier, 2009, p. 102 "Il semble possible d'aller un peu plus loin en créant a minima une obligation de notification des failles de sécurité à la CNIL, des critères et des seuils devant être définis pour ne pas la submerger. Cette obligation pèserait sur tous les responsables de traitement. Bien maîtrisée et encadrée, l'obligation de notification des failles desécurité peut être une incitation forte au renforcement de la sécurité des données".

92 Boer & Grimmius, 2009, p. 10.

93 http://www.ez.nl/dsresource?objectid=163644&type=PDF.

94 Koorn & Ter Hart, 2004, p. 15-22.

95 De nieuwsrubriek van het World Data Protection Report van maart 2009 (vol. 9. nr. 3, p. 30) vermeldt dat in de Verenigde Staten TRUSTe finds that small businesses don't take online privacy seriously. Meer dan 50% heeft geen privacy policy en 21% is onzeker of er wel beveiligingsmaatregelen (o.a. encryptie van webpages) zijn genomen.

96 Baker, e.a., 2009 p. 47.

97 Financial Times 21 November 2007: "Massive data loss hits UK", p. 1.

Aanbeveling VI aan de verantwoordelijken en adviserende accountants:

Bereken vooraf de Return on Investment van PET-maatregelen, opdat er een gewogen management beslissing genomen wordt over de invoering van privacybeschermende maatregelen en reputatieschade kan worden voorkomen.

8.8. Aanbevelingen voor de aanpassing van de EU-privacyrichtlijnen

In mei 2009 is de Europese Commissie gestart met een 'public consultation' over de uitdagingen waarmee de EU privacyrichtlijnen door de vele technologische innovaties zullen worden geconfronteerd. Het zal wel een jaar of drie duren voordat de Commissie hierover een rapport zal publiceren. Tegelijkertijd onderzoeken de OECD en de Raad van Europa of de Guidelines respectievelijk de Convention 108 ook moeten worden herzien. Hieronder volgen in paragraaf 8.8.1 aanbevelingen voor de aanpassing van de Richtlijn 95/46/EG. In paragraaf 8.8.2 staan de aanbeveling om de verantwoordelijke manager voor de gegevensverwerking persoonlijk aansprakelijk te stellen voor privacy inbreuken, alsmede de aanbeveling productaansprakelijkheid voor privacyveilige producten en diensten in te voeren. In paragraaf 8.8.3 zijn drie aanbevelingen opgenomen om 'privacy by design' wettelijk verplicht te stellen, verplichte PIA; gebruik van PET 'by default'; en de wettelijke verplichting dat de gebruiker van elke dienst en (netwerk) infrastructuur ook de optie voor de gebruiker bestaat anoniem gebruik kan maken. In paragraaf 8.8.4 wordt betoogd dat in elk informatiesysteem terugkoppeling aan en controle door de gebruiker moet worden geboden. Op grond van de resultaten van de research binnen het Europese Framework Programme verwacht ik dat binnen vijf jaar 'data track' en 'sticky policies' in het ontwerp van informatiesystemen een vaste plaats hebben gevonden.

8.8.1. Algemene wetsaanpassingen

Zoals in hoofdstuk 2 vermeld, voorziet Poullet dat de ict-ontwikkelingen een derde generatie privacywetgeving[98] noodzakelijk zullen maken. Deze ontwikkeling is met de e-privacyrichtlijn 2002/58/EG en de universele dienstenrichtlijn 2002/22/EG[99] in feite al in gang gezet. De structuur en de rechten die aan de gebruiker worden toegekend, wijzen daarop. De derde generatie privacywetgeving zal een "increased

98 De eerste generatie startte met de EVRM: Privacy als recht om gevoelige gegevens, huis, gezin en familierelaties af te dekken tegenover de buitenwereld; de tweede generatie loopt van de Raad van Europa Convention N° 108 (1981) tot de EU Charter on fundamental rights (2000: verbreding van bescherming tot alle persoonsgegevens – 3 principes: legitimiteit van de verwerking, recht op transparante verwerking voor de betrokkene en de rol van de toezichthouder (DPA) om het evenwicht tussen de betrokkene en de verantwoordelijke te bewaren.

99 OJ L 108, 24.4.2002, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

protection of the intimate sphere beyond the DP directive" met zich meebrengen.[100] De uitspraak van 27 februari 2008 van het Bundes Verfassungsgericht wijst ook in deze richting:

> "Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" en "Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt."[101]

Poullet stelt dat de EU-Richtlijn 95/46/EG ten gevolge van de steeds verdergaande ontwikkelingen van de ict op een viertal punten moet worden uitgebreid:
1. nieuwe persoonsgegevens;
2. middelen waarmee gegevens worden verwerkt;
3. een nieuwe groep van verantwoordelijken;
4. de doelstellingen.[102]

Ad 1 Nieuwe persoonsgegevens
a. Biografische gegevens: AMI-sensoren registreren en leggen continu biografische gegevens vast. Dat zijn de gegevens die door gebeurtenissen gedurende het dagelijkse leven van een individu ontstaan.
b. Verkeers- en de locatiegegevens: dat is elk gegeven dat wordt verwerkt met betrekking tot het transport van de communicatiesignalen, zoals besproken in paragraaf 2.6.2.

   Die zorgen er volgens Poullet voor, dat "instantaneous slices of my life, far beyond my traditional expectation"[103] direct worden verwerkt. Zoals uit hoofdstuk 2 van dit boek blijkt, zijn de verkeers- en locatiegegevens privacygevoelig.
c. 'Anchorage point' ook wel genaamd 'matching identifiers'gegevens.[104]

   Dit zijn identificerende gegevens van een individu of van een voorwerp dat tot een individu behoort. Dergelijke 'matching identifiers' maken het voor overheid en bedrijfsleven mogelijk om in verschillende databases gegevens bij elkaar te zoeken om correlaties of profielen van een individu te maken.
d. 'Identifiers' ook wel contactdata genoemd: Dit zijn gegevens die het mogelijk maken dat dienstverleners met een persoon of zijn eindapparatuur ogenblikkelijk

100 Poullet, 2009, p. 18; Poullet, 2009(A), p. 3.
101 BVerfG, 1 BvR 370/07 vom 27-2-2008, Absatz-Nr. (1-333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.
102 Poullet, 2009, p. 4.
103 Poullet, 2009, p. 4.
104 Poullet, 2009, p. 4.

contact kunnen maken en onmiddellijk actie kunnen ondernemen (bijvoorbeeld door middel van de banners op het scherm) of door een cookie achter te laten, zoals bij de in hoofdstuk 6 besproken dienstverlening van Ixquick. Volgens Poullet is noodzakelijk een specifieke regelgeving te treffen voor 'anchorage point data' en voor contactdata (bijvoorbeeld cookies, verkeersgegevens en RFIDs die de persoonlijke ruimte van individuen binnendringen), zonder dat er in alle gevallen sprake van persoonsgegevens is (in de betekenis van de EU-Richtlijn 95/46/EG). Poulet geeft als voorbeeld een RFID in een winkelwagentje waarop een klein scherm is geplaatst waarmee het mogelijk is de persoon tijdens het winkelen persoonlijk gerichte reclame per product te zenden. Poullet: "Can we consider that data is becoming personal just because it is possible through this data to have an impact towards an individual?"[105] In hoofdstuk 2 wees ik er op, dat de Article 29 Working Party in haar Opinion nr. 4/2007 uitgebreid commentaar heeft gegeven op de reikwijdte van het begrip persoonsgegevens in de Richtlijn 95/46/EG. Op bladzijde 7 stelt zij dat: "The concept of personal data includes information kept in any form, e.g., on paper, in the form of information stored in a computer memory by means of binary code, or in analogue form on a videotape, for instance. In particular, sound and image data qualify as personal data (…), insofar as they may represent information on an individual." De Article 29 WP hanteert een ruime uitleg van het begrip persoonsgegevens, zodat de vraag van Poullet bevestigend kan worden beantwoord.

Ad 2 De middelen waarmee persoonsgegevens worden verwerkt

In hoofdstuk 2 is aangegeven dat de wetgever in artikel 5.3[106] en artikel 14.3 [107] van de e-privacyrichtlijn 2002/58/EG privacybeschermende bepalingen heeft voorgeschreven voor terminals. Poullet schrijft dat hij verwacht dat deze aanpak zich in andere wetgeving zal doorzetten. Zo kan het vereiste van 'privacy by design' (PET-toepassen in informatiesystemen) afgelezen worden uit: "(…) recent opinions of the Article 29 Working Party about P3P and RFID Information systems (I.S.) and I.S. Products must be at the benefit of the society and of the citizen's liberties (…) recital 2 of the DP Directive implies the obligation to design the products in order to ensure the respect of citizen's privacy and to avoid any privacy threats."

Ad 3 Een nieuwe groep van verantwoordelijken

Naast de traditionele actoren, zoals de verantwoordelijke, de betrokkene, de bewerker en de toezichthouder, vindt Poulet dat ook de nieuwe actoren, zoals de

105 Poullet, 2009, p. 5.

106 Article 5.3 "(...) storing of information, or to gaining access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC (…)".

107 Article 14.3: "Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications".

producenten van eindapparatuur, software en programmatuur die in chips is ingebouwd ('firmware'), een plaats in de wetgeving moeten krijgen. Bijvoorbeeld uit de tekst van de e-privacyrichtlijn 2002/58/EG, die in hoofdstuk 2 is toegelicht, is vast te stellen dat leveranciers van openbare communicatiediensten wordt opgedragen a) vertrouwelijk om te gaan met persoonsgegevens, b) deze te beveiligen conform het risiconiveau dat bij de verwerking behoort en c) verkeers- en locatiegegevens op een rechtmatige manier te gebruiken. Bovendien blijkt dat als gevolg van de ontwikkelingen binnen de ict de rol van verantwoordelijke en betrokkene in de zin van de EU-Richtlijn 95/46/EG tegelijkertijd door een en dezelfde persoon of organisatie kan worden vervuld. Doordat intelligente software agents (ISAs) (zie hoofdstuk 6) persoonsgegevens verzamelen en uitwisselen, kan de gebruiker van ISAs ook de rol van verantwoordelijke krijgen, wanneer de software agents PII van de andere partijen tijdens de transactie ontvangt. Poullet wijst op hetzelfde fenomeen bij Web 2.0 waar "data subjects are becoming at the same time data controllers".[108]

Ad 4 Aanpassing van de doelstellingen

Ter bescherming van het individu dienen de doelstellingen van de privacybeschermende wetgeving te worden uitgebreid. Poulet somt in deze context de volgende punten op, die een uitbreiding rechtvaardigen:

1. "The Right not to be submitted continuously to advertisements; 2. The Right not to be excessively controlled (with regard to video-surveillance and electronic government); 3. The Right not to be profiled without being informed and the right to have knowledge of the inferences beyond the application of a profile; 4. Severe limits as regards intrusion into the human body like RFID implants; 5. Limits as regards consent as a basis for a legitimate processing."[109]

Aanbeveling VII aan de Europese wetgever:

Pas de tekst van de EU-privacyrichtlijn 95/46/EG aan in lijn met de nieuwe technologische ontwikkelingen, zodat rekening wordt gehouden met:

1. nieuwe persoonsgegevens;
2. nieuwe middelen waarmee gegevens worden verwerkt;
3. de nieuwe groep van verantwoordelijken;
4. de gewijzigde doelstellingen;
5. de ontwikkelingen op het gebied van 'ambient intelligence'.

8.8.2. Uitbreiding van de aansprakelijkheid

In interviews die in het kader van deze dissertatie zijn uitgevoerd met verantwoordelijken in Zweden, Nederland, het Verenigd Koninkrijk en Zwitserland,

108 Poullet, 2009, p. 11.
109 Poullet, 2009, p. 11.

werd de vraag gesteld of men de privacywetgeving beter zou naleven als er een kans was dat de overtreding van de privacywet zou worden ontdekt. Hierop reageerden de ondervraagden schouderophalend. In het interview bij een Zweedse multinational deelden de betrokken managers, na discussie over een zeer ernstig privacyincident, mee dat vier jaar procederen en enige miljoenen euro's schadevergoeding te verwaarlozen is in verhouding tot de schade die ontstaat door de verslechterde reputatie van het bedrijf: "In terms of overall impact on the business, costs are not an issue since we have to fix it to earn back trust."[110] Volgens de EU-Richtlijn 95/46/EG is de verantwoordelijke aansprakelijk voor privacyinbreuken. Dit houdt in dat uiteindelijk de aandeelhouders voor de boetes en schadevergoedingen opdraaien. Voor het management van de organisatie blijkt daar geen afschrikwekkende werking van uit te gaan.

In interviews in Nederland bij twee multinationals werd dezelfde vraag als in Zweden over de aansprakelijkheid gesteld. Als antwoord gaven de ondervraagde managers dat zij het veel effectiever achtten wanneer de verantwoordelijke manager zelf aansprakelijk wordt gesteld voor de privacyinbreuken, vergelijkbaar met de 'Sarbanes-Oxley Act' (SOX). In artikel 302 van de Amerikaanse Sarbanes-Oxley Act van 2002[111] over 'corporate responsibility for financial reports' bepaalt lid 4 (A): "the signing officers are responsible for establishing and maintaining internal controls." Dit ervaren de ondervraagde managers wel als afschrikwekkend. Als iets dergelijks voor in de Wbp of EU-Richtlijn 95/46/EG zou staan, dan zou dat een groot verschil kunnen maken voor de handhaving van de privacywetgeving.[112] In een van de interviews in het kader van dit proefschrift in Nederland stelde een Chief Privacy Officer van een grote onderneming dat:

> "Sarbanes-Oxley makes a CEO and CFO manager personally liable. SOX only covers privacy, if the financial risk of privacy risks is going over a certain threshold. If it is going over a certain level I have to report my boss and eventually (above 10 Million Euros) it becomes a board issue. Privacy in itself is almost never raising a big financial issue under SOX. Privacy is much more a compliance issue and is a lawyer's problem. Privacy is not considered as a serious risk issue. SOX, however, is about risk issues!"[113]

De wet zou beter kunnen worden nageleefd wanneer de aansprakelijkheidsparagraaf in de wetgeving over de bescherming van persoonsgegevens de verantwoordelijke operationele manager aansprakelijk zou stellen. Voor productaansprakelijkheid lijkt zich een consensus af te gaan tekenen. Net zoals producenten van onveilige auto's aansprakelijk gesteld kunnen worden, zou dit ook voor ontwerpers van privacyonveilige informatiesystemen moeten gelden.

110 Transcript interview Zweden 24 Februari 2008, p. 2 en 3.
111 H.R. 3763 (2002) An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.
112 Ribbers, Dijkman & Borking, 2007, p. 6.
113 Ribbers, Tjeng & Borking, 2008, p. 4.

Borking en Foukia schrijven dat ontwerpers van software agents zoals PISA (zie hoofdstuk 6), mogelijk aansprakelijk kunnen worden gesteld:

> "(...) agents while operating, violating the DPD or other privacy laws, should be held liable under product liability rules, if the design and architecture of the agent allows violation of the data subject's privacy. True, in the case of unlawful processing of personal data, the EC system of law is that the data subject always can hold the controller responsible (article 23 (1) Directive 95/46/EC). A controller can't defer his responsibility for privacy violations to a third party developer, even if this developer has deviated from the agreed design. However if there are design defects that cause violation of someone's privacy the controller can sue for product liability irrespective of disclaimers of warranty. Liability lawsuits between the controller and the third party developer or any person or company which had anything to do with fabricating or distributing the privacy defect agent are ruled under civil or common law and not under privacy legislation."[114]

Poullet deelt deze mening en stelt eveneens dat op termijn een situatie kan ontstaan: "towards a system of 'Products liability' in case of commercialization of non privacy compliant terminals (towards telecommunication companies and terminal equipment manufacturer's)."[115]

Aanbeveling VIII aan de Europese- en Nederlandse wetgever:
1. Stel in eerste instantie niet de verantwoordelijke zoals gedefinieerd in de EU-Richtlijn 95/46/EG voor de onrechtmatige persoonsgegevensverwerking aansprakelijk, maar de manager die direct bij de verwerking betrokken is, vergelijkbaar met de aansprakelijkheidsregeling in de Amerikaanse SOX.
2. Voer productaansprakelijkheid in voor privacyonveilige informatiesystemen, vergelijkbaar met de productaansprakelijkheid voor onveilige producten.

8.8.3. Vier wetsaanpassingen voor 'privacy by design'

In hoofdstuk 7 is aangegeven dat het belang van privacywetgeving voor de adoptie van PET significant is. Een wettelijk verplichte 'privacy by design'[116] draagt ertoe bij dat burgers en consumenten hun persoonsgegevens met een gerust hart aan de overheid en het bedrijfsleven kunnen verstrekken.[117]

Om ervoor te zorgen dat 'privacy by design' op korte termijn een reële optie is, is het noodzakelijk dat privacy by design gedefinieerd wordt en er drie wijzigingen worden doorgevoerd in de Europese en nationale wetgeving op het gebied van de bescherming van persoonsgegevens:

---

114 Borking & Foukia, 2008, p. 3.
115 Poullet, 2009, p. 10.
116 J.A.G. Versmissen & A.C.M. de Heij, Elektronische overheid en Privacy. Bescherming van Persoonsgegevens in de Informatiestructuur van de Overheid, Achtergrondstudies en Verkenningen 25, Den Haag, 2002.
117 The Commission Communication May 2, 2007, promoting Data Protection by PETs: "PETs are a prerequisite for creating confidence in the I.S."

1. De wetgeving moet uitdrukkelijk de verantwoordelijke (in de zin van de richtlijn) verplichten een privacyrisico, privacyimpact- of bedreigingsanalyse uit te voeren, voordat een systeem wordt ontworpen c.q. op de markt wordt gebracht. De Europese privacyrichtlijnen en de daarop geënte nationale wetgevingen van de EU-lidstaten schrijven op dit ogenblik alleen in algemene zin beveiliging van persoonsgegevens voor. Zij voegen daaraan toe dat de verantwoordelijke rekening moet houden met de risico's die ontstaan bij verwerking van persoonsgegevens.[118] De wet- en regelgeving is op dit punt niet verplichtend genoeg en zou uitdrukkelijk zo'n privacy-bedreigings- of risicoanalyse moeten voorschrijven. Zonder een privacybedreigings- of -risicoanalyse kan de verantwoordelijke niet met zekerheid vaststellen welke privacyrisico's er ontstaan bij de verwerking van persoonsgegevens en de introductie van nieuwe informatiesystemen. Ook kan hij niet bepalen welke PET-maatregelen nodig zijn om de geconstateerde risico's te verkleinen. Het zou aanbeveling verdienen om het begrip risico[119] in de Wbp en EU-privacyrichtlijnen te definiëren om de potentiële risico's bij de verwerking van persoonsgegevens vast te stellen. Daarnaast moet (de toelichting op) deze wetgeving duidelijker aangeven wat de potentiële risico's bij de verwerking van persoonsgegevens kunnen zijn.

In hoofdstuk 4 zijn verschillende methodologische aanpakken voor privacyrisico- en bedreigingsanalyses besproken.

2. De privacywetgeving zou uitdrukkelijk PET moeten voorschrijven als technisch middel om de persoonsgegevens te beschermen. In de Wbp is tengevolge van het Amendement Scheltema-de Nie en Wagenaar[120] artikel 13 aangevuld. De voorgeschreven beveiligingsmaatregelen zijn er mede op gericht om onnodige verzameling en verdere verwerking te voorkomen. Daarmee is echter nog niet expliciet aangegeven dat PET bij de beveiliging van persoonsgegevens moet worden overwogen. De Europese Commissie dringt daarop aan in de Commission Communication van 2 mei 2007 waarin staat dat "PETs are a prerequisite for creating confidence in the I.S."

Met name door de ongerustheid die is ontstaan rond de potentiële toepassingen van RFIDs, zijn steeds meer stemmen opgegaan om PET wettelijk verplicht te stellen. Poullet van het 'Centre de Recherche Informatique et Droit' van de Universiteit van Namen adviseert uitdrukkelijk een bepaling toe te voegen aan de

118 Fairchild & Ribbers, 2008, p. 88-91.
119 Risico is het product van de kans op ongewenste gevolgen en de schade die dit kan veroorzaken voor de betrokkene, de verantwoordelijke of de bewerker. Hierbij moet worden uitgegaan van situaties die redelijkerwijs te verwachten zijn.
120 Tweede Kamerstukken 1999-2000, 25 892, nr. 22.

privacyrichtlijnen: "to impose the implementation by default of PETs to terminal equipments' suppliers."[121]

3. In de wetgeving dient opgenomen te worden dat gebruikers de optie moeten hebben om diensten en infrastructuren ook anoniem te kunnen gebruiken.[122] Dit zal ervoor zorgen dat de verantwoordelijke adequate PET maatregelen structureel inzet om een veilige anonimiteit te garanderen.

Aanbeveling IX aan de Europese wetgever/de Europese Commissie:

Neem in de Richtlijnen 95/46/EG en 2002/58/EG de volgende drie verplichtingen op:

1. De verantwoordelijke (in de zin van de richtlijn) dient een privacyrisico-, privacyimpact- of bedreigingsanalyse uit te voeren, voordat een systeem wordt ontworpen c.q. op de markt wordt gebracht. Een dergelijke privacyrisicoanalyse dient aan de Data Protection Authority voorafgaande aan de bouw van het systeem te worden voorgelegd.
2. PET dient als technisch middel om de persoonsgegevens te beschermen 'by default' te worden toegepast; 'Privacy by design' moet als privacy realisatiebeginsel in de richtlijn te worden opgenomen.
3. Gebruikers dient standaard de optie te worden geboden om diensten en infrastructuren ook anoniem te kunnen gebruiken.

8.8.4. Controle en terugkoppeling

Wanneer de juiste PETs in informatiesystemen zijn toegepast, kunnen persoonsgegevens goed beschermd worden. Burgers en consumenten krijgen bovendien nog meer vertrouwen als het informatiesysteem gecertificeerd is waaruit de privacyveiligheid blijkt en er een (afdwingbare) overeenkomst of algemene voorwaarden zijn waaruit blijkt dat de verantwoordelijke c.q. verwerker van de persoonsgegevens de privacypreferenties van de gebruiker van het systeem respecteert.

Sommer & Crane schrijven echter dat: "Being able to say that another party can be completely trusted to handle personal information with today's technology is probably unrealistic. Unless we can 1) completely isolate the processing from the operator and 2) rely on the technology and implementation, we have to rely on some level of faith in the other party. Requirement 1) is unrealistic since in practice virtually every application is likely to involve some form of human intervention, including access to the information after the 'trusted' processing is complete. Requirement 2) is currently difficult to demonstrate."[123] Zoals in

121 Poullet, Brussels, 2009.
122 Klüver, Peissl, & Tennøe, 2006, p. 52.
123 Sommer & Crane, 2008, p. 105.

hoofdstuk 4 paragraaf 4.5 is beschreven, hebben Bellotti en Sellen ervaring met 'media spaces' en de reacties van de mensen die in die 'media spaces'[124] werken. Op basis van die ervaring zien zij ingebouwde controle, reciprociteit en terugkoppeling van de gegevensverwerkende AMI-systemen als ultieme middelen "to safeguard data privacy and preventing that potential records of our activity may be kept and possibly manipulated and used at a later date and out of their original context."[125] Volgens hen schept dit het optimale vertrouwen van het individu in AMI-systemen.

De resultaten van de privacyimpact- en bedreigingsanalyses leiden tot de conclusie dat wanneer de verantwoordelijke zeker wil zijn van een goede privacybescherming de koppeling van de verkregen persoonsgegevens met een pseudo-identiteit van de gegevensverstrekker de beste garanties biedt. Dat vereist dat het individu bij het afgeven van zijn persoonsgegevens zijn pseudo-identiteiten moet gaan beheren. Zodra het mogelijk is de persoonsgegevens van een label te voorzien zodat de betrokkene zijn persoonsgegevens kan volgen (zgn. data tracking[126] zie hoofdstuk 5 en 6) en de verantwoordelijke 'sticky policies' of 'kleefbeleid' toepast op de gegevens die verwerkt worden dan is de situatie bereikt dat de gegevens kunnen worden verwerkt volgens de privacyvoorkeuren van het individu. IBM Research heeft inmiddels aangetoond dat data tracking en 'sticky policies' ervoor kunnen zorgen dat de persoonsgegevens worden verwerkt conform de overeengekomen voorwaarden zelfs nadat de informatie is onthuld en de gebruiker er geen controle meer over heeft.[127] 'Obligation management' (zie paragraaf 6.4) dient een standaard onderdeel van de architectuur van het informatiesysteem te zijn. Privacybescherming kan alleen maar werken als de gegevensverwerkers het basisprincipe respecteren dat het individu het onvervreemdbare recht op informationele zelfbeschikking heeft zoals het Bundes Verfassungsgericht in 1983 heeft duidelijk gemaakt.[128]

Aanbeveling X aan de Europese wetgever:

Zorg voor wetgeving die controle, reciprociteit en terugkoppeling aan de gebruiker van informatiesystemen voorschrijft met name voor AMI-systemen. Bevorder dat Obligation Management Systemen een vast onderdeel van het informatiesysteem worden, dat persoonsgegevens verwerkt.

---

124 *Media spaces* zijn werkplekken voor onderzoekers waar continue multimedia verbindingen (beeld, geluid, dataverwerking) tussen elke werkplek en iedere onderzoeker ingeschakeld zijn.

125 Bellotti & Sellen, 1993, p. 7-8; Bellotti & Sellen, 1993(A).

126 Hansen, Schwartz & Cooper, 2008, p. 23.

127 Karjoth, Schunter, & Waidner, 2003, p. 7.

128 Urteil von 15 Dezember 1983, BVerfGE 65,1 ff(43): "eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht mehr vereinbar wären, in der Burger nicht mehr wissen können, wer, was, wann und bei welcher Gelegenheit über sie weist" in Prinzipien des deutschen Datenschutzrechts, H. Ehmann, Trier, 1999.

8.9. Law is code

Bellotti heeft bij haar verslag over 'media spaces' geschreven, dat het doelbindingsprincipe in de OECD-guideline, (zie hoofdstuk 2), problematisch kan zijn voor AMI-systemen. zoals EuroPARC's RAVE systeem van Xerox. Dit systeem stimuleert 'serendipity' (toevallige ontdekkingen) tijdens het onderzoek en bij zo'n systeem, schrijft Belotti: "We cannot comply with such (purpose binding) principle. The point and the advantage of the technology is that information is gathered as a resource, and the purpose of the data cannot be specified until it is used, if at all, at some unpredictable time in the future."[129]

Bellotti's opmerking brengt mij terug bij het beginpunt van deze dissertatie, waar ik stelde dat de titel van mijn boek geïnspireerd is door Lessig's uitspraak "code is law."[130] Haar opmerking bevestigt wat Lessig beschrijft in zijn boek Code and Other Laws of Cyberspace. Systeem- en softwareontwikkelaars ontwerpen codetechnische protocollen en netwerkarchitecturen. Daarmee bepalen zij de weg waarlangs de gebruiker van informatiesystemen (vaak moet) lopen en de manier waarop 'deuren' worden geopend of gesloten blijven. Sterker nog: de ontwikkelaar bepaalt daarmee wat wel of niet mogelijk is, of beter gezegd: wat wel of niet *mag* en *moet.*"[131] Dergelijke normen die bij het gebruikmaken van de elektronische infrastructuur gelden, staan los van enige democratische inspraak of toetsing.[132] Schmidt noemt dit regulering door middel van architectuur.[133]

Dat is een gevaarlijke ontwikkeling. Wij moeten bewust zijn van wat er zich in *cyberspace* afspeelt. Hoe willen wij dat cyberspace eruit ziet en hoe willen wij in die virtuele wereld leven? Welke normen en waarden zullen daar gelden? Zijn het onze waarden en normen? Zullen onze grondrechten gerespecteerd worden? De code van cyberspace kan onze grondrechten reflecteren of waarden scheppen die juist inconsistent zijn met onze waarden. Hoe meer de invloed van cyberspace groeit, hoe meer het van belang wordt dat onze duur bevochten grondrechten ook onverkort gerespecteerd worden in cyberspace. Lessig wijst erop "There is nothing to guarantee that the regime of values constitued by code will be a liberal regime; and little reason to expect that an invisible hand of code writers will push it in that direction. Indeed, to the extent that code writers respond to the wishes of commerce, a power to control may well be tilt that this code begins to take. (...) The threats to values implicit in the law – threats raised by changes in the architecture of code – are just particular examples of a more general point: that more than law alone enables legal values, and that law alone cannot guarantee them."[134] Dit geldt ook voor de bescherming van onze privacy.

---

129 Bellotti & Sellen, 2003, p. 93.
130 Lessig, 1999, p. 6.
131 Franken, 2001, p. 7.
132 Bing & Selmer, 1980, p. 319-338.
133 Schmidt, 2004.
134 Lessig, 1999 (A), p. 546.

Tijdens mijn onderzoek voor dit proefschrift vroeg ik mij herhaaldelijk af waarom ik zo graag andere wetenschappen betrek bij mijn werk om de privacy van de burger te beschermen. De aanleiding ligt zeker in mijn constatering dat het recht op de bescherming van persoonsgegevens niet 'self-executing' is en er zeer veel inbreuken plaatsvinden. Rechtshandhaving achteraf levert vaak geen effectieve preventieve bestrijding van de privacyinbreuk op. Net zoals in de metafoor van de cholerabestrijding die ik in het begin van dit boek gebruikte, kan de patiënt individueel geholpen zijn, maar de ziekte is daarmee niet uitgeroeid. Het kwaad dat eenmaal is geschied, kan niet meer hersteld worden. In cyberspace blijft alles bewaard. Het lag voor de hand dat ik zou teruggrijpen op mijn jarenlange werkervaring in de ict-industrie om te zoeken naar methodes die mogelijkerwijs inbreuken kunnen voorkomen en daardoor het vertrouwen van de burger in de correcte verwerking van zijn gegevens niet ondergraven.

Ik liet mij verleiden door de overtuiging dat wetenschappen met een wiskundige basis 'hardere in plaats van zachtere' oplossingen zouden kunnen bieden voor het probleem van de privacyinbreuken. Door de rechtsregels in programmacode om te zetten hoopte ik een panacee te vinden of op z'n minst een effectief hulpmiddel dat zo veel mogelijk privacyproblemen kon tegengaan bij de verwerking van gegevens in informatiesystemen.

Omdat noch de rechtswetenschap, noch de computerwetenschap mij een verklaring konden geven waarom, ondanks het feit dat iedereen erkent dat privacy een belangrijk grondrecht is, PET niet op grote schaal in informatiesystemen werd en wordt toegepast, vroeg ik mij af of ik in het onderzoek iets essentieels had gemist. Ik besloot het antwoord op de zesde onderzoeksvraag: *Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?* (OV 6) te gaan zoeken binnen de economische wetenschappen en het probleem van de privacybescherming niet vanuit het individu te benaderen, maar vanuit de organisaties, vanuit de verantwoordelijken. Dit ondanks de waarschuwing van Feldman, die stelt dat teveel vertrouwen in wetenschappelijke regels:

> "may not work well for providing answers to law's questions"[135] en dat "over time many assumptions of law and economics have come under attack (...) an increasing body of literature has argued that institutional interactions are far more complex than the founders of the law and economics originally suggested"[136]

Weliswaar was het antwoord op de zesde onderzoeksvraag dat er inderdaad belangrijke belemmeringen bestaan, maar tegelijkertijd levert de economische benadering bruikbare inzichten op, waar de jurist, beslisser en beleidsmaker hun voordeel mee kunnen doen. Door de bevindingen in hoofdstuk 7 en de

135 Feldman, 2009, p. 7.
136 Feldman, 2009, p. 64-65.

aanbevelingen in hoofdstuk 8 toe te passen wordt de weg vrijgemaakt voor grootschalige toepassing van privacyveilige systemen en kan een organisatie met succes privacybeschermende maatregelen in informatiesystemen en infrastructuur implementeren en daardoor het vertrouwen van burger en consument in de privacybescherming vergroten.

Hoewel het inderdaad mogelijk is datamodellen en architecturen te ontwerpen die de privacywetgeving nauw volgen, is het echter dringend noodzakelijk de research voor privacyveilige informatiesystemen met name in de ambient intelligence omgeving met kracht voort te zetten. Een gestandaardiseerde privacyontologie dient op korte termijn te worden ontwikkeld om de brug te slaan tussen het privacyrecht en ict. Door de gestandaardiseerde privacyontologie zullen de ontwerpers van informatiesystemen en softwareprogrammeurs beter informatiesystemen kunnen ontwerpen die nauwgezet de EU-privacyrichtlijnen volgen en het in machinetaal vastgelegde privacybeleid uitvoeren.

Voorwaarde daarbij is dat hardware- en softwareontwerpers en juristen nauw overleg met elkaar voeren.[137] Ras merkt op: "niet vaak hebben juristen verstand van de inzet van (informatie)technologie",[138] terwijl computerwetenschappers niet zijn opgeleid om rechtsregels te interpreteren, de ontwikkeling daarvan in te schatten en de rechtsregels in het ontwerp zo aan te passen dat datgene wat rechtsregels beogen te beschermen intact blijft. Zoals in hoofdstuk 5 is beschreven, bleek tijdens het ontwerp van ontologieën voor de gegevensbescherming in het kader van het PRIME-onderzoek, dat zonder een ter zake kundig jurist de output in meer dan 90% van de gevallen onzinnige resultaten opleverde.

Het frustreerde de ontwerpers dat het persoonsgegevens beschermend recht niet voldoende concreet, te ambigu was en te veel onzekerheden[139] bevat door het gebruik van open normen. Die open normen zorgen er juist voor dat juristen voldoende flexibiliteit aan de dag leggen om regels op nieuwe situaties toe te passen. Kohnstamm stelde tijdens de door de Europese Commissie georganiseerde Data Protection Conference dat "open norms in the Directive are inevitable, even desirable, and have stood the test of time".[140] Zonder open normen had de EU-Richtlijn 95/46/EG niet kunnen overleven.

Als het binaire systematische 'code is law', ontworpen door hardware- en softwareontwikkelaars, voor ons elektronisch maatschappelijk verkeer de norm wordt, dan kan dat alleen maar leiden tot een inflexibel verstard systeem. Dat systeem zal nieuwe problemen slechts binnen het binaire kader kunnen benaderen

137 Schmidt, 2004, p. 23 "…de duurzaamheid van ons rechtssysteem gebaat is bij juristen, die verstand hebben van informatica."
138 Ras, 2006, p. 247.
139 Hoewel in de kringen van de computer wetenschappers men bekend is met het Heisenbergs uncertainty principle.
140 Kohnstamm, 2009, p. 5.

en ervoor zorgen dat het individu zich niet meer vrij en creatief in de samenleving kan ontwikkelen. 'Law in the books'[141] kan dan niet meer 'law in action'[142] zijn dat in staat is zich aan te passen aan steeds veranderende omstandigheden. Het zou kunnen leiden tot het einde van het recht,[143] zoals wij dat nu kennen.

In dit proefschrift pleit ik er nu juist voor om 'code is law' om te draaien en, in samenspraak met informatici en juristen die voldoende kennis hebben van de informatica, 'law is code' na te streven. Het woord 'is' heeft een relatieve betekenis maar duidt nochtans op het noodzakelijke gebruik van ict als digitale ondersteuning van het recht. Zonder die ondersteuning is het privacyrecht niet handhaafbaar.

Door te streven naar 'law is code' kunnen wij voorkomen dat er een inflexibele en ondemocratische samenleving ontstaat waar binaire normen en architecturen gelden en er geen plaats is voor de bescherming van de persoonlijke levenssfeer met zijn veelheid aan uitingsvormen.

De samenleving zal steeds meer gedigitaliseerd worden. Er zal geen maatschappelijk gebied meer zijn waar de invloed van ict zich niet zal doen laten gelden. Mulder poneerde tijdens het congres van het Nederlands Mediation Instituut op 8 november 2003 drie stellingen namelijk:

1. Geschillen met betrekking tot internettransacties zullen binnenkort door computers worden opgelost.
2. De kosten van rechtspraak kunnen alleen omlaag door toepassing van het internet.
3. Geschillenbeslechters zullen zoals alle beroepsgroepen ict gaan gebruiken.[144]

De digitalisering/informatisering van onze samenleving zal de behoefte aan juristen met een goed inzicht in de ict sterk doen toenemen. Om op die behoefte in te spelen is het op korte termijn noodzakelijk om iedere jurist tijdens de kandidaatsfase verplicht een jaar kennis te laten maken met de basisbeginselen van de informatica en daarin een tentamen te laten afleggen. De onderbouwing hier voor kan geleend worden van de Universiteit van Stockholm:

> "The fast progress in the IT area is also reflected in the development of legal understanding of problems relating to the introduction of technology. All inventions bring about new problems with them, and in this respect IT is no exception. One example of a quick reaction to new legal problems arising in connection with IT is the fact that Sweden was the first country to issue a separate Act on the Protection of Privacy in Connection with the Use of Computers (in 1973),

141 Volgens Esser, 1956: het historisch-dogmatische systeem dat in de codificatie is neergelegd.
142 Ter Heide, 1967, p. 4-5, staat law in action voor het 'open' casuistische probleemdenken dat tegenover het 'gesloten' deductieve denken staat.
143 Pound, 1966, p. 25-47.
144 Mulder, 2003, www.nmi-mediation.nl, Actueel 2003, nr. 8.

> which has led to the solution of numerous legal problems relating to IT and telecommunications. This has also helped in amassing knowledge, and enabled various authorities and interest groups to be established in the field. At Stockholm University the Swedish Law and Information Technology Research Institute was established at the Department of Law in 1968, and has been active ever since."[145]

Op de probleemstelling: *Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker?* is een positieve oplossing gevonden door de combinatie van rechtswetenschappen, informatica en economische wetenschappen.

Privacybescherming vereist een multidisciplinaire aanpak. Met gebruikmaking van PET-maatregelen en door de uit de wet voortvloeiende juridische specificaties in informatiesystemen in te bouwen kan het verzamelen, verwerken en het verspreiden van persoonsgegevens privacyveilig plaatsvinden. De DOI-theorie van Rogers uit de economische wetenschappen geven de weg aan hoe PET-maatregelen in informatiesystemen bevorderd kunnen worden. Zo kan worden voorkomen dat code is law werkelijk bestaat.

Veel informatiesystemen zijn in 2009 niet privacyveilig en er kunnen en zullen bij ongewijzigd beleid ernstige privacyinbreuken plaatsvinden, die het vertrouwen in onze samenleving zullen kunnen schokken. Het onderzoek naar surveillance samenleving geeft aan dat onze privacy op het spel staat.

Privacyinbreuken kunnen voorkomen worden als de overheid en het bedrijfsleven privacyveilige informatiesystemen gaat gebruiken, waardoor de burger, consument en gebruiker erop kunnen vertrouwen dat hun persoonsgegevens zullen worden verwerkt overeenkomstig de wet en hun privacyvoorkeuren. Daardoor zullen zij ook in de komende AMI-wereld zichzelf effectiever tegen privacyinbreuken kunnen beschermen. Zo wordt voorkomen dat de privacybescherming erodeert, het vertrouwen in elkaar en de samenleving steeds meer verdwijnt en onze samenleving een onmenselijk gezicht krijgt.

145 http://www.juridicum.su.se/jurweb/utbildning.

Samenvatting

> The White Rabbit put on his spectacles. `Where shall I begin, please your Majesty?' he asked. 'Begin at the beginning,' the King said gravely, `and go on till you come to the end: then stop.'
> Lewis Carroll, Alice in Wonderland, Chapter XII Alice Evidence, London, 1995, p.182.

Privacyrecht is code
Over het gebruik van Privacy Enhancing Technologies

Dit boek verkent twee zaken. Aan de ene kant onderzoekt het of privacybeschermende informatiesystemen preventief kunnen worden ingezet om onze persoonsgegevens en onze persoonlijke ruimte effectief te kunnen beschermen. Aan de andere kant onderzoekt het of 'privacy enhancing technologies' (PET) kunnen worden toegepast in informatiesystemen om onze privacy adequaat te beschermen. In acht hoofdstukken heb ik geprobeerd de volgende probleemstelling te beantwoorden:

Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker, beide in de zin van de Europese Richtlijn 95/46/EG.

In de context van de probleemstelling worden in dit boek zes onderzoeksvragen behandeld, die in hoofdstuk 1 zijn opgesomd. De resultaten hiervan leiden tot het antwoord op de probleemdefinitie.

De onderzoeksvragen zijn:

OV 1: Welke juridische specificaties kunnen voor informatiesystemen uit de algemene beginselen betreffende persoonlijke informatie en de privacy wet- en regelgeving worden afgeleid?

OV 2: *Is onze informationele privacy in gevaar doordat de overheid en het bedrijfsleven de burger preventief in de gaten houden ter bestrijding van fraude-, misdrijf-, en terrorismebestrijding?*

OV 3: Met welke privacybedreigingen en -risico's moeten de burger en de ontwerper van systemen rekening houden?

OV 4: Wat houdt het concept Privacy Enhancing Technologies (PET) in?

OV 5: Is het mogelijk privacyveilige architecturen en systemen te ontwerpen en te bouwen?

OV 6: Wanneer het mogelijk blijkt te zijn om privacyveilige systemen te ontwikkelen, bestaan er dan belemmeringen in organisatorische en economische zin om op grote schaal PET in informatiesystemen te implementeren?

Hoofdstuk 1

De omgevingsanalyse in hoofdstuk 1 vormt de aanleiding voor OV 1. Daaruit blijkt dat in postindustriële landen, zoals de Verenigde Staten, Canada, Australië, Japan en de landen van de Europese Unie, informatie- en communicatiesystemen worden gebruikt, die op een steeds verfijndere manier gegevens over personen verzamelen, opslaan, uitwisselen, (her)gebruiken, identificeren, analyseren en monitoren. Uit de omgevingsanalyse blijkt ook dat burgers (als inwoners, patiënten, hotelgasten, passagiers, studenten, kopers op internet, etc.) bang zijn dat de overheid, het bedrijfsleven en andere organisaties hun persoonlijke informatie misbruiken. Deze bezorgdheid wordt gevoed doordat er steeds meer informatiesystemen zijn, die via internet of andere netwerken verbonden kunnen worden met databanken en automatisch en onbelemmerd (persoons)gegevens kunnen uitwisselen. Hoe meer persoonlijke informatie beschikbaar is, des te groter wordt het risico van identiteitsdiefstal door kwaadwillige personen die persoonsgegevens van burgers zonder hun toestemming zich toe-eigenen en misbruiken. Burgers en consumenten zijn niet in staat na te gaan wat er met hun persoonsgegevens gebeurt en aan wie die worden verstrekt. Het ligt voor de hand dat zij controle willen hebben en houden over het gebruik van hun persoonsgegevens. In de praktijk blijkt het echter voor burgers en consumenten zeer moeilijk hun rechten op het gebied van de bescherming van persoonsgegevens te handhaven. Indringende technologieën zetten de persoonlijke ruimte (een onzichtbaar veld dat ieder mens omringt en voelbaar wordt als andere mensen te dichtbij komen) en de informationele privacy steeds meer onder druk. Zonder technische hulpmiddelen zal deze situatie in de toekomstige 'ambient intelligence omgeving' (AMI) sterk verergeren. AMI's zijn elektronische omgevingen die gevoelig en ontvankelijk zijn voor de aanwezigheid van mensen.

Hoofdstuk 2

Onze persoonlijke levenssfeer en onze persoonlijke informatie worden wettelijk beschermd. De begrippen 'privacy', 'persoonlijke ruimte' 'identiteit' en 'persoonsgegevens' zijn in dit hoofdstuk verkend. Vervolgens worden de algemene grondslagen over persoonlijke informatie die ten grondslag liggen aan de privacybescherming in kaart gebracht. Deze algemene grondslagen zijn uitgewerkt in de privacy realisatiebeginselen, die in de Convention 108 van de Raad van Europa, de OECD-richtlijnen en in de EU-Richtlijnen 95/46/EG en 2002/58/EG zijn vastgelegd en worden hier toegelicht. Hierbij komen ook de opvattingen van de Article 29 Working Party en een aantal relevante uitspraken van het Europese Hof voor de Rechten van de Mens en het Europese hof van Justitie aan

de orde. De privacy realisatiebeginselen (dat zijn de uitgangspunten om privacybescherming te effectueren) hebben directe gevolgen voor de ontwikkeling en de technische specificaties van informatiesystemen. Het gaat hierbij bijvoorbeeld om de beginselen van gegevensminimalisering, doelbinding en transparantie, (informatieverschaffing en toegangrechten) en informatiebeveiliging. Het antwoord op de eerste onderzoeksvraag leidt tot de opsomming van zeven noodzakelijke juridische specificaties voor het ontwerpen van privacyveilige informatiesystemen. In hoofdstuk 2 is aangegeven dat de data retentie Richtlijn 2006/24/EG gevolgen heeft voor de privacy bescherming. Er zijn een aantal kritische kanttekeningen bij de EU-privacyrichtlijnen geplaatst.

Hoofdstuk 3
Alvorens in te gaan op de privacybedreigingen vanuit de omgeving van het informatiesysteem komt de risicotoezichtsamenleving aan de orde die ertoe leidt dat privacyinbreuken toenemen. In dit hoofdstuk zijn enkele maatschappelijke ontwikkelingen toegelicht, die de erosie van privacy lijken te bevorderen. Met name is ingegaan op een aantal surveillance (recherche) technologieën, zoals data warehousing, data mining, videocamera's, biometrie en localisering (bijvoorbeeld via mobiele telefoons). De overheid en het bedrijfsleven zetten deze technologieën in om diensten aan te bieden, maar evenzeer om terrorisme, misdaad en fraude te bestrijden. Zijn '9/11' en de Richtlijn 2006/24/EG of de daarvan afgeleide wetgeving verantwoordelijk voor de afbrokkeling van onze privacy? Het antwoord op die 'schuldvraag' is ontkennend. In dit hoofdstuk wordt gesteld dat de diepere oorzaak voor de antiterrorismewetgeving niet direct ligt in de aanslagen die wereldwijd de afgelopen zes jaar hebben plaatsgevonden, maar in de geleidelijke ontwikkeling van onze netwerksamenleving. In die samenleving is de nadruk steeds meer op risicoanalyse komen te liggen. Om de collectieve veiligheid in de samenleving zo goed mogelijk te garanderen is een vorm van surveillance opgekomen die door de ict wordt ondersteund. Panoptische technologie zal steeds vaker worden ingezet om mensen heimelijk in de gaten te houden. Omdat de sensoren (RFIDs) die ons omringen steeds kleiner worden, zal surveillance door overheid en bedrijfsleven voor het individu steeds onzichtbaarder (vooral in een AMI-omgeving) worden. Het is de vraag in hoeverre individuen en groepen in zo'n surveillancemaatschappij zelf nog kunnen bepalen hoeveel ze blootgesteld willen worden aan toezicht en hoezeer zij de persoonlijke informatie kunnen beperken die over hen verzameld en gebruikt wordt. Toezichtsystemen zijn voor een leek vaak te technisch om te begrijpen. Zij zijn steeds meer onzichtbaar en gaan daardoor ongemerkt op in de alledaagse structuren en systemen van de maatschappij: op het werk, thuis, op school, op reis en bij het gebruik van telecommunicatie. De risicotoezichtmaatschappij zorgt voor sociale uitsluiting en informatieapartheid. Aanbiedingen met kortingen worden bijvoorbeeld niet aangeboden aan mensen uit achterstandswijken omdat daar geen koopkracht is of dubieuze debiteuren wonen. Het antwoord op de tweede onderzoeksvraag bevestigt dat onze privacy op het spel staat wanneer er geen privacyveilige informatiesystemen voor de surveillance worden ingezet.

Hoofdstuk 4
In dit hoofdstuk wordt betoogd dat, om persoonsgegevens te mogen verwerken en privacybescherming in informatiesystemen te kunnen inbouwen het noodzakelijk is vooraf een privacyrisico- en bedreigingsanalyse uit te voeren. Daarbij moet niet alleen een beveiligingstechnische maar ook een juridische afweging worden gemaakt. Uit artikel 17 van Richtlijn 95/46/EG kan niet anders worden geconcludeerd dan dat een privacyrisico of bedreigingsanalyse *ex ante* een *sine qua non* is. Organisaties negeren echter deze wettelijke eis massaal alsof deze verplichting niet zou bestaan. Uit een onderzoek van KPMG uit 2004 blijkt dat 95 procent van alle Nederlandse organisaties bij de verwerking van persoonsgegevens in strijd met de Wet bescherming persoonsgegevens handelt en dat privacyinbreuken op grote schaal plaatsvinden.

De privacyrisico- en bedreigingsanalyses brengen de gevaren bij de verzameling, verwerking, uitwisseling, en verspreiding van persoonsgegevens voor het individu en de gegevensverwerkende organisaties aan het licht. De Europese privacyrichtlijnen en de daarop geënte nationale wetgevingen van de EU-lidstaten schrijven voor dat de beveiliging van persoonsgegevens zodanig moet zijn dat die risico's worden afgedekt.

Er zijn zeven risicoanalyse- en risicomanagementmethoden behandeld, zoals onder meer de methode van de Registratiekamer (nu CBP) om de risicoklasse voor een specifieke verwerking van persoonsgegevens te bepalen. Daarnaast zijn aan bod gekomen de privacy impactanalyse (PIAs), die door de Treasury Board van de Canadese overheid is ontwikkeld, de privacy bedreigingsanalyse met de pentagonale aanpak die in het Europese PISA-project is ontwikkeld en de privacybedreigingsontologie, die voor het eerst in 2007 in het Noorse PETWEB-project is toegepast. Het is belangrijk om een privacyrisico- of bedreigingsanalyse uit te voeren die met zo veel mogelijk omstandigheden rekening houdt. Vaak geven beveiligingsdeskundigen vanuit de praktijk een opsomming van potentiële privacyinbreuken en daarmee verbonden bedreigingen en risico's. Dit verdient niet de voorkeur. Een ontologische beschrijving van bedreigingen is geschikter.

Uit de onderzochte privacyrisico- en bedreigingsanalyses is duidelijk geworden dat persoonsgegevens het best beschermd kunnen worden als ze geanonimiseerd of gescheiden worden van andere gegevens. Dat laatste betekent dat de persoonsgegevens wel worden verwerkt, maar dat de identificerende persoonsgegevens direct worden losgekoppeld van de overige persoonsgegevens. De derde onderzoeksvraag levert een lijst van privacybedreigingen op.

Hoofdstuk 5
Dit hoofdstuk behandelt de vierde onderzoeksvraag door de inhoud en reikwijdte van het concept 'privacy enhancing technologies' (PET) te verkennen en gaat na hoe PET kunnen bijdragen aan de bescherming van persoonsgegevens in informatiesystemen. Daarnaast wordt onderzocht welke rol is weggelegd voor de 'Identity Protector' (IDP) en hoe de privacy realisatiebeginselen in programmacode kunnen worden omgezet. In dit hoofdstuk is een aantal belangrijke ontwerpelementen in

samenhang met PET besproken, die kunnen worden ingezet bij de het ontwerp en de bouw van privacyveilige systemen. Het concept PET kan theoretisch gezien worden als een belangrijke aanvulling op het bestaande juridische kader en de technologische uitwerking daarvan. PET kunnen ervoor zorgen dat organisaties persoonsgegevens niet of aanmerkelijk minder gebruiken of volgens de wettelijke voorwaarden verwerken. De privacybescherming door de verantwoordelijken wordt hierdoor in de praktijk geen lege huls. Bovendien stellen PET de burger en consument in staat de verwerking van hun persoonsgegevens te controleren zodat hun vertrouwen in de rechtmatige verwerking ervan toeneemt. De in dit hoofdstuk besproken research toont aan dat de privacy van burgers en consumenten steeds effectiever kan worden beschermd. De noodzaak om adequate technologische middelen te ontwikkelen om de persoonlijke levenssfeer te beschermen wordt steeds groter. Steeds meer transacties zullen in de nabije toekomst niet alleen meer direct tussen mensen plaatsvinden, maar in toenemende mate rechtstreeks tussen informatiesystemen, software agents, intelligente sensoren en robots. In dit hoofdstuk zijn tevens de gereedschappen om persoonsgegevens te beschermen behandeld, zoals encryptie, 'rule-based' privacy managementsystemen en privacy ontologieën.

Hoofdstuk 6

Dit hoofdstuk behandelt de vijfde onderzoeksvraag aan de hand van vier privacyveilige informatiesystemen die met succes gerealiseerd zijn in verschillende sectoren van de samenleving. In de vier voorbeelden zijn de ontwerpbeginselen en technieken uit hoofdstuk 5 toegepast. Deze vier voorbeelden tonen aan dat persoonsgegevens van individuen technisch goed zijn te beschermen zonder dat de functionaliteit van informatiesystemen in gevaar komt. Het concept PET speelt als onderdeel van de informatiearchitectuur een belangrijke rol bij de bescherming van persoonsgegevens. Om persoonsgegevens van het individu adequaat te beschermen, moeten PET een onderdeel van de informatiearchitectuur zijn. Dit betekent doorgaans dat de architectuur fundamenteel moet worden herzien, vooral met betrekking tot de onderlinge relaties van de onderdelen en de relaties met de omgeving van het systeem. Integratie van PET in nieuw te ontwikkelen systemen is een reële optie. PET zijn het meest effectief in het proces van het verzamelen van persoonsgegevens, omdat de privacy dan bij de bron wordt beschermd. De besproken metazoekmachine Ixquick in dit hoofdstuk geeft daar blijk van. Zoals uit het voorbeeld van het ziekenhuis Veldwijk-Meerkanten blijkt, kunnen met PET de persoonsgegevens tijdens verwerking en opslag uitstekend beschermd worden. Complexere systemen als NTIS en ViTTS zouden zonder PET niet kunnen bestaan. Ook zijn PET goed inzetbaar bij de verspreiding van gegevens, omdat PETs voorkomen dat gegevens ongeoorloofd aan elkaar gekoppeld worden. Het PISA-project toont aan, dat PETs persoonsgegevens afdoende binnen netwerkomgevingen kunnen beschermen ondanks de complexiteit om privacyrecht in systemen in te bouwen en te handhaven. Organisaties maken nog weinig gebruik van privacymanagementsystemen die verwerking conform de privacyregels afdwingen. Het PISA-project is een

geavanceerde toepassing daarvan en levert kennis op die gebruikt kan worden in een 'ambient intelligence'-omgeving.

Hoofdstuk 7
Hier is de zesde onderzoeksvraag beantwoord, waarom privacyveilige architecturen nauwelijks worden geïmplementeerd en PET nauwelijks worden toegepast. De organisatorische en economische belemmeringen bij de adoptie van PET worden geanalyseerd, onder meer aan de hand van casestudies. Het blijkt dat organisaties door een groot aantal factoren beïnvloed worden bij hun beslissing om wel of niet PET toe te passen. Wanneer de positieve adoptiefactoren worden benut, zouden organisaties PET sneller op grote schaal in hun informatiesystemen kunnen toepassen. Het gaat hierbij vooral om organisaties die een grote informatie-intensiteit kennen, vanuit hun organisatiestrategie een grote behoefte hebben persoonsgegevens te beschermen en financieel en operationeel daartoe in staat zijn. Om PET toe te passen moet de organisatie een bepaalde maturiteit hebben. Het hoofdstuk gaat hierop in. Of PET binnen een organisatie kunnen worden toegepast hangt af van de maturiteit die de organisatie heeft op het gebied van Identity & Access Management (IAM) en privacybescherming. Het verloop van deze processen en het beslissingsmoment om PET toe te passen wordt in drie gerelateerde S-curven uitgedrukt. Beproefde businessmodellen om in PET te investeren bestaan niet. Om te investeren in PET, is een positieve businesscase vereist die de financiële haalbaarheid van de PET investering aantoont. Daarom wordt in dit hoofdstuk een aantal methoden besproken om de rentabiliteit van investeringen te berekenen waaronder de 'Return On Investment'-methode met een specifieke investeringsformule voor PET (ROI-PI) en de 'Net Present Value'-formule. Empirische gegevens over privacyincidenten zijn in de Europese Unie niet beschikbaar, waardoor de consequenties van dergelijke incidenten niet accuraat kunnen worden ingeschat en de rendementsberekeningen onnauwkeurig zijn. Een verplichte bekendmaking en registratie van verlies of diefstal van persoonlijke informatie, zoals voorzien in het wijzigingsvoorstel van de Richtlijn 2002/58/EG, zullen ervoor zorgen dat dergelijke gegevens op termijn wel beschikbaar komen.

Hoofdstuk 8
Dit hoofdstuk heeft de onderzoeksvragen uit hoofdstuk 1 weer opgepakt, de probleemstelling beantwoord en komt met tien aanbevelingen die zijn gebaseerd op de positieve adoptiefactoren voor PET uit hoofdstuk 7. Naast voorlichting is de rol van de privacytoezichthouder (Data Protection Authorities (DPAs)) van cruciaal belang voor de implementatie van PET in informatiesystemen. De DPAs, zoals het CBP in Nederland, zouden zich niet ex post (klachtenbehandeling en controles achteraf), maar vooral ex ante (preventief adviserend) moeten opstellen. Zij zouden hun technologische experts als PET consulenten moeten inzetten. Die kunnen aan de hand van de privacyrisico-, privacybedreigings- of privacyimpactanalyses (PIAs) vaststellen of de in te voeren informatiesystemen voldoen aan de privacywetgeving en kunnen zo nodig adviseren PET toe te

passen. De expertise over PET-toepassingen is echter schaars. Het zou daarom wenselijk zijn een PET Expertisecentrum in het leven te roepen. Om PET succesvol in nieuwe informatiesystemen te implementeren beveel ik een specifiek PET-stappenplan aan. Het hoofdstuk sluit af met voorstellen voor een aantal aanpassingen van de Richtlijn 95/46/EG die noodzakelijk zijn om persoonsgegevens beter te beschermen. Privacyveilige systemen zorgen voor het noodzakelijke vertrouwen van de burger en consument dat hun persoonsgegevens worden verwerkt overeenkomstig hun privacyvoorkeuren en de wet- en regelgeving. Met ingebouwde PET-maatregelen in informatiesystemen zullen zij zichzelf ook in de komende AMI-wereld effectiever tegen privacyinbreuken kunnen beschermen.

Uit de de research is op te maken dat wij privacyveilige systemen kunnen bouwen (het *hoe* in de probleemstelling), maar dat deze ook voorzien dienen te zijn van een certificaat met de verklaring, dat het systeem privacyveilige verwerking van persoonsgegevens waarborgt. Voor algemeen maatschappelijk *vertrouwen* is het nodig dat privacyveilige systemen grootschalig worden ingezet. Nochtans als er geen politieke wil is om de privacy adequaat te beschermen en men gaat onverkort door met het gebruik van privacy onveilige informatiesystemen in onze risicotoezichtsamenleving dan dreigt er ernstig gevaar voor onze privacy.

Summary

Privacy Law is Code
About the deployment of privacy enhancing technologies

The title is inspired by Lessig's adage: 'Code is Law'. This dissertation deals with two issues. On the one hand it explores whether information systems that safeguard privacy can be used preventatively on the other hand it investigates whether privacy-enhancing technologies (PET) can be implemented in information systems.

In eight chapters I have tried to find an answer to the following problem definition: *how can personal information of citizens in information systems be protected that effectively, that people can (continue to) be assured (trust) that their personal data are not collected, processed, stored and circulated unlawfully by the party responsible (the controller) and the processor, both in the sense of the European Union Directive 95/46/EC.*

Within the context of the problem definition this dissertation discusses six research questions, which have been enumerated in chapter 1, that will produce the answer to the problem definition. The first research question deals with the legal requirements that Directive 95/46/EC; researchquestion 2 deals with the negative effect of the surveillance state on privacy; the third research question investigates the privacy threats; the fourth research question explores the concept of privacy enhancing technologies (PET); researchquestion 5 investigates the possibilities for constructing information systems which are privacy safe and research question 6 deals with the adoption obstacles for the deployment of PET.

Chapter 1
The analysis of today's environment provokes the first research question. It shows that in post-industrial countries such as the United States, Canada, Australia, Japan and the member states of the European Union, information and communication systems are used which collect, store, exchange, (re)use, identify, analyze and monitor data of persons in an increasingly sophisticated manner.

From the environment analysis in this chapter it also becomes clear that citizens (e.g. inhabitants, patients, hotel guests, passengers, students, buyers on the internet etc.) fear that the authorities, the business world and other organizations

are misusing their personal data. This concern is fostered by the existence of a growing number of information systems that can be linked to data bases via internet or other networks and can automatically and freely exchange (personal) data. The more personal data that is available, the greater the risk of identity theft by malicious persons who appropriate and misuse personal data of citizens without their permission.

Citizens and consumers are not in a position to check what is happening to their personal data and to whom they are being distributed. It goes without saying that they want to have control over and keep check on the use of their personal details. However, in actual practice it proves to be very difficult for citizens and consumers to assert their rights in the field of the protection of personal data. Intrusive technologies increasingly put pressure on the personal domain (an invisible sphere surrounding each human being and that becomes perceptible when other people are trespassing) and the informational privacy. Without technical resources, this situation will deteriorate sharply in the coming ambient intelligence (AMI) environment. AMIs are electronic environments, which are sensitive and receptive to the presence of people.

Chapter 2

The law protects our individual privacy and our personal data. This chapter explores the terms 'privacy', 'personal domain', 'identity' and 'personal data'. Subsequently, the general fundamentals with respect to personal data that form the basis of privacy protection are mapped out. These general fundamentals are worked out in the privacy realization principles, laid down in Convention 108 of the Council of Europe, the OECD directives and in the EU Directives 95/46/EC and 2002/58/EC and which have been explained in this chapter. In this respect the views of the 'Article 29 working Party' and a number of relevant rulings of the European Court for Human Rights and the European Court of Justice are also considered. The privacy realization principles (the starting points for effectuating privacy protection that are discussed in chapter 2) have direct consequences for the development and technical specifications of information systems. This for example concerns the principles of data minimization, purpose binding and transparency (the supply of information and access rights) and data protection. As a result of the first research question seven legal requirements for privacy safe information systems have listed. Chapter 2 points out that the EU data retention Directive 2006/24 has consequences for the protection of privacy. It puts a number of critical comments with respect to the EU privacy directives.

Chapter 3

Before going into the privacy threats in the field of the information systems, this chapter examines the risk-monitoring society that has resulted in an increase in privacy violations. Also it elucidates a number of social developments, which seem to be conducive to the erosion of privacy. Particular attention is paid to various surveillance (criminal investigation) technologies such as data warehousing, data

mining, video cameras, biometrics and localization (e.g. via cellphones). The authorities and trade and industry employ these technologies in order to offer services but also to combat terrorism, crime and fraud. Are '9/11', the Directive 2006/24/EC or any legislation derived from this directive responsible for the crumbling of our privacy? The answer to that question of 'guilt' is negative. Chapter 3 argues that the deeper cause for the anti-terrorism legislation does not directly lie in the attacks carried out all over the world during the past six years but in the gradual development of our network society. That society has increasingly put the emphasis on risk analysis. In order to guarantee collective security in society as much as possible, a form of surveillance has emerged which is supported by ict. Panoptic technology will increasingly be used to monitor people. Because the sensors (RFIDs) surrounding us are getting smaller all the time, surveillance by the authorities and the business world will become more and more imperceptible (particularly in AMI environments) for individuals. It remains to be seen to what extent individuals and groups in such a surveillance society can make their own decisions as regards the level of exposure to surveillance and to what extent they can limit the personal data that is collected and used. To a layman surveillance systems are often too technical to be understood. They invisibly and as a result imperceptibly merge into the day-to-day structures and systems of society: at the workplace, at home, at school, whilst travelling and whilst using telecommunication. The risk surveillance society creates social sorting and information apartheid. Special offers with discounts for example are not given to people from underprivileged areas because people living there have no purchasing power or they are considered poor credit risks. The second research question results in the conclusion that in our surveillance society our privacy is at risk if the surveillance is executed with non-privacy protective information systems.

Chapter 4

This chapter stresses the point that in order to be allowed to process personal data and to be able to build privacy protection into information systems, it will be necessary to carry out a privacy risk, impact or threat analysis. In doing so, not only an assessment from a security technical point should be made but legal issues should also be considered. From article 17 of EU Directive 95/46 it cannot be concluded otherwise that privacy risk analysis or treat analysis *ex ante* is a *sine qua non.* However, organizations widely ignore this statutory requirement as if this obligation would not exist. An investigation conducted by KPMG in 2004 shows that 95 percent of all Dutch organizations is acting contrary to the Personal Data Protection Act (Wbp) in the processing of personal data and that privacy is violated on a large scale.

Privacy risk analyses and threat analyses bring to light the dangers in the collection, exchange and circulation of personal data for the individual person and the data processing organizations. The European privacy directives and the national legislation of the EU member states engrafted onto those directives set out a standard of protection of personal data that ensures that those risks will be

covered. Chapter 4 considers the third research question and raises seven risk analysis and risk management methods, such as i.e. the method of the 'Registration Chamber' (presently Dutch Data Protection Authority: 'College Bescherming Persoonsgegevens') to determine the risk class with respect to a specific form of processing of personal data. In addition it deals with the privacy impact analysis (PIA) developed by the Treasury Board of the Canadian authorities, the privacy threat analysis containing the pentagonal approach developed in the European PISA project and the privacy threat ontology, which was first applied in 2007 in the Norwegian PETWEB project. It is important to conduct a privacy risk or privacy threat analysis in which circumstances are taken into account as much as possible. Often security experts from actual practice list the potential privacy violations and the relative threats and risks. This is not considered preferable, an ontological specification of threats would be more suitable. From the privacy risk and threat analyses that have been investigated it becomes clear that personal data can best be protected if they have been anonymized or have been separated from other data. This means that the personal data are actually being processed but that the identifying personal data are immediately unlinked from the other personal data. The research question results in 14 generic privacy threats.

Chapter 5
This chapter explores the fourth research question dealing with the substance and implications of the privacy enhancing technologies concept (PET) and examines how PET can contribute to the protection of personal data in information systems. In addition it investigates the role reserved for the Identity Protector (IDP) and how privacy realization principles can be converted into a program code. In this chapter a number of important draft elements in combination with privacy enhancing technologies that can be used in the development of systems in which privacy is secured are discussed. The PET concept may theoretically be seen as a significant complement to the existing legal framework and its implementation as far as organization is concerned. PET can ensure that organizations do not use personal data or minimize their use or process them in accordance with the statutory provisions. As a result the protection of privacy by the parties responsible does not become an empty shell. Moreover PET enables citizens and consumers to keep a check on the processing of their personal data that consequently increases their confidence in the lawful processing of data. Research discussed in this chapter shows that the privacy of citizens and consumers can be safeguarded in an increasingly effective manner. There is an ever-growing need to develop adequate technological means to protect the individual privacy. After all, in the near future more and more transactions will be carried out not only directly between people but also increasingly directly between information systems, software agents, intelligent sensors and robots. This chapter also discusses the tools to protect personal data, such as encryption, rule-based privacy management systems, data tracking, sticky policies and privacy ontologies.

Chapter 6

On the basis of a number of models, this chapter deals with information systems with enhanced privacy that has been realized successfully in different sectors of society. In this chapter four examples are worked out in which the design principles and techniques of chapter 5 have been applied. These four examples demonstrate that personal data of individuals can be protected properly technically without endangering the functionality of the information systems. The PET concept, as part of the data architecture, plays an important role in the protection of personal data. In order to protect the personal data of individuals effectively, PET needs to form part of the data architecture. This generally involves a fundamental revision of the architecture, especially as regards the internal relations of the components and the connections with the environment of the system. The integration of PET in newly to be developed systems is a realistic option. PET is most effective in the collection of personal data, because privacy will then be protected at source. The meta-search machine Ixquick, discussed in this chapter, demonstrates this. As shown by the example of the Veldwijk-Meerkanten hospital, with the use of PET, sensitive medical data (personal data) can be protected extremely well during processing and storage. More complex systems such as the National Trauma Information System (NTIS) and the Victim Tracking and Tracing System (ViTTS) could not exist without PET. PET can also be used effectively in the circulation of data because PET prevents the unlawful linking of data. The PISA project demonstrates that PET is able to adequately protect personal data in network environments despite the complexity to build in and uphold privacy legislation in systems.

Organizations as yet make little use of privacy management systems that force data to be processed in conformity with privacy rules. The Privacy Incorporated Software Agent (PISA) project is an advanced application in this respect and provides knowledge that may be used in an ambient intelligence environment. The answer to fifth research question whether privacy safe information systems can be built successfully, is affirmative.

Chapter 7

Here has been examined the sixth research question why privacy secured architectures is scarcely implemented and PET is hardly used. It analyses the organizational and economic impediments to the adoption of PET, among others on the basis of case studies. It becomes clear that organizations are influenced by a large number of factors in their decision whether or not to implement PET. If the positive adoption factors would be utilized, organizations would be able to implement PET in their information systems much faster on a large scale. This particularly applies to organizations with large information intensity and which on account of their organization strategy have a great need to protect personal data and to be financially and operationally capable of doing so.

In order to implement PET, the organization needs to have a certain degree of maturity. The chapter deals with this issue in further detail. Whether PET can be applied within an organization depends on the maturity of said organization in the field of Identity & Access Management (IAM) and privacy protection. In chapter 7 the progress of these processes and the decision-taking moment to implement PET are outlined in three related S-curves. Business models to invest in PET do not exist. Investment in PET requires a positive business case demonstrating the financial feasibility of PET. For that reason a number of methods are discussed in this chapter to calculate the cost-effectiveness of investments including the Return On Investment method containing a specific investment formula for PET (ROI-PI) and the Net Present Value formula. Empirical information on privacy incidents in the European Union is not available, making it impossible to assess the consequences of such incidents properly and rendering the calculations on return inaccurate. A compulsory disclosure and recording of the loss or theft of personal data, as provided for in the proposed amendment of the EU-Directive 2002/58, will ensure that this information will be available in the future.

Chapter 8

This study ends with a number of concluding observations and produces ten recommendations. This chapter returns to the investigation issues in chapter 1 and presents a number of recommendations based on the positive adoption factors for PET from chapter 7. In addition to the supply of information, the role of the Data Protection Authorities (DPAs) is of vital importance for the implementation of PET in information systems. The DPAs, such as the CBP (Data Protection Authority) in the Netherlands should not adopt an ex post attitude (handling complaints and carrying out checks afterwards) but actually adopt an ex ante attitude (rendering pre-emptive advice). They should be deploying their technological experts as PET consultants. On the basis of analyses of privacy risk, privacy threat or privacy impact (PIAs) they could assess whether the information systems to be implemented comply with privacy legislation and if necessary they could advise the use of PET. However, expertise on PET applications is scarce. For that reason it would be advisable for a PET expertise centre to be set up. In order to implement PET successfully in new information systems, the book recommends a specific PET step-by-step plan. The chapter concludes with proposals for a number of amendments of the EU directive 95/46 necessary for the improved protection of personal data. As a result citizens and consumers may become more confident that their personal data will be processed in accordance with their privacy preferences and the rules and regulations. The PET measures incorporated in information systems will enable them to protect themselves more effectively against privacy violations in the coming AMI world.

The research of today shows that we can built privacy safe information system (the *how* in the problem definition), but these systems need to be equipped with a certificate (privacy seal) declaring that the system warrants the privacy safe

processing of personal data, and these systems have to be deployed on a large scale in society in order to generate the general *trust* of the citizens. However if there is the lack of political imperative to protect our privacy adequately with PET and if we continue the use of privacy unsafe information systems in our risk-surveillance society, then great dangers for our privacy is at hand.

Lijst van aanbevelingen

Hieronder volgen de aanbevelingen die in hoofdstuk 8 (paragrafen 8.5 t/m 8.8) zijn gedaan.

Aanbeveling I aan het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en het Ministerie van Justitie en de Data Protection Authorities (College bescherming Persoonsgegevens):

Maak bij de voorlichting over 'privacy enhancing technologies'(PET) gebruik van de positieve adoptiefatoren voor PET. Voer op basis van het maturiteitsniveau van de overheidsorganisaties PET standaard in alle informatiesystemen in, conform de motie Nicolaï (1999).

Aanbeveling II aan de Data Protection Authorities (College Bescherming Persoonsgegevens):

Zorg voor unanimiteit in de EU met betrekking tot het gebruik van PET. Draag dezelfde boodschap over PET EU-breed uit. Bevorder dat PET standaard ('by default') wordt toegepast teneinde de privacyveiligheid van informatiesystemen te stimuleren.

Aanbeveling III aan de Data Protection Authorities en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties:

Richt een Europees respectievelijk landelijk PET Expertisecentrum op en/of bevorder de oprichting van 'PRITAC' op EU-niveau.

Aanbeveling IV aan de verantwoordelijken:

Voer voordat een opdracht wordt gegeven voor de ontwikkeling van een informatiesysteem of programmatuur waarmee persoonsgegevens worden verwerkt een multi-actoranalyse uit. Daarmee worden mede automatiseringsdebacles voorkomen.

Aanbeveling V aan de verantwoordelijken:

Volg het in dit boek uiteengezette stappenplan om privacyveilige systemen te verwezenlijken.

Aanbeveling VI aan de verantwoordelijken en adviserende accountants:

Bereken vooraf de Return On Investment van PET maatregelen (ROI-PI), opdat er een gewogen management beslissing genomen wordt over de invoering van privacybeschermende maatregelen en reputatieschade kan worden voorkomen.

Aanbeveling VII aan de Europese wetgever:
Pas de tekst van de EU-privacyrichtlijn 95/46/EG aan in lijn met de nieuwe technologische ontwikkelingen, zodat rekening wordt gehouden met:

1. nieuwe persoonsgegevens;
2. nieuwe middelen waarmee gegevens worden verwerkt;
3. de nieuwe groep van verantwoordelijken;
4. de gewijzigde doelstellingen;
5. de ontwikkelingen op het gebied van ambient intelligence

Aanbeveling VIII aan de Europese wetgever:

1. Stel in eerste instantie niet de verantwoordelijke zoals gedefinieerd in de Richtlijn 95/46/EG voor de onrechtmatige persoonsgegevensverwerking aansprakelijk, maar de manager die direct bij de verwerking betrokken is, vergelijkbaar met de aansprakelijkheidsregeling in de Amerikaanse SOX.
2. Voer productaansprakelijkheid in voor privacyonveilige informatiesystemen, vergelijkbaar met de productaansprakelijkheid voor (onveilige) producten.

Aanbeveling IX aan de Europese wetgever/de Europese Commissie:
Naast een expliciete definiering van het begrip 'privacy by design': neem in de Richtlijnen 95/46/EG en 2002/58/EG de volgende drie verplichtingen op:

1. De verantwoordelijke (in de zin van de Richtlijn) dient een privacyrisico, privacy impact- of bedreigingsanalyse uit te voeren, voordat een systeem wordt ontworpen c.q. op de markt wordt gebracht; een dergelijke privacyrisicoanalyse dient aan de Data Protection Authority voorafgaande aan de bouw van het systeem te worden voorgelegd. Bevorder de standaardisatie van de Privacy Impact analyse (PIA).
2. PET dient als technisch middel om de persoonsgegevens te beschermen 'by default' te worden toegepast; 'privacy by design' moet als privacyrealisatiebeginsel in de richtlijn te worden opgenomen.
3. Gebruikers dient standaard de optie te worden geboden om diensten en infrastructuren ook anoniem te kunnen gebruiken.

Aanbeveling X aan de Europese wetgever:
Zorg voor wetgeving die controle, reciprociteit en terugkoppeling aan de gebruiker van informatiesystemen voorschrijft.

Protocol case studies

Date of interview:

A. Company/Organization general data
   1. Name Company/Organization:
   2. Address Company/ Organization:
   3. Name(s) of person(s) interviewed:
   4. Function(s) of person(s) interviewed
   5. What is the primary operation of the organization?
   6. What different processing operations are occurring in the organization?
   7. Do you have a written security policy?
   8. Do you have a security risk analysis?
   9. Do you have a privacy risk/threats analysis?

B. Strategy

   10. How does Privacy relate to the objectives/strategy of your firm?
       a. Is it considered as a legal must
       b. Is it considered as potentially important but not essential
       c. Is it considered as a potential strategic driver for market share, customer retention and acquisition?
       d. How would you describe the information intensity (information content used and generated) of your firm
   11. How would you describe your identity and privacy processes?
       a. There is no official policy/program established
       b. There is a beginning of staffing and organizing a program
       c. Some key initiatives are being launched
       d. There is an established program that can be evaluated
       e. The program is in maintenance mode focusing on refinement
   12. Do you have a privacy infrastructure? I.e. is there a function accountable for privacy protection? Yes/No
       a. Privacy office (officer)
       b. Privacy policy and procedures
       c. Personnel training and awareness
       d. Privacy enhancing tools (specify)
       e. Privacy audits
       f. Other...
   13. Is privacy protection part of the management cycle? Yes/No

14. Is there a separate budget for privacy protection? Yes/No
15. If yes, What is the amount of the privacy budget?
16. How much do you spend on privacy?
    a. How much do you spend (or if no budget exist: how much would you like to spend) on the above components of your privacy infrastructure?
    b. What are the most important components in terms of total spend?
    c. What is the percentage of the turnover spent for privacy?
17. Please plot your organization in the IAM maturity Model (handed over).

C. Privacy attitudes

18. Are employees privacy aware?
19. Do you consider privacy legislation workable/complex?
20. Does the compliance/pressure to privacy legislation play a role in your organization? Yes/No
21. How do you estimate the chance of being caught for privacy violations by the data protection authority?
22. Does this influence your attitude towards privacy protective measures? Yes/No
23. Are privacy incidents (internally) reported? Yes/No

D. Privacy Incidents/breaches

24. Please, Consider/Imagine a serious privacy breach: what are/ would be the tangible financial consequences?
    a. Investigation and forensics
    b. Outbound contact costs
    c. Inbound contact costs
    d. PR & communication to restore reputation
    e. Legal defense
    f. Security consultants
    g. Lost business
    h. Customer acquisition costs
    i. System and process redesign costs
    j. Other...
25. Please, Consider a serious privacy breach: what are the intangible consequences?
26. Does assuring privacy give you a market (competitive) advantage?
27. Can you give an estimate of costs in case of:
    a. Regular small privacy breaches
    b. A large privacy breach

c. Can you give an 'informed opinion' about the likelihood that each of the two would happen

28. How would you estimate the costs of:
    a. Ad hoc processes
    b. Well-established processes
    c. Fully optimized including

E. Aspects about PETs-innovation

29. How do you qualify your organization with regard to innovation?
30. Is your (top) management open to accept changes that accompany innovation?

F. Aspects of PETs-complexity

31. Are PETs measures compatible (resembles the preceding measures) in your organization? Yes/No
32. Do you consider PETs implementation and use as complex (need specialized knowledge/ expertise)?
33. Are there key persons within your organization that can take the lead in the adoption process of PETs?

G. Aspects of PETs -testability

34. Is the testability of PET possible in small-scale experiments in your organization?

H. Aspects of PETs - business case – costs

35. Is there a PETs budget (amount please)? Yes/No
36. Has any damage occurred die to privacy incidents? Yes/No
37. Do you believe that PET implementation is expensive?

I. Aspects of PETs – advisors/advisory institutions

38. Are external advisors been consulted concerning PETs implementation? Yes/No
39. Which organizations/advisors have been consulted/involved in the implementation of PET?

J. Aspects of PETs – social recognition – visibility & marketing – integration into processes

40. Is PETs visible for your customers/employees?
41. Is PETs liked in your organization or by your customers?
42. Can PET be woven into your business processes?

Referenties

A

Abie H., PETWeb model Ontological analysis of privacy threat impact in State of the Art of Privacy-Enhancing Technology (PET) – *Deliverable D 3.3* van het PETWeb project, Oslo 2007.

Albrecht K., RFID Tag, You're it, *Scientific American* September 2008, vol. 299, nr. 3.

Agre P.E. & M. Rotenberg, Technology and Privacy: The New Landscape, Cambridge (Massachusetts) 2001.

Aldhouse F., What might Data Protection look like in 2026? Manchester 2005; http://www.ico.gov.uk/upload/documents/ 2005/dpa_conference_1.pdf.

Amoore L., Biometric Borders: Governing Mobilities in the War on Terror, *Political Geography* 2006, 25(2), p. 336-351.

Ammelrooy P. van, Gifmengers duiken op adresboek Internet, *De Volkskrant* 26 juli 2008.

Anderson R., Why cryptosystems fail, *Conference on Computer and Communications Security*, *Proceedings of the 1st ACM conference on Computer and communications security*, New York, 2003.

Anderson R., *The Economics of Security and Privacy*, Toronto, 2004.

Andweg R. & T. van der Tak, Privacy, een oud verschijnsel, een nieuw probleem, *Ars Aequi XXIV,* Privacy, themanummer 3 maart 1975.

Andreassen F.L., Are the Norwegian Internet users ready for the new threats to their information? A survey on awareness and use of preventive technologies (master's thesis), Gjøvik 2007.

Andriessen V., Nederlandse Internetzoekmachine Ixquick ontvangt eerste Europese privacycertificaat, *Financieel Dagblad* 15 juli 2008.

Arendzen I., J.B.F.C. van den Assum, R.M. den Hartog-van Ter Tholen, T.F.M. Hooghiemstra & R.J.Terwiel, *Regelgeving Medisch-wetenschappelijk onderzoek, Tekst en Toelichting*, Den Haag 2007.

Article 29 Working Party. Voor de geraadpleegde Opinions, zie de lijst achter deze bibliografie.

Assagioli R., *Psychosynthesis*, Harmondsworth 1986.

B

Bahr N.J., *System Safety Engineering and Risk Assessment: A Practical Approach*, London, 1997.

Baker W.H., A. Hutton, C. D. Hylender, Ch. Novak, Ch. Porter, B. Sartin, P. Tippett & J.A.Valentine, *2009 Data Breach Investigations Report*, Basking Ridge N.J., 2009.

Baladi M., D. Mowers, A. Steven & P. Verwold, A. Steven, Password Management, *Microsoft Architect Journal*, Redmond July, 2006.http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund_2.mspx?mfr=true.

Ball K., D. Lyon, D. Murakami Wood & C. Raab, *A Report on the Surveillance Society*, Manchester 2006.

Banisar D., *Privacy and Human Rights, An international Survey of Privacy Laws and Developments*, Washington D.C., 2006.

Bäumler H, Datenschutz in der Informationsgesellschaft von Morgen, Berlin 1998.

Bäumler H., & A. Von Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, Braunschweig/Wiesbaden 2002.

Bayer J. & N. Melone, A Critique of Diffusion Theory as a Managerial Framework for Understanding Adoption of Software Engineering Innovations, *The Journal of Systems and Software*, 1989/2.

Beck U., *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt a.M. 1986.

Beck U., *The Risk Society*, 1992 Newbury Park CA.

Beirens L., Data Retention, The Belgian Implementation of the EU Directive 2006/24/EC, (presentatie) KUL, Leuven 2006.

Bekkers V., Advanced thematic course: State and Network, (presentatie) Rotterdam 2007.

Bellotti V. & A. Sellen, Design for Privacy in Ubiquitous Computing Environments, *Proceedings of the Third European Conference on Computer Supported Cooperative Work* (ECSCW '93) Milan, 1993 (A).

Bellotti V. & A. Sellen, *Design for Privacy in Ubiquitous Computing Environments*, Cambridge (UK) 1993.

Bemelmans T.M.A., *Bestuurlijke informatiesystemen en automatisering*, Deventer, 2000.

Bench-Capon T., *Ontologies and Legal Knowledge-Based Systems Development,* in: J. Donkers J, L. Mommers, E. Postma & A. Schmidt, Liber Americorum ter gelegenheid van de 60e verjaardag van prof. dr. H. Jaap van den Herik, Maastricht & Leiden 2007.

Bennett C. & C. Raab, The Governance of Privacy: Policy Instruments in Global perspective, 2nd ed., Cambridge, (MA) 2006.

Berg B. van den, Ik ga op reis en ik neem mee.., Over de toekomst van het begrip 'persoonlijke ruimte', in: V. Frissen & J. de Mul (red.). De draagbare Lichtheid van Het bestaan, Kampen 2008.

Berkvens J.M.A., J.J.F.M. Borking, C.F. van Geest, N.J. Rinkel, H.A. van der Schraaf & G.P.V. Vandenberghe, *Achter de Schermen van Automatiseringscontracten*, Alphen aan den Rijn/Brussel 1987 & 1989.

Berne E., *Games people play, The psychology of human relationships*, 3rd impression, London 1966.

Berthold O., H. Federrath en S. Kopsell, WebMIXes: A System for Anonymous and Unobservable Internet Access, *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley (CA), 2000.

Berthold O., A. Pfitzman & R. Standtke, 'The Disadvantages of Free MIX Routes and How to Overcome Them', *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley (CA), 2000.

Bing J. & K.S. Selmer (eds.), *A Decade of Computers And Law*, Oslo 1980.

Bing J. (ed.), *Handbook of Legal Information Retrieval*, Amsterdam, NewYork, Oxford, 1984.

Blarkom G.W. van, *WPR en Ziekenhuisinformatiesystemen*, *NTMA* nr. 88, juni 1997, p. 29-32.

Blarkom G. van, Patent Application Number 9712459.8 (application date 14th June 1977) München.

Blarkom G.W. van, Guaranteeing requirements of data-protection legislation in a hospital environment with privacy-enhancing technology, *BJHCIM (The British Journal of Healthcare Computing & Information Management*), May 1998, Vol. 15, number 4.

Blarkom G.W. van & J.J. Borking, *Beveiliging van Persoonsgegevens, Achtergrond en Verkenningen 23*, Den Haag 2001.

Blarkom G.W. van, Meer kanten aan PET: PET in de praktijk bij Meerkanten, *Privacy & Informatie*, nr. 5, 2002.

Blarkom G.W. van, J.J. Borking, & J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents*, Den Haag, 2003.

Blarkom G.W. van, S. Kenny, J.J. Borking, M. van Breukelen, A.P. Meyer & A.K. Ahluwalia, *Design Method in Handbook of Privacy and Privacy-Enhancing Technologies*, G.W. van Blarkom, J.J.Borking. J.G.E.Olk, Editors, Den Haag, 2003.

Bock K., Pricing Privacy, Privacy by design, Utopia or possible future? Presentatie, Brussel 2009 beschikbaar via http://www.cpdpconferences.org/. Voor meer informatie: www.european-privacy-seal.eu/.

Boer L. & T.K. Grimmius, Melding Maken? Internationale quickscan meldplicht gegevensverlies, Een onderzoek in opdracht van het Ministerie van Economische zaken, Zoetermeer 2009.

Borking J.J., Gelijke behandeling of gelijke deelname, *Nieuwsbrief Buitenlandse Werknemers* 1971, nr. 7.

Borking J.J., De Wetgeving van onze buurlanden met betrekking tot de buitenlandse weknemer, *Nieuwsbrief Buitenlandse Werknemers* 1973. nr. 3.

Borking J.J, Internationale Arbeidsmigratie, *Nieuwsbrief Buitenlandse Werknemers* 1973, nr. 5.

Borking J.J., Een gat in de Auteurswet, Object Code niet beschermd, *Informatie* 1983, nr. 4.

Borking J.J., Drafting Contracts to Protect Software, *Il Foro Padano 1983, nr. 3.*
Borking J.J., Commerciele en Technische bescherming van programmatuur, *Informatie* 1983, nr. 7/8.
Borking J.J., Bescherming van Software in Japan, *Bijblad bij de Industriële Eigendom* 1983, nr. 11.
Borking J.J., Over programmatuurpiraterij en de opsporing daarvan, *Informatie* 1983, nr. 11.
Borking J.J., Bescherming van de persoonlijke levenssfeer, de tussenstand, in: L. R. van Dullemen, *Negen aspecten van computertechnologie en maatschappij*, Den Haag 1984.
Borking J.J., Het WIPO voorstel inzake programmatuurbescherming, in: H. Koppelaar & F.V.B.M. Mutsaerts (red.), *Computerfraude en Informatiebeveiliging*, Amsterdam/Brussel 1984.
Borking J., Patent Protection of Software in Continental Europe, A Status Quo, *Computer Law & Practice* 1984, nr. 1.
Borking J., Pro and Cons of Allowing Copyright, *Computer Law & Practice* 1984, nr. 2.
Borking J.J., Wijziging van de Auteurswet noodzakelijk om computerprogrammatuur optimaal te beschermen, *Informatie* 1984, nr. 3.
Borking J.J., Contractuele bescherming van programmatuur, *Informatie* 1984, nr. 7.
Borking J.J., Octrooirechtelijke en auteursrechtelijke bescherming van programmatuur in een aantal Europese landen, *Informatie* 1984, nr. 12.
Borking J.J., Import Duties on Software, *Computer Law & Practice* 1985, nr. 2.
Borking J.J., Contract Solutions in Software Protection, *The Computer Law and Security Report* 1985, Issue 1 & 2.
Borking J.J., Object code, een auteursrechtelijk enigma?, *Informatie* 1985, nr. 1.
Borking J.J., Drafting Contracts to Protect Software, *Revue Internationale de la Concurrence*, 1985, nr. 1.
Borking J.J., *Third Party Protection of Software and Firmware, Direct protection of zeros and ones*, Amsterdam, New York, Oxford 1985.
Borking J.J., Invoerrechten over de waarde van programmatuur uit niet EG landen, *Informatie* 1985, nr. 5.
Borking J.J., De resultaten van een rechtssociologisch onderzoek naar de juridische bescherming van programmatuur, *Informatie* 1985, nr. 10.
Borking J.J., Nieuwe Franse, Engelse en Duitse wetgeving betreffende computerprogrammatuur, *Informatie* 1986, nr. 2.
Borking J.J., *Internationale ontwikkelingen op het gebied van de juridische bescherming van software en chips*, Deventer 1986.
Borking J.J., De Zweedse oplossing van het programmatuur en chips beschermingsvraagstuk, *Informatie* 1986, nr. 5.
Borking J.J., Privacybescherming: De Internationale Stand van Zaken, *Informatie,* speciaal nummer mei 1986.

Borking J.J., Enige Kanttekeningen bij informaticaverzekeringen, *Informatie* 1987, nr. 1.
Borking J.J., Risico's voortvloeiend uit productaansprakelijkheid voor programmatuurmakers, *Informatie* 1987, nr. 10.
Borking J.J., Results of a Socio-Legal Survey Regarding the Legal Protection of Software, *Software Protection* 1987, nr. 6.
Borking J.J., Lokale netwerken (LAN's) en toegevoegde waarde netwerken (VAN's) in: F. de Graaf (red.), *Hoofdstukken Informaticarecht*, Alphen aan den Rijn 1987.
Borking J.J., Juridische kanttekeningen bij programmatuur contracten, in: B.A.A. Hopstaken & A. Kranendonk (red.), *Beslissen over Bits en Bytes*, Amsterdam/ Brussel 1990.
Borking J.J., Regelgeving en Kwaliteitsbevordering door Brancheorganisaties, in: H. Franken (red.), *Dossier Onderneming & Automatisering*, 1993.
Borking J.J., H.L. van Rossum, M.E. van Biene-Hershey, J.N.M. Koppes, A.W. Neisingh, J.H. Sneep & H. de Zwart, *Beveiliging van persoonsregistraties*, Den Haag 1994.
Borking J.J., Privacy Technology. A new challenge in cyberspace, in: P. Ippel, G. de Heij & B. Crouwers (eds.), *Privacy Disputed*, Den Haag 1995.
Borking J.J. & W.J. Vriedhoff, *Van Missie tot Bedrijfsplan*, Alphen aan den Rijn 1995.
Borking J.J., *Back to Anonymity – Privacy Enhancing Technologies*, Proceedings of the 17th International Conference on Data protection, Copenhagen 1995.
Borking J.J., Privacy technologie, een nieuwe uitdaging in Cyberspace in: B.N. Westerbrink, *Juridische aspecten van het Internet*, Amsterdam 1996.
Borking J.J, Der Identity-Protector, *Datenschutz und Datensicherheit (DuD)* 1996, nr. 11.
Borking J.J., Partijen moeten hun problemen zelf oplossen, *De Automatiseringsgids* 1997, nr. 11.
Borking J.J., Healthcards, protection or intrusion of privacy, in: L. van den Broek & A.J. Sikkel, *Health Cards '97* (Studies in Health Technology and Informatics, vol. 49), Amsterdam 1997.
Borking J.J. & T. Hooghiemstra, Electronic patient records and hospital information networks, in: H. Runnenberg, *Health Information Initiatives in the Netherlands*, Hillegom 1998.
Borking J.J., M. Artz & L. van Almelo, *Gouden Bergen van Gegevens*, Den Haag 1998.
Borking J.J., 2008 – Ende der Privatheit?, in: H. Bäumler (ed.), *Der Neue Datenschutz*, Berlin 1998.
Borking J.J., Nieuwe Privacy-wet versterkt noodzaak tot maatregelen in de IT-sfeer, *Informatiemanagement* 1998, oktober nr. 10.
Borking J.J., Data Warehousing en Data Mining, in: J.L. Boers, *Informatiebeveiligings Jaarboek 1999/2000*, Den Haag 1999.

Borking J.J., B.M.A. van Eck & P. Siepel, Intelligent Software Agents and Privacy, *A&V* 13, Den Haag 1999.
Borking J.J. & J.B.F. Mulder, Tien jaar lessen in Geschillenoplossing in de ict branche: Psychologische factoren van doorslaggevend belang!, in: H. Franken, J.J. Borking & P.C. van Schelven, *12 over de SGOA*, Den Haag 1999, p. 81-90.
Borking J.J. & H. Mulder, Vijftien jaar Geschillenoplossing maakt valkuilen zichtbaar, *De Automatiseringsgids* 25 april 1999 (A), nr. 25.
Borking J.J., Erwartungen an die Datenschutzbeauftragten im Internet, in: H. Bäumler (Hrsg.), *E-Privacy, Datenschutz im Internet*, Wiesbaden 2000.
Borking J.J., Mag het een bitje minder zijn?, *Compact* 2001, nr. 4.
Borking J.J., Privacy Incorporated Software Agent (PISA), *Datenschutz und Datensicherheit*, (DuD) 2001, nr. 7.
Borking J.J., Geschillenoplossing van Offline naar Online: de visie van de Stichting Geschillen Oplossing Automatisering, *Computerrecht* 2001, nr. 5.
Borking J.J., E-Privacy, Wat nu?, in: P.B. Cliteur, H.J. van den Herik, N.J.H. Huls & A.H.J. Schmidt, *It ain't necessarily so*, Liber Amicorum voor prof. dr. H. Franken, Leiden 2001.
Borking J.J., Privacy-Enhancing Technologies (PET), Darf es ein Bitchen weniger sein?, *Datenschutz und Datensicherheit (DuD*) 2001, nr. 10.
Borking J.J., R. Coolen, J. Giezen & P. Verhaar, *PISA EU research project IST – 26038, Methodology of Threat Analysis, Deliverable 7 (D. 2.1),* Brussels 2001.
Borking J.J. & C.D. Raab, Laws, PETs and Other Technologies For Privacy Protection, *Journal of Information, Law and Technology (JILT*, januarie 2001.
Borking J.J., *On PET and Other Privacy Supporting Technologies*, Brussels 2001.
Borking J.J., Privacy Incorporated Software Agent (PISA): Proposal for Building a Privacy Guardian for the Elecronic Age, in: H. Federrath (ed.), *Designing Privacy Enhancing Technologies, Design Issues in Anonymity and Unobservability*, Berlin 2001.
Borking J.J., Geschillenoplossing van offline naar online, *Computerrecht* 2001, nr. 5.
Borking J.J., PET: Het privacyprobleem structureel opgelost, *Informatiebeveiliging* september 2001, nr. 5, p. 4-7.
Borking J.J., Checklist administratieve organisatie, in: J.M.A. Berkvens & J. Holvast, *Schriftelijke praktijkcursus De nieuwe wet bescherming persoonsgegevens II*, Eindhoven 2002.
Borking J.J., Privacy Enhancing Technologies, (PET): Online and Offline, a structural contribution towards the solution of informational privacy problems, in: W. Peissl (Hrsg.) *Privacy, Ein Grundrecht mit Ablaufdatum?*, Wien 2003.
Borking J.J., The Status of Privacy Enhancing Technologies, in: E. Nardelli, S. Posadziejewski & M. Talamo (eds.), *Certification and Security in E-Services*, Boston 2003.
Borking, J.J., PET, Het derde Spoor, Een terugblik, *Privacy & Informatie* 2002, nr. 5.

Borking J.J., Les 2, Leergang Nieuwe Privacy Wet, Over Administatieve Organisatie, Beveiliging, Privacy Enhancing Technologies (PET) en Privacy Audits, in: J.M.A. Berkvens & J. Holvast, *Schriftelijke praktijkcursus De nieuwe wet bescherming persoonsgegevens*, Eindhoven 2003.

Borking J.J., What are PETs?, Report for the European Commission, Brussels 2003.

Borking J.J., Privacy Rules for Intelligent Software Agents, *TILT*, nr. 15, Bern 2003.

Borking J.J., Privacy Standards for Trust, *Jusletter* 3 oktober 2005, Bern 2005.

Borking J.J., Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization, CEN CWA (CEN Workshop Agreement) #15263, Brussels 2005.

Borking J. & C. Liddie, PET for PHIPA, Toronto 2005,www.theprivacynetwork.org/SSN/PrivacyBootcamp/Standards/Documents.

Borking J.J. & R.F. Koorn, Witboek 'Privacy Enhancing Technologies voor Beslissers', *Privacy & Informatie* (P&I) 2005, nr. 5.

Borking J.J. & F. Van Vliet, Ixquick Rapport CS-X-080711-002, Kiel 2008.

Borking J.J. & N. Foukia, Privacy Rules for Software Agents, A Horrendous Challenge for Developers Toronto 2008,www.theprivacynetwork.org/SSN/PrivacyBootcamp/Standards/Documents.

Borking J.J., Adoptie van Online Geschillenoplossing door Organisaties, in: P.C. van Schelven, R&P 170, *Van geschil tot oplossing*, Deventer 2008.

Borking J.J., Organizational Motives for Adopting Privacy Enhancing Technologies (PETs), *Data Protection Review Comunidad de Madrid*, Madrid 2009 http://www.dataprotectionreview.eu & http://prise.oeaw.ac.at/conf_contrib.htm.

Borking J.J., A. Bourka & K. Whelan, Voluntary Technology Dialogue Framework (VTDF), CEN/ISSS, WS DPP N048, Brussels 2009.

Borking J.J., Why Adopting Privacy Enhancing Technologies (PETs) Takes So Much Time, Seattle 2009, http://petsymposium.org/2009/HotPETs.

Borking J.J., El "business case" de PET (Tecnologías de Mejora de la Privacidad) y el sello EuroPrise, Madrid 2009 http:// www.dataprotectionreview.eu.

Borking S.M., *The Fascinating History of Shopping Malls*, Den Haag 1998.

Bos T., Adoptie van Privacy-Enhancing Technologies bij Publiek-Private Samenwerking, Den Haag 2006.

Boyle M., C. Edwards & S.Greenberg, The Effects of Filtered Video on Awareness and Privacy, *Proceedings CSCW 2000*, ACM Press New York 2000.

Brandon D.H. & S. Segelstein, *Data Processing Contracts, Structure, Contents and Negotiation*, New York 1976.

Brands S.A., *Rethinking Public Key Infrastructures and Digital Certificates, Building in Privacy*, Cambridge (MA) 2000.

Bradsher K., Privacy Chipped Away, *International Herald Tribune*, August 13, 2007.

Breukelen M. van, A.P. Meyer, A. Ricchi & J.J. Borking, Privacy Transfer Rules and Privacy Protection Measures (Deliverable D.3) PISA research project: IST-2000-26038, Brussels 2002.

Breukelen M. van, A. Ricchi & P. Bison, Applying the Handbook: The Job Market Case, in: G.W.van Blarkom, J.J.Borking & J.G.E.Olk, Handbook of Privacy Enhancing Technologies, The Case of Intelligent Software Agents, The Hague, 2003.

Breukelen M. van, *Demo Scenario Review PISA Demonstrator*, Delft 2003.

Breukelen M. van & A.P. Meyer, Aspects of the PISA demonstrator, in: G.W. van Blarkom, J.J. Borking & J.G.E. Olk, *Handbook of Privacy Enhancing Technologies, The Case of Intelligent Software Agents*, The Hague 2003.

Broeck W. van den & B. Desmet, *Critical Design Review, Software Engineering*, VUB (Vrije Universiteit Brussel), Brussel 2003, http://wilma.vub.ac.be/~se1/documents/critical-design-review.txt.

Buitelaar J.C. & J.J. Borking, De invulling van de FG functie bij een ministerie, *Privacy en Informatie* (P&I) 2005, nr. 1.

Bunyan T., Statewatch News Online, http://www.statewatch.org/news/, december 2005.

Burkert H., Privacy-Enhancing Technologies: Typology, Critique, Vision in: P.E. Agre & M. Rotenberg, Technology and Privacy: The New Landscape, 3e druk, Cambridge/Massachusetts 2001.

Burt R., D. Rousseau, S. Sitkin & C. Camerer, Not so different after all, a cross-discipline view of trust, *Academy of Management Review* 1998, nr. 3.

Bygrave L.A., Electronic Agents and Privacy, *International Journal of Law and Information Technology* 2001, vol. 9, nr. 3.

C

Calcutt D., Report of the Committee on Privacy and Related Matters, Cmnd 1102, London 1990.

Camp L.J. & S. Lewis, Economics of Information Security, Boston 2004.

Camp L.J. & C. Wolfram, Pricing Security, *Proceedings of the CERT Information Survivability Workshop*, Boston 2000.

Cambell D., *Development of Surveillance Technology and Risk of Abuse of Economic Information*, European Parliament, Luxembourg, 1999.

Cameron K., *The laws of Identity*, Seatle 2005.

Camenish J., R. Leenes & D. Sommer (eds.), Privacy and Identity Management for Europe, Brussels, 2008.

Camp L.J., Economics of Information Security, Boston 2004.

Canon J.C., Privacy, *What Developers and IT Professionals Should Know*, Boston, 2004.

Cranor L.F., Privacy tools, in: H. Baumler, (Hrsg), *e-Privacy, Datenschutz im Internet, Vieweg*, 2000.

Cardholm L., *Adding Value to business performance through cost benefit analyses of information security management*, Gävle 2006.
Caronni G., Anonymität-Die Kehrseite der Medaille, *DuD* 22 (1998) nr. 11.
Carr V.H. jr., Technology Adoption and Diffusion, Montgomery (AL) 1996, http://www.au.af.mil/au/awc/awcgate/innovation/adoptiondiffusion.htm:.
Cas J. & Ch. Hafskjold, Access in ict and Privacy in Europe, Experiences from technology assessment of ict and Privacy in seven different European countries, in Klüver L., W. Peissl & T. Tennøe, *ict and Privacy in Europe*, Geneva 2006.
Casassa Mont M., *A System to Handle Privacy Obligations in Enterprises,* HPL Technical report, Bristol 2005.
Casassa Mont M., *Module-Feature Specification Obligation Management System,* HPL Technical Report, Bristol 2006.
Cassassa Mont M., *On the need to explicitly manage privacy obligation policies as part of good data handling practices*, HPL Technical Report, Bristol 2006.
Casassa Mont M., Privacy Models and Languages: Obligation Policies, in: J. Camenish, R. Leenes & D. Sommer, *Privacy and Identity Management for Europe,* Brussels 2008.
Castells M., *The Power of Identity*, Oxford 2004.
Castells M., *The Rise of the Network Society New York*, 2004.
Cartrysse K., *Private computing and mobile code system* (proefschrift) TU Delft, Delft 2005.
Cavoukian A., *Getting to the Truth about Privacy & Security*, Toronto 2002.
Cavoukian A. & T.J. Hamiliton, *Privacy Payoff, How Successful Businesses Build Customer Trust*, Toronto 2002.
Cavoukian A., *Access & Privacy Excellence, 20 years in the making*, Toronto, 2007.
Cavoukian A. & A. *Stoianov, Biometric Encryption, A Positive-Sum Technology that Achieves Strong Authentican, Security and Privacy*, Toronto 2007.
Celko J. & J. McDonald, Don't Warehouse Dirty Data, *Datamation* October 15, 1995.
Chakrabarti S., *Bluetooth Scatternet Formation and Internetworking with 802.11 and GPRS*, Kalyani 2002.
Chaum D., Untraceable Electronic Mail, Return address and Digital Pseudonyms, *Communication of the ACM*, February 1981.
Chaum, D. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, *Journal of Cryptology* 1988, nr. 1.
Chaum, D. Achieving Electronic Privacy, *Scientific American* August 1992.
Chellapa R. & P. Pavlou, Perceived information security, financial liability and consumer trust in electronic commerce transaction, *Logistics Information Management 2002*, vol. 15, nr. 5/6.
Chellappa R.K. & S. Shivenda, An economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization, *Journal of Management Information systems*, 2008, vol.24, nr.3.

Claerhout B., Moderne Privacybescherming, het nut van privacy enhancing techniques, *Revue Hospitals B* 2005, vol. 3, nr. 1.
Clarke R., Business Cases for Privacy-Enhancing Technologies, in: R. Subramanian (ed.), *Computer Securoty, Privacy and Politics: Current Issues, Challenges and Solutions*, Hersey 2007.
Clarke R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, Canberra 2009, http://www.rogerclarke.com/DV/Intro.html.
Clauß S. & M. Köhntopp, Identity management and its support of multilateral security, *Computer Networks* 2001, vol. 37.
College Bescherming Persoonsgegevens, Jaarverslag 2001.
College Bescherming Persoonsgegevens, Jaarverslag 2002.
College Bescherming Persoonsgegevens, Jaarverslag 2003.
College Bescherming Persoonsgegevens, Den Haag, 2005, Advies Z 2005-1198 Voorstel van Wet Algemene Bepalingen Burger Service Nummer (30312),
College Bescherming Persoonsgegevens, Den Haag, 2006, Advies Z 2005-0807 Wetsvoorstel gebruik Burger Service Nummer in de Zorg (30380).
College Bescherming persoonsgegevens, Jaarverslag 2007.
College bescherming persoonsgegevens, Advies Wetsontwerp Implementatie Europese Richtlijn Dataretentie, Den Haag 2007.
Compeau D., C.A. Higgins & S. Huft, Social Cognitive Theory and Individual Reactions to Computing Technology, A Longitudional Study, *MIS Quaterly* 1999, nr. 2.
Cottier B., Un régime unique de protection des données pour une pluralité de systèmes politiques, juridiques, économiques et culturels: utopie ou réalité? (presentatie & paper), 27th International Data Protection and Privacy Commissioner Conference, Montreux 2005.
Corvers S. & A. Schmidt, Aanbesteding en Innovatie, een inleiding in *Legal Requirements Engineering*, Leiden 2008.
Crane S., *Transcription of Group 1 and 2 recordings workshop*, Report, Bristol 2008.
Crouwers-Verbrugge B.J., B.M.A. van Eck & E. Schreuders, *Persoonsgegevens beschermd*, Uitspraken van de Registratiekamer, Den Haag 1997.
Culnan M.J. & R.J. Bies, Consumer Privacy: Balancing economic and justice considerations, *Journal of Social Issues* 59, nr..2.

D

David R., *Les Grands Systèmes de Droit Contemporains*, Paris 2002.
Davies D.W. & W.L. Price, Security for computer Networks, An Introduction to Data Security, in: *Teleprocessing and Electronic Funds Transfer*, Chichester/ New York, 1994.
Demuth T. & A. Rieke, Anonym in World Wide Web, *DuD* 22 (1998), nr. 11.
Deng, M., L. Fritsch & K. Kursawe, Personal Rights management, in: G. Danezis & P. Golle (eds.) Privacy Enhancing Technologies – Proceedings of the 6th workshop on privacy enhancing technologies PET 2006, Berlin 2006.

Détraigne Y. & A.M. Escoffier, *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information, fait au nom de la commission des lois n° 441 (2008-2009), Paris 2009. Ook beschikbaar via : http://www.senat.fr/noticerap/2008/r08-441-notice.html.

Dietz, J.L.G. & J.B.F. Mulder, Transformation of organisations requires constructional knowledge of business systems, Hawaii International Conference in Systems Sciences1998.

Dietz J.L.G., *Enkele gedachten over architectuur in de ict*, Delft 2002.

Dietz, J.L.G., *Enterprise Ontology, Theory and Methodology*, Berlin/Heidelberg, 2006.

Diffie W. & S. Landau, Brave New World of Wiretapping, *Scientific American* September 2008, vol. 299, nr. 3.

Dijkman R.J. & J.J. Borking, Interview met Management Ixquick, Den Haag 27 december 2007, in: P.M.A. Ribbers, *Privacy Risks, Benefits and Costs (PRIME F3)*, Brussels 2008.

Dijkman R.J., *A Model for Risks, Benefits and Costs When Implementing Privacy Enhancing Technologies* (scriptie), Tilburg 2008.

Dinev T. & P. Hart, An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, vol. 17, nr. 1, 2006.

Dinev T. & P. Hart, Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use, *e-Service Journal* 2006.

Dinev T. & M. Bellotto, P. Hart, V. Russo, I. Serra & C. Colautti, Privacy calculus model in e-commerce – a study of Italy and the United States, *European Journal of Information Systems* 2006, nr. 15.

Dongen C. van, Computers en Privacy, *Informatie* januari 1976, nr. 1.

Donkers H. & B. Beugelaar, *IT Governance, Performance & Compliance*, Groningen 2008.

Donkers J., L. Mommers, E. Postma & A. Schmidt, Liber Americorum ter gelegenheid van de 60e verjaardag van prof. dr. H. Jaap van den Herik, Maastricht/Leiden 2007.

Driml S., Enhancing Security with an IT Network Awareness Center in *Information Systems Control Journal*, 2003, vol. 4, *http://www.isaca.org/Template.cfm?Section=Home&Template=/Search/SearchDisplay.cfm.*

Dumortier J. & C. Goemans, *Legal Challenges for Privacy Protection and Identity Management*, Xth Proceedings of the NATO/NASTEC Workshop on Advanced Security Technologies, in: vol. X, Networking, Bled (Slovenia)15-18 September 2003, Berlin 2004.

Duthler A.W., *Met Recht een TTP!* (proefschrift), Universiteit Leiden 22 september 1998, Deventer 1998.

Dyson E., Reflections on Privacy 2.0, *Scientific American* September 2008, vol. 299, nr. 3.

E

Earl M.J., *Management strategies for Information Technology*, New York 1989.
EPIC, *Defining Privacy*, Privacy and Human Rights Report 2006: http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Defining.html.
Esser J., Grundsatz und Norm in der richterlichen Fortbildung des Privatrecht, Tübingen 1956.
Etzioni A., *The New Golden Rule: Community and Morality in a Democratic Society*, New York 1996.
Etzioni A., *The Limits of Privacy*, New York 1999.
Europese Hof van Justitie. Voor geraadpleegde jurisprudentie van de Europese Hof van Justitie over privacy bescherming, zie de lijst achter deze bibliografie.
Europese Toezichthouder voor gegevensbescherming, (Rapport) SWIFT, Brussel 2007. http://www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=nl.

F

Fairchild A. & P. Ribbers, Privacy-Enhancing Identity Management in Business, in Privacy and Identity Management for Europe, J. Camenish, R. Leenes & D. Sommer (eds.) Brussels 2008.
Federath H. (ed.), Designing Privacy Enhancing Technologies, in: *Design Issues in Anonymity and Unobservability*, Berlin 2000.
Feigenbaum L., I. Herman, T. Hongsermeier. E. Neumann & S. Stephens, The Semantic Web in Action, *Scientific American* December 2007.
Feldman A.M. & J. Kim, *The Hand Rule and United States v. Carroll Towing Co. Reconsidered*, Working Paper Brown University Providence, Rhode Island 2002.
Feldman R., *The role of Science in Law*, Oxford 2009.
Felten, E.W., Freedom to Tinker, http://www.freedom-to-tinker.com/index.php?p=317.
Feng, P., Rethinking Technology, Revitalizing ethics, Overcoming Barriers to Ethical Design, *Science and Engineering Ethics* 2000, vol. 6, p. 207-220.
Fichman R.G., The Diffusion and Assimilation of Information Technology Innovations, in: R.W. Zmud e.a., *Framing the Domains of IT Management: Projecting the Future through the Past*, Cincinnati: 2000.
FIDIS, Future of Identity in the Information Society: The IST FIDIS Network of Excellence, www.fidis.net geraadpleegd 2009.
Fink J. & Kobsa A., A review and analyses of commercial use modeling servers for personalization on the World Wide Web, *User modeling and User-adapted Interaction* 2000, vol. 10.
Fischer-Hübner S., *IT-Security and Privacy – Design and Use of Privacy-Enhancing Security Mechanisms*, Springer Scientific Publishers, Lecture Notes of Computer Science,LNCS 1958, Berlin 2001.
Fischhoff B., S. Lichtenstein, P. Slovic, S.L. Derby, R.L. Keeney, *Acceptable Risk*, Cambridge 1981.

Flaherty, D.H, Privacy Impact Assessments: An Essential Tool for Data Protection, *Privacy Law & Policy Reporter*, October 2000, vol. 7, nr. 5.
Flaherty, D.H., Privacy Impact Assessment: an essential tool for data protection, (presentation and paper), Privacy Laws & Business, Annual Conference, Cambridge 2004.
France E., *The Response of The Data Protection Registrar*, Manchester 1997.
Franken H., Dominee en Koopman, College ter gelegenheid van de opening van het facultaire jaar 1996/1997, Leiden 1996.
Franken H., J.J. Borking & P.C. van Schelven, *12 over SGOA*, Den Haag 1999.
Franken H. & J.J. Borking, Tien jaar Stichting Geschillenoplossing Automatisering, *Tijdschrift voor Arbitrage* 2000, nr. 1.
Franken H., *Nemo Plus*… (oratie), Universiteit Leiden, Deventer 2001.
Franken H. & J.J. Borking, De oplossing van geschillen, in: R.E. van Esch & J.E.J. Prins (red.), *Recht en elektronische handel*, Deventer 2002..
Franken H., J.E.J. Prins, R.E. van Esch, A.A. Quadvlieg, E.J. Dommering, A.W. Koers, A.H.J. Schmidt, B.J. Koops & A.M.B. Lips, *Zeven essays over informatietechnologie en recht*, Den Haag 2003.
Franken H. & H.W.K. Kaspersen & A.H. de Wild, *Recht en Computer,* (5e druk), Deventer 2004.
Freedman W., *The right of privacy in the computer age*, New York 1987.
Friedewald M., E. Vildjiounaite & D. Wright (eds.), *Safeguards in a World of Ambient Intelligence (SWAMI), the brave new world of ambient intelligence: A state-of-the-art review* (report), Brussels 2006.
Frijda N.H, *De Emoties*, Amsterdam 1988.
Fritsch L., State of the art of Privacy Enhancing Technology (PET), Deliverable 2.1, PETWeb Research project, Oslo 2007.
Fritsch L., Å. Skomedal, H. Abie, J.J. Borking, F. Andressen, E. Snekkenes & N. Sørsdal, PETweb Privacy Requirements Analysis Deliverable D.1.1, PETWeb Research project, Oslo 2007.
Frissen P.H.A., De Lege Staat, Amsterdam 1999.

G

Gaver W., Realizing a video environment: EuroParc's RAVE system, *Proceedings ACM conference on Human factors in Computing Systems* CHI'92, Montery (CA) 1992.
Gellman R., Privacy, Consumers, and Costs – How the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete, (presentation and paper) Washington D.C. 2002, http://www.epic.org/reports/dmfprivacy.html.
Gerling R.W., *Datenschutz und neue Medien*, Göttingen 1998.
Gestel G.P.C. van, Creating an Identity and Access Management Maturity Model, (scriptie) Tilburg 2007.

Gibbons J.H. (ed.) Scientific Validity of Polygraph Testing, A Research Review and Evaluation, A Technical Memorandum, Office of Technology Assessment, Washington 1983.
Giesen P. & S. Broersen, Nog een heel leven voor zich, *De Volkskrant* 7 juli 2007, Katern: Kennis.
Gilbert N., Dilemmas of privacy and Surveillance: Challenges of Technology change, (presentation and paper), London 2007.
Glenn, H.P., *Legal Traditions of the World*, Oxford 2000.
Goemans C., Anonimiteit op het Internet, (presentation and paper), Leuven 2002.
Goldberg I., D. Wagner, & E. Brewer, *Privacy-Enhancing Technologies for the Internet*, Berkeley 1997.
Goldhaber M.D., *People's History of the European Court of Human Rights*, Newark, N.J. 2007.
Gordon L.A. & M.P. Loeb, L.J. Camp & S. Lewis (eds.), The Economics of Information Security Investment, in: The Economics of Information Security, Boston 2004.
Groebel J. & R.A. Hinde. *Aggression and War*, Cambridge 1989.
Groenewegen L.P.J. & A. Ollongren, *Informatica, een Theoretische Inleiding*, Den Haag 1982.
Gruber. T. R., Toward principles for the design of ontologies used for knowledge sharing, *International Journal of Human-Computer Studies*, vol. 43, issues 4-5, November 1995.
Gürses S., Privacy Enhancing Tools: An Exploration of their Potentials and Limits, (presentation and paper) Leuven 2009.

H

Hackathorn R., Data Warehousing Energizes your Enterprise, *Datamation* February 1, 1995.
Hahn U., K. Askelson, & R. Stiles, *Managing and Auditing Privacy Risks*, ltamonte Springs, Florida 2008, http://www.theiia.org/guidance/technology/gtag/gtag5/.
Hameed A., D. Sleeman & A. Preece, *Detecting Mismatches among Experts Ontologies acquired through Knowledge Elicitation*, Aberdeen 2001.
Hansen M., *Identity Management Systems (IMS), Identification and Comparison Study* (report), Kiel 2003.
Hansen M., A. Schwartz & A. Cooper, Privacy and Identity Management, *IEEE Security and Privacy*, March/April 2008, vol. 6, nr. 2.
Hansen M., Concepts of user-centric identity management for privacy-enhancing security technologies, (presentation and paper) PRISE Conference, Vienna 2008.
Hempel L. & E. Töpfer, *CCTV in Europe*, Berlin 2004.
Herreweghen E., M. Waidner, P. Bramhall, J. Cuellar, J. Tappe, S. Holtmanns & F. Schasfoort, *Privacy Enhancing Technologies and Identity Management Systems in Enterprises* (report), Brussels 2003.

Hert P. de & S. Gutwirth, A Constitutional approach to European Data protection and the Constraints of the Courts, (presentation and paper), Brussels 2007, www.cpdpconferences.org/Resources/DeHert-Gutwirth.pdf.

Hes R. & J. Borking, Privacy Enhancing Technologies: The Path to Anonymity, The Hague 2000.

Hes R., T.F.M. Hooghiemstra & J.J. Borking, At Face Value, On biometrical identification and privacy, Registratiekamer A.V. 15, Den Haag 1999.

Hintum van P., *De dictatuur van het Volk*, interview met Paul Frissen, hoogleraar Bestuurskunde, *De Volkskrant* 7 november 2009, p. 35.

Hoff C. van 't, Q.C. van Est, & A. Krom, *De Digitale Generatie. Een blik op toekomst van de informatiesamenleving via de generatie die als eerste is opgegroeid met ict*, Den Haag, 2005, www.teknologiradet.no/dm_documents/final_061018_med_norsk_ sammendrag_6330A.pdf.

Hogben G., *Ontologies and System Design* (report), Ispra 2003.

Hogben G. & I. Vakalis, *Ontology Capture Methodology* (report), Ispra 2005.

Hong J.I., J.D. Ng, S. Lederer & J.A. Landay, Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems, *Proceedings of the 2004 Conference on Designing Interactive Systems: processes, practices, methods and techniques*, Cambridge (MA) 2004.

Holvast J. & J.M.A. Berkvens (red.), De Nieuwe Privacywet, Leergang, Eindhoven 2002.

Holvast J., Wet *bescherming persoonsgegevens: Stappenplan en checklist*, Amsterdam 2002, www.holvast.nl/doc/311200315563785211443 90.PDF.

Horlings E., M. Botterman, E. Frinking, R. Hamer, A. Lierens, L. Valeri & M. van de Voort, *Werkbare vormen van Privacy Enhancing Technologies*, Den Haag 2003.

Horst J., van der, *To PET or not to PET*, *P&I* 2003, nr. 4.

Hosein G., Responding to Threats to Privacy (Report Privacy International) London 2005.

Huang P.H., *The Law and Economics of Consumer Privacy Versus Data Mining*, Philadelphia 1998.

Huizenga J., Privacy Incorporated Software Agent, presentatie tijdens de International Conference on Safeguards in a World of Ambient Intelligence, Brussels, 21-22 March 2006, http://swami.jrc.es.

Hulsman B.J.P & P.C. Ippel, *Personeelsinformatiesystemen, de wet persoonsregistraties toegepast, Achtergronden en verkenningen 1*, Den Haag 1994.

Hussain D. & K.M. Hussain, *Information Resource Management*, Homewood, Illinois 1984.

Hustinx P.J., Bescherming van Persoonsgegevens op Koers, *Rechtsgeleerd Magazijn Themis* 2004, nr. 5.

Huydecoper S.M. (red.), *Wet bescherming persoonsgegevens en ICT*, Den Haag 2006.

I

Iachello G. & G.D. Abowd, Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing, *CHI 2005 Papers*, Portland, Oregon.

ICL, Latest Patent Applications: C1372 Secure Database 14-06-97, *Intellectual Property Department*, issue 97/2, London 1997.

Irsel H.G.P. van & G.J.P. Swinkels, Investeren in informatie technologie: Take IT or leave IT, *Informatie* 1992, themanummer november 1992.

Ismail E.S. & Y.A. Hasan, Fail-Stop Designated Recipient Signature Scheme and its Applications, *Matematika* 2007, vol. 23, nr 1.

J

Jacobs B., Privacy and Computer Security, Very Briefly (presentation), Brussels 2009, www.cpdpconferences.org.

Jaret P., Stalking the world's epidemics, The Disease Detectives in National Geographic, vol. 179, nr. 1, January 1991.

Jeyaraj A., J.W. Rottman & M.C. Lacity, A review of the predictors, linkages, and biases in IT innovation adoption research, *Journal of Information Technology* 2006, nr.1.

Juan, S., Do Lie Detectors really work?, *Biology* 16 June 2006, http://www.theregister.co.uk/2006/06/16/the_odd_body_polygraph/.

Jung C.G., *Traumsymbole des Individuationprozesses*, Olten 1984.

Jung C.G., *Aion, GW 9/11*, Olten 1951.

Jung C.J., *The integration of the personality*, Toronto 1939, vetaald in *Bewust en Onbewust* door P. de Vries-Elk, Rotterdam 1989.

K

Kankanhale A., H.H. Teo, B. Tan & K.K. Wei, An integrative study of information systems security effectiveness, *International journal of information management* 2003, 23, nr. 2.

Karjoth G., M. Schunter & M. Waidner, *The Platform for Enterprise Privacy Practices- Privacy-enabled Management of Customer Data*, Zurich 2003.

Keen P.G.W., *Concurrentiebeleid & Informatietechnologie*, Amsterdam/Brussel 1991.

Keanini T., Vulnerability management technology: a powerful alternative to attack management for networks - Storage Networking Computer Technology Review May 2003, http://findarticles.com/p/search?tb=art&qa=Tim+Keanini.

Kehaulari Goo S., Senator Kennedy Flagged by No-Fly List, *Washington Post* 20 August 2004.

Kelly K., *Out of Control: The new biology of machines, social systems and the economic world*, reading, Mass., Wokingham 1994.

Kenny S. & L. Korba, Applying Digital Rights Management Systems to Privacy Rights Management, *Journal of Computers and Security* November 2002, vol. 21, nr. 7.

Kenny S. & J. Borking, The Value of Privacy Engineering, *The Journal of Information, Law and Technology* (JILT) March 2003, http://elj.warwick.ac.uk/jilt/02-1/kenny.html.

Kerkmeester H.O., *Recht en speltheorie, een economisch model voor het ontstaan van staten en recht* (dissertatie EUR), Lelystad 1989.

Kerr I., The Internet of Things, ...Well then, why not people?, presentatie tijdens de 29th International conference of Data Protection and Privacy Commissioners, Montreal 2007.

Kessel W., *Technik und Datenschutz*, Schwerin 1996.

Kielman H.H., *Politiële gegevensverwerking en Privacy, Naar een effectieve waarborging* (proefschrift), Leiden 2010.

Krisch, A., The role of Business and personal data protection (presentatie), Brussels 19 mei 2009, p. 8, http:/ec.europa.eu/justice_home/fsj/privacy.

Klaver, M., M. van Lieshout, L. Pennings, P. Verhaar & J. Holvast, *Privacy Enhancing Technologies en Overheidsinformatiesystemen*, Delft 2002.

Kleve P., Juridische Iconen in het informatietijdperk (proefschrift Erasmus Universiteit), Deventer 2004.

Klüver L., W. Peissl & T. Tennøe, *ICT and Privacy in Europe*, Geneva 2006.

Koelewijn W.I., *Privacy en Politiegegevens, Over geautomatiseerde normatieve informatie-uitwisseling* (proefschrift), Leiden 2009.

Kohnstamm, J., Supervisory Authorities and the Data Subject (presentatie), Brussels 18 mei 2009, p. 5, http:/ec.europa.eu/justice_home/fsj/privacy.

Koops B.J., R. Poels, R. Leenes. M. Lips, C. Prins, A. Vedder & M. Groenhuijsen, *Veiligheid en privacy in 2030: twee toekomstscenario's*, Tilburg 2005.

Koops B.J. & M.M. Prinsen, Glazen woning, Transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit, *NJB* 12 maart 2005.

Koorn R.F. & J. Ter Hart, Privacy: Van Organisatorisch Beleid naar Privacy Enhancing Technologies, *Compact* 2004, nr. 3.

Koops B.J., Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer) criminalisering van de maatschappij, *Computerrecht* 2003, nr. 2.

Koorn R., H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen & J.J. Borking, *Privacy Enhancing Technologies, Witboek voor Beslissers*, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Den Haag 2004.

Korff D., *EuroPrise Criteria Catalogue*, version 3, Kiel 2009, http://www.european-privacy-seal.eu/awarded-seals/de.

Kosta E. & P. Valcke, Retaining the Data Retention Directive*, Computer Law Security Report* 2006, nr. 22.

Kottenhagen-Edzes P., *Immateriële schade: tendensen en wensen*, Maastricht 2000.

Kropf J.W., Independance Day: how to move the Global privacy dialogue forward, *World Data Protection Report* February 2009, vol. 9, nr. 2.

Kuner Ch., *European Data Protection Law: Corporate Compliance and Regulation*, second edition, Oxford 2007.

Kutschera, F. von & A. Breitkopf, *Einführung in die moderne Logik*, München 1971.

L

Lace S. (ed.), *The Glass Consumer: Life in a surveillance society*, London 2005.

Lau F., S.H. Rubin, M.H. Smith & L. Trajkovic, Distributed Denial of Service Attack, *IEEE* 2000.

Leerentveld, J.P.M.J. & G.W. van Blarkom, *Raamwerk Privacy Audit, Samenwerkingsverband Audit Aanpak*, Den Haag 2000.

Leeuw E. de, S. Fisher-Hubner, J. Tseng & J. Borking (eds.), Policies and Research, *Identity Management*, Boston 2008.

Leisner I. & J. Cas, Convenience in ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries, in: Klüver L., W. Peissl & T. Tennøe, *ICT and Privacy in Europe*, Geneva 2006.

Lessig L., *Code and Other Laws of Cyberspace*, New York 1999.

Lessig L., The law of the Horse: What Cyberlaw might teach, *Harvard Law Review* 1999, vol. 113:501, lessig.org/content/articles/works/finalhls.pdf.

Leune C.J., Access Control and service-Oriented Architectures (proefschrift), Tilburg 2007.

Leyden J., AOL sued over search engine data release, *The Register* 26 September 2006, http://www.theregister.co.uk/2006/09/26/aol_privacy_breach_lawsuit/ & http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/.

Leyden J., *Hackers debut malware loaded USB ruse*, http://www.channelregister.co.uk/2007/04/25/usb_malware/.

Lieshout M.J. van, Privacy Enhancing technologies: een zaak van lange adem, *Privacy & Informatie* 2002, nr. 5.

Little A.D., *Management of Research & Development*, Boston 1991.

Little E.G. & G.L. Rogova, *An Ontological Analysis of Threat and Vulnerability*, Paper of ICIF '06, 9th International Conference on Information Fusion, Buffalo 2006.

Lips M., S. Nouwt, R.A. Ghosh & R. Glott, *Roadmap for Socio-Cultural and Economic Research in Privacy And Identity Management RAPID – Roadmap for Advanced Research in Privacy and Identity Management* (report), Brussels 2003.

Lubbe J.C.A. van der, *Basismethoden Cryptografie*, Delft 1994.

Lucas K., *Economic Evaluation of a Company's Information Security Expenditures*, New York 2005.

Lyon D. (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital discrimination*, New York 2003.

Lyon D., *Surveillance after September 11*, Cambridge 2003 (A).

M

Maedche A., *Ontology Learning for the Semantic Web*, Boston 2002.

Marx G.T., Ethics for the New Surveillance, *The Information Society*, vol. 14, issue 3, August 1998.

Matthijssen K., *Rendement van Investering in informatiebeveiliging – Een praktische aanpak*, Tilburg 2006.

Meta Group, *Privacy enhancing Technologies,* Ministry of Science, Technology and Innovation, København 2005.

Michael J., *Privacy and Human Rights 1*, Paris 1994.

Millard C., *Data Protected*, A report on the status of data protection legislation in the European Union in 2005, London 2005.

Mileti D.S., Disasters by Design; A Reassessment of Natural Hazards in the United States. Washington D.C. 1999.

Minsky M. & D. Riecken, A Conversation with Marvin Minsky about agents, *Communications of the ACM* July 1994, vol. 37, nr. 7.

Mom P., Invoer Burger Service Nummer minacht de privacy, *Overheid Innovatief* 2007, nr. 1.

Moor J.H., Towards a theory of privacy in the information age, *Computers and Society* 1997, 27(3).

Morssink P.J., De implementatie van PET in informatiesystemen, *Privacy & Informatie* 2002, nr. 5.

Moyer M., Pulling up worms, *Scientific American* June 2009, vol. 300 nr. 6.

Mulder J.B.F. & J.L.G. Dietz, *Business Architecture based on the integration of Communication, Actors and Production*, Delft 2002.

Mulder J.B.F., *Rapid Enterprise Design* (proefschrift), Delft 2006.

Mulder J.B.F.& J.J. Borking, De eerste praktische ervaringen met elektronische geschillenoplossing in Nederland, *Computerrech*t 2006, nr. 5.

Mulder J.B.F. , Th.J. Mulder & J.J. Borking, Geschillenoplossing via Internet, *ADR Conflicthantering in de praktijk* 2006, nr. 5.

Mulder J.B.F & J.J. Borking, Diagnose-behandelcombinaties en ICT – ondersteuning bij geschillenoplossing, *Informatie* 2007, nr. 5, p. 31-35.

Mulder Th.J., *Leiders en informatiesystemen* (oratie), Maastricht 1990.

Mulder R.V. de, K.H. Oey & P.C. van Schelven, Veiligheid en IT, IT en Veiligheid, in: E.R. Muller, *Veiligheid, Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn 2004.

Muller F., *Beknopt Latijns-Nederlands Woordenboek*, Groningen 1958.

Murakami Wood D. & K. Ball, A Report on the Surveillance Society, London 2006.

N

Nas S., *Veiligheid versus privacy*, Dwars congres (presentatie), Amsterdam 2004.

Nath Ch. & W. Peissl, Security, in: L. Klüver, W. Peissl & T. Tennøe, *ICT and Privacy in Europe*, Geneva 2006.

Nationale Ombudsman rapportnummer: 2008/232 21 oktober 2008: Identiteitsfraude,
Den Haag 2008.
Negroponte N., *Being Digital*, London 1995.
Nieuwenhuis A.J., *Tussen privacy en Persoonlijkheidsrecht, Een grondrechtelijk en rechtsvergelijkend onderzoek* (proefschrift), Nijmegen 2001.
Norris C., *Criminal Justice, Expert Report*, Manchester 2006.

O

Olle T.W., H.G. Sol & A.A. Verrijn-Stuart (eds.): *Information Systems Methodologies. A Framework for Understanding*, Boston 1988.
Ortony A., G.L. Clore & A. Collins, *The Cognitive Structure of Emotions*, Cambridge 1988.
Ouwehand A.W, Stichting Informatie Voorziening Zorg, de Informatiestructuur werkwijze LADIS (Landelijk Alcohol en Drugs Informatie Systeem), (presentatie en paper), Den Haag 2002.
Oven J.C. van, *Leerboek van Romeinsch Privaatrecht*, Leiden 1948.
Overbeek P. & W. Sipman, *Informatiebeveiliging*, 2e druk, 's Hertogenbosch 1999.
Overkleef-Verburg G., *De Wet persoonsregistraties, Norm, toepassing en evaluatie* (proefschrift), Katholieke Universiteit Brabant, Tilburg 8 september 1995.

P

Padfield C.F., *Law Made Simple*, London 1983.
Patrick A.S., *Privacy, Trust, Agents & Users: A Review of Human-Factors Issues Associated with Building Trustworthy Software Agents*, Ottawa 2001.
Patrick A.S., *Just-In-Time Click-Through Agreements: Interface Widgets for Facilitating User Understanding and Confirming Informed, Unambiguous Consent*, Ottawa 2002.
Patrick A.S. & S. Kenny, From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interaction, in: R. Dingledine, *Privacy Enhancing Technologies*, Berlin 2003.
Paulus S., Implementing Criteria in the Production of Security Technology (presentation), Vienna 2008.
Peekel S., *Information Security Maturity, A qualitative framework for information security management* (scriptie), Tilburg 2006.
Peissl W., Surveillance and Security, a dodgy realitionship, *Journal of Contingencies and Crisis Management* 2003, vol. 11, nr. 1.
Pfitzman A. & M. Waidner, Networks without user observability-Design options, Advances in Cryptology- EUTOCRYPT '85: Proceedings of a workshop on the theory and application of cryptographic techniques, Berlin 1986.
Pfitzman A., M. Hansen & E. van Herreweghen, *Privacy-Enhancing Identity Management, IPTS report*, IBM Research, Zurich 2002.

Pfitzmann A. & M. Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology* (report), Dresden 2008.
Pierson C., *The Modern State*, London 1996.
Pisello, T., *Return on Investment For Information Technology Providers – Using ROI as a Selling Management Tool*, New Canaan Connecticut 2001.
Pol W. van de, *Onder de tap – afluisteren in Nederland*, Amsterdam 2006.
Polkinghorne J., *Quantum Physics and Theology*, New Haven 2007.
Porter M.E., V.E. Millar, How Information gives you competitive advantage, *Harvard Business Review* August 1985.
Posner R., An Afterword, *Journal of Legal Studies*1972, vol. 1.
Poullet Y., About the e-privacy Directive:Towards a third generation of Data Protection Legislations? (presentation), Brussels 2009. http://www.cpdpconferences.org/
Prins J.E.J., De bescherming van persoonsgegevens: de betrokkene betrokken, http://arno.uvt.nl/show.cgi?fid=4871#N_1 1998
Prins J.E.J., What's in a name? De juridische status van een recht op anonimiteit, *Privacy en Informatie* 2000, nr. 4.
Prins J.E.J., Burgerservicenummer en veiligheid: een kwetsbare relatie, (presentatie) ICT-Kenniscongres, Amsterdam 2006.
Prins J.E.J., Een recht op identiteit, *Nederlandsch Juristenblad* 2007, nr. 14, p. 849.
PRIME (Privacy and Identity Management in Europe), Whitepaper, Brussels 2005, http://privare.fbk.eur.nl/whitepaper/.
Ponemon L., 2008 Annual Study: U.S. Cost of a Data Breach, online beschikbaar: http://download.pgp.com/pdfs/Ponemon_COB-2007_US_071127_F.pdf.
Purser S.A., Improving the ROI of the security management process, *Journal of Computers & Security* 2004.

Q

Quathem K. van, Security breach notification in Europe: coming closer, *World Data Protection Report*, February 2009 vol. 9, nr. 3.

R

Ras S.G., Council: een praktisch initiatief voor online oplossen van geschillen, *Computerecht* 2006, nr. 5.
Regan P.M., *Legislating Privacy: Technology, Social Values and Public policy*, Chapel Hill (NC) 1995.
Reid P.J., *Rude Awakening Ahead, Report NCR*, Dayton, Ohio 2000, http://www.ncr.com/media-_in-for-mation/-2000/aug/pr080100b.htm.
Reidenberg J., Lex Informatica: The formulation of Information Policy Rules Through Technology, *Texas Law Review* February 1998, vol. 76, nr. 3.
Rennie J., Seven Paths to Privacy, *Scientific American* September 2008, vol. 299, nr. 3.

Reinberger M.L. & P. Spyns, Unsupervised text mining for the learning of DOGMA inspired ontology, STAR Lab technical report # 3, Brussels 2005.
Reinberger M.L., W. Daelemans & P. Spyns, *Engineering of Ontologies, VUB STAR lab Report #27*, Brussels 2005.
Ribbers P.M.A., *Privacy Process Requirements, Deliverable PRIME F 1*, Brussels 2007.
Ribbers P.M.A., *Privacy Implementation, Deliverable PRIME F2*, Brussels 2007 (A).
Ribbers P.M.A., *Privacy Risks, Benefits and Costs, Deliverable PRIME F3*, Brussels 2008.
Ribbers P.M.A., A. Fairchild, J. Tseng & J.J. Borking, *Extended Business Case Analysis* (report), Brussels 2008.
Riesewijk B. & J. Warmerdam, *Het slagen en falen van automatiseringsprojecten*, Nijmegen 1988.
Riet O.A.W.T. van de, *Multi-Actor Policy Settings, Navigating Between Negotiated Nonsense & Superfluous Knowledge* (proefschrift) Delft 2003.
Rijsenbrij D.B.B., *Informatiebeleid, -planning en -architectuur*, Utrecht 2002.
Rockley A., *Managing Enterprise Content*, Edmonton 2004, http://www.im.gov.ab.ca/sitearchives/conference2004/pdf/session2-5.pdf.
Roessler T., Anonymität im Internet, *Datenschutz und Datensicherheit DuD* 22 1998, 11.
Rogers E.M., *Diffusion of Innovations*, 5th edition, New York 2003.
Rooij J. de, Privacymanagement en Enterprise Privacy Manager, *Privacy & Informatie* oktober 2003, 6e jaargang nr. 5.
Rooij J. de, Verwaarlozing Privacy Kost Geld, *Computable: in bedrijf* 2004, nr. 15.
Rooy D. van & J. Bus, *Informal note on privacy & identity in the digital society & economy in response to the guiding questions of the draft agenda*, Oxford 2009.
Rommelse A.F., *Zwarte Lijsten. Belangen en effecten van waarschuwingssystemen*, Den Haag 1995.
Roos A.L.C., *Wet bescherming persoonsgegevens*, S&J #199, Deventer 2005.
Rossum, H. van, H. Gardeniers, J. Borking, A. Cavoukian, J. Brans, N. Muttupulle, N. Magistrale, Privacy-Enhancing Technologies: The Path to Anonymity, *Achtergrondstudies en Verkenningen* nr. 5a, Den Haag/Toronto 1995.
Roßnagel A., A. Pfitzmann & H-J. Garstka, *Modernisierung des Datenschutzrechts*, Berlin 2002.
Rotenberg M., *Privacy & Human Rights*, Washington DC 2006.
Rothfeder J., *Privacy for Sale*, New York 1992.
Rundle M., *International Data Protection and Digital Identity Management Tools*, Athena 2006.

Russell B., *History of Western Philosophy and its connection with political and social circumstances from the earliest times to the present day*, 10th impression, London 1967.

S

Saint-Exupery A. de, *Le Petit Prince*, Paris 2007.

Samarati P., E. Damiani, S. De Capitani di Vimercati, *Multiple and Dependable Identity Management, R & D Issues*, Report RAPID project, Brussels 2002.

Sampson A., *The Changing Anatomy of Britain: the handbook for the 80's*, London 1983.

Schelven P.C., *Van Geschil tot Oplossing*, Deventer 2009.

Schermer B.W. & M. Durinck, *Privacyrechtelijke aspecten van RFID*, Den Haag 2005.

Schermer B.W., M. Durinck & L.Bijmans, Juridische Aspecten van Autonome Systemen, Leidschendam 2005.

Schermer B.W., *RFID & Privacy voor Managers*, Den Haag 2006.

Schermer B.W., *Software Agents, Surveillance, and the Right to Privacy: a legislative framework for agent-enabled surveillance* (proefschrift), Leiden 2007.

Schijndel P. van, *Identiteitsdiefstal* (scriptie), Leiden 2007.

Schilfgaarde van P. & B. Nooteboom, *Vertrouwen*, KNAW, Amsterdam 2009.

Schmidt A.H.J., *Bedreigen computers ons rechtssysteem?* (oratie), Leiden/Deventer, 2004.

Schmidt, A.H.J. & R.D. Gill, Over statistisch bewijs. *Expertise en Recht* 2008, nr. 5.

Schmidt, A.H.J. & S.F.M. Corvers, *Aanbesteding & Innovatie. Een inleiding in Legal Requirements Engineering*, Boxtel 2009.

Smit N., *Business Continuity Management – A maturity model* (scriptie) Rotterdam 2005.

Smits, M, Taming Monsters: The cultural domestication of new technology, *Technology in Society* 2006, vol. 28, p. 489-504.

Schneider B., *Beyond Fear, Thinking sensibly about security in an uncertain world*, New York 2003.

Schneier B., Threat Modeling and Risk Assessment, in: H. Bäumler, *E-privacy, Datenschutz im Internet*, Wiesbaden 2000.

Scholten C.E.J., E.W.P. Koot & J.J. Borking, Millennium & Mediation, *Computerrecht* 1999, nr. 5.

Schwarz P. & J.R. Reidenberg, *Data Privacy Law: A Study of US Data Protection Law and Practice*, Michie 1996.

Secord P.F. & C.W. Backman, *Social Psychology*, Boston 1964.

Sheppard B.H., J. Hartwick & P.R.Warshaw, The Theory Of Reasoned Action, *Journal of Consumer research* 1988, nr. 3.

Skomedahl A., *PETWEB-Privacy Enhancing Technology for large scale web based services*, Hell (N) 2008, www.nr.no.

Sommer D., *The PRIME Architecture, in J.Camenish, R.Leenes & D.Sommer, Privacy and Identity Management for Europe*, Brussels 2008.
Sotoodeh M., *Ontology-Based Semantic Interoperability in Emergence Management* (PhD onderzoeksvoorstel), Vancouver 2007.
Solove D.J., A Taxonomy of Privacy, *University of Pennsylvania Law Review*, 7 January 2006, vol. 154, nr. 3.
Solove, D.J., *A Taxonomy of Privacy, GWU Law School Public Law Research Paper No. 129*, Washington D.C. 2006 (A), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622.
Solum L.B., Legal Personhood for Artificial Intelligence, *North Carolina Law Review* 1992, vol. 70.
Sonnenreich W., *Return On Security Investment (ROSI): A Practical Quantitative Model,* New York 2006.
Sprokkereef A., A. Leenes, B. Jacobs, R. Veldhuis & M. Snijder, *Sla vingerafdrukken niet centraal op*, *De Volkskrant* 26 juni 2009.
Spyns P. & G. Hogben, *Validating an automated evaluation procedure for ontology triples in the privacy domain*, STAR lab technical report # 18, Brussels 2005.
Stampfel G., W.N. Gansterer & M. Ilger, *Implications of the EU Data Retention Directive 2006/24/EC*, Wien 2006,http://www.cs.univie.ac.at/upload//970/ImplicationsEUDR.pdf.
Stol H.R., *A Framework dor evodence-based policy making using IT, A Systems Approach* (proefschrift), Tilburg 2009.
Strassmann P.A., *The Business Value of Computers*, New Canaan, Connecticut 1990.
Strik T., Senaat moet privacy burger bewaken, *De Volkskrant* 6 juli 2009.
Stuurman C., *Technische Normen en Het Recht* (proefschrift), Amsterdam 1995.
Susser E.S., D.B. Herman & B. Aaron, Combating the Terror of Terrorism, *Scientific American*, August 2002.
Syverson P.F., D.M. Goldschlag & M.C. Reed, *Anonymous Connections and Union Routing*, Washington 1997.

T

Tang Y., *PRIME Ontology Capture Methodology* (report), Brussels 2005.
Teepe W., *Reconciling Information Exchange and Confidentiality, A Formal Approach* (proefschrift), Nijmegen, 2007.
Tettero O., *Intrinsic Information Security: Embedding Security Issues in the Design Process of Telematics Systems, Telematica Instituut Fundamental Research Series, No. 006* (proefschrift), Enschede 2000.
Teufel H. III, *Privacy Impact Assessments, The Privacy Office Official Guidance, US Department of Homeland Security*, Washington DC 2007.
Thomas R., *Evidence Submitted by the Information Commissioner 2007, Home Affairs Committee Inquiry into 'The Surveillance Society?'*, London 2007.

U

Uschold M. & M.Gruninger, Ontologies and semantics for seamless connectivity in *ACM SIGMOD Record* 33, nr. 4, 2005.

V

Valverde M. & M. Mopas, Insecurity and the Dream of Targeted Governance, in: W. Larner & W. Walters (eds.) *Global Governmentality: Governing International Spaces*, London 2004.

Varella F.J., *Slapen, Dromen en Sterven*, Leuven 1998.

Vedder A.H., Het einde van de individualiteit? Groepsprofilering, datamining, brute pech en dom geluk, *Privacy en informatie* 1998, nr. 3, p. 115-120.

A. Vedder, L. Van der Wees, B.J. Koops & P. De Hert, *Van Privacy Paradijs tot Controlestaat?, Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag 2007.

Veer, van 't A. & J.J. Borking, *Interactief-spelen.com* (rapport), Den Haag 1997.

Venkatesh V. & F.D. Davis, A theoretical Extension of the Technology Acceptance Model, Four Longitudinal Field studies, *Management Science* 2000, nr. 2.

Venkatesh V., User Acceptance of Information Technology: Towards a Unified View, *MIS Quarterly* 2003, nr. 3.

Verdonck, Klooster & Associates, *Study into National Implementation of the European Data Retention Directive*, Zoetermeer 2006.

Verhaar P.J.A., T.G.A. van Rhee, H.A.M. Luiijf, R. Hes, T.F.M. Hooghiemstra & J.J. Borking, Biometrics and Privacy, TNO Physics and Electronics Laboratory Report FEL-99-C247, The Hague 1999

Verheij L.F.M., *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy*, Zwolle 1992.

Versmissen J.A.G., Sleutels Van Vertrouwen, TTP's, digitale certificaten en privacy, *A&V Achtergronden en Verkenningen* 2001, nr. 22, Den Haag.

Versmissen J.A.G. & A.C.M. de Heij, *Elektronische overheid en Privacy. Bescherming van Persoonsgegevens in de Informatie-Structuur van de Overheid Achtergrondstudies en Verkenningen 25*, Den Haag 2002.

Vey Mestdagh C.N.J. de, Privacy en ICT, in: C.N.J. de Vey Mestdagh, J.J. Dijkstra & S.C. Huisjes, *ICT-recht voor de praktijk,* Groningen 2008.

Vidalis S. & A. Jones, *Analyzing Threat Agents & Their Attributes, School of Computing Technical Report CS-05-04*, Pontypridd (UK) 2005.

Vila T., R. Greenstadt & D. Molnar, L.J. Camp & S. Lewis (eds.), *Why we can't be bothered to read privacy policies, in The Economics of Information Security*, Boston 2004.

Vlachakis J., M. Eirinaki & S.S. Anand, *An integrated web personalization platform based on content structures and usage behavior* (report), Athena 2004.

Vliet F. van, *Short Public Report on Ixquick Evaluation*, Kiel 2008, http://www.european-privacy-seal.eu/awarded-seals/de-080001p/.

Vries H. de, Opinie van de artikel 29 Werkgroep over privacy en zoekmachines, *Niewsbrief Kennedy Van der Laan*, Amsterdam 2008.

W

Waidner M., *Unconditional Sender and Recipient Untraceability in spite of active attacks*, Berlin 1990, http://64.233.183.104/search?q=cache:QQzPncvUcZIJ:www.semper.org/sirene/publ/Waid_90fail-stopDC.

Walter C., A little Privacy Please, *Scienific American* July 2007, p.74-75.

Warmerdam J., B. Riesewijk, F. Huijgen & S. van den Berg, Automatiserings-projecten: slagen of falen, Samenvattend verslag van een onderzoek naar de betekenis van sociaal-organisatorische factoren in de automatiseringsdienst-verlening, Nijmegen 1988.

Warren S. & L. Brandeis, The Right to Privacy, *Harvard Law Review* 1890, vol. 4, p. 193-220.

Waters N., Rethinking information privacy-a third way in data protection?, *Privacy Law and Policy Reporter* 2000, nr. 6.

Waters N., Privacy Enhancing Technologies, *Privacy Law & Policy Reporter* 1995, PLPR.113.

Waters R., US group implants electronic tags in Works, *Financial Times* 12 February 2006.

Watts L. & L. Macaulay*, Development of Guidance on Data protection in Systems Design*, 2000.

Wayt Gibbs W., Considerate Computing, *Scientific American* 2005, vol. 292, issue 1.

Weichert T., Datenschutz bei Suchmachinen, *Medien und Recht* #4, Berlin 2007.

Weiser M., The Computer for the 21st Century, *Scientific American* # 265, September 1991.

Westin A.F., *Privacy and Freedom*, New York 1967.

Westin A.F., *Data Protection in the Global society*, Washington D.C. 1997.

Westin A.F., Privacy and Freedom, *Communications of the ACM* 2005, vol. 48, issue 8.

Westin A.F, The Functions of Anonimity; From Biblical Times to the Information Age (presentation), Seminar The Concealed I, University of Ottawa, 4 March 2005, http://www.anonequity.org/concealedI.

Wijkstra J., Privacybeschermende maatregelen in de IT-sfeer nodig, *Informatie Management* oktober 1998.

Wijskamp B., J. ter Hart, R. Koorn, *Casus beschrijving Nationaal Trauma informatie Systeem, toepassing van Privacy Enhancing Technologies bij traumacentra* (rapport), Utrecht 2004.

Williams A., The Ever-expanding Universe of Google, *International Herald Tribune* October 15 2006.

Wishaw R.W.A., *De gewaardeerde klant. Privacyregels voor credit scoring*, Den Haag 2000.

Wissink M.H., *Richtlijnenconforme interpretatie van burgerlijk recht*, Deventer 2006.
Wittgenstein L., *Philosophische Untersuchungen Teil 1*, translated by G.E.M. Anscombe, Oxford 1953.
Wright D., *Privacy and Trust in the Ubiquitous Information Society*, Karlsruhe 2008.
Wright S., *An Appraisal of the Technologies of Political Control, European Parliament*, Strasbourg1998.

Y
Yeffeth G. (ed.), *Taking the Red Pill, Science, Philosophy and Religion in The Matrix*, Dallas 2003.
Yin, R.K., *Case Study Research, design and methods*, Thousand Oaks, Ca, 2003.
Younger K., *Report of the Committee on Privacy Cmnd.5012*, London 1972.

Z
Zipf G.K., *Human Behaviour and the Principle of Least-Effort*, Cambridge (MA) 1949.
Zuccato A., Privacy risk management in a business environment, in: P.Duquenoy, S. Fischer-Hübner, J. Holvast & A. Zuccato, *Risks and Challenges of the Network Society*, Karlstad 2004.
Zwenne G.J. & B. Schermer, *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen*, Den Haag 2005.
Zwenne G.J., A.W. Duthler, M. Groothuis, H. Kielman, W. Koelewijn & L. Mommers, *Eerste fase evaluatie – Wet Bescherming persoonsgegevens*, Leiden 2007.
Zwenne G.J. & A.H.J. Schmidt, Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens (Tweede Kamer 31145). *Mediaforum* 2008, 20 (7).

Lijst van geraadpleegde documenten van de article 29 working party[1]

WP 159 Legislation Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive).

WP 150 Legislation Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).

WP 148 Specific Opinion 1/2008 on data protection issues related to search engines.

WP 147 Specific Working Document 1/2008 on the protection of Children's Personal Data.

WP 136 General Opinion 4/2007 on the concept of personal data.

WP 114 Specific Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

WP 106 General Report on the obligation to notify the national supervisory authorities (…) and the role of the data protection officers in the European Union.

WP 105 Specific Working document on data protection issues related to RFID technology.

WP 100 General Opinion on more harmonized information provisions.

WP 91 Specific Working Document on Genetic Data.

WP 90 Specific Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC.

---

1 Alle documenten zijn beschikbaar via: **http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm**.

WP 89 Specific Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.

WP 80 Specific Working document on biometrics.

WP 56 Opinion on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (2002)

WP 37 Specific Working document "Privacy on the Internet" – An integrated EU approach to On-line Data Protection (2000).

WP 30 General Recommendation 1/2000 on the Implementation of Directive 95/46/EC.

Lijst van geraadpleegde jurisprudentie van het europese hof van justitie over privacy bescherming[1]

ECJ Judgment of the European Court of Justice of 20 May 2003 Joint Affairs C-465-00, C-138/01 and C-139/01 (Österreichischer Rundfunk).

ECJ Judgment of the European Court of Justice of 06 November 2003 in Case C-101/01 (Bodil Lindqvist).

ECJ Judgment of the European Court of Justice of 30 May 2006 Joint Affairs C-317/04 and C-318/04 (Passenger Name Records).

ECFI Judgment of the Court of First Instance of 12 September 2007 in Case T-259/03 (Kalliopi Nikolaou).

ECJ Judgment of the European Court of Justice of 29 January 2008 in Case C-275/06 – (Promusicae v. Telefónica).

ECJ Judgement of the European Court of Justice of 16 December 2008 in Case C-524/06 (Huber v. Federal Republic of Germany).

ECJ Judgement of the European Court of Justice of 16 December 2008 in Case C-73/07 (Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy).

ECJ Judgment of the European Court of Justice of 10 February 2009 in Case C-301/06 (Data Retention Directive – Ireland v. Parliament and Council).

1 Vonnissen van het Europese Hof zijn beschikbaar via:http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en.

Curriculum Vitae

John Borking, geboren te Breda op 30 augustus 1945, legde in 1973 het doctoraal examen vrije studierichting rechten (hoofdvak rechtsfilosofie) aan de Rijksuniversiteit Leiden af. Hij is werkzaam geweest als *legal counsel* en *company secretary* voor Rank Xerox Nederland B.V. te Amsterdam, Rank Xerox Manufacturing Nederland B.V te Venray, Rank Xerox Manufacturing S.A. te Lille en Rank Xerox Ltd te London. Hij was directeur van de COSSO, de vroegere brancheverenigingvoor de IT-industrie en commissaris van Børsen Nederland B.V.

Van 1994 tot 2006 was hij vicevoorzitter van de Registratiekamer, lid en buitengewoon lid van het College Bescherming Persoonsgegevens en hij is thans lid van het College Toezicht op de Kansspelen.

John Borking is ondermeer medeoprichter van de Stichting Geschillenoplossing Automatisering, de Stichting Examenkamer en de Stichting Valkenburg Groen.

Hij participeerde in diverse researchprojecten van de Europese Commissie en participeert in een EU researchproject op het gebied van privacy en identiteitsmanagement en in een door de Noorse overheid gesubsidieerd onderzoek over technologische privacybescherming binnen het Internet. Hij is voorzitter van de CEN/ISSS working party on data protection in Brussel.

John Borking is directeur/eigenaar van Borking Consultancy te Wassenaar en ict mediator/arbiter.