9

HET FAILLIET VAN HET GRONDRECHT OP DATAPROTECTIE

Bert-Jaap Koops ▪

Dataprotectie is een mooi grondrecht dat in de afgelopen decennia vorm heeft gekregen. Het bouwwerk van dataprotectie wankelt echter: wet en praktijk lopen zo ver uiteen, dat de vraag gerechtvaardigd is of dataprotectie als grondrecht nog een toekomst heeft. Aan de hand van wetsevaluaties en technische ontwikkelingen in de databanksamenleving wordt betoogd dat dragende pijlers van dataprotectie – dataminimalisatie en doelbinding – niet langer te handhaven zijn. De orthodoxe oplossing om te streven naar dataprotectie 2.0 door meer voorlichting, meer handhaving en Privacy Enhancing Technologies (PET's), kan beter plaatsmaken voor een radicaal andere strategie: datamaximalisatie en tweezijdige transparantie.

1 Inleiding

Vergelijk de Richtlijn bescherming persoonsgegevens:

> 'Overwegende dat elke verwerking van persoonsgegevens ten opzichte van de betrokkenen eerlijk en rechtmatig dient te geschieden; dat de verwerking met name adequate en ter zake dienende, gegevens moet betreffen die met de doeleinden stroken en dat deze doeleinden expliciet en geoorloofd moeten zijn en moeten zijn vastgesteld bij het verzamelen van de gegevens; dat de doelstellingen van latere verwerkingen niet onverenigbaar mogen zijn met de oorspronkelijk omschreven doelen; (…)
> Overwegende dat bepaalde verwerkingen betrekking hebben op gegevens die de verantwoordelijke niet rechtstreeks van de betrokkene heeft verkregen; dat gegevens voorts rechtmatig kunnen worden meegedeeld aan een derde, ook al was zulks ten tijde van het verkrijgen van de gegevens van de betrokkene niet voorzien; dat in al deze gevallen de informatie aan de betrokkene dient te worden verstrekt op het moment van de registratie van de gegevens of, uiterlijk, wanneer de gegevens voor de eerste maal aan een derde worden meegedeeld; (…)
> Overwegende dat een ieder over het recht moet kunnen beschikken toegang te verkrijgen tot de gegevens die het voorwerp van een verwerking vormen en hemzelf betreffen, zodat hij zich van de juistheid en de rechtmatigheid van de verwerking ervan kan vergewissen; (…)'[1]

met onze digitale schaduw:

> 'Zowel binnen de publieke als de private sector worden op uitgebreide schaal persoonsgegevens verwerkt. De gemiddelde Nederlander is zich hier weliswaar van bewust, maar heeft verder weinig inzicht in het aantal bestanden waarin hij geregistreerd staat, de doeleinden waartoe hij geregistreerd staat en de partijen die toegang hebben tot deze bestanden. (...) [D]an komen wij op basis van de in kaart gebrachte informatiestromen en de bijbehorende verwerkingen binnen de publieke en de private sector tot de schatting dat de gemiddelde Nederlander staat geregistreerd in tot 250 tot 500 bestanden. (…) Dit betekent dat het aantal

▪ Prof. dr. B.J. Koops is hoogleraar regulering van technologie bij TILT – *Tilburg Institute for Law, Technology, and Society*, Universiteit van Tilburg.

1 Richtlijn 95/46/EG, *PbEG* L281, 23 nov. 1995, p. 31-50, overwegingen 28, 39 en 41.

> bestanden waarin de gemiddelde Nederlander staat in absolute zin wellicht afneemt, maar dat het aantal doeleinden waarvoor deze bestanden worden gebruikt en de partijen die er toegang tot hebben stijgt. (...) Hoewel concrete cijfers ontbreken is de stijging van het aantal databases in de private sector nog sterker geweest. Ook binnen de private sector zien we dat databases voor steeds meer doeleinden worden aangewend (…)',[2]

en je kunt constateren dat er vermoedelijk een stevige discrepantie bestaat tussen het 'recht in de boeken' en het 'recht in de praktijk'. Toegegeven, het zijn wat selectieve citaten, maar toch. Wie wil reflecteren op het grondrecht op dataprotectie in het huidige tijdperk, waarin elke Nederlander zich volgens de titel van deze bundel BN'er mag noemen omdat haar gegevens (kennelijk) bij het publiek bekend zijn, zal zich de vraag moeten stellen hoe het recht op papier zich verhoudt tot de praktijk van alledag.

Die vraag wordt weliswaar vaker gesteld, met veelal sombere antwoorden als resultaat, maar de uiterste consequentie van die sombere antwoorden wordt zelden getrokken. Die uiterste consequentie is dat we een veel fundamentelere vraag moeten stellen, die raakt aan de wortels van het grondrecht. Mijn bijdrage aan de reflectie op dataprotectie die deze bundel beoogt te bieden, is deze fundamentele vraag te stellen en te beantwoorden: heeft dataprotectie als grondrecht nog wel een toekomst?

Om u, lezer, maar vast te waarschuwen: ik zal deze vraag negatief beantwoorden. Aan de hand van diverse evaluaties van de wetgeving met betrekking tot bescherming van persoonsgegevens en een nadere analyse van de databankwereld waarin we leven, zal ik betogen dat de grondslagen van dataprotectie niet meer van deze tijd zijn. In deze bundel, geïnitieerd door het NJCM met als doelstelling om de grondrechtelijke dimensie van dataprotectie voor het voetlicht te brengen en het belang daarvan te onderstrepen, kies ik voor deze insteek als advocaat van de duivel. Dataprotectie is een mooi streven, maar als het ideaal zó ver van de werkelijkheid staat, moeten we dan niet op zoek naar andere beschermingsmechanismen?

2 Het grondrecht op dataprotectie

Dataprotectie is een prachtig bouwwerk, dat sinds enkele decennia is gefundeerd in de grondrechten. In 1983 werd het opgenomen in de Nederlandse Grondwet: artikel 10 bevat een opdracht aan de wetgever om regels te stellen 'ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens' (lid 2), inclusief 'de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens' (lid 3). Het is mij niet helemaal duidelijk waarom de wetgever juist deze twee principes van dataprotectie heeft opgenomen in de Grondwet en niet andere die zijn vastgelegd in Verdrag 108 van de Raad van Europa uit 1981.[3] Belangrijk is in elk geval dat het internationale dataprotectiebouwwerk dat voor een belangrijk deel rust op Verdrag 108 (en de vergelijkbare OESO-richtlijnen[4]) uitgaat van principes

2 B. Schermer & T. Wagemans, *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*, Amsterdam: Considerati 2009, p. 40-41.

3 Verdrag tot bescherming van personen in verband met de automatische verwerking van persoonsgegevens, Straatsburg 18 januari 1981, ETS 108.

4 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

van doelspecificatie, doelbinding en dataminimalisatie, dat wil zeggen dat gegevens alleen voor gespecificeerde doelen mogen worden verwerkt, gegevens noodzakelijk moeten zijn voor het gestelde doel, en dat verwerking verenigbaar moet zijn met dat doel.

Verdrag 108 evenals de Grondwet had de bedoeling om dataverwerking in goede banen te leiden door ervoor te zorgen dat data niet ongebreideld konden worden verwerkt of opgeslagen, in de nasleep van de publieke onrust in de jaren '70 over de snelle opkomst van computerregistratie bij bijvoorbeeld de volkstelling in Nederland ('de schrik van 1971').[5] Behalve in Verdrag 108 is dataprotectie ook een onderdeel van artikel 8 EVRM, en bovendien als zelfstandig grondrecht – afgesplitst van het recht op privacy waar het wel verwant aan is maar zeker geen tweelingbroer – opgenomen in artikel 8 van het Handvest van de Grondrechten van de Europese Unie,[6] dat met het Verdrag van Lissabon inmiddels formeel rechtskracht heeft gekregen. Deze laatste codificatie noemt als dataprotectieprincipes niet alleen het recht op inzage en correctie, maar ook eerlijke verwerking, doelspecificatie, toestemming of gerechtvaardigde wettelijke grondslag, alsook toezicht door een onafhankelijke autoriteit.

De Nederlandse wetgever heeft aan de regelingsopdracht van art. 10 lid 2-3 Gw voldaan door de Wet persoonsregistraties (Wpr) uit 1988,[7] die in 2001 werd vervangen door de Wet bescherming persoonsgegevens (Wbp),[8] mede als implementatie van Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.[9] De Wbp is opgehangen aan concepten als 'identificeerbaarheid', 'herleidbaar tot een natuurlijk persoon' en de verantwoordelijke die het aanspreekpunt is voor de rechten en plichten.

3 Evaluaties van dataprotectiewetgeving

Het probleem met dataprotectie is dat het er op papier mooi uitziet, maar in de praktijk niet zo werkt. Dat blijkt niet alleen uit de inleiding en diverse andere bijdragen in deze bundel, maar vooral ook uit de successieve evaluaties van de dataprotectiewetgeving. Het is goed om stil te staan bij de evaluatie van de Wpr die in 1995 werd uitgevoerd. De sociaal-wetenschappelijke evaluatie noemde de Wpr een 'ingewikkeld, moeilijk toegankelijk en slechts in geringe mate bruikbaar regelsysteem'. Bovendien was het matig gesteld met de naleving: '[i]n vele situaties is van doelbereiking in het geheel geen sprake.' Waar de wet wel werd nageleefd kwam dit niet door de wet maar gebeurde het om allerlei andere redenen.[10] Dat is op zich prettig, maar het onderstreept wel dat de wet veelal zijn werk niet deed.

Als we vervolgens kijken naar de evaluatie die onlangs is uitgevoerd van de opvolger van de Wpr, de Wbp, dan blijkt dat we eigenlijk precies dezelfde conclusies kunnen trekken. De eerste fase van de evaluatie, op basis van literatuuronderzoek, gaf aan dat de Wbp evenzeer

5 F. Kuitenbrouwer, 'Privacy en persoonsregistratie: een overzicht', in: F. Kuitenbrouwer, D.W.F. Verkade & R.J.M. van der Horst, *Drieluik privacybescherming*, Deventer: Kluwer 1984, p. 3-74 op p. 5-7.
6 *PbEG* C364/1, 18 dec. 2000.
7 *Stb.* 1988, 665.
8 *Stb.* 2000, 302; inwerkingtreding *Stb.* 2001, 337.
9 *PbEG* L281, 23 nov. 1995.
10 J.E.J. Prins e.a., *In het licht van de Wet persoonsregistraties: zon, maan of ster? Verslag van een sociaal wetenschappelijke evaluatie van de Wet Persoonsregistraties*, Alphen aan den Rijn: Samsom 1995.

ingewikkeld is: het 'gelaagde en gecompartimenteerde systeem voor de bescherming van persoonsgegevens is bijzonder complex geworden en tendeert soms zelfs naar overregulering'. 'Daarmee wordt de doelstelling van het vaststellen van een begrippenapparaat dat bruikbaar is voor rechtsvorming en voor de afweging van belangen niet (ten volle) gerealiseerd.' En met betrekking tot naleving blijkt 'dat veel rechten en plichten (…) niet optimaal worden uitgeoefend door een gebrek aan bekendheid van deze rechten en plichten' en dat 'de nadere invulling van materiële normen via zelfregulering maar beperkt gerealiseerd' is.[11]

De tweede fase van de evaluatie, een empirisch onderzoek naar de praktijk van de werking van de Wbp, trekt de 'algemene conclusie (…) dat de doelstellingen van de Wbp, het waarborgen van evenwicht tussen het privacybelang en andere grondrechten en het versterken van de positie van personen van wie gegevens worden verwerkt, nog niet ten volle worden gerealiseerd.'[12] Wie het rapport goed leest, ziet dat dit een wat eufemistische formulering is voor een tamelijk bedroevende naleving van de wet in de praktijk.

Het 'nog' in deze conclusie lijkt ook wat optimistisch. Als veertien jaar na de evaluatie van de Wpr, en zeven jaar na de inwerkingtreding van de Wbp, nog steeds het 'beeld naar voren [komt] van een wet die in de rechtspraktijk nog niet erg leeft, betrekkelijk lastig hanteerbaar wordt geacht en waarbij een op de toepassing gerichte privacygemeenschap en -cultuur nog niet in de volle breedte tot ontwikkeling is gekomen',[13] kan men zich afvragen wat er moet gebeuren om de doelstellingen van de Wbp dan wél ten volle te realiseren en een privacycultuur in de volle breedte tot ontwikkeling te laten komen. In elk geval zijn de wetgeving en het toezicht op de naleving daarvan in de afgelopen vijftien jaar niet voldoende gebleken om een substantiële waarborg te bieden van de bescherming van persoonsgegevens in de praktijk. Ten opzichte van de conclusies van de sociaal-wetenschappelijke evaluatie van de Wpr uit 1995 zijn we niet wezenlijk opgeschoten, lijkt me. Evenmin is, om in termen van de inleiding van deze bundel te spreken, de gemiddelde betrokkene ook maar enigszins meer 'betrokken' geraakt bij de bescherming van persoonsgegevens; de rechten van burgers en consumenten op inzage en correctie worden nauwelijks uitgeoefend, al is het maar omdat ook aan de kant van de betrokkenen de wet en de rechten weinig bekend zijn.

Dan hebben we nog de Commissie-Brouwer-Korff, oftewel de Commissie veiligheid en persoonlijke levenssfeer, die begin 2009 een bestuurlijk met spanning afgewacht rapport uitbracht over het zoeken naar de balans tussen veiligheid en de bescherming van de persoonlijke levenssfeer. Het rapport zou concrete(re) handvatten bieden voor afwegingen in de praktijk, die – blijkens de wetsevaluaties – zo moeilijk zijn te maken op basis van de generieke en complexe Wbp. De commissie brengt in het rapport een nuchtere en nuttige boodschap: laten we 'gewoon doen', dat wil zeggen niet krampachtig omgaan met de belangenafweging ('*gewoon* doen'), maar gewoon aan de slag gaan ('gewoon *doen*').[14] Helaas zegt het rapport niet helemaal hoe je die

11 G.-J. Zwenne, A.-W. Duthler, M. Groothuis e.a., *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntanalyse*, Leiden: eLaw@Leiden 2007, <http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969>, p. 13.

12 H.B. Winter, P.O. de Jong, A. Sibma e.a., *Wat niet weet wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Den Haag: WODC 2008, p. 10 <http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#>.

13 Ibid.

14 Commissie veiligheid en persoonlijke levenssfeer, *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer*, Den Haag 2008, <http://www.minbzk.nl/116513/rapport-'gewoon-doen>.

afweging dan moet maken; de zes grondslagen van het 'richtinggevende kader' zijn weliswaar belangrijke en relevante grondslagen (zoals zorgen voor transparantie, integriteit en naleving), maar richting geven ze nauwelijks. En daar ging het nou juist om: de werkvloer heeft moeite met bepalen wat nu precies wel of niet mag worden gedaan met gegevens, en voor het maken van die materiële afweging helpen de procedurele vuistregels niet veel.

Mijn conclusie uit dit alles is dat we een complex wettelijk kader hebben dat weinig richting geeft, dat onbekend is bij betrokkenen en op de werkvloer en ook heel moeilijk te vertalen is naar concrete afwegingen en beslissingen voor omgang met persoonsgegevens op de werkvloer. In die zin kunnen we de kwalificatie die Frank Kuitenbrouwer, een van de dataprotectiedeskundigen van het eerste uur, gaf aan de Wpr – een 'krakkemikkige wet' – naadloos doortrekken naar de Wbp, ook omdat deze wet eigenlijk evenals zijn voorganger, in Kuitenbrouwers woorden, 'vanuit het gezichtpunt van de informatica bij inwerkingtreding reeds gedateerd' is, zoals de volgende paragraaf zal laten zien.[15]

4 De harde werkelijkheid

Wat in de evaluaties van de Wbp wat onderbelicht is gebleven, maar een cruciale factor is – zo blijkt ook uit andere bijdragen in deze bundel – is de rol van technologie. We leven in databankenland. Bart Schermer en Ton Wagemans hebben een onderzoek uitgevoerd waarin zij schatten dat de gemiddelde Nederlandse burger in 250 à 500 databanken staat geregistreerd (zie het citaat in par. 1 hierboven). De volgende passages uit hun rapport kunnen dienen als nadere toelichting op de harde werkelijkheid van databankenland:

> 'In de publieke sector is het totale aantal databases in de afgelopen 20 jaar met ongeveer een factor 10 gestegen en het aantal bestanden waar een gemiddelde Nederlander in geregistreerd staat met ongeveer een factor 4. De discrepantie tussen deze twee factoren vloeit voort uit het feit dat steeds meer verwerkingen gecentraliseerd worden, hetzij door één centrale database te bouwen, hetzij door decentrale databases aan elkaar te koppelen. Dit betekent dat het aantal bestanden waarin de gemiddelde Nederlander staat in absolute zin wellicht afneemt, maar dat het aantal doeleinden waarvoor deze bestanden worden gebruikt en de partijen die er toegang tot hebben stijgt. (...)
> Een tweede constatering binnen de publieke sector is dat de bestanden van instanties steeds vaker aan elkaar worden gekoppeld via bijvoorbeeld verwijsindexen en inkijkfuncties (Suwinet, EPD, EKD, DKD). Hierdoor krijgen overheidsinstanties een steeds completer beeld van de burger. (...) Hoewel concrete cijfers ontbreken is de stijging van het aantal databases in de private sector nog sterker geweest. Ook binnen de private sector zien we dat databases voor steeds meer doeleinden worden aangewend, maar deze doeleinden blijven primair beperkt tot de eigen organisatie.'[16]

Vergelijkbare constateringen zijn te vinden in de vele literatuur over privacy in relatie tot databanken en geautomatiseerde gegevensverwerking.[17] De databanken waarin we liggen

15 F. Kuitenbrouwer, *Het recht om met rust gelaten te worden. Over privacy*, Amsterdam: Balans 1991, p. 161.
16 Schermer en Wagemans, *supra* noot 3, p. 40-41.
17 Zie bijv. S. Garfinkel, *Database Nation. The death of privacy in the 21st century*, Cambridge: O'Reilly 1999; D.J. Solove, *The digital person: technology and privacy in the information age*, New York: New York University Press 2004; House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, London 2009, <http://www.parliament.the-stationery-office.com/pa/ld/ldconst.htm>.

opgeslagen worden steeds meer gekoppeld en – fysiek of virtueel – gecentraliseerd. Het aantal doeleinden waarvoor die gegevens worden gebruikt en het aantal partijen dat daar toegang tot heeft stijgt, en blijft stijgen. In deze databankwereld zijn doelspecificatie en doelbinding problematisch en geen realiteit. Gegevens worden verzameld voor vage of meervoudige doelen, of hergebruikt voor andere doelen die tussendoor opkomen en die niet te voorzien waren toen de gegevens werden verzameld in een databank. Ook het principe van dataminimalisatie – alleen die data verwerken die noodzakelijk zijn voor het gestelde doel, en vernietigen zodra ze niet meer nodig zijn – staat haaks op de realiteit van databankenland. Integendeel, de praktijk laat zich veel meer karakteriseren door datamaximalisatie.

Dat heeft mede te maken met het maatschappelijke, sociale en politieke klimaat van risicobeheersing en wat je zou kunnen noemen 'preventivisering': de dringende behoefte om zoveel mogelijk risico's uit te sluiten en rampen koste wat kost te voorkomen.[18] Dat doen we vooral door zoveel mogelijk gegevens op te slaan – je weet maar nooit waar ze goed voor zijn – en als ze dan toch opgeslagen liggen, is het ook wel handig om ze te kunnen gebruiken voor allerlei doeleinden in de toekomst.

Daar komt nog bij dat databanken ook een nieuw soort kennis faciliteren, die een belangrijke meerwaarde biedt in een informatiemaatschappij: datadelven (*data mining*) en profilering.[19] Door terabytes aan data door te ploegen, ontdek je nieuwe verbanden, die iets kunnen zeggen over individuen of groepen. Profilering heeft tal van toepassingen in de publieke en private sector en is een enorme groeimarkt. Om zinvol verbanden te kunnen ontdekken en profielen te kunnen maken, zijn grote databanken nodig, liefst met data uit verschillende contexten en van verschillende bronnen. Datadelven en profilering staan dus eveneens haaks op de uitgangspunten van dataminimalisatie en doelbinding.

Daar komt nog een andere zwakte van de dataprotectiewetgeving bij. Bij profilering gaat het niet zozeer om de identificeerbaarheid van individuele personen, maar om het gebruik van een profiel voor herkenning van personen als een bepaald type persoon – een groepsprofiel: mensen uit postcode 5037 zijn hoog opgeleid en dus interessant voor aanbiedingen van financiële diensten – of als dezelfde persoon die je uit een bepaalde context kent – een geïndividualiseerd maar niet per se identificeerbaar persoon: de gebruiker van de computer waarop ik deze lange vinger (*cookie*) plaatste, was de vorige keer op zoek naar maandverband en nu naar luiers.[20] Op het proces van profilering is de dataprotectiewetgeving niet toegesneden, omdat het niet per se om identificeerbare individuen gaat. Bovendien is profilering vaak intransparant voor degenen die worden geprofileerd, niet alleen hoe een profiel tot stand is gekomen en waarom het wordt toegepast, maar vaak ook voor het feit dát profilering wordt toegepast. Zonder besef dat beslissingen worden genomen op basis van een profiel toegepast op een virtuele identiteit,

18 Vgl. U. Beck, *Risk society: towards a new modernity*, London; Newbury Park, CA: Sage Publications 1992; D. Garland, *The culture of control: crime and social order in contemporary society*, Chicago: University of Chicago Press 2001; C.R. Sunstein, *Laws of fear: beyond the precautionary principle*, Cambridge, UK/New York: Cambridge University Press 2005.

19 Zie voor een overzicht M. Hildebrandt & S. Gutwirth (red.), *Profiling the European Citizen. Cross-disciplinary perspectives*, New York: Springer 2008.

20 Zie over de problematiek van groepsprofielen A.H. Vedder, 'Het einde van de individualiteit? Datamining, groepsprofilering en de vermeerdering van brute pech en dom geluk', *Privacy & Informatie* 1998-3, p. 115-120, en over andere vormen van individualiseerbaarheid R.E. Leenes, 'Do You Know Me? Decomposing Identifiability', *University of Ottawa Law and Technology Journal* 2008-1, <http://ssrn.com/abstract=1084878>.

heeft iemand niets aan dataprotectierechten op inzage en correctie of het recht niet onderworpen te worden aan volledig geautomatiseerde beslissingen (art. 42 Wbp).

De werkelijkheid anno 2010 is dat we als digitale personen leven in databanken, en dat we als personen van vlees en bloed bar weinig invloed uitoefenen op de manier waarop we als digitale personen in databankenland worden behandeld. Over onze digitale schaduw in databanken die steeds meer gedecontextualiseerd raken, zijn onze dataprotectierechten steeds moeilijker uit te oefenen. Ter illustratie van wat het betekent in de werkelijkheid anno 2010 je rechten van de Wbp uit te oefenen, citeer ik een verzoek dat ik een tijdje geleden verstuurde:

> 'Beste Amazon.co.uk,
> Kunt u mij informeren op basis waarvan u mij *Maurice* van E.M. Forster en *Giovanni's Room* van James Baldwin heeft aangeraden? Ik vraag dat vanwege art. 35 Wbp.[21] Uw suggestie heeft kennelijk te maken met het feit dat ik drie weken geleden *The Lost Language of Cranes* van David Leavitt bij u kocht, want dat noemt u als aanleiding. Maar dan had ik toen ik dat boek kocht wel graag van u willen horen dat u dat zou gebruiken om mij op andere boeken te wijzen, op basis van art. 33 Wbp.[22] Heeft u mij misschien door de aankoop van dat boek van Leavitt geprofileerd als iemand die geïnteresseerd is in homoseksualiteit, wat een thema is in de door u gesuggereerde boeken? Maar homoseksualiteit is een gevoelig persoonsgegeven (zie art. 16 Wbp[23]). Kunt u daarom alstublieft al deze data verwijderen, omdat het onrechtmatig is voor u om deze data te verwerken (zie wederom art. 16 Wbp) en verwerking ervan is bovendien niet relevant voor het feit dat ik bij u boeken koop (zie art. 36 lid 1 Wbp).[24] En wilt u mij een schriftelijke bevestiging sturen dat u inderdaad mijn gevoelige persoonsgegevens hebt verwijderd (zie art. 36 lid 2 Wbp)?[25]
> Alvast bedankt, en met vriendelijke groeten,
> Bert-Jaap Koops'

Ik laat het aan de lezer over zich voor te stellen hoe een organisatie als Amazon.co.uk op een dergelijk verzoek reageert.

21 'De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt' (art. 35 lid 1 Wbp).

22 '1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen' (art. 33 Wbp).

23 'De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf (…)' (art. 16 Wbp).

24 'Degene aan wie overeenkomstig artikel 35 kennis is gegeven van hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen' (art. 36 lid 1 Wbp).

25 'De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed' (art. 36 lid 2 Wbp).

5 Oplossingsrichtingen

Uit de voorgaande paragrafen blijkt dat we niet alleen te maken hebben met complexe regelsystemen en wetgeving die weinig bekend of hanteerbaar zijn bij betrokkenen en op de werkvloer, maar ook met pijlers van wetgeving als doelbinding en dataminimalisatie die haaks staan op de huidige praktijk van gegevensverwerking. Data, databanken en profielen tieren welig. Doelbinding is steeds moeilijker vol te houden; het is nu al een onrealistisch uitgangspunt en zal naar mijn inschatting in de toekomst een onmogelijk te handhaven principe zijn. De aanknopingspunten van de Wbp, zoals identificeerbaarheid en een duidelijk aan te wijzen verantwoordelijke, zijn steeds minder te hanteren. Het hele dataprotectiestelsel valt nauwelijks te handhaven. Kortom, als we kijken naar de staat van het bouwwerk van dataprotectie, dan ben ik geneigd te concluderen dat het een ruïne is. En hoewel een ruïneus kasteeltje heel pittoresk kan staan in een heuvelige omgeving voor de bezoekende toerist, is het geen adequaat onderkomen voor bewoners om beschut en beschermd in te leven. We zullen dus iets moeten doen aan deze ruïne, en ik zie daarvoor twee mogelijke oplossingsrichtingen.

5.1 De orthodoxe aanpak

De eerste en voor de hand liggende richting is de klassieke, orthodoxe aanpak: het bouwwerk renoveren. Dat is de oplossing die de dataprotectiegemeenschap collectief nastreeft:[26] zorgen dat de gaten in de muren en de daken worden gedicht, dat de fundamenten worden verstevigd, isolatie wordt aangebracht, en wie weet een extra torentje wordt bijgebouwd. De complexiteit van de regelgeving moet worden teruggebracht door te simplificeren waar dat mogelijk is. Onduidelijkheden moeten worden weggenomen door vage en complexe begrippen te verhelderen en betere handvatten voor interpretatie te ontwikkelen. Onbekendheid op de werkvloer en bij individuen moet worden weggenomen door meer voorlichting te geven aan betrokkenen en dataverwerkers. De kloof tussen wet en praktijk zal worden gedicht door meer, beter en strakker te handhaven. De nieuwe technologische uitdagingen van databankenland worden ter hand genomen door onderzoek te doen naar manieren om contextuele integriteit te kunnen hanteren in die databankwereld.[27] En dat alles gaan we vooral ook doen door technologie in te zetten als oplossing: de welbekende *privacy-enhancing technologies* (PET's)[28] en de iets minder bekende maar even relevante *transparancy-enhancing technologies* (TET's).[29]

Over al deze renovatieactiviteiten wordt veel geschreven en nagedacht, en dat is best nuttig. Een dichtgemetselde bres en een spouwmuur met wat innovatief isolatiemateriaal zou zo maar

26 Zie onder andere de aanbevelingen in de bovengenoemde evaluatierapporten, jaarverslagen van het College Bescherming Persoonsgegevens (<http://www.cbpweb.nl/>), rapporten van de Artikel 29-Werkgroep (<http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/>), S. Gutwirth, Y. Poullet, P. De Hert e.a. (red.), *Reinventing data protection?*, New York: Springer 2009.

27 Vgl. H. Nissenbaum, *Privacy in Context*, Stanford Law Books 2009.

28 Registratiekamer, Information and Privacy Commissioner (Ontario) en TNO, *Privacy-enhancing technologies: the path to anonymity. Achtergrondstudies en verkenningen*, Rijswijk, Toronto: Registratiekamer en Information and Privacy Commissioner 1995.

29 Over TET's, zie M. Hildebrandt, 'D7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools', *FIDIS* 2008, <http://www.fidis.net/resources/deliverables/>.

het verschil kunnen maken voor het overleven van de eerstvolgende strenge winter. Maar het is een achterhoedegevecht, dat zich richt op de technologie en de wereld van gisteren. Vereenvoudiging, meer voorlichting, meer handhaving en PET's gaan uiteindelijk niet werken; we zeggen al vijftien jaar dat we dat moeten doen, en het dataprotectiebouwwerk staat er niet beter voor dan in 1995. De uitgangspunten van dataprotectie verdragen zich niet meer met de harde werkelijkheid van vandaag de dag. Als we de klassieke aanpak volgen en meer van hetzelfde blijven doen, is er gerede kans dat we in 2025 hetzelfde type conclusies gaan trekken over de Wpp (Wet persoonsgegevens en profielen) als we in 2007-2008 trokken over de Wbp en in 1995 over de Wpr.

5.2 De radicale aanpak

Er is een andere oplossingsrichting voorhanden: we kunnen het bouwwerk afbreken en er iets heel nieuws voor in de plaats zetten. Deze radicale aanpak sluit enigszins aan op de tendens van toenemend burgerrechten- en mensenrechtenactivisme die Corien Prins in de inleiding van deze bundel signaleert, maar dan in een veel extremere vorm. Deze aanpak bevat twee componenten.

De eerste component is datamaximalisatie. Deze strategie hanteert de tactiek van de hooiberg: als je een speld te verbergen hebt, bouw er dan een grote hooiberg omheen. Een voorbeeld van deze tactiek is de *Jam Echelon Day*,[30] een activistische campagne om het Echelonsysteem te verslaan – het wereldomvattende afluisternetwerk van Angelsaksische geheime diensten. Wereldwijd werden mensen opgeroepen om op 21 oktober 1999 bij elk bericht onderaan zo'n vijftig willekeurig gekozen woorden te plaatsen uit het bestand van trefwoorden die rode alarmbellen deden afgaan bij de NSA (de National Security Agency) en andere afluisterinstanties.[31] Als veel mensen in veel berichten dit soort woorden gaan noemen, dan is het filteren op trefwoorden volstrekt zinloos geworden. Natuurlijk past het systeem zich dan aan en worden er dan weer nieuwe datadelf-zoekmethoden ontwikkeld binnen Echelon, maar daar kunnen de datamaximaliserende activisten dan vervolgens hun emailtactieken weer op aanpassen. Een collectieve actie van datamaximalisatie zou zo de strijd kunnen aangaan met een van de grootste datastofzuigersystemen ter wereld.

Datamaximalisatie sluit ook aan op een fenomeen dat we op het internet steeds vaker tegenkomen: 'digitaal exhibitionisme'. Mensen zetten allerlei persoonsgegevens op het internet, soms de gekste dingen en details, soms hun hele hebben en houden. Mensen delen informatie, maar zeker ook desinformatie, met 'het publiek', soms als overlevingsstrategie – je moet gegevens wel openbaarmaken als je mee wilt komen – maar soms ook wel als levensstijl. Dat zien we zeker bij de jongere generaties, maar soms ook wel bij oudere generaties die – in het tijdperk waarin Big Brother een prototypisch tv-programma en mediaformule is geworden – op zoek zijn naar het kwartiertje roem van Warhol. (Inderdaad, iedereen kan makkelijk BN'er worden.) Een belangrijk mechanisme hierbij is dat het zelf publiceren van gegevens over jou op het web

30 Zie <http://www.jamechelon.org/>.

31 Bijvoorbeeld 'ATF DOD WACO RUBY RIDGE OKC OKLAHOMA CITY MILITIA GUN HANDGUN MILGOV ASSAULT RIFLE TERRORISM BOMB DRUG KORESH PROMIS MOSSAD NASA MI5 ONI CID AK47 M16 C4 MALCOLM X REVOLUTION CHEROKEE HILLARY BILL CLINTON GORE GEORGE BUSH WACKENHUT TERRORIST'. Zie C. Oakes, 'Monitor This, Echelon', *Wired* 22 oktober 1999, <http://www.wired.com/politics/law/news/1999/10/32039>.

het gevoel geeft dat je controle houdt over je imago en daarmee ook over je zelfbeeld. Identiteitsconstructie in een web 2.0-samenleving vraagt misschien ook wel om strategische datamaximalisatie van persoonsgegevens. Digitaal exhibitionisme is een nieuwe vorm van verzet tegen de intransparante, overal loerende *surveillance*maatschappij:

> 'exhibitionism and voyeurism seem to offer new tools for consumer resistance against the electronic surveillance systems in networked markets and are inextricably interwoven with consumers' desire for control over their information (…). [U]ltraexhibitionism is to be understood as an act of resistance against the surreptitious modes of profiling, categorization, and identity definition that are being performed by others on the consumer whenever he or she enters the electronic 'consumptionscape'.[32]

De strategie van datamaximalisatie vergt een nieuwe manier van denken, die aansluit bij andere innovaties in wat vroeger de 'nieuwe economie' heette. Professionele amateurs doen met zijn allen dingen die vroeger alleen overheden of grote organisaties deden; waardevolle informatie wordt gratis gedistribueerd op grote schaal in ruil voor wat persoonsgegevens of advertenties; *crowdsourcing* en virale marketing; het zijn allemaal nieuwe methoden die gebaseerd zijn op een explosie van data en een herwaardering van de waarde van die data.[33] Sommige mensen hebben deze manier van denken geheel geïnternaliseerd; voor anderen – en zeker voor de dataprotectiegemeenschap – vergt het een radicale omslag in hun wereldbeeld. Maar wereldvreemd hoeft het niet te zijn. Het momenteel modieuze voorbeeld van dé privacybedreiging in web 2.0 is dat je op Hyves wilde dingen zegt of compromitterende foto's plaatst die later tijdens een sollicitatiegesprek tegen je gebruikt kunnen worden. Dat mag nu misschien wel zo zijn, maar over tien jaar kan het even goed zijn dat een Brave Hendrik-profiel tegen je werkt omdat je werkgever verwacht dat je een 'authentiek' Hyves-profiel, inclusief scherpe kantjes, hebt. Bovendien heeft die werkgever tegen die tijd ook wilde haren op het internet achtergelaten, die je tijdens het sollicitatiegesprek aan de orde kunt stellen als jouw oude Hyves-koeien uit de sloot worden gehaald.

Dat brengt ons bij de tweede component van de radicale aanpak, de tweezijdige glazen samenleving. Het is niet erg als alle Nederlanders BN'ers zijn van wie alle gegevens 'op straat' liggen, zolang er maar goede waarborgen zijn voor foutencorrectie en toezicht op eerlijke behandeling. We leven al in een glazen samenleving,[34] en dat moeten we vooral gaan benutten. We moeten terugkijken. Deze strategie wordt uitgelegd en onderbouwd door David Brin in *The Transparent Society*. Hij betoogt dat 'we may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction.'[35] En dat licht om terug te kijken in de glazen samenleving komt van het collectief van degenen die bekeken worden: 'the cameras *are* coming. You can rail against them, shaking your fist in futile rage at all the hovering lenses.

32 N. Dholakia & D. Zwick, 'Privacy and Consumer Agency in the Information Age: Between Prying Profilers and Preening Webcams', *Journal of Research for Consumers* 2001-1, **PAGINANUMMERS?.**

33 Vgl. M. Mason, *The pirate's dilemma: how youth culture reinvented capitalism*, New York: Free Press 2008; C. Anderson, *Free: The Future of a Radical Price*, New York: Hyperion 2009.

34 J. Kohnstamm & L. Dubbeld, 'Glazen samenleving in zicht', *NJB* 2007-37, p. 2369-2375.

35 D. Brin, *The transparent society: will technology force us to choose between privacy and freedom?*, Reading, Mass.: Perseus Books 1998, p. 23.

Or you can join a committee of six billion neighbors to control the pesky things, making each one an extension of your eyes.'[36]

We moeten er dus voor zorgen dat het glas transparant is aan twee kanten, en dat Big Brother, Soft Sister, de bureaucraten van *Der Prozeß* of wie er ook maar achter de camera's zitten die ons in de gaten houden, evenzeer worden bekeken. Dan verkrijgen we maximale transparantie die waarborgt dat degenen die beslissingen nemen over individuen verantwoording moeten afleggen over hun beslissingen. Web 2.0 en de andere vormen van de 'wisdom of crowds' zijn in deze benadering het antwoord op de klassieke vraag *quis custodiet ipsos custodes?* De bewakers worden bekeken door het collectief van de bewaakten.[37] Dat wil niet zeggen dat elk individu altijd zelf moet terugkijken; integendeel, de kracht van de massa is erin gelegen dat er altijd wel iemand is die terugkijkt, en die een oneerlijke of oneigenlijke beslissing over een individu, gebaseerd op irrelevante of onjuiste persoonsgegevens of profielen, aan de kaak kan stellen op de marktplaats van de publieke opinie.

De radicale aanpak probeert dus de zwakte van dataprotectie – onmacht om de datawoekering in databankenland in toom te houden – om te vormen in een sterkte, door de uitgangspunten van dataminimalisatie en doelbinding los te laten en om te draaien. Databazen raken het spoor bijster als er collectief aan datamaximalisatie wordt gedaan. En als ze ook gedwongen worden om zelf maximaal transparant te zijn over hun gegevensverwerkingen, kunnen ze ter verantwoording worden geroepen door het collectief als ze een individu oneigenlijk behandelen op basis van verkeerde of irrelevante gegevens.

6 Conclusie

Heeft dataprotectie als grondrecht nog een toekomst? Ik ben door de jaren heen skeptisch geworden over deze vraag, en neig inmiddels naar een negatief antwoord. Dataprotectie was best een leuk grondrecht, voor zolang als het duurde. Het was geen slecht idee in de jaren '70, maar eigenlijk al achterhaald voordat het goed en wel was ingevoerd. Het bouwwerk uit de jaren '80 kon niet uit de voeten met de netwerksamenleving, en het daartoe aangepaste bouwwerk uit de jaren '90 – met de Richtlijn voorop – kan niet uit de voeten met een (risico)samenleving die afhankelijk is van aan elkaar gekoppelde databanken met exabytes aan data die voor uiteenlopende en meervoudige doeleinden worden gebruikt. Dataminimalisatie en doelbinding zijn romantische idealen die, als ze al ooit in de praktijk van de twintigste eeuw zeggingskracht gehad hebben, hopeloos achterhaald zijn in de eenentwintigste eeuw.

In plaats van te streven naar dataprotectie 2.0 met een orthodoxe aanpak van meer voorlichting, meer handhaving en meer PET's, en krampachtig proberen de geest weer terug in de fles te krijgen die er al minstens vijftien jaar uit is, is het mogelijk realistischer en productiever om in het diepe te springen en te kiezen voor de radicale aanpak van datamaximalisatie en volstrekte transparantie. 'De burger in beeld' die als rode draad door deze bundel loopt, kan weliswaar

36 Ibid., p. 333.

37 Vgl. het Anopticon van Umberto Eco ('L'Anopticon', in: U. Eco, *Il secondo diario minimo*, Milano: Bompiani 1992, p. 176), waarin de eenzame bewaker door alle gevangenen bekeken kan worden, maar nooit weet of en door wie hij in de gaten wordt gehouden. Een vertaling van deze mini-dagboeknotitie van Eco is te vinden in B.J. Koops, 'Law, Technology, and Shifting Power Relations', *Berkeley Technology Law Journal* 2010-2, **PAGINANUMMERS?**, <http://ssrn.com/abstract=1479819>.

niet de regie overnemen over het gebruik van de observatiemiddelen die haar zo gedetailleerd in beeld brengen, maar de burger kan wel het onderscheidend vermogen van de observatoren vertroebelen door álles in beeld te vertonen. En als het beeld tweezijdig is en iedereen kan terugkijken naar de observatoren, zorgen we voor bewaking van de bewakers door de collectieve 'boeren, burgers en buitenlui in beeld'.

Laten we ons vrolijk maken over *function creep*, *mission creep* en wat voor *creeps* er ook maar rondlopen in de databankwereld. Ja, we worden overal bekeken. Men weet alles van ons. En we kunnen overal op worden beoordeeld. Maar dat is niet zo erg in een volstrekt transparante samenleving. In je blootje staan is gênant en bedreigend in de Kalverstraat, maar niet op een naaktcamping waar iedereen in adams- of evakostuum rondloopt. Als we collectief over de schouder kunnen meekijken bij databazen die beslissingen nemen over individuen, dan zal iemand die ons onfatsoenlijk of onbehoorlijk of onterecht durft te behandelen genadeloos worden afgestraft. Het zal altijd wel door iemand worden opgemerkt in het glazen web 2.0 – door een ombudsman, een journalist, een privacyactivist, een verveelde tiener, een liberale radicaal of anders wel door de weduwe uit Appelscha die, met dank aan de universele dienstverplichting,[38] ook aangelijnd is en achter de geraniums toch ook iets te doen moet hebben.

Door maximale transparantie te creëren, kunnen we nieuwe waarborgen en een nieuw evenwicht door tegenwicht inbouwen in de glazen samenleving waar we inmiddels in leven en vermoedelijk mee moeten leven. Iemand die het waagt door het glas te kijken en ons oneerlijk of onfatsoenlijk te behandelen, wordt genadeloos afgestraft door het collectief dat altijd en overal meekijkt. En was het daar uiteindelijk niet allemaal om begonnen met het dataprotectiebouwwerk, dat dataverwerkers personen eerlijk en fatsoenlijk behandelen?

38 Vgl. *Kamerstukken II* 1995/96, 24 163, nr. 29.