Not for quotation : do only refer to the published version
Alleen referen naar de gepubliceerde versie

DE HERT P. & S. GUTWIRTH, "Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek" in E.R. MULLER (red.),* Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn, Kluwer, 2004, 587-631.

Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek

Paul De Hert & Serge Gutwirth[1]

1. Inleiding
2. Privacy
3. Weerstanden
4. Het complexe krachtenspel achter privacy
5. Het kader van de democratische rechtsstaat
6. De drie constitutionele principes van de democratische rechtsstaat
7. De democratische rechtsstaat bedient zich van twee instrumenten
8. Privacy als een opaciteitsinstrument, een instrument voor het trekken van grenzen
9. Gegevensbescherming als instrument voor transparantie
10. Een evenwichtige privacypolitiek steunt op twee pijlers
11. Illustraties van een gewenste privacypolitiek
12. Afronding

1. Inleiding

Veiligheid krijgt een centrale plaats in het politiek beleid van de eeuwwisseling. In onze risicomaatschappij is veiligheid het rechtsgoed bij uitstek geworden dat via het recht moet worden beschermd. De wetgever produceert een bijna eindeloze stroom nieuwe wetsvoorstellen en wijzigingsvoorstellen van oude wetten, en in de toelichting op die voorstellen is altijd wel ergens het thema van de (on)veiligheid te vinden als reden waarom die wijziging noodzakelijk is. Gevolg is dat de rechtsbescherming van de burger het vaak moet ontgelden, opgeofferd aan de veiligheid van het (potentiële) slachtoffer, de enige die er soms beter van wordt.[2]
Deze tendens is bepaald niet exclusief in Nederland te signaleren, maar lijkt eerder een verschijnsel dat in Europa en in de VS allesoverheersend is sinds zeker een jaar of tien. Na 11 september 2001 is nog een aanzienlijke versnelling van dit proces waarneembaar. De gebeurtenissen van 11 september hebben een ongeziene druk geplaatst op grondrechten zoals

[1] Paul De Hert is hoofdocent aan de Universiteit Leiden en docent aan de Vrije Universiteit Brussel; Serge Gutwirth is hoofddocent aan de Vrije Universiteit Brussel en docent aan de Erasmus Universiteit Rotterdam. Deze tekst is een op de Nederlandse situatie gerichte bewerking van ons gezamenlijk rapport *Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence* (56 p.) dat integraal zal worden geannexeerd aan op 6 oktober 2003 in het Europees Parlement voorgestelde raport : *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE) by the Institute for Prospective Technological Studies (IPTS), Joint Research Centre, European Commission.
[2] T. Prakken, 'Veiligheid of vergelding? Een bezinning over aard en functie van het strafrecht in de postmoderne risicomaatschappij', introductietekst geschreven en gepresenteerd naar aanleiding van de Nederlandstalige strafrechtdag, Maastricht 20 juni 2003

privacy, vrijheid van meningsuiting en vrijheid van vereniging. Nationale veiligheidsdiensten en gerechtelijke diensten hebben op verbluffend snelle wijze een verruiming van hun mandaat kunnen uitlokken, vaak ten koste van de idee van *checks and balances* of van transparantie en *accountability*. Wetgevers hebben 'gekoerst' om bij de eerste te kunnen zijn in het stemmen van veiligheidswetten, vaak zonder een open debat.
In een klimaat van grote zorg voor publieke veiligheid kan men zich de vraag stellen wat de toekomst mag zijn van de burgerrechten en vrijheden en van de open samenleving. Twee jaar na 11 september spitsen we deze belangrijke vraag toe op het grondrecht privacy. Eerst geven we aan welk belang aan dit grondrecht toekomt, welke weerstanden het oproept, hoe het kadert in de democratische rechtsstaat of open samenleving die we kennen, hoe we de relatie tussen het grondrecht op privacy en de beginselen van *data protection* moeten begrijpen en tenslotte hoe we deze inzichten dienen te incorporeren in de in het noodzakelijk wetgevend werk. Ons verhaal is geenszins een abstract verhaal kenmerkend voor rechtstheoretische geschriften. Integendeel tonen we aan de hand van concrete wettelijke initiatieven dat deze inzichten veel van het actuele 'wetgeven' kenmerkt in het bijzonder in Nederland. In vele opzichte kan Nederland dan ook als model staan voor de zoektocht naar een evenwichtige grondrechtenpolitiek in deze 'grondrechtenonvriendelijke' tijd.

2. Privacy

Door het civiliseren van onze samenleving schijnt de rol van de vroegmoderne grondrechten die nodig waren om het einde van de politiestaat te markeren, uitgespeeld. Rechten als het verbod op foltering en het verbod op willekeur bij aanhouding staan op slaapstand. De overheid hanteert andere middelen waarbij aanzienlijk minder bloed vloeit en toch bijna steeds een beter resultaat wordt geboekt. Die nieuwe overheidsinstrumenten verklaren precies waarom een grondrecht op privacy zo'n grote maatschappelijke betekenis toekomt in deze samenleving. Privacy laat zich lezen als een verbod op elektronische willekeur en als een bewaker tegen digitale huisvredebreuk. Privacy belichaamt met andere woorden een hedendaags instrument voor het in de liberale politieke theorie terecht noodzakelijke geachte tegengewicht voor een maatschappelijke actor die in staat is het individu te verpletteren.[3]
Het is in dit opzicht wellicht een goede zaak dat in de rechtsleer een ruim privacybegrip wordt gehanteerd: naast het denken over privacy als het recht om met rust gelaten te worden, ziet men privacy als het recht om zich te beschermen tegen handelingen of beslissingen die van invloed zijn op de levensomstandigheden en dus op de vrijheid van de betrokkene. Privacy wordt alzo een deelaspect van het recht op vrijheid.[4]
Ook de Europese rechtspraak over de reikwijdte van artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)[5] gaat in de richting van een ruime invulling van het privacybegrip en gerelateerde begrippen zoals *communicatie* en *correspondentie*.[6] Over het privacybegrip stelde het arrest *Niemitz*[7] dat

---

[3] Cf. P. De Hert & B.-J. Koops, ' Privacy is nog steeds een grondrecht. Pleidooi voor de uitsluiting van onrechtmatig bewijs', *Ars Aequi*, 2001, december, (vol. 50), 972-975

[4] In die zin : S. Gutwirth, *Privacyvrijheid ! De vrijheid om zichzelf te zijn*, The Hague, Rathenau Instituut/Otto Cramwinckel, 1998, 152 p.; S. Gutwirth, *Privacy and the information age*, Lanham/Boulder/New York/Oxford, Rowman & Littlefield Publ., 2002, 158 p.; S. Gutwirth, '*Privacyvrijheid* een voorwaarde voor maatschappelijke diversiteit' in *Eenheid en verscheidenheid in recht en rechtswetenschap*, A.M.P. Gaakeer & M. A. Loth (Red.), *SI-EUR Reeks 28* , Arnhem, Kluwer/Gouda Quint, 2002, 95-138; F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Brussel/Parijs, Bruylant/L.G.D.J, 1990, 849 p. en F. Rigaux, *La vie privée. Une liberté parmi les autres ?*, Brussel, Larcier, 1992, 317 p.. Zie over de voor- en nadelen van een ruim privacybegrip: Paul De Hert, *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woning en communicatie*, Gent, Mys en Breesch Uitgeverij, 1998, 69-84 en Peter Blok, *'Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlands en Amerikaans recht*, Boom Juridische uitgeverij, 2002, 372p.

[5] Deze bepaling bepaalt dat eenieder recht heeft op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Zie uitvoerig over alle hieronder besproken arresten: Paul De Hert, *Artikel 8 EVRM en het Belgisch recht, o.c.*, 364p.

[6] In *Klass* bepaalde het EHRM dat ook telefoonverkeer onder de bescherming van artikel 8 valt. Het Hof kiest daarbij niet voor een extensieve interpretatie van het begrip correspondentie maar voor een combinatie van privé-leven en correspondentie. In *Malone* gaf het Hof aan dat ook *metering records* en in het bijzonder het gekozen telefoonnummer integraal deel uitmaken van de beschermde communicatie. Cf. EHRM 2 augustus 1884 (*Malone*), *NJ* 1988, 534; Hofman 1995, 70-71; A.J. Nieuwenhuis, 'Vertrouwde en virtuele bescherming', *NJCM-Bulletin* 4, 1998, 429. In het arrest *P.G. en J.H. t. het Verenigd Koninkrijk* (*infra*) is het EHRM is van mening dat de opname van het stemgeluid aangemerkt dient te worden als een registratie van een

werknemers een gerechtvaardigd belang hebben om ook gedurende het uitvoeren van bedrijfsmatige activiteiten relaties met andere mensen aan te kunnen gaan. Een zekere mate van vrijheid om met anderen al dan niet persoonlijk te kunnen communiceren zonder inmenging door de werkgever is in dat kader onontbeerlijk. Artikel 8 EVRM beschermt het individu niet alleen tegen inbreuken door de overheid, maar tegen inbreuken door particulieren, zoals werkgevers. In *Halford* maakt het Hof duidelijk dat ook telefoongesprekken, gevoerd met een zakelijk toestel, of onder een zakelijk nummer, onder de bescherming van artikel 8 vallen.[8] Mevrouw Halford was Assistant Chief Constable bij een Engels politiekorps. In verband met een rechtszaak tegen haar werkgever wegens ongelijke behandeling had zij de beschikking over een tweede telefoon die was uitgezonderd van de standaardcontrole van de telefoons van het politiebureau. Uit het bewijs dat in de rechtszaak was overlegd, kon worden afgeleid dat de werkgever waarschijnlijk de gesprekken die via de speciale telefoon waren gevoerd, had afgeluisterd. Het Hof overwoog dat 'the right to private life and correspondence' zich ook uitstrekt tot de werkplek. Omdat er geen waarschuwing was gegeven dat de telefoongesprekken werden opgenomen, had zij een 'reasonable expectation of privacy', hetgeen werd versterkt door bijkomende factoren waaronder het feit dat de telefoon specifiek ter beschikking was gesteld voor privé-gebruik. Het enkele bekend zijn van de mogelijkheid tot meeluisteren of opnemen rechtvaardigt op zichzelf het gebruik daarvan evenwel niet. Kenbaarheid van de (mogelijkheid tot) controle is niet meer dan een basisvoorwaarde voor de rechtmatigheid ervan.

Uit het reeds genoemde arrest *P.G. en J.H. t. het Verenigd Koninkrijk* blijkt dat het voortaan denkbaar is om, niet alleen in de private of professionele sfeer, maar ook in de publieke sfeer een beroep te doen op de bescherming geboden door het privacygrondrecht. Deze principiële erkenning van het concept *publieke privacy* gebeurde een jaar eerder in het arrest *Rotaru t. Roemenië*.[9] Steunend op eerdere arresten zoals *Amann t. Zwitserland* en verwijzend naar de beginselen van het *data protection* recht (infra), verklaarde het Hof, in deze zaak over een door de veiligheidseisen geficheerd persoon, dat 'publieke informatie' over een persoon onder de werking van art. 8 EVRM valt, wanneer deze systematisch verzameld wordt of blijvend wordt opgeslagen in overheidsbestanden.[10]. In het arrest *P.G. en J.H. t. het Verenigd Koninkrijk* wordt naar deze passage uit *Rotaru* verwezen, maar gaat het Europees Hof verder. Het Hof stelt voorop dat het begrip 'privé-leven' een ruim begrip is dat moeilijk te definiëren is. Het begrip omvat in ieder geval het recht op identiteit, op persoonlijke ontwikkeling en het recht op het ontwikkelen en onderhouden van relaties met anderen en de buitenwereld. Deze relaties kunnen ook een zakelijk karakter hebben. Dit betekent dat de bescherming van het privé-leven zich tot het publieke domein kan uitstrekken (§ 56).[11]

---

persoonsgegeven (§ 59) en onder de werking van art. 8 EVRM valt (§ 6o), Tevens wordt het opvragen van de nummers die gedraaid waren met de telefoon eveneens gezien als een handeling die onder toepassing van het privacygrondrecht valt. Over nieuwere toezichttechnieken zijn nog geen uitspraken. Over het algemeen wordt echter aangenomen dat het EHRM te zijner tijd door een verdragsdynamische interpretatie ook e-mail onder artikel 8 zal brengen. Cf. H.H. de Vries, 'Vertrouwelijkheid van e-mail in arbeidsverhoudingen', p. 116-117 in H.W.K Kaspersen & C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer 2001,p. 111-139; L. Ascher. & W. Steenbruggen, 'Het Emailgeheim op de werkplek. Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk', *NJB*, 2001-37, 1788.

[7] EHRM 16 december 1992 (*Niemitz*), *NJ* 1993, 400.

[8] EHRM 25 juni 1997 (*Halford*), *NJ* 1998, 506.

[9] EHRM, 4 mei 2000 (*Rotaru t. Roemenië*), *ECHR*, 2000-V. Het arrest is tevens opgenomen in *Revue trimesterielle des droits de l'homme*, 2001, 138-183, noot O. De Schutter.

[10] EHRM, Rotaru t. Roemenië, *l.c.*, § 43.

[11] Cf. EHRM, 25 september 2001 (*P.G. en J.H. tegen het Verenigd Koninkrijk*), § 56. Ten aanzien van het antwoord op de vraag wanneer zich een inmenging in het privé-leven voordoet in geval een persoon zich in het publieke domein bevindt, zijn volgens het Hof een aantal factoren relevant. In een situatie waarin iemand weet dat hij gefilmd wordt of anderszins wordt waargenomen, zijn *reasonable expectations of privacy* van belang, maar niet doorslaggevend. Het privé-leven komt in het geding wanneer het (opgenomen) materiaal systematisch of blijvend wordt opgeslagen. Het is daarom dat het EHRM eerder heeft uitgemaakt (in de zaak *Rotaru tegen Roemenië*) dat een dossier met daarin de door de veiligheidsdienst verzamelde gegevens over een persoon onder de werking van art. 8 EVRM valt, ook in geval de gegevens niet op een heimelijke of slinkse wijze zijn verkregen. Het Hof wijst verder nog op de zaak *Amann tegen Zwitserland*, waarin het aannam dat een kaartsysteem met gegevens over de klager een inbreuk op zijn privé-leven vormde, ook al betrof het geen gevoelige gegevens en ook al waren deze waarschijnlijk nooit geraadpleegd. Men leze: P. De Hert, 'Het Europees Hof Rechten van de Mens erkent publieke privacy. De legaliteitseis en het politioneel optreden in het licht van artikel 8 EVRM', *Nieuw Juridisch Weekblad*, 2002, Vol. 1/4, 9 oktober 2002, 116-122.

3. Weerstanden

Het voorgaande leert dat privacy een modern en actueel recht vormt en terecht ruim wordt begrepen. Dat privacy zijn rol als modern grondrechtenijkpunt min of meer succesvol vervult, kan gemeten worden aan de weerstanden die het grondrecht oproept. Te denken hierbij valt aan recente boekwerken waarin precies getracht wordt de grijparmen van dit recht te beperken teneinde in naam van het algemeen belang of het gemeenschapsbelang meer armslag te geven aan collectiviteiten.[12] Ook in vele discussies over *law and order* wordt beargumenteerd dat misdadigers geen recht op privacy hebben, omdat het recht niet kan strekken tot het beschermen van onwettelijkheden. Dit argument, dat nog steeds kan rekenen op instemming bij velen, is niet nieuw[13] en zeker niet eigen aan het privacygrondrecht en de kritiek erop.
Relatief nieuw is het argument dat wij allen, en dus niet alleen de schurken, teveel privacy genieten en dat daar in het belang van de publieke veiligheid wat moet worden afgedaan. Dit argument stond onder meer centraal in een schrijven van justitieminister Donner aan de Tweede Kamer.[14] Volgens de minister moeten de privacyregels worden versoepeld ten behoeve van de strijd tegen terrorisme en zware misdaad. Hij wil onder meer de politie de bevoegdheid geven ook langdurig de gegevens op te slaan van personen die niet worden verdacht van een strafbaar feit. Nu is die opslag nog aan strenge regels van gebruik en tijdelijkheid onderworpen. Meer in het bijzonder wil de minister in de Wet Politieregisters de mogelijkheid opnemen om zogeheten themaregisters te openen. Onder bijvoorbeeld het thema terrorisme kunnen dan gegevens worden opgeslagen over personen van wie aanwijzingen bestaan dat zij wellicht betrokken zijn bij het beramen, voorbereiden of plegen van terreurdaden. Zoals reeds gezegd hoeft het niet om verdachte activiteiten te gaan. Aanknopingspunt is dat het gaat om informatie die de politie relevant acht, wat ruimer is dan strafrechtelijke relevante informatie.[15] Het terrorismeregister wordt verder aangevuld met gegevens uit open bronnen zoals websites en openbare registers en met informatie van het Meldpunt Ongewone Financiële Transacties en allerlei andere registers en databanken van de politie.[16]

Kenmerkend voor het rapport *Gegevensuitwisseling en Terrorismebestrijding* is de zure toon richting wetgever en controlerende instanties. Het project wil de politie en de AIVD gezamenlijk in staat stellen om van burgers een 'onbeperkt houdbare' dossier op te bouwen, zonder dat controlerende instanties zoals College Bescherming Persoonsgegevens en de wetgever zich inhoudelijk met de dossiervorming kunnen bemoeien.
Terecht plaatste de Twentse hoogleraar communicatiewetenschap Jan van Dijk vraagtekens bij het gebrek aan privacyevenwicht in het rapport. Hij vermoedt een gebrekkige reflectie over de vermeende efficiëntie en de te verwachte discriminatie van bepaalde bevolkingsgroepen van de geplande maatregelen.[17] Interessant is de beschouwing die hij

---

[12] Zie bijvoorbeeld Amitai Etzioni, *The Limits of Privacy*, New York: Basic Books 1999.
[13] Zie onder meer Jeremy Bentham, 'Principles of the Penal Code', in *Theory of Legislation*, (based on manuscripts written around 1788, collected by E. Dumont and first published in 1802), Oxford: Oxford UP, Vol. II, 1914, Part IV (Chapter LVI), p. 263-264.
[14] Cf. Marc van den Eerenbeemt, 'Privacywet moet worden versoepeld', in de *Volkskrant*, 9 januari 2003.
[15] Cf. Dossier Terrorisme, via Recht.nl. In het rapport *Gegevensuitwisseling en Terrorismebestrijding* dat eind januari 2003 werd verspreid, wordt een treffend voorbeeld gegeven hoe die themaregisters zouden kunnen werken: *Zo is bijvoorbeeld het enkele feit dat iemand in Nederland vlieglessen volgt op zichzelf onvoldoende om gegevens over hem op te slaan. Dit gegeven aangevuld met andere relevante informatie kan echter wel leiden tot de conclusie dat het doel van een themaregister terrorisme de opslag van gegevens over die persoon rechtvaardigt.'*
Eigenlijk wordt met dit voorbeeld toegegeven dat de politie zich voortaan begeeft op het terrein dat aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) wordt voorbehouden. Sterker nog, de plannen gaan verder dan wat onder de Wet op de inlichtingen- en veiligheidsdiensten mogelijk is. Cf. Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002), *Staatsblad* 2003, 212. Deze wet hervomde de twee bestaande diensten (Binnenlandse Veiligheidsdienst (BVD) en Militaire Inlichtingendienst (MID)). Deze heten voortaan Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD).
[16] Van belang is tevens is het voornemen om de informatie-uitwisseling tussen financiële toezichthouders en de AIVD te versoepelen (*infra*).
[17] 'Ik vraag me af of het ooit zal helpen om misdaden op te lossen. Het probleem van de politie is niet dat ze te weinig informatie heeft, maar dat ze geen weg weten te vinden in de veelheid aan informatie. Ze hebben de tijd niet om alles nauwkeurig te

hieraan koppelt over privacyweerstanden bij de Nederlandse politie. 'Het is niet omdat ze er direct gebruik van willen maken, maar omdat het blijkbaar frustrerend is dat ze af en toe tegen de wet oplopen. Dus als ze alvast maar die mogelijkheid krijgen, dan kunnen ze er altijd desgewenst nog gebruik van maken. Hetzelfde geld voor identificatieplicht, het gaat erom dat iemand niet even 'fuck off' tegen de politie kan zeggen, en dat de agent dan niets terug kan doen als hij om een identificatie vraagt. Het kost veel te veel werk om daadwerkelijk iedereen om een ID te vragen.'[18]

4. Het complexe krachtenspel achter privacy

Hoger schreven we dat privacy een belangrijke rol vervult in het tot stand brengen van een evenwichtige grondrechtenpolitiek en dit *min of meer succesvol*. Probleem met privacy is de eerder complexe sociale verankering in de samenleving. Anders dan bij veel andere maatschappelijke waarden zijn er niet louter voor- en tegenstanders. Bovendien zijn er minstens drie partijen in het geding: burgers, de overheid en het bedrijfsleven en elk heeft een wat ambivalente houding tegenover privacy:[19] De overheid beschermt met wetgeving de privacy van burgers. Tegelijkertijd verschaft de overheid zich steeds meer bevoegdheden om de communicatie tussen burgers naar eigen believen af te tappen. De meeste burgers zijn terughoudend in het verstrekken van hun persoonsgegevens. Tegelijkertijd smullen velen van televisieprogramma's als Big Brother en zouden veel ouders hun kinderen het liefst permanent in de gaten willen houden. Bovendien koesteren sommige onrealistische veiligheidsverwachtingen en worden overheidsdiensten afgerekend wanneer zich onvoorspelbare gebeurtenissen zoals rampen en aanslagen voordoen. Bedrijven, tenslotte, hebben marketingmedewerkers in dienst om zoveel mogelijk persoonsgegevens te verzamelen en te analyseren. Tegelijkertijd zijn de meeste bedrijven erg karig in het verstrekken van eerlijke informatie over hun eigen doen en laten.

Juridisch vertaalt zich dit spanningsveld in wetgeving of gewoonten die nu eens in het voordeel voor de enen spelen dan wel in dit van de anderen. Een commentator aarzelt niet om de zere plekken voor het bedrijfsleven aan te wijzen in de recente Nederlandse en Europese wetgeving.[20] Zo geeft de Wbp (waarover straks meer) burgers een steeds sterkere rechtspositie krijgen tegenover het bedrijfsleven. De Wbp bevestigt onder meer dat bedrijven niet ongelimiteerd persoonsgegevens mogen verzamelen, bewaren en doorverkopen - ook niet op internet. Een Europese richtlijn verbiedt bovendien het gebruik van ongevraagd elektronische reclame ('spam') en is daarmee strenger voor de reclamebranche dan de Nederlandse wetgever. Ook het hoger besproken rapport *Gegevensuitwisseling en Terrorismebestrijding* wijst op 'verlies' van het bedrijfsleven, ditmaal in de relatie tussen bedrijven en de overheid. De Nederlandse Bank, de Autoriteit Financiële Markten en de Pensioen- en Verzekeringskamer kunnen nu nog zelf beslissen of zij informatie over mogelijke financiering van terrorisme doorgeven aan de geheime dienst.[21] Die beslissing zou, volgens de plannen, in handen van de minister van Financiën moeten komen, onder meer omdat de toezichthouders soms onvoldoende inzicht hebben in het belang van de informatie-uitwisseling. De AIVD kan daar doorgaans geen open kaart over spelen.

Een vergelijking van de onderlinge posities leert dat van de drie partijen vooral de overheid haar positie verstevigd door privacybeperkende maatregelen die aan anderen worden opgelegd.[22] Het voornemen tot registers met niet-verdachten is van aard ook burgers bezorgd

---

controleren en op te slaan, iets wat erg belangrijk is bij databestanden. Het zal ze alleen maar meer werk opleveren' (prof. Jan van Dijk in AW, 'Schot voor de boeg voor datajacht', via Netkwesties.nl, 23 januari 2003).

[18] Prof. Jan van Dijk in AW, 'Schot voor de boeg voor datajacht', via Netkwesties.nl, 23 januari 2003.

[19] WZ, 'Twee stappen achteruit: ruimere opsporingsbevoegdheden hollen privacybescherming uit', *www.Bitsoffreedom.nl*, 9 augustus 2001, 1.

[20] WZ, *l.c.*, 2.

[21] Over deze problematiek, meer algemeen: Eric Schreuders, e.a., *Als de politie iets wil weten* .., Sdu Uitgevers, Den Haag, 1999, 148p

[22] WZ, *l.c.*, *www.Bitsoffreedom.nl*, 9 augustus 2001.

te maken die in regel aan 'boeven' het privacylicht niet gunnen. De in 2002 tot stand gekomen Wet op de inlichtingen- en veiligheidsdiensten geeft de AIVD en MIVD vergaande aftapbevoegdheden: ze mogen elke vorm van telecommunicatie aftappen, waarbij ze ook eventuele versleuteling ongedaan mogen maken.[23] Verder hebben de inlichtingendiensten onbeperkte en ongecontroleerde toegang tot abonneegegevens van alle telecommunicatieleveranciers en onbeperkte en ongecontroleerde toegang tot verkeersgegevens (wie belt wanneer met wie en hoelang duurt dat). Zelfs degene die een bericht of bestand heeft versleuteld, is verplicht om op verzoek van de inlichtingendiensten de versleuteling ongedaan te maken. Dit laatste aspect, de medewerkingplicht, is voor ons rechtssysteem vrij apart en toch heeft het zich zonder al te veel problemen kunnen doorzetten.[24]
Volgens Van Dijk is het vooral de 'oude elite' die zich tegen de privacybeperkingen verweert, terwijl de bevolking niet weet wat haar boven het hoofd hangt. Het probleem is volgens hem dat de noodzaak van privacy soms moeilijk is uit te leggen aan burgers en politici: 'je moet wel haast een jurist zijn om het allemaal te snappen, je moet dieper over deze zaken nadenken, dat is niet iedereen gegeven'.[25] Ten dele wordt deze opvatting bevestigd door wetenschappelijk onderzoek.[26] De meningen bij de burgers over hoever de overheid inbreuk mag maken op privacy om misdaad te kunnen opsporen, zijn verdeeld en onderhevig aan wisselende factoren. Vast staat evenwel dat hoe ongrijpbaarder of zichtbaarder een opsporingsmethode, des te minder de mensen er wakker van liggen. Dat geeft te kennen over een privacypolitiek in een onveilige informatiemaatschappij. Ook speelt mee dat de complexe natuur van privacy een debat over de privacygevolgen van een maatregel de parten kunnen spelen. Dit diffuus karakter van privacy brengt ons bij de volgende erg belangrijke vragen: 'wat is privacy?', 'is privacy meer dan de Wbp?'; 'wie waakt er over onze privacy?' en 'wat is data protection?'. Bij de beantwoording van die vragen verkiezen we een korte omweg te maken terug naar de fundamenten van ons rechtssysteem. We bekijken allereerst hoe onze democratische rechtsstaat functioneert en welke technieken binnen dit kader worden aangewend.

5. Het kader van de democratische rechtsstaat

De opkomst van de democratische rechtsstaat heeft geboorte gegeven aan een andere manier om met macht om te springen.[27] Als reactie op een periode van absolute en arbitraire heerschappij belichaamde hij een nieuw staatsconcept waarin voortaan macht beperkt is, juist omdat het expliciete doel is de individuele vrijheid te bevorderen en te beschermen. De oude omnipotente soeverein moest plaats maken voor een staatsorganisatie gekenmerkt door een reeks ingebouwde mechanismen van machtsbeperking en waarin ook ruimte is voor individuele vrijheid en zelfontplooiing. De eindtermen van een democratisch rechtsstatelijk project zijn dan ook paradoxaal want het doel is immers een maatschappelijke orde in het leven te roepen die zich tot doel stelt individuele vrijheid mogelijk te maken: én eenheid

[23] Zij hebben hiervoor wel toestemming nodig van de minister van Binnenlandse Zaken en Koninkrijksrelaties, die vergunningen afgeeft voor de duur van drie maanden. Vroeger had de AIVD nog de handtekeningen van vier verschillende ministers nodig.
[24] Een belangrijk principe in onze rechtsstaat is dat een verdachte niet hoeft mee te werken aan zijn eigen veroordeling. Tot nu toe waren er twee uitzonderingen op: een verdachte moet meewerken aan een bloedproef, bijvoorbeeld bij een verdenking van alcoholgebruik in het verkeer, en hij moet meewerken aan een DNA-test door bijvoorbeeld slijm, huidschilfers of haar af te staan. Maar als het gaat om huiszoeking door de politie zijn Nederlandse burgers niet verplicht tot medewerking. Ze hoeven dus niet te vertellen waar hun kluis zich bevindt en evenmin hoeven ze de sleutel van die kluis te overhandigen. De Wiv stelt echter dat verdachten wél hun digitale sleutels en wachtwoorden moeten inleveren. Het geeft de richting aan in dewelke ons strafsysteem zal evolueren binnen het grote kader van de informatiemaatschappij. Cf. WZ, *l.c.*, 2.
[25] Prof. Jan van Dijk in AW, 'Schot voor de boeg voor datajacht', via Netkwesties.nl, 23 januari 2003
[26] Bert-Jaap Koops en Anton Vedder, *Opsporing versus privacy. De beleving van burgers,*Den Haag, Sdu 2001.
[27] Onder democratische rechtsstaat verstaan wij de staatsvorm die (in de westerse wereld) onder invloed van de politieke verlichting (Locke, Rousseau, Montesquieu, Becarria, ...) gestalte kreeg vanaf de periode eind 17de-begin 19de eeuw met als symbolische momenten de Engelse *glorious revolution* en zijn *Bill of rights* (1688), de Amerikaanse onafhankelijkheidsstrijd uitmondend in de *Declaration of Independence* (1776) en de *Constitution* (1788-1791) en tenslotte de Franse revolutie en de *Déclaration des droits de l'homme et du citoyen* (1789). Voor een uitgebreidere bespreking zie Serge Gutwirth, 'De polyfonie van de democratische rechtsstaat' in *Wantrouwen en onbehagen*, Mark Elchardus, (red.), Balans 14, Brussels, VUBPress, 1998, 137-193.

(orde), én verscheidenheid (vrijheid) dienen te worden gerealiseerd.[28] Het zijn elkaars constitutieve voorwaarden. M.a.w. dient te worden voldaan aan twee doelstellingen die tot elkaar in spanning staan: het mogelijk maken van individuele vrijheid en diversiteit, maar dat wel binnen een duurzaam geheel dat toch als een eenheid functioneert.
De *double bind* van het project is duidelijk. Enerzijds moet er een zo groot mogelijke vrijheid komen voor een zo groot mogelijk aantal individuen. Zonder individuele vrijheid en veelheid aan inzichten, opinies, projecten en gedragsmogelijkheden is er geen democratische rechtsstaat. Deze laatste wordt dan ook minder gekenschetst doordat een verkozen meerderheid er de macht uitoefent dan doordat hij de macht van diezelfde meerderheid begrenst en beperkt. Maar anderzijds moet een democratische rechtsstaat er tegelijk voor zorgen dat hij blijft voortbestaan. Een verregaande individualisering kan immers leiden tot de desintegratie van het geheel, waarin ook de individuele vrijheid teloor gaat.
Kortom : de democratische rechtsstaat belichaamt een orde die constitutief is voor individuele vrijheid en tegelijkertijd diezelfde vrijheid moet beperken. Spanningen zijn *legio* want het project wordt steeds in twee tegengestelde richtingen getrokken: aan de ene kant loert de chaos van de te verregaande individualisering; aan de andere kant de totalitaire verleiding waaraan elke orde (macht) bloot is gesteld. Het recht kan in zo'n opzet niet louter instrumentalistisch -als loutere bevelstructuur voor het beleid- worden benaderd; het moet integendeel, zonder te verzaken aan zijn dubbele binding, de complexe maatschappelijke (machts)verhoudingen beheren door ze met elkaar in relatie te brengen en te bemiddelen teneinde conflicten te kanaliseren.[29]

6. De drie constitutionele principes van de democratische rechtsstaat

Algemeen

Het functioneren van een democratische rechtsstaat is bijgevolg een complexe aangelegenheid waarbij het bewerkstelligen van evenwichten, het balanceren, het compenseren, het dwingen en vrijlaten steeds samen aan de orde zijn. Zulke complexiteit is natuurlijk ook aanwezig bij de uittekening van het concreet juridisch-institutioneel uitvoeringsplan van het project. Daarom ook dat de door de 17/18de eeuwse denkers en revolutionairen geformuleerde hervormingen tot en met de huidige structuren van de democratische rechtsstaten eveneens op ingewikkelde, dynamische en evenwichtszoekende

---

[28] Hierover zie o.m. : M. Delmas-Marty, *Pour un droit commun*, Le Seuil/La librairie du XXe siècle, Paris, 1994, 306 p.; M. Delmas-Marty, *Vers un droit commun de l'humanité*, Paris, Textuel, 1996, 126 p.; A.C. 't Hart, *Mensenwerk ? Over rechtsbegrip en mensbeeld in het strafrecht van de democratische rechtsstaat*, Mededelingen van de Koninklijke Nederlandse Akademie van Wetenschappen, Afdeling Letterkunde, Noord-Hollandsche, Amsterdam, 1995, Nieuwe reeks, Deel 58, no. 4, 40 p.; A. Touraine, *Qu'est-ce la démocratie ?*, Paris, Fayard, 1994, 297 p. en A. Touraine, *Pourrons-nous vivre ensemble ? Egaux et différents*, Paris, Fayard, 1997, 395 p. Maar ook in de rechtspraak van het Hof te Straatsburg wordt dikwijls gewezen op de fundamentele plaats van diversiteit en veelheid aan meningen en levensvormen in een democratische rechtsstaat.

[29] Zulke relationele opvatting van het recht, die door A.C. 't Hart & R. Foqué werd uitgewerkt en gethematiseerd, vindt zijn wortels in het Verlichtingsdenken (o.m. van Montesquieu en Beccaria) dat een directe reactie belichaamde tegen de absolute macht van de vorst onder het ancien régime en derhalve ook tegen het imperativistisch rechtsdenken waarin het recht wordt herleid tot de bevelen of wilsuitingen van de soeverein. Hiertegenover geeft het relationeel rechtsdenken aan het recht de functie, om binnen de grenzen van zijn concepten, bemiddelend op te treden tussen de verschillende maatschappelijke machten en dat juist om absolute machtsverhoudingen onmogelijk te maken. Horizontale bemiddelingen treden in de plaats van de verticale bevelen. In een relationeel rechtsbegrip dient het recht dan twee functies te vervullen door ze op elkaar te betrekken: een rechtsbeschermende functie, die een rem beoogt te zijn op de ontsporingen van de macht en een instrumentele functie, die gericht is op de schepping van de mogelijkheden voor een maatschappelijke orde waarin vrijheid kan worden verwezenlijkt. Die verwevenheid tussen het instrumentele en machtskritische aspect impliceert dat het recht essentieel een bemiddelende rol te spelen heeft: het herbepaalt de verhouding tussen de maatschappelijke machten steeds opnieuw in functie enerzijds van de vrijheid van de individuen en anderzijds van de sturing van het gemeenschappelijke project waarin diezelfde vrijheid centraal staat. Zie vooral in R. Foqué en A.C. 't Hart, *Instrumentaliteit en rechtsbescherming. Grondslagen van een strafrechtelijke waardendiscussie*, Arnhem/Antwerpen, Gouda Quint/Kluwer, 1990, 501 p. Zie o.m. ook in R. Foqué, *De ruimte van het recht*, Arnhem, Gouda/Quint, 1992, 44 p.; R. Foqué, 'Rechtsstatelijke vernieuwing. Een rechtsfilosofisch essay' in P. Kuypers, R. Foqué & P. Frissen, *De lege plek van de macht. Over bestuurlijke vernieuwing en de veranderende rol van de politiek*, Amsterdam, De balie, 1993, 18-44; R. Foqué 'Rechtsstatelijke evenwichten in de trias politica', *l.c.*, 1-5; A.C. 't Hart, *Recht als schild van Perseus. Voordrachten over strafrechtstheorie*, Leerstoel Theodore Verhaegen 1989-1990 - Vrije Universiteit Brussel, Arnhem/Antwerpen, Gouda Quint/Kluwer, 1991, 191 p.; A.C. 't Hart, *Mensenwerk ?*, *o.c.*, 40 p., A.C. 't Hart, *De meerwaarde van het strafrecht*, Sdu, Den Haag, 1997, 318 p. en A.C. 't Hart, *Hier gelden wetten ! Over strafrecht, Openbaar Ministerie en multiculturalisme*, Arnhem, Gouda Quint, 2001, 270 p. Tevens: S. Gutwirth, *Waarheidsaanspraken in recht en wetenschap. Een onderzoek naar de verhouding tussen recht en wetenschap met bijzondere illustraties uit het informaticarecht*, VUBPress/MAKLU, Brussel/Antwerpen, 1993, 235 et seq. en S. Gutwirth, 'De polyfonie ...', *o.c.*, 152 et seq.

leest zijn geschoeid. Meer concreet proberen zij in de schoot van één geheel, de democratische rechtsstaat, drie tot elkaar in spanning staande en elkaar soms overlappende *constitutioneel verankerde* principes te verenigen[30]: de erkenning van fundamentele rechten en vrijheden van de mens, de rechtsstatelijkheid (of *rule of law*) en de democratie.[31] Ze worden hieronder alledrie kort besproken.

Fundamentele rechten en vrijheden

In de eerste plaats erkennen de grondwetten van democratische rechtsstaten een reeks fundamentele rechten en vrijheden (kortweg: mensenrechten). Deze functioneren in het hart van het politieke project om de individuen te beschermen tegen een ontspoorde machtsuitoefening.[32] In beginsel is het de staat niet toegelaten om zich met deze rechten en vrijheden in te laten. Zij functioneren als een schild. De fundamentele rechten en vrijheden belichamen in die zin tegelijk een erkenning van de macht van de individuen èn de ondergrens van de inmenging van de staatsmacht. Bijgevolg beschikken de individuen over een reeks elementaire prerogatieven tegen de staatsmacht (en vandaag de dag ook tegen andere maatschappelijke machten).

Voor een goed begrip van privacy is het essentieel voor ogen te houden dat de erkenning van de mensenrechten meteen ook de erkenning van het individu als een autonome en onafhankelijke actor inhoudt. Het individu bestaat voortaan los van de staat, maar ook van een door de meerderheid gestuurd beleid. De mensenrechten beschermen het individu tegen J.S. Mills spreekwoordelijke *tyranny of the majority.* Zij roepen een ruimte van autonomie en zelfbepaling in het leven die de individuen beschermt tegen de excessieve sturing van hun gedrag. In één woord : zij creëren de privé sfeer.[33]

De fundamentele rechten en vrijheden stellen echter niet uitsluitend perken aan de macht van de staat; zij maken het voor de burgers eveneens mogelijk om aan het politieke gebeuren te participeren (*empowerment*).[34] Dit verklaart waarom het in de Westerse politieke traditie niet zo moeilijk is om een *overlapping consensus* te vinden met betrekking tot het belang van fundamentele vrijheden zoals de uitingsvrijheid, de gewetensvrijheid en vrijheid van vereniging. Deze mensenrechten maken het voor de burgers mogelijk om hun conceptie van het goede op rationele wijze te vormen en na te streven. [35] En dit legt dan weer uit waarom grondwettelijke normen keuzen uitdrukken. Westerse constituties voorzien lijsten van mensenrechten die bredere noties zoals vrijheid en waardigheid concretiseren. Een eenvoudige grondwet die vooropstelt dat iedere burger over een allesomvattend 'recht op vrijheid' beschikt bestaat niet en wordt ook niet nagestreefd. Volgens Raz kan '(s)uch a right, if it exists, (...)not capture our concern for liberty because it is indiscriminate. It protects

---

[30] Hieronder worden deze drie principes om didactische redenen elk afzonderlijk beschouwd. Het is evenwel zo dat ze in de praktijk in elkaar lopen. Bepaalde implicaties die ik verder zal afleiden uit één van de principes, kunnen dan ook toegeschreven worden aan het samenspel van twee of drie van de principes. Dikwijls wordt de mensenrechtelijke bescherming van het individu overigens beschouwd als een aspect van de rechtsstatelijkheid.

[31] Twee van deze principes werden al in niet mis te verstane termen expliciet vooropgesteld in art. 16 van de Franse *Déclaration* van 1789 : "Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de constitution".

[32] In het verlengde van de oorspronkelijke Verlichtingsfilosofie (Locke, Rousseau, ...) gaat het om *natuurlijke rechten* die worden geacht vooraf te gaan aan elke staatsvorming en onopzegbaar, onvervreemdbaar, heilig en onvergankelijk te zijn (cf. *Declaration of independence* en *Déclaration des drois de l'homme et du citoyen*). Zij behoren van nature toe aan ieder individu om de loutere reden dat hij een mens is. Het is hier niet de plaats om het debat aan te gaan over de theorie van het natuurrecht. Elders hebben we, door Rawls geïnspireerd, een politieke en constructivistische (pragmatische) benadering van de mensenrechten voorgesteld en uitgewerkt : P. De Hert & S. Gutwirth, 'Rawls' political conception of rights and liberties. An unliberal but pragmatic approach to the problems of harmonisation and globalisation' in *Epistemology and Methodology of Comparative Law*, M. Van Hoecke (Ed.), Proceedings of the *Epistemology and Methodology of Comparative Law*-conference held in Brussels on October 24th - 26th, 29 p. (verschijnt in januari 2004 bij Hart Publ., Oxford)

[33] Uiteraard is deze sfeer van autonomie niet absoluut. Ook de autonomie kan worden op rechtmatige wijze worden begrensd met het oog op de bescherming van de rechten en vrijheden van anderen en het algemeen belang. Dat geldt a fortiori voor het privacygrondrecht, maar maakt het daarom niet minder belangrijk.

[34] C. Schneider, 'The Constitutional Protection of Rights in Dworkin's and Habermas' Theories of Democracy', *UCL Jurisprudence Review*, 2000, (101-121) 118.

[35] John Rawls, *Justice as Fairness. A Restatement*. Cambridge: Harvard UP, 2001, § 13.4.

equally the liberty to eat green ice-cream and to religious worship'.[36] Constitutionele normen bevatten dan ook de expliciete vooropstelling van bepaalde waarden als zijnde fundamenteel. Een notie als vrijheid wordt te vaag en te weinig onderscheidend beschouwd om van enig nut te zijn voor een filosofische, ethische en politieke definiëring van de plichten van de staat en de burgers en hun onderlinge verhoudingen.[37] Bijgevolg bevatten de mensenrechten eveneens duidelijke opties die uitdrukken hoe een gemeenschap omspringt met de idee dat zij burgers wenst die aan het publieke gebeuren kunnen participeren.

Rechtsstatelijkheid

In de tweede plaats verankeren de grondwetten van democratische rechtsstaten de principes van de rechtsstatelijkheid[38]: zij constitueren een rechtsstaat. De genoemde principes streven er opnieuw naar de macht van het bestuur te beperken, doch nu gebeurt die niet meer door het vaststellen van limieten aan het bereik van de macht, maar door het uitdokteren van een 'interne' organisatie van de machtsuitoefening. De leidraad van de *rule of law* is de onderwerping van het bestuur en de staatsmacht aan een geheel van restrictieve en controlerende constitutionele regels en mechanismen.[39]

In de eerste plaats veronderstelt de rechtsstatelijkheid het beginsel van de legaliteit van het overheidshandelen: besturen kan alleen in overeenstemming met het recht. Dit betekent dat de publieke overheden gebonden zijn door hun eigen regels en hun machten uitsluitend kunnen uitoefenen op een wettelijke wijze. Alle machten emaneren van de grondwet (die op zijn beurt wordt verondersteld de wil van het soevereine volk te vertalen) en elke machtuitoefening moet interpreteerbaar zijn als de uitdrukking van een constitutionele bepaling. Hierdoor wordt het bestuur aanspreekbaar en kan het ter verantwoording worden geroepen. Deze essentiële *accountability* van de overheidsmacht impliceert eveneens dat het overheidshandelen controleerbaar en transparant is. De rechtsstatelijkheid verwijst verder 'naar de gedachte dat moderne samenlevingen *door wetten en niet door mensen worden geregeerd,* dat het gezag, met andere woorden, onpersoonlijk en niet persoonlijk wordt uitgeoefend. Geen willekeurige bevelen van een persoon, maar redelijke wetten moeten de samenleving ordenen. Die wetten hebben op hun beurt als centraal kenmerk dat zij *algemeen* zijn, in alle gevallen voor alle personen gelijk (zouden moeten) gelden en 'abstractie maken' van particuliere verschillen tussen mensen en situaties. Dit impliceert de formele gelijkheid tegenover de wet'.[40]

In de tweede plaats leidt de rechtsstatelijkheid tot de implementatie van de *trias politica* of een systeem van evenwicht van machten. Doelstelling is de staatsmacht te spreiden over verschillende machtscentra met onderscheiden bevoegdheden en functies. Om de macht te beperken wordt een pluraliteit van machtshaarden in het leven geroepen die elkaar op dynamische wijze in evenwicht moeten houden door een systeem van wederzijdse controle (*checks and balances*). Dit stelsel kan uiteindelijk worden teruggevoerd tot de beroemde zinnen uit Montesquieu's *De l'esprit des lois*: "Pour qu'on ne puisse abuser du pouvoir, il faut que, par la disposition des choses, le pouvoir arrête le pouvoir".[41] Om macht te remmen, moet hij worden opgesplitst. In plaats van de ondeelbare, absolute, centrale en personifieerbare soeverein komt een constructie waarbij de soevereiniteit wordt verdeeld tussen verschillende concurrerende machtscentra die samen dienen te handelen én elkaar wederzijds controleren. Deze *balance of power* leidt tot begrenzing en kanalisering van de staatsmacht en past bijgevolg in het ideaal van een geordende (liberale) samenleving waarin de individuele vrijheid centraal staat. "Machtsconcentratie moet vermeden worden door *checks and*

---

[36] J. Raz, *The Morality of Freedom*, (1986), Oxford, Clarendon Press, 1988, 245-247; D. Feldman, *Civil Liberties & Human Rights in England and Wales*, Oxford, Clarendon Press, 1993, 7-11.

[37] D. Meuwissen, 'Reactie van D.H.M. Meuwissen op de brief van C.W Maris', *Ars Aequi*, 1998, vol. 47, 673-677; M. Heirman, 'De mensenrechten: alleen het individu is universeel', in J. De Tavernier & D. Pollefeyt (eds.), *Heeft de tradtitie van de mensenrechten toekomst?*, Leuven, Acco, 1998, 29-30.

[38] Verwante begrippen zijn : constitutionalisme, de heerschappij van het recht, de *rule of law*, de *Rechtsstaat*, de *prééminence du droit, ...*

[39] J. Chevallier, *L'Etat de droit*, Paris, Montchrestien, 1994, 11

[40] Koen Raes, *Tegen betere wetten in. Een ethische kijk op het recht*, Gent Academia Press, 1997, 1.

[41] Montesquieu, *De l'esprit des lois*, t. 1, Paris, Garnier-Flammarion, 1979, 293.

balances. Waar standen, klassen, organisaties, individuen *in juridicis* op elkaar botsen moet de ene macht de andere macht afstoppen opdat de tirannie, ook die van de meerderheid, wordt vermeden. In deze botsing van strevingen moet het mogelijk zijn dat rationeel handelende individuen in en door hun organisaties een strategie weten te vinden die tot gecoördineerd gedrag leidt".[42] Kortom: een centralistische machtsorganisatie moet wijken voor het principiële pluricentrisme van de macht.[43] Een zodanig systeem impliceert de wederzijdse *accountability* van de staatsmachten, en dus opnieuw de wederzijdse transparantie en controleerbaarheid van de wetgevende, uitvoerende en, *last but not least*, uitvoerende macht.

Democratie

In de derde plaats erkennen de grondwetten van democratische rechtsstaten de idee van de politieke zelfdeterminering van het volk en de principes van de democratische vertegenwoordiging. Na de periode van de vorst-soeverein breekt die van het soevereine volk aan. Gezag, macht en *government* zijn voortaan alleen dan legitiem als zij emaneren van het volk en als dusdanig reconstrueerbaar zijn. De verschillende variaties op het thema van het sociaal contract (Beccaria, Locke, Rousseau, Hobbes, ...) zijn in die zin telkens metaforen die het mogelijk maken om het ontstaan en het constitueren van een politieke gemeenschap gebaseerd op de wil van het volk te funderen.[44] De soeverein wordt dan geacht gevormd te zijn geweest door bv. de optelsom van de stukjes door de individuen afgestane vrijheid (cf. Beccaria) of door de *volonté générale* (cf. Rousseau). Anders uitgedrukt: de maatschappelijke macht (de 'soevereiniteit') moet dankzij zulke grondslagentheoretische begrippen steeds kunnen worden teruggevoerd tot het volk.

In de democratie staat bijgevolg de participatie van de burgers aan het beleid centraal. Zowel de wetgeving als het beleid dienen in principe afgestemd te zijn op het algemeen belang en de wil van het volk. Dat wordt gerealiseerd doorheen verkiezingen die de representativiteit van de organen en instellingen moeten verzekeren. Zowel de wetgever als de regering vinden als gevolg van de toepassing van de meerderheidsregel een draagvlak in het volk dat hen rechtstreeks of onrechtstreeks verkiest. Tegen deze achtergrond, waarin de participatie van de burgers aan de politieke besluitvorming zich opdringt, is het overigens duidelijk dat een democratie niet denkbaar is zonder dat een permanent open en publiek debat wordt gevoerd over de normen en waarden die zij dient te verwerkelijken. Zonder mogelijkheid tot onafhankelijke en vrije opinievorming voor de burgers of zonder onafhankelijke stem van het volk, komt de democratie in ademnood.[45] Tenslotte moeten systemen van democratisch bestuur procedures voorzien van rechtstreekse en onrechtstreekse controle van de gezagsdragers door de burgers. De democratische legitimiteit impliceert dus opnieuw de transparantie en *accountability* van het bestuur en de politieke besluitvorming, maar nu vooral t.a.v. van de burgers en hun organisaties.

7. De democratische rechtsstaat bedient zich van twee instrumenten

Algemeen

Uit het voorgaande (randnummers 5 en 6) kan worden afgeleid dar de opkomst en ontwikkeling van de democratische rechtsstaat gepaard is gegaan met de uitvinding van twee complementaire soorten instrumenten die hetzelfde doel beogen: het beperken en beheersen van macht. Enerzijds zien we de ontwikkeling van instrumenten die strekken tot de niet-inmenging in individuele aangelegenheden en bijgevolg de opaciteit van het individu beschermen. Anderzijds werden instrumenten bedacht om de transparantie, controleerbaarheid en *accountability* van machtshebbers te organiseren en te verzekeren. In

[42] W.J. Witteveen, *Evenwicht van machten*, Zwolle, Tjeenk Willink, 1991, 70.
[43] R. Foqué, 'Rechtsstatelijke evenwichten ...', *l.c.*, 2-3. Cf. ook R. Foqué, 'Rechtsstatelijke vernieuwing. Een rechtsfilosofisch essay', *l.c.*, 18-44.
[44] Hierover o.m. R. Foqué & A.C. 't Hart, *Instrumentaliteit en rechtsbescherming, o.c.*, o.m. op 67-180.
[45] R. Foqué, 'Rechtsstatelijke evenwichten ...', *l.c.*, 1-5 en R. Foqué, 'De ethische rol van de onafhankelijke rechter', *Trema. Tijdschrift voor de rechterlijke macht*, 1993-11, 462 et seq.

het verdere verloop van deze bijdrage (randnummers 8 en 9) zullen we privacy verbinden aan de eerste categorie, te weten de instrumenten van opaciteit, terwijl we data protection zullen conceptualiseren vanuit de tweede categorie, met name de instrumenten van transparantie.

Macht begrenzen via instrumenten van opaciteit

Daar het de kernbetrachting is van de democratische rechtsstaat om een orde te bevorderen die wordt gedreven door individuele vrijheid, staat de bescherming van het individu tegen inmengingen van de staat centraal. Bijgevolg kan het bestaan van een privé-sfeer waarbinnen het individu een geprivilegieerde status geniet, niet worden onderschat. Hiermee is meteen gezegd waarom instrumenten van opaciteit die de individuen afschermen tegen interferenties van de staat van cruciaal belang zijn in een democratische rechtsstaat.

De ideeën achter deze instrumenten kunnen nog het best worden verduidelijkt door de functie van de zogenaamde eerste generatie rechten van de mens in herinnering te brengen. Doorheen de erkenning en positivering van mensenrechten legden de revoluties van de 17de-18de eeuw in Engeland, de Verenigde Staten en Frankrijk de basis voor een scherpere scheiding tussen de publieke en de private sferen.[46] De constitutionele verankering van deze fundamentele rechten heeft bijgedragen tot de creatie van een sfeer van individuele autonomie en zelfbepaling, waarbinnen de burger zichzelf kan zijn en zijn leven naar goeddunken kan leiden zonder inmenging van de staat. De mensenrechten hebben de individuen als macht erkend door de erkenning van hun vrijheden en prerogatieven. En spiegelsgewijs werden grenzen aan de staatsinmenging getrokken door de erkenning van de individuele autonomie.

De rechten van de mens kunnen dan ook worden begrepen als instrumenten die strekken tot de bescherming van individuen tegen de inmenging van staten (en private actoren). Zij leggen een onthouding van ongewenste interventies op in zaken die essentieel worden geacht voor de individuele vrijheid. Vanuit een fysiek perspectief, met name dat van de onschendbaarheid van het lichaam, wordt deze zorg voor het respect van vrijheid uigedrukt door het recht op leven, het verbod van foltering en onmenselijke behandeling en het recht op veiligheid (en de bescherming tegen willekeurige vrijheidsberovingen dat het inhoudt). Deze mensenrechten bieden doorgaan een absolute (foltering) tot sterke (leven) bescherming. Individuele vrijheid is ondenkbaar indien mensen gemakkelijke of willekeurig aan lichamelijke dwang kunnen worden onderworpen. Het is overigens precies een doel van de democratische rechtsstaat om *geweld* uit te bannen (wat niet betekent dat ook macht moet worden uitgebannen, die moet worden gekanaliseerd, wat iets heel anders is, infra).

Een tweede illustratie is te vinden in de onschendbaarheid van de woning. Reeds in de negentiende-eeuwse grondwetten wordt die expliciet en zelfstandig aan de orde gesteld. In de Nederlandse grondwet is het huisrecht thans afzonderlijk opgenomen in art. 12. De belangrijkste mensenrechtelijke verdragen vermelden de woning in hun bepaling over privacy. De woning is onschendbaar en dat wordt doorgaans strafrechtelijk gewaarborgd. *The sanctity of the home*. De overheid, maar ook de andere burgers dienen de grenzen van de woning -*my home, my castle*- te respecteren. Voorbij de huisdeur zijn de individuen *meer* vrij van inmenging door derden en de overheid. Dat draagt bij tot hun waardigheid en ontwikkeling. De woning is een geprivilegieerde setting waar het privacybelang zwaarder weegt dan elders.[47] Het is de plaats waarbinnen ieder zijn gedrag in de grootste vrijheid bepaalt, wars van de dwang en mores die uitgaan van het sociale en zijn talloze geplogenheden en gedragsvoorschriften. Maar uiteraard wordt niet alles wat in de woonst gebeurt beschermd. Huiszoekingen kunnen worden bevolen in het kader van strafrechtelijke onderzoeken mits wordt voldaan aan een reeks stringente voorwaarden. Misdrijven en wederrechtelijke handelingen worden niet verschoond doordat zij thuis plaatsgrijpen. Maar

[46] Dat wordt overigens bevestigd door historisch onderzoek, zie *Histoire de la vie privée*, P. Aries & G. Duby (eds) Volume 4: *De la Révolution à la Grande Guerre,* M. Perrot (ed.), Paris Seuil,1987, 637 p.

[47] Zo blijkt uit de Amerikaanse rechtspraak bijvoorbeeld dat het thuis bekijken en bezitten van obscene films waarvan de verspreiding bij het publiek is verboden onder bescherming van het huisrecht valt. Of nog, dat het thuis vermaken van gasten door de maaltijd naakt op te dienen niet op dezelfde wijze kan worden verboden als het openhouden van restaurants en bars waar naakt wordt gedanst.

het bijzondere privacygehalte dat aan de woonst wordt gegeven maakt dat het betreden van de woonst door derden en in het bijzonder door politie en gerecht in principe streng wordt gereglementeerd.

De verhoudingen tussen de opaciteitsinstrumenten en de individuele vrijheid is ver van eenvoudig te noemen. Zo deze instrumenten in de eerste plaats om vrijheid bekommerd zijn is de relatie tussen beide toch ambigu. Opaciteitsinstrumenten kunnen er immers toe leiden dat de toestemming van het individu moet onderdoen voor maatschappelijke belangen.[48] Opaciteitsinstrumenten zijn essentieel normatief in de zin dat de (grond)wetgever door hun gebruik, in de plaats van het individu, keuzen maakt over wat wenselijk en onwenselijk is met betrekking de individuele vrijheid. Deze collectieve en normatieve dimensie van de opaciteitsinstrumenten verduidelijkt de complexe verhoudingen tussen de rechten van de mens en de individuele vrijheid. Het schadebeginsel als criterium om ontoelaatbare schendingen van de individuele vrijheid te identificeren, moet wijken voor een meer formeel criterium.[49] Een *ad hoc* belangenafweging wordt vervangen door een categorische.[50] Opaciteitsinstrumenten maken de afloop van conflicten meer voorspelbaar: de belangenafweging zou op deze manier (op voorhand) in het voordeel van het individu zijn beslecht.[51]

Nochtans is het niet vanzelfsprekend dat een categorische belangenafweging altijd in het voordeel van de groots mogelijke bescherming van de individuele vrijheid speelt. Dit laatste zal bijvoorbeeld niet het geval zijn wanneer (constitutionele) teksten intrusies in de woning voorzien op voorwaarde van een huiszoekingsbevel. Daarom is het juister om de nadruk te leggen op de normatieve eerder dan op de rechtsbeschermende functie van de opaciteitsinstrumenten. Met zulke instrumenten stelt de (grond)wetgever duidelijke en harde normen. Keuzen over de manier waarop vrijheidsbelangen moeten worden afgewogen aan andere belangen worden in abstracto gemaakt. Dit werkt complexiteitsreducerend. Natuurlijk kan de reductie van complexiteit ook volledig ten nadele van de vrijheid worden gerealiseerd, maar dat zou volledig haaks staan op de geest van de Westerse democratische rechtsstaat zoals we die hierboven al beschreven. Deze hypothese kan dus niet ongenuanceerd *au sérieux* genomen worden.
Hieraan weze nog toegevoegd dat de opaciteitsinstrumenten niet noodzakelijkerwijs de vorm moeten aannemen van een mensenrechtelijke bepaling in een nationale of internationale grondwettelijke tekst. Het instituut van de onderzoeksrechter bijvoorbeeld, dat wordt geregeld door het straf(proces)recht is een mooie illustratie van een opaciteitsinstrument in de mate dat het een duidelijke en harde keuze belichaamd betreffende de bescherming van de persoonlijke levenssfeer. In common law systemen bestaat zo'n instituut echter niet. En zelfs de grondwetten van continentaal-Europese landen (België en Nederland) houden het zwijgen over de onderzoeksrechter niettegenstaande zijn positie in het strafprocesrecht cruciaal is. Er is strikt genomen geen fundamenteel recht op een strafrechtelijk onderzoek gevoerd door een onderzoeksrechter, maar er bestaat wel een geheel van regels dat zo'n recht doen bestaan.

Macht kanaliseren via instrumenten van transparantie
De tweede set instrumenten is verbonden met de principes van de democratische rechtsstaat die strekken tot het beperken van de staatsmacht door het ontwerpen van mechanismen van controle door de burgers, andere staatsmachten en speciaal daartoe opgerichte organen (en niet, zoals de eerste set, door het trekken van grenzen aan de staatsmacht door de erkenning

[48] Een mooi voorbeeld wordt ons gegeven door de bepalingen van de Europese privacyrichtlijn 95/46 die een publiekrechtelijk regime in het leven roept waarvan niet kan worden afgeweken door een contract van privaatrechtelijke aard. Als een gevolg hiervan is een overeenkomst waarbij een datasubject afstand doet van sommige van zijn rechten onder de richtlijn nietig. Zelfs indien we verder zullen argumenteren dat *data protection* vooral van een transparantie-instrument is, stelt het toch perken en limieten die de uitdruking zijn van 'harde' keuzen.
[49] J. Ravanas, noot bij Cour de Cassation (Fr.), 5 maart 1997, *Recueil Dalloz*, (Cahier Jurisprudence), 1998, vol. 34, (474-476), 475
[50] *Ibid.*
[51] *Ibid.* : 'Que la liberté devienne un droit, la protection en sort renforcée'.

van een private sfeer). Deze instrumenten hebben als gemeenschappelijk kenmerk dat zij trachten publieke (en private) spelers te dwingen tot *good practices* door te focussen op de transparantie van besluitvormingsprocessen die uiteraard een *conditio sine qua non* voor accountability en een verantwoording verschuldigd en afleggend bestuur. Het systeem van *checks and balances* installeert bijvoorbeeld de wederzijdse transparantie van de staatsmachten, terwijl de *accountability* van het bestuur t.a.v. de burgers een vrije en gemakkelijke toegang tot overheidsinformatie en het bestaan van laagdrempelige controle en participatieprocedures veronderstelt. Terzake kunnen eveneens onafhankelijke gespecialiseerde organen of watchdogs worden opgericht die de opdracht hebben het doen en laten van de overheid in een bepaald gebied te controleren.

De opaciteitsinstrumenten zijn van een heel andere orde dan de transparantie-instrumenten. Terwijl de laatste gericht zijn op de controle en de kanalisering van legitieme machtsuitoefening strekken de eerste tot de bescherming van burgers tegen een illegitieme en excessieve machtsuitoefening. De laatste houden rekening met het feit dat de verleidingen tot machtsmisbruik en -afwending groot zijn en maken het voor de burgers en speciaal daartoe opgerichte watchdogs mogelijk om de wijze waarop macht wordt aangewend na te gaan. Transparantie-instrumenten richten tegenmachten op. De opaciteitsinstrumenten bepalen dan weer wat in principe niet tot het bereik van de overheid en private actoren behoort, en derhalve meteen ook wat zo belangrijk wordt geacht dat het moet worden afgeschermd tegen publieke en private inmengingen. Aan de ene kant is er een gereguleerde aanvaarding, aan de andere vinden we verbodsbepalingen, die doorgaans uitzonderingen voorzien.

De eerste categorie, de transparantie-instrumenten, valt in grote mate samen met het administratief recht dat, althans in principe, de *accountability* van publieke actoren organiseert en bevordert. Dezelfde logica kan worden gevonden in het arbeidsrecht. Zonder te tornen aan de machts- en gezagsrelaties tussen werkgevers en werknemers voorziet het arbeidsrecht immers een soort van procedurele rechtvaardigheid die vorm krijgt doorheen de vooropstelling van talrijke regels die moeten worden gevolgd wanneer terzake beslissingen worden genomen. Omwille van de machtsonevenwichten tussen werkgevers en werknemers kunnen deze beslissingen maar moeilijk worden gecontesteerd, maar ze kunnen wel worden geëvalueerd op het vlak van de naleving van de procedures.
De tweede categorie, de transparantie-instrumenten is bijzonder bruikbaar wanneer het erop aankomt de verhoudingen tussen private actoren te regelen. Het vertrekpunt voor de benadering van zulke verhoudingen is natuurlijk dat deze actoren dezelfde rechten en vrijheden hebben en dus in principe zelf in staat zijn tot de bescherming van hun belangen. De individuele toestemming en de *ad hoc* belangenafweging zijn terzake dan ook pertinente instrumenten. Enkel na een zorgvuldige rationele reflexie en ondersteund door harde argumenten, bijvoorbeeld met betrekking tot ongelijke machtsverhoudingen, zal de overheid (de wetgever) hierin mogen tussenkomen door middel van 'harde normen' of 'keuzen' die het gevolg zijn van een categorische afweging van belangen.

8. Privacy als een opaciteitsinstrument, een instrument voor het trekken van grenzen

Nederland
In de Grondwet staan meerdere privacyrelevante bepalingen. Zo bevat artikel 12 Grw. een duidelijk verbod op het schenden van de woning en stelt artikel 13 Grw. grenzen aan schendingen van het communicatiegeheim. Van allergrootst belang is natuurlijk artikel 10 Grw. Deze bepaling luidt: "1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake 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".

Wij zijn erg gewonnen voor dergelijke bepalingen die ertoe strekken het individu te beschermen tegen ongebreidelde machtsuitoefening door het trekken van grenzen. Deze Grondwetsbepalingen worden verder geëxpliciteerd in het strafwetboek en ademen door in de publiekrechtelijke en strafprocesrechtelijke regelingen van allerlei overheidsbevoegdheden die aan bepaalde voorwaarden worden gekoppeld teneinde de geest van de Grondwetsbepalingen te respecteren.

Het Europees Verdrag voor de Rechten van de Mens

Toch gaat onze voorkeur uit naar de formulering van het privacygrondrecht in het Europees Verdrag voor de Rechten van de Mens (EVRM).[52] Ten eerste ontbreekt het in Nederland aan een grondwettelijk hof, waardoor de grondwetsbepalingen niet echt leven en nieuwe evoluties buiten het bereik blijven van de grondwettelijke bescherming.[53] Bovendien maakt het tweede lid van artikel 8 EVRM beter duidelijk dat aan grondrechtelijk beschermde belangen een hoge positie toekomt en dat het niet volstaat een wet te stemmen om eraan op legitieme wijze afbreuk te doen. Zelfs al is een privacybeperking wettelijk voorzien en voldoet zij aan de doeleinden die in artikel 8 EVRM zijn opgesomd, dan nog is vereist dat de beperking *noodzakelijk is in een democratische samenleving* en niet verder reikt dan wat strikt noodzakelijk is.[54] Deze voorwaarde "brengt noodzakelijkerwijze een ultieme belangenafweging met zich, een moment van waardeoordeel, dat noch door exegese van de tekst, noch door het hanteren van logische regels wordt beheerst".[55]

O.i. vormt zo'n voorgeijkte belangenafweging de essentie van het grondrechtelijke denken.[56] Te weinig laten de Europese rechters zich hiertoe verleiden en te veel verkiezen zij de veiligere toetsing aan de eis van legaliteit (is er een wet?).[57] Een actieve wetgever met grote zorg voor veiligheid kan uit deze lakse opstelling zijn voordeel doen en via wetgeving vergaande bevoegdheden creëren.[58]

9. Gegevensbescherming als een instrument voor transparantie

De beginselen van data protection

Het privacygrondrecht werd in de voorbije decennia aangevuld met een grondrecht op bescherming van persoonsgegevens. Dit *data protection* grondrecht wordt in ons land doorgaans geconstrueerd en geconcipieerd als deelaspect van het grondrecht op bescherming van de persoonlijke levenssfeer. In andere landen zoals Italië, Portugal en Spanje wordt het

---

[52] "1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen".

[53] Over de problemen in verband met de beperkte reikwijdte van artikel 13 Gw.: W.A.M.Steenbruggen, 'Dodo of feniks: het communicatiegeheim in het digitale tijdperk?' *Mediaforum*, 2003-4, via IvIR.nl

[54] Over deze voorwaarde: K. Rimanque, 'Noodzakelijkheid in een democratische samenleving -een begrenzing van beperkingen aan grondrechten', in *Liber Amicorum Frédéric Dumon,* Antwerpen, Kluwer Rechtswetenschappen, 1983, deel II, p. 1220. Deze auteur onderscheidt *pertinentie* en *proportionaliteit* (p. 1228).

[55] K. Rimanque, *o.c.*, 1229. Zie tevens p. 1227 waar de auteur er op wijst dat de toetsing van de noodzakelijkheidsvoorwaarde door het Hof niet beperkt is tot een marginale toetsing.

[56] Cf. S. Gutwirth, 'De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens', *Tijdschrift voor Privaatrecht*, 4/1993, 1409-1477.

[57] Deze vastelling verdient evenwel grondigere bestudering, waarvoor hier niet de ruimte is. Een uitzondering hierop vormt de reflectie over het begrip noodzaak in het Europees arrest Klass en de toepassing van een op noodzaak gesteunde redenering in Hof 's-Hertogenbosch 2 juli 1986, *NJ* 1987, 51 (e moet een noodzaak bestaan om van cameratoezicht gebruik te maken. Dit betekent dat het gebruik van permanent cameratoezicht op de werkvloer –ook al is dit kenbaar voor de werknemer– waarbij de gehele bedrijfsruimte in de gaten wordt gehouden en niet is gebleken van enige noodzaak hiertoe als onrechtmatig kan worden aangemerkt).

[58] Dit blijkt goed uit de presentatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002 door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. In de mededeling over deze wet heet het dat 'met de nieuwe wet wordt voldaan aan de eisen die het nationale en internationale recht stellen. Zo vloeit uit het Europees Verdrag van de Rechten van de Mens (EVRM) voort dat het werk van inlichtingendiensten voorzienbaar en kenbaar moet zijn voor de burger. Deze transparantie vormt een belangrijk element in de nieuwe wet'. Over de vergaande reikwijdte van de gecreëerde bevoegdheden wordt met geen woord gerept.

daarentegen afzonderlijk verwoord in de Grondwet,[59] een voorbeeld dat terecht ook gevolgd werd door de opstellers van artikel 8 van het Handvest van de Grondrechten afgekondigd door de instanties van de Europese Unie te Nice op 7 december 2000.
De uitgangspunten van het *data protection* grondrecht zijn niet in een regel te vatten. In het kort komen ze neer op doelbinding, transparantie en het toekennen van rechten aan personen waarover gegevens worden verwerkt. Onder doelbinding wordt begrepen dat het (wettig) doel waarvoor persoonsgegevens worden verzameld de meetlat is voor het beoordelen van de legitimiteit van hun gebruik. Verder gebruik zal zijn toegestaan als het niet onverenigbaar is met het doel waarvoor de gegevens zijn verzameld. Een belangrijk onderdeel van het transparantiebeginsel is de verplichting voor degene die verantwoordelijk is voor de verwerking van de persoonsgegevens om hierover de nodige informatie te verstrekken aan de betrokkenen. De 'geficheerde' persoon beschikt tenslotte over welbepaalde concrete subjectieve rechten zoals dit op kennisgeving, op inzage en correctie, en op ondersteuning bij de afdwinging van zijn rechten door een onafhankelijke toezichthouder (in Nederland het College Bescherming Persoonsgegevens, *infra*).
Deze uitgangspunten worden in steeds grotere mate door het Straatsburgse Hof beschouwd als centrale uitgangspunten bij de toepassing van artikel 8 EVRM op problemen inzake informationele privacy (*supra*). Zij zijn tevens gecodificeerd in internationale teksten. Behoudens het Handvest van de Grondrechten in de Europese Unie, waarvan al sprake, zijn ze ook opgenomen in de bindende Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens,[60] en in het door Nederland geratificeerde en in de schoot van de Raad van Europa onderhandelde Verdrag 108 van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens.[61]

De Wbp

De belangrijkste regels voor het vastleggen en gebruiken van persoonsgegevens zijn in Nederland vastgelegd in de Wet bescherming persoonsgegevens (Wbp).[62] De Wbp heeft betrekking op alle gebruik - 'verwerkingen' - van persoonsgegevens, van het verzamelen ervan tot en met het vernietigen van persoonsgegevens.[63] Dit ruime begrip 'verwerking', alsmede het zeer ruime begrip 'persoonsgegevens'[64] verklaart waarom de Wbp in beginsel op elke elektronisch ondersteunde opsporingsmaatregel van toepassing is. Dat kan tellen voor de rechtsbescherming. Bovendien kan de wet worden ingeroepen tegen ongeveer elke denkbare persoon of instantie, van de buurman die hatelijke telefoontjes pleegt, over de disco die gastenlijsten aanlegt tot het gemeentebestuur dat camera's laat plaatsen. Dit ruim toepassingsveld verklaart het bovensectorale karkater van de Wbp met algemene normen over de verwerking van persoonsgegevens die voor alle rechtsgebieden gelden, derhalve - tenzij uitgezonderd - zowel doorwerken in het bestuursrecht, het privaatrecht als in het strafrecht.[65]

---

[59] Art. 10, tweede en derde lid Grw. noemen het recht op bescherming van persoonsgegevens, maar door de opname van dit recht in art. 10 Grw. wordt aangegeven dat het niet gaat om een zelfstandig grondrecht.
[60] Richtlijn 95/46/EG, *PbEG* 1995, nr L 281.
[61] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 28 januari 1981, Trb. 1988 7 en Trb. 1993, 116 en 157 (ratificatie)
[62] Wet bescherming persoonsgegevens, Stb. 2000, 302 en de Wet van 5 april 2001 tot wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens, Stb. 2001, 180. Deze wet is op 23 november 1999 unaniem door de Tweede Kamer aangenomen en op 3 juli 2000 door de Eerste Kamer aanvaard. De wet is op 1 september 2001 van kracht geworden.
[63] Artikel 1, onder b, Wbp omschrijft ‘verwerken’ als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens en bevat zodoende een zeer ruime omschrijving van verwerken. In de Wbp genoemde handelingen die in ieder geval als verwerkingen zijn te beschouwen zijn: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen, vernietigen, verkrijgen, doorvoer, en doorgifte.
[64] Een ruime definitie van het begrip persoonsgegevens wordt op internationaal terrein gegeven in zowel artikel 2, onder a, van het Straatsburgse Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegeven als in artikel 2, onder a, van de algemene EG-Privacyrichtlijn. Het eerst vermelde verdrag spreekt in artikel 2, onder a, over: “‘personal data’ means any information relating to an identified or identifiable individual (‘data subject’)”.
[65] G. Overkleeft-Verburg, 'Wet bescherming persoonsgegevens. Continuïteit en verandering', *Nederlands juristenblad*, afl. 2001/29. Vanuit grondrechtelijk oogpunt vervult de Wbp meerdere functies. Afgezien van de concretisering van

De Wbp valt in een aantal onderdelen uiteen. De kern van de regeling wordt gevormd door hoofdstuk 2, de inhoudelijke normen betreffende de verwerking van persoonsgegevens. Dit hoofdstuk bevat een opsomming van plichten van de persoon of instelling die persoonsgegevens verwerkt. Een vuistregel is dat de verantwoordelijke zelf onderzoekt of de gegevens voldoende juist, nauwkeurig en actueel zijn.[66] Een andere vuistregel vormt het reeds besproken doelbindingsprincipe.[67] Een opvallende verbodsbepaling vormt artikel 16: in beginsel is verboden de verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Hetzelfde verbod geldt, aldus artikel 16 Wbp, voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
Tegenover de plichten van de persoon of instelling die gegevens verwerkt staan rechten voor de betrokkene (geregistreerde). Deze beschikt over een recht op actieve informatieverstrekking door of namens de verantwoordelijke, alsook een recht op inzage, correctie en verzet zoals is vastgelegd in de hoofdstukken 5 en 6, met de mogelijkheid van uitzonderingen in artikel 43 Wbp. De wet bevat verder nog een aansprakelijkheidsregeling,[68] en een regeling voor de doorgifte van persoonsgegevens naar landen buiten de Europese Unie.[69]

Een kerngedachte van het *data protection* grondrecht luidt dat de materie zo complex is voor de burger dat het traditionele, reactieve systeem van rechtshulp (rechtsers, ombudsman, klachtencommissie, ...) moet worden aangevuld met een 'pro-actief systeem' van gratis rechtshulp door een onafhankelijk orgaan, met politiebevoegdheden, dat waakt over de toepassing van de gegevensbeschermingswet en via vergunningsplichten toeziet op verwerkers van gegevens. Alle Europese *data protection* wetten bevatten daarom een hoofdstuk over de instelling, taken en bevoegdheden van deze onafhankelijke toezichthoudende commissies. Zo ook de Wbp. Het College bescherming persoonsgegevens (Cbp) houdt, krachtens de Wbp, toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Bij het Cbp moet het gebruik van persoonsgegevens worden gemeld, tenzij hiervoor een vrijstelling geldt. Het Cbp adviseert de regering en organisaties over de bescherming van persoonsgegevens en onderwerpen die daarmee samenhangen. Het Cbp toetst gedragscodes en bemiddelt in geschillen tussen burgers en gebruikers van persoonsgegevens. Op eigen initiatief of op verzoek van een belanghebbende kan het Cbp onderzoeken of de manier waarop persoonsgegevens in een bepaalde situatie zijn gebruikt, in overeenstemming is met de wet en daaraan zonodig gevolgen verbinden. Voor in gebreke blijven bij de melding kan een boete worden opgelegd. Bij overtreding van de wet of daarop gebaseerde regelingen kan het Cbp overgaan tot bestuursdwang of een dwangsom opleggen.
Het grote belang van de Europese onafhankelijke privacyorganen ligt o.i. niet in dergelijke bestuursrechtelijke taken. Hun belangrijkste rol is die van privacywaakhond vergelijkbaar met een soort consumentenbond. Vooral het Nederlandse Cbp heeft zich laten kennen als een zeer

---

grondrechtenaanspraken geeft de wet in particuliere relaties horizontale werking aan de privacygrondrechten, terwijl deze in de relatie overheid-burger tevens als formeel-wettelijke beperkingsgrondslag ex artikel 10, eerste lid Grw. fungeert.

[66] Art. 11, lid 2 Wbp.

[67] Art.7 en 9 Wbp.

[68] In verband met aansprakelijkheid voor privacyschendingen zijn van belang de artt. 49 en 50 Wbp. In art. 49 Wbp wordt een recht op schadevergoeding toegekend wanneer in strijd is gehandeld met de bepalingen van de Wbp. In art. 50 Wbp wordt de mogelijkheid gegeven tot het vorderen van een verbod om te voorkomen dat (nog verder) in strijd met deze wet wordt gehandeld. De bepaling van art. 49 Wbp beoogt – behoudens met het oog op het vereiste van toerekenbaarheid – geen afwijking van het geldende aansprakelijkheidsrecht. In beginsel zal schending van de verplichtingen uit de Wbp een handelen in strijd met een wettelijke plicht als bedoeld in art. 6:162 lid 2 BW opleveren. Daarbij verdient het opmerking dat de schade bij een inbreuk op de privacy van een burger veelal uit niet-vermogensschade (ook wel immateriële schade) bestaat. Deze schade komt voor vergoeding in aanmerking. Art. 49 lid 2 Wbp bepaalt dat voor andere schade dan vermogensschade een vergoeding naar billijkheid wordt toegekend.

[69] Hoofdregel is dat persoonsgegevens alleen mogen worden doorgegeven naar derde landen met een passend beschermingsniveau. Buiten die gevallen is doorgifte alleen toegestaan op basis van een wettelijke uitzondering of met vergunning van de Minister van Justitie. De afgifte van een vergunning vindt plaats nadat het CBP daarover advies heeft uitgebracht.

alerte waakhond die door middel van uitstekende rapporten en een goede persvoorlichting het Nederlandse én Europese publiek tracht te sensibiliseren over privacyproblemen en de mogelijkheden van de Wbp en de Europese richtlijn. Op deze rol komen we terug.

Twee opmerkingen

Een eerste opmerking betreffende *data protection* in Nederland betreft de vindplaats. Naast de Wbp bevatten andere wetten eveneens *data protection* bepalingen. Het klinkt wat ongewoon, maar de Wet op de inlichtingen- en veiligheidsdiensten 2002 vormt hiervan een goed voorbeeld. Deze wet spelt niet alleen nieuwe (en oudere) opsporingsmaatregelen uit voor de genoemde diensten, doch geeft tevens aan hoe de burger zich tot deze diensten kan wenden met (bijv.) een verzoek tot kennisname van zijn of haar persoonsgegevens.[70] Het laat zich raden dat de AIVD en MIVD niet in alle gevallen 'hun' geheimen en gegevens dienen prijs te geven, doch dat wordt ook niet vereist door *data protection*. Andere, wat meer onschuldige vindplaatsen van *data protection* principes in Nederland zijn de Wet politieregisters, de Wet gemeentelijke basisadministratie persoonsgegevens, de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag en de Kieswet.[71] Bestuursrechtelijk kan men de *data protection* principes ook in verband brengen met de beginselen van goed bestuur.[72] Dat wordt goed geïllustreerd door artikel 6 Wbp dat bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Het gebruik van open normen zoals behoorlijk en zorgvuldig maakt het mogelijk om binnen een breder kader (grondrechten, verbodsbepalingen, onverenigbaarheden, ...) fijnmaziger te reguleren en te normeren. Niemand weet op voorhand wat behoorlijk of zorgvuldig is, maar in een concreet geval of conflict kan dat, al dan niet met de hulp van een onafhankelijk toezichtorgaan, worden uitgezocht.

Een tweede aansluitende opmerking betreft het ethisch karakter van *data protection*. De Wbp is geen wet van verbieden en bestraffen. De hoger besproken bepaling die de verwerking van gevoelige gegevens verbiedt (artikel 16 Wbp) is een opvallende uitzondering, die bovendien bij nadere lectuur van de wet wordt uitgehold door talrijke uitzonderingen. De kracht van de Wbp schuilt niet in het bewerkstelligen van materiële rechtvaardigheid. De wet plaatst nergens een taboe op gegevensverwerking, doch ademt de boodschap uit dat verwerking van gegevens over anderen is toegelaten mits een aantal spelregels worden gerespecteerd. De Wbp ziet op procedurele rechtvaardigheid en op de correcte bejegening van en de uitleg aan geregistreerde burgers met de wens hun bereidheid op te schroeven om een systeem te accepteren waarbinnen anderen (overheidsdiensten, bedrijven, particulieren) een recht hebben 'hun' gegevens te verwerken en beslissingen te nemen die een weerslag hebben op hun informationele zelfbestemming. De idee van procedurele rechtvaardigheid verklaart de nadruk op transparantie in de Wbp. Deze transparantie wordt op verschillende wijzen bereikt: door de actieve informatieplicht, door het bekomen van toestemming voor het verwerken van gegevens en door het primaat van het doelbindingsprincipe dat maakt dat de geregistreerde er op kan vertrouwen dat gegevens niet worden aangewend voor doeleinden die hij niet kent. De idee van procedurele rechtvaardigheid verklaart ook waarom in de Wbp weinig zwart-wit bepalingen staan of verbodsbepalingen. Duidelijke antwoorden geven op de vraag 'mag dit of niet?' is niet de sterkste kant van de Wbp. Dat moet de verantwoordelijke zelf maar uitmaken, eventueel gecontroleerd door de geregistreerde die het Cbp of de rechter kan inschakelen. In vergelijking met de wetten in andere lidstaten van de Unie, is vooral de Wbp, in feite een erg bedrijfs- en overheidsvriendelijke kopie van de Europese richtlijn, in dit bedje ziek. De tekst zet zwaar in op de idee van zelfregulering binnen sectoren via gedragscodes en laat grote delen van de maatschappelijke activiteit rond persoonsgegevens rusten op de soepele criteria

[70] Deze wet legt de AIVD en MIVD op om gegevens die niet meer actueel zijn te vernietigen (art. 43) en laat hen alleen toe om gegevens te verzamelen van personen 'die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de democratische rechtsorde' (art. 13).

[71] Cf. art. 2 Wbp.

[72] Zieover data protection als *good information practices*, het reeds vermelde werk van Peter Blok. Arbeidsrechtelijk spreken we van beginselen van goed werkgeverschap.

voor een rechtmatige gegevensverwerking in artikel 8 Wbp en in het bijzonder op die ene in feite weinigzeggende bepaling volgens dewelke een gegevensverwerking toelaatbaar is wanneer ze 'noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert'.[73] Deze bepaling ademt de in de sfeer van de grondrechten onwenselijke gedachte uit dat alles een kwestie is van afweging van gelijke belangen,[74] doch valt te billijken met de overweging dat niet elke (on)rechtmatige verzameling dan wel verstrekking van (persoons)gegevens een inbreuk vormt op de grondrechten

Het procedureel georiënteerde karakter van de Wbp verklaart verder het belang van de toestemming als geldige grond tot verwerking. Dit verklaart tevens de klemtoon op niet-materiële noties zoals 'toereikend, ter zake dienend en niet bovenmatig' (art. 11 Wbp.). Wij zijn geenszins tegen deze oriëntatie op procedure, doch het spreekt vanzelf dat zonder hardere, materiële normen of grenzen er een element ontbreekt. Onze hypothese is dat hiervoor wellicht bewust voor werd gekozen.[75] Het resultaat is een beschermingsregime in de wet met een kameleontische aard die ervoor zorgt dat de enkele open materiële normen uit de Wbp in de toepassing sectorspecifiek worden ingekleurd, onder invloed van de grondslagen van de verschillende rechtsgebieden. De criteria voor een rechtmatige gegevensverwerking in artikel 8 Wbp vormen daartoe het aanknopingspunt.[76]

10. Een evenwichtige privacypolitiek steunt op twee pijlers

Algemeen

Hierboven schreven we dat de democratische rechtsstaat zich bedient van twee rechtsinstrumenten, die we voor het gemak opaciteits- en transparantie-instrumenten hebben genoemd. De combinatie van beide instrumenten werd nodig geacht om enerzijds macht te begrenzen en anderzijds macht te kanaliseren. Het spreekt voor zich dat deze combinatie ook moet worden gehanteerd in de veelkleurige moderne privacyproblematiek. Er is immers geen reden om te vermoeden dat achter elektronische opsporingsmaatregelen of verwerkingen geen krachtenspel schuilt of om ervan uit te gaan dat de krachten die aan het werk zijn zichzelf zullen begrenzen of reguleren. Daarvoor staat er te veel op het spel en wat nu precies ook op het spel moge staan, het zal alleen maar toenemen in onze zich ontplooiende informatiesamenleving waarin eenieder steeds meer digitale sporen achter zich laat.
De combinatie van privacy gedacht als opaciteitsinstrument en gegevensbescherming als transparantie-instrument heeft alles om deze dubbele rechtstatelijke taak van het begrenzen en het kanaliseren waar te maken.
Veeleer dan ons over te geven aan praktische argumenten en onderbouw, wensen we via een praktisch voorbeeld aan te geven waarom vandaag de combinatie niet voldoende gerealiseerd wordt. Kortweg luidt onze stelling dat aan het tweede instrument teveel zorg voor de problemen van de informatiemaatschappij wordt overgelaten en dat ondersteuning door grotere inzet van het eerste instrument wenselijk is.

Doorgifte passagiersgegevens aan de Verenigde Staten

In 2002 geraakte bekend dat de Amerikaanse overheid voor nationale veiligheidsdoeleinden op grond van wettelijke verplichtingen aangenomen na de gebeurtenissen van 11 september 2001, vliegtuigmaatschappijen vraagt om passagiersgegevens te verstrekken uit de

[73] Art. 8f Wbp.
[74] Deze gedachte is fout. Grondrechten geven precies aan dat in sommige gevallen aan bepaalde belangen een hoger gewicht toekomt. In de belangenafweging vertaalt zich dit door een meer principiële toets waarbij in beginsel veel gewicht toekomt aan de grondrechtelijke beschermde belangen. Zie reeds hierboven.
[75] Onze stelling luidt dat hiervoor goede argumenten bestaan in het licht van de gelijkstelling van *data protection* met transparantie-instrumenten en beginselen van behoorlijk bestuur.
[76] G. Overkleeft-Verburg, 'Wet bescherming persoonsgegevens. Continuïteit en verandering', *Nederlands juristenblad*, afl. 2001/29.

reserveringssystemen van de vluchten op de VS. Naast naam- en adresgegevens betreft het o.a. gegevens over reisroute, betaalwijze, creditcard nummer, eventuele medische informatie en gegevens over deelname aan *frequent flyer* programma's. Tevens willen de autoriteiten toegang tot de reserveringssystemen op Europees grondgebied. Deze gegevens worden opgeslagen in een centrale database in de VS.[77]
Het veiligheidsproject dat steunt op de idee van het aanleggen van profielen van verdachte reizigers die worden geweerd, heeft veel protest veroorzaakt.[78] Op een hoorzitting van het *Committee on Citizens' Freedoms and Rights* in het Europees Parlement over de problematiek *traveller profiling*, presenteerde de mensenrechtenorganisatie EPIC een document over de grondrechtenrisico's voor zowel Europese als Amerikaanse reizigers: omdraaien van het vermoeden van onschuld, veralgemeend spioneren, delen van 'third party data', langdurig bijhouden van passagiersgegevens, gebrek aan toegang, 'judicial remedies' en publiek debat.[79]
Het volstaat je de machteloosheid in te beelden van een gehaaste zakenman die plots geen vluchtticket krijgt te Schiphol omdat hij vele zakencontracten heeft in Moslimlanden. Aan welke deur dient deze persoon te kloppen?
Zelf hebben we de indruk dat een groot deel van de Europese heisa, zeker in beleidsmiddens, te maken heeft met het gevoel door de Amerikanen te slim af geweest te zijn. Ogenschijnlijk hebben de Amerikanen immers geen al te grote data protection doodzonden gepleegd.
- Ondanks tekortkomingen in het Amerikaanse gegevensbeschermingsrecht, heeft de EU niet besloten tot een veto tegen gegevensdoorgifte naar de VS, doch deze onder voorwaarden toegelaten.[80]
- De Amerikanen hebben de Europese maatschappijen *gevraagd* om de passagiersgegevens ter beschikking te stellen.
-Het verzamelen van gegevens in een databank met het oog op *matching* en profilering wordt in de Wbp en de Europese richtlijn niet verboden. Integendeel, de richtlijn zwijgt in alle talen over dergelijke operaties en werkt slechts een algemeen kader uit voor alle 'verwerkingen' zonder daarbij enige moeite te doen om risicovolle van niet-risicovolle verwerkingen te onderscheiden.
- Europa is geenszins gekant tegen veiligheidsmaatregelen zoals profilering. Integendeel, heel het instituut van Europol valt alleen te begrijpen als de uitdrukking van de wens om ook in Europa te komen tot *intelligence* en data-verrijking.[81] Dit spreekt eveneens uit de hoger besproken Nederlandse plannen om themaregisters mogelijk te maken en ook uit het Spaanse voorstel om een Europese variant te ontwikkelen van het Amerikaanse systeem van *traveller profiling*.[82]

De reactie van de gegevensbeschermingsorganen
M.b.t. dit dossier maken we een dubbele vaststelling: het Europese *data protection* systeem heeft de rol gespeeld die het moet spelen doch dit is op zich niet voldoende om het dossier op

---

[77] Cf. Cbp, 'Verstrekking passagiersgegevens door luchtvaartmaatschappijen aan VS' bericht verspreid op 27 februari 2003 via http://www.cbpweb.nl/structuur/pag_nieuws.htm Een goede bespreking van het Amerikaanse systeem met juridische bronverwijzingen geeft: Europees Parlement, Resolutie van het Europees Parlement over de overdracht van persoonsgegevens door luchtvaartmaatschappijen bij transatlantische vluchten, Document nr. B5-0187/2003 (P5_TA-PROV(2003)0097), Notulen van 13 maart 2003, via http://www3.europarl.eu.int
[78] Voor een goede verslaggeving rond dit dossier: EPIC, 'Dossier: EU-US Airline Passenger Data Disclosure', via www.epic.org
[79] C. Laurant, 'Statement' Committee on Citizens' Freedoms and Rights, Justice and Home Affairs Public Seminar: *Data Protection since 11 September 2001: What Strategy for Europe?*, European Parliament – (March 25, 2003), (15p.) 9 via epic.org
[80] De Europese Unie (EU) -richtlijn verbiedt, op enkele uitzonderingen na (o.a. toestemming van de betrokkene, of een afdoende overeenkomst), export van persoonsgegevens naar landen die geacht worden een inadequaat privacy-beschermingsniveau te bieden. De Verenigde Staten van Amerika zijn naar de mening van de EU zo'n land en dus zou export van persoonsgegevens naar Amerika verboden zijn, behoudens voor zover een van uitzonderingen van toepassing is. Om dit gevolg te vermijden zijn de EU en de VS de zogeheten 'Safe Harbor Principles' (SHP) overeengekomen die adequate bescherming in Amerika zouden moeten waarborgen. Men leze: P. Blok, Botsende rechtsculturen bij transatlantisch gegevensverkeer, *Nederlands juristenblad*, 2001, p. 1607-1612; P. De Hert., 'European Data Protection and E-Commerce: Trust Enhancing?' in J.E.J., Prins, P.M.A. Ribbers, H.C.A. van Tilborg, A.F.L. Veth & J.G.L. van der Wees (eds), *Trust in Electronic Commerce*, Den Haag, Kluwer Law International, 2002, 171-230.
[81] P. De Hert, 'Europols databanken', *Vigiles. Tijdschrift voor politierecht*, 1996/3, 36-44.
[82] Initiative of the Kingdom of Spain with a view to adopting a Council Directive on the obligation of carriers to communicate passenger data, COUNCIL OF THE EUROPEAN UNION, Brussels, 25 March 2003 , (OR. es), 7161/03, 7p. te consulteren via http://www.statewatch.org/news/2003/mar/spainpassengers.pdf

een bevredigende wijze af te ronden. Deze vaststelling steunen we op een korte historiek van de genomen stappen. Na het bekend worden van het Amerikaanse initiatief volgde zeer snel een reactie. Het Cbp, tezamen met privacywerkgroep van de Europese nationale toezichthouders (de zgn. Artikel 29-werkgroep[83]) constateerde reeds in 2002 diverse problemen op het gebied van de bescherming van persoonsgegevens rond deze verstrekking aan de Amerikaanse autoriteiten. In oktober vertrekt een eerste kritiek op het initiatief met een verzoek tot bijsturing en aanpassing.[84] Begin 2003 wijst het CBP de Minister van Verkeer en Waterstaat op dit advies van de werkgroep. Ondertussen vinden over de verstrekking gesprekken plaats tussen de Europese Unie en de Verenigde Staten, ten dele op grond van het advies van de werkgroep. Dit resulteert in een gezamenlijke verklaring van de Europese Commissie en de Amerikaanse autoriteiten gericht is op het bereiken van een akkoord op grond waarvan het is toegestaan passagiersgegevens te verstrekken aan de Amerikaanse autoriteiten.[85] Hierop volgt een resolutie van het Europees parlement[86] en een brief van de Artikel 29-werkgroep met kritiek op de gang van zaken. In de brief van 13 juni 2003 uit de Artikel 29-werkgroep zich kritisch over de tot nu toe behaalde resultaten in het overleg tussen de Europese Commissie en de Verenigde Staten (VS), over de doorgifte van passagiersgegevens naar de VS door Europese luchtvaartmaatschappijen.[87] Persoonsgegevens mogen alleen doorgegeven worden naar landen buiten de Europese Unie (derde landen) als daar een adequaat beschermingsniveau aanwezig is. De werkgroep stelt dat het niveau van bescherming in de Verenigde Staten in dit geval niet voldoende is. De werkgroep is van oordeel dat de Verenigde Staten de passagiersgegevens alleen mogen gebruiken indien deze informatie noodzakelijk is voor de bestrijding van terrorisme. Van belang hierbij is dat er maar een beperkt aantal gegevens mag worden verstrekt en de bewaartermijn van deze gegevens verder beperkt dient te worden. De Artikel 29-werkgroep concludeert tevens dat er onvoldoende garanties zijn van de Amerikaanse autoriteiten dat deze bepalingen zullen worden nageleefd. De werkgroep adviseert de Europese Commissie dan ook met klem in de onderhandelingen met de Verenigde Staten te komen tot een systeem voor de verstrekking van passagiersgegevens dat past binnen de Europese privacywet- en regelgeving. Parallel met deze initiatieven verstuurt het Cbp in februari 2003 een brief naar de luchtvaartmaatschappijen die op de VS vliegen en de reisorganisaties.[88] In de brief wordt gewezen op de verplichting van de maatschappijen om hun klanten te informeren over de verstrekking van hun persoonsgegevens aan de Amerikaanse autoriteiten. Deze verplichting vloeit voort uit de Wet bescherming persoonsgegevens (artikelen 33 en 34), aldus het Cbp.
Op 2 september 2003 volgt (eindelijk) een doorbraak in dit dossier. Een woordvoerder van de Europese Commissie laat weten dat het Amerikaanse systeem onder de huidige voorwaarden onverenigbaar is met het Europees gegevensbeschermingsrecht en dat de Amerikanen niet in staat zijn om garanties te bieden voor de bescherming van de gegevens.[89] Ook de zorg dat de Amerikanen in het bezit van gevoelige gegevens zouden komen (of deze door matching zouden bekomen) werd niet passend beantwoord. In theorie wordt daarmee een groen licht gegeven voor sanctionering door de data protection autoriteiten van de luchtvaartmaatschappijen die met de doorgifte doorgaan. Op 22 september is er nieuw overleg

[83] De werkgroep ontleent haar naam aan artikel 29 van de EG-Privacyrichtlijn 95/46/EG. Alle toezichthoudende autoriteiten op het gebied van bescherming van persoonsgegevens van de Europese Unie nemen deel aan deze werkgroep, die een belangrijke rol speelt in de totstandkoming van Europees beleid. De werkzaamheden van de werkgroep leveren een bijdrage aan de ontwikkeling van Europese normen en gemeenschappelijke interpretaties en in een aantal gevallen ook aan de privacybewustwording op internationaal niveau.
[84] Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, aangenomen op 24 oktober 2002, 11647/02/ENWP 66 via http://europa.eu.int/comm/internal_market/privacy/docs/
[85] Joint Statement, Brussels, 17/18 February 2003 via http://www.cbpweb.nl/structuur/pag_nieuws.htm
[86] Europees Parlement, Resolutie van het Europees Parlement over de overdracht van persoonsgegevens door luchtvaartmaatschappijen bij transatlantische vluchten, Document nr. B5-0187/2003 (P5_TA-PROV(2003)0097), Notulen van 13 maart 2003, via http://www3.europarl.eu.int
[87] Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, aangenomen op 13 juni 2003, 11070/03/EN WP 78, via http://europa.eu.int/comm/internal_market/
[88] Cf. Cbp, 'Verstrekking passagiersgegevens door luchtvaartmaatschappijen aan VS' bericht verspreid op 27 februari 2003 via http://www.cbpweb.nl/structuur/pag_nieuws.htm
[89] Woordvoerder Reijo Kemppinen aangehaald in 'EU: U.S. Anti-Terror Flight Rules Breach Privacy' 2 september 2002 via http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=3374162

gepland tussen Europees Commissaris bevoegd voor douanezaken, Frits Bolkestein met een niet nader genoemde *senior U.S. Homeland Security official*. In het persbericht wordt terecht twijfel geuit bij de mogelijkheden om luchtvaartmaatschappijen te beboeten. Deze maatschappijen moeten immers dan kiezen tussen een Europese sanctie of de Amerikaanse dreiging tot intrekking van hun vliegvergunning op Amerika.

Evaluatie

Evalueren we het voorgaande dan valt op dat het *data protection* systeem alert reageert op nieuwe problemen en dit zowel op nationaal als op supranationaal niveau. Het zou ons te ver brengen om dit allemaal exhaustief te brengen, doch ondanks de tegenstellingen tussen de Amerikaanse en Europese invulling van *data protection* schijnt dit rechtsssysteem de *common ground* te vormen voor de transatlantische gesprekken die aan de gang zijn. Ook dat toont de kracht van *data protection* aan.

Toch blijkt het systeem van *data protection* de zaak niet helemaal te kunnen klaren. Er is een politieke opvolging nodig om de druk op de ketel te houden. In het bijzonder valt op dat de gegevensbeschermingsautoriteiten het groen licht van een politiek gemandateerde (Frits Bolkestein) om de handhavingsmaatregelen waarover ze beschikken, in te zetten. Bovendien is het dan nog maar de vraag of ze deze wel wel degelijk toepassen.[90]

Tussen de lijnen door hebben we al aangegeven waar het echt probleem zit. In het streven naar algemeengeldigheid gaat *data protection* voorbij aan de noodzaak te discrimineren en te begrenzen. Alles is een 'verwerking' wat wil zeggen dat het aanleggen van een adressenbestand en het maken van een profiel dezelfde status krijgt. Alles is een 'persoonsgegeven' wat maakt dat een foto van een persoon (erg veelzeggend en voldoende voor velen om een oordeel op te baseren) dezelfde waarde krijgt toegemeten als een geschreven stukje informatie over diezelfde persoon. De macht wordt op die wijze niet ernstig genomen. Hier past geen formele benadering, maar is meer nodig. De echte pijnpunten van machtsuitoefening (door de overheid of door private actoren) moeten worden gediscerneerd en bekeken in het licht van het tweevoudig instrumentarium begrenzing en kanalisering. Wat is het echte pijnpunt bij profilering? Zelfs ogenschijnlijk banale gegevens kunnen mits verrijking leiden tot risicovolle en discriminerende aanwendingen. De keuze van maaltijd op een vliegtuig of de achternaam zijn evidente indicaties voor religieuze achtergronden, doch de verwerking van passagiersgegevens wordt in principe niet in verband gebracht met het principieel verbod op verwerking van religieuze gegevens neergelegd in het hoger besproken artikel 16 Wbp. Wat is nog een pijnpunt in dit dossier? De VS vragen de luchtvaartmaatschappijen meewerking aan het systeem onder dreiging van intrekking van vliegvergunningen. Wil een samenleving duidelijk maken dat zelfs onder dergelijke zware dreiging geen meewerking mag worden verleend, dan is een zwaarder instrument vereist dan *data protection*. Een profielverbod of een verbod tot medewerking aan profilering in het Wetboek van Strafrecht zou een beter signaal vormen aan de luchtvaartmaatschappijen bij hun deliberatie over het Amerikaanse 'verzoek'.[91]

---

[90] De Italiaanse toezichthouder heeft de vliegtuigmaatschappij Alitalia verboden om nog verder persoonsgegevens te verstrekken. Het uitblijven van een vergelijkbaar initiatief door het Cbp heeft alvast geleid tot kamervragen (Tweede Kamer) aan minister van Justitie Donner. Cf. 'SP stelt vragen over privacy op vluchten VS', *Staatscourant*, 29 juli 2003, (nr. 143), 5.

[91] Niets belet evenwel om dit verbod in te schrijven in de Wbp zelf, bijvoorbeeld door een inlassing van een nieuwe bepaling die in de lijn van artikel 15 van de Europese richtlijn, maar dan strenger en explicieter voorwaarden koppelt aan het werken met profielen. De Wbp is niet helemaal vreemd aan de privacylogica van begrenzing (kanaliseren moet immers van een bepaalde grens verstrekken). Procudurele regels zoals de eis dat gegevens in regel niet aan derden mogen gegeven worden, kunnen mits verharding resulteren in duidelijke verbodsbepalingen. Ter vergelijking. Toen deze wet in werking trad werd duidelijk dat het erin vervatte verbod op het verstrekken van 'bijzondere gegevens' waaronder strafrechtelijke gegevens in strafdossiers en in automatiseringssystemen, implicaties had voor de praktijk. Tegelijk met de Wbp trad de 'Aanwijzing verstrekking van strafrechtelijke gegevens aan derden voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing Wbp)' in werking. De Aanwijzing bepaalt dat de verstrekking van strafrechtelijke gegevens aan derden niet langer op basis van de WOB geschiedt, maar moet voldoen aan de strenge eisen van privacybescherming in de Wbp. Ook de media worden als derden beschouwd en, waar de WOB aan de Wbp is aangepast, bevat artikel 10 lid 1 nu een absolute weigeringsgrond: er worden geen strafrechtelijke persoonsgegevens openbaar gemaakt, tenzij de persoonlijke levenssfeer daardoor kennelijk niet wordt geschaad. Dat betekent, zoals de Aanwijzing ook stelt, dat de WOB 'vrijwel nooit meer als basis kan gelden voor actieve dan wel passieve persvoorlichting over persoonsgegevens door het OM', behalve als het 'tot de taak van het openbaar ministerie behoort om in het kader van de behandeling van een strafzaak informatie aan de media te verstrekken'. Van een informatieplicht, zoals onder het WOB-regime (en dus ook onder de Richtlijn voorlichting opsporing en vervolging) is geen sprake meer. Informatieverschaffing

Andere 'ongelukkige' illustraties
We zouden nog andere voorbeelden kunnen geven van een te eenzijdige aanpak van actuele grondrechtenproblemen. Zo hebben we ons verbaasd over het niet gefundeerde vertrouwen bij de Belgische Cbp en bij het beleid in de Belgische Wbp als kader voor de problematiek van camerabewaking.[92] Dat in die wet het woord 'camera' niet valt en het filmen van mensen in niets wordt onderscheiden van meer gewone verwerkingen van persoonsgegevens (zoals het aanmaken van adressenlijsten) zet toch aan het denken. Het is alleszins nooit gezien: een problematiek die bijna dagelijks de pers haalt wordt gewoon genegeerd. In Nederland treft ons dan de ogenschijnlijk drukke activiteit van het Cbp rond controle door de werkgever van e-mails, maar de adviezen van het Cbp worden door geen enkele arbeidsrechter gevolgd of gebruikt en in die adviezen wordt ten onrechte een heel onduidelijk antwoord gegeven op de vraag op de essentiële vraag 'of een werkgever zonder enige individuele of collectieve kennisgeving e-mails mag controleren'.[93] Een zelfde ongewenste onduidelijkheid op het vlak van de vraag naar transparantie en begrenzing blijft hangen in de geschriften van het Cbp over zgn. zwarte lijsten en in het document 'Informatieblad Opnemen telefoongesprekken op de werkplek',[94] maar deze analyse kunnen we hier niet verder uitwerken. Wat we nodig achten is niet dat per problematiek een geheel nieuw en expliciet kader tot stand wordt gebracht, maar wel dat de kernvraagstukken eruit worden gelicht en dat waar nodig fundamentele keuzen of verboden worden geformuleerd. Het wetboek van strafrecht is een uitgelezen plek voor dergelijke *interdits fondamentaux*,[95] maar andere plekken zoals de Grondwet, het administratief-, arbeids- of privaatrecht zijn ook denkbaar. In een volgende paragraaf illustreren we dit.

11. Illustraties van een gewenste privacypolitiek

11.1. Spam & data retention
Onze eerste illustratie geeft goed aan in welke mate een problematiek die oorspronkelijk werd omkaderd door het gegevensbeschermingrecht kan uitkristalliseren en ondersteund worden door een logica van begrenzing. Eind mei 2002 koos het Europees parlement voor expliciete toestemming bij reclame-mail: opt-in bij zowel *spam* als *cookies*.[96] Daarmee kwam een einde aan een jarenlange onzekerheid over een vraagpunt dat door het gegevensbeschermingsrecht open was gelaten. Als gevolg van de keuze mogen bedrijven niet langer ongevraagd willekeurige burgers bestoken met e-mail en sms-jes. Consumenten moeten expliciet toestemming geven voor elektronische reclame. Het Europees Parlement is tegen de verwachting in akkoord gegaan met de richtlijn voor bescherming van persoonsgegevens bij elektronische communicatie die het verbod regelt. Men stond voor de keus van een systeem volgens opt-in (alleen e-mail versturen als iemand dat wenst) of opt-out (mail sturen mag, behalve als iemand aangeeft het niet te willen ontvangen). Bedrijven mogen wel bestaande klanten mailen, op voorwaarde dat ze duidelijk aangeven hoe consumenten een eind kunnen maken aan de mail. Eind 2003 moet de EU-richtlijn zijn omgezet in nationaal recht. De

---

aan de media is nu een bevoegdheid, geen verplichting. De Richtlijn zal dan ook in die zin worden aangepast en het ziet er naar uit dat het informeren van de media vele malen terughoudender zal zijn dan thans. Cf. C.H. Brants & C. Kelk, 'Kroniek van het strafrecht 2001', *Nederlandsch juristenblad*, 2002, Volume 77, Nr. 10, 456-467.

[92] P. De Hert & S. Gutwirth, 'Camera's en de noodzakelijke ontgroening van de privacywet', *Rechtskundig Weekblad*, 1994-95, (Nr. 4) 105-113; P. De Hert, O. De Schutter & S. Gutwirth, , 'Pour une réglementation de la vidéosurveillance', *Journal des tribunaux*, 21 September 1996, 569-579.

[93] P. De Hert, , 'Kenbaarheid van bedrijfscontrole op e-mail en internetgebruik. Factoren die spelen bij de chaos rond dit leerstuk', *Privacy & Informatie*, 2002, no. 1, 26-30.

[94] Dit informatieblad is bestemd voor de werknemers in organisaties waar telefoongesprekken worden opgenomen. Dit informatieblad gaat onder andere in op de volgende vragen als: 'Op welke grond is het opnemen van telefoongesprekken toegestaan?' en 'Welke rol speelt de ondernemingsraad?'. Cf. http://www.cbpweb.nl/documenten

[95] S. Gutwirth & P. De Hert, 'Een theoretische onderbouw voor een legitiem strafproces. Reflecties over procesculturen, de doelstellingen van de straf, de plaats van het strafrecht en de rol van slachtoffers', *Delikt en Delinkwent*, vol. 31/10, december 2001, 1048-1087.

[96] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector electronische communicatie (richtlijn betreffende privacy en electronische communicatie), *PB L* 201 van 31.7.2002, 37-47.

regeling gaat verder dan de Wbp die het gebruik van e-mail adressen alleen toestaat als het om reclame voor producten gaat die een duidelijk verband hebben met het oorspronkelijke doel waarvoor de adressen zijn verzameld. E-mail adressen lukraak doorverkopen is er dus, wettelijk gezien, niet meer bij.

Dezelfde Europese richtlijn gaat ook in op de privacyregels voor het bewaren van 'verkeersgegevens' (wie belt wanneer met wie?). Met betrekking tot de gegevensopslag mogen de lidstaten volgens het compromis de bescherming van persoonsgegevens opheffen ten behoeve van strafrechtelijke onderzoeken of de nationale of openbare veiligheid, maar alleen als dat 'in een democratische samenleving noodzakelijk, redelijk en proportioneel' is. Lidstaten kunnen voor het bewaren van gegevens voor een beperkte periode wetgevingsmaatregelen treffen, op voorwaarde dat deze stroken met het gemeenschapsrecht, met inbegrip van artikel 6 van het EU-Verdrag en het EVRM. Ook achter deze 'veiligheidsvriendelijke' bepaling schuilt o.i. een aanvulling op de klassieke gegevensbeschermingslogica. Enerzijds wordt de marge voor *data retention* beperkt door het inlassen van de voorwaarde van de 'beperkte periode', anderzijds wordt een expliciete keuze gemaakt voor deze opsporingsmethode zodat de burger weet waaraan hij zich kan verwachten bij het surfen op het Internet. Het lijkt cynisch om dit laatste een privacylogische illustratie te noemen, doch dat is precies wat we bedoelen. Deze vorm van machtsuitoefening wordt niet verboden, maar integendeel 'gekozen' en begrensd, waardoor het verweven ideaal van instrumentaliteit en rechtsbescherming wordt gerealiseerd. Niet heldere situaties worden vermeden. Te denken valt aan de inzet van zachte dwang door de politie om informatie die ze niet 'mogen' krijgen, toch te krijgen.[97]
Het ideale grondrechtenevenwicht is in deze problematiek zeker nog niet bereikt. De erkenning van een grondrecht op anonimiteit kan helpen om het dilemma tussen enerzijds de roep om veiligheid en anderzijds de bescherming van privacy en communicatievrijheid beter te onderkennen.[98] Door zo'n expliciete aanvaarding wordt een signaal gegeven dat normloosheid op het Internet niet kan en dat de consument met vertrouwen kan surfen. Tegelijkertijd kan dan worden vastgesteld onder welke voorwaarden anonimiteit snel kan worden opgeheven bij een verdenking van ernstige straffeiten of veiligheidsfeiten.

11.2 Cameratoezicht

Er bestaan zeer veel soorten identificatie- en spionagetechnieken, waarvan de combinatie de mogelijkheid opent van een doortastende controle en transparantmaking van de burger. Cameratoezicht is exemplarisch voor dit geheel. De genoemde controletechnieken hebben het (perverse) effect dat zij een subtiele, quasi onzichtbare, maar zeer doeltreffende gedragsbeïnvloeding mogelijk maken binnen het maatschappelijke veld. Opzichtelijke fysieke dwangmiddelen wijken voor fijnmazige 'zachte' controletechnieken, waardoor het volledige

---

[97] Zie voor een vergelijkbare visie op de voorstellen tot het creëren van data retention bevoegdheden geformuleerd door de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (Commissie-Mevis): C.H. Brants & C. Kelk, *l.c.*, 460. Vgl. Cf. Gerechtshof 's-Gravenhage, 15 november 2002, rolnummer 2200302102, via rechtspraak.nl. Het Gerechtshof 's-Gravenhage heeft in dit arrest bepaald dat de politie het IP-adres van de computer van een verdachte mag achterhalen zonder medeweten van verdachte. De politie mag echter niet zelf of via derden in computers snuffelen. Een IP-adres is een code die nodig is voor toegang tot internet, te vergelijken met een nummerbord van een auto. De politie heeft in deze zaak weliswaar het IP-adres van de computer van de verdachte achterhaald, maar heeft daarbij niet ingebroken in de computer van de verdachte. Een IP-adres is nodig om verder onderzoek te kunnen doen. Voor dit eventuele verdere onderzoek (onderzoek naar de inhoud van een computer, bijvoorbeeld) gelden echter strengere eisen. De rechtbank had eerder bepaald dat het achterhalen van het IP-adres leidde tot onrechtmatig verkregen bewijs. Het hof heeft dat nu teruggedraaid.

[98] L. Asscher & A. Ekker, 'Anonimiteitswet is hard nodig', *de Volkskrant*, 26 augustus 2003. Zie voor een uitvoerige en gelijkluidende stellingname het werk van de Tilburgse hoogleraar Corien Prins. Men leze onder meer: Nicoll, C. & Prins, J.E.J., 'Anonymity: Challenges for politics and law', in C. Nicoll, J.E.J. Prins, M.J.M. van Dellen (eds.), *Digital anonymity and the law - tensions and dimensions*, Uitgeverij T.M.C.Asser Press, Information technology and law series - volume 2, 2003. Merken we op dat de Raad van Europa recent een *Declaration on freedom of communication on the Internet* opstelde. De Declaratie legt de rechten en vrijheden vast die burgers hebben bij internetgebruik. De Raad besloot dit op basis van artikel 10 EVRM. De rechten op internetvrijheid zijn verankerd in 7 principes. Zo heeft iedere Europeaan formeel het recht om zich anoniem op internet te begeven. Overheden mogen echter, als men daar aanleiding toe heeft, speuren naar de identiteit van een internetgebruiker. Daarnaast moeten overheden de beschikbaarheid van internettoegang stimuleren. Cf. Declaration on freedom of communication on the Internet (Council of Europe) http://www.coe.int/T/E/Communication_and_Research/Press/News/

dagelijkse leven van de burgers op zachte maar indringende wijze wordt gestuurd.[99] Inderdaad, wie in het oog wordt gehouden of sporen nalaat gedraagt zich anders: het individu handelt dan in functie van wat een ander weet of kan weten. Zo wordt gedrongen gedrag geproduceerd.[100] Visuele toezichtstechnieken creëren (machts)verhoudingen waarin de ene actor het gedrag van de andere stuurt, ofschoon deze laatste per definitie over de vrijheid beschikt om anders te handelen. Door toedoen van camera's wordt de vrije gedragskeuze in een bepaalde richting 'geholpen'. Bijgevolg beperken camera's de vrijheid en hebben zij aanzienlijke repercussies op het vlak van de autonomie en de individuele vrijheid van de burgers.
Als dusdanig raken camera's aan fundamentele en essentiële waarden van de democratische rechtsstaat. Zulks blijkt trouwens genoegzaam uit de reeks positiefrechtelijke normen waardoor hun plaatsing in een problematisch licht komt te staan. Zo staan camera's haaks op de privacy van de burgers, die hun autonomie en individuele vrijheid waarborgt.[101] Inderdaad, ook de Hoge Raad omschreef het privacyrecht als zijnde niet begrensd tot de ruimte van de eigen woning: het is het recht om zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf; het is het recht onbevangen met zichzelf te zijn.[102] Het privacy-grondrecht beschermt in die zin de individuele zelfbeschikkingsvrijheid, de gedragsalternatieven en de elementaire weerstand van de burgers tegen macht. Camera's schenden met andere woorden een juridische waarde die helemaal bovenaan de normenhiërarchie prijkt, zowel internationaal als nationaal.
Quasi geen enkel grondrecht geniet een absolute bescherming. Ook de vrijheid van de privacy vindt zijn beperkingen in de vrijheden van anderen of in het algemeen belang. Zo goed als steeds zijn juridisch geldige afwijkingen mogelijk, maar zulks slechts in het licht van een afweging van rechten en belangen. Al te snel wordt evenwel vergeten dat in dergelijke afweging van grondrechten en belangen de vrijheid van de privacy zwaar moet wegen precies omdat zij normenhiërarchisch zo hoog staat aangeschreven.[103] In toepassing van art. 8,2 EVRM, bijvoorbeeld, betekent een correcte grondrechtenafweging dat de gewaarborgde vrijheid van het privé-leven (in verticale verhoudingen) slechts onder bepaalde voorwaarden kan worden beperkt: legaliteit, noodzakelijkheid, legitimiteit en subsidiariteit. De toepassing van zulke spelregels op toezichtcamera's geplaatst door de overheid geeft volgend resultaat: hun plaatsing is in beginsel niet toegelaten omdat de privacy wordt geschonden; slechts in uitzonderlijke gevallen, waarin minder invasieve middelen ondoeltreffend blijken, kan erop worden teruggevallen voor bepaalde gewichtige wettelijke doeleinden en mits voldoende rechtszekerheid wordt geboden.[104]

Landen zoals Nederland en Frankrijk hebben zeer vroeg gereageerd op bepaalde misbruiken met camera's en microfoons die onder meer door Watergate eind jaren zestig aan het licht kwamen. De Nederlandse wet van 7 april 1971 houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer verrijkte het strafwetboek met art. 139b tot 139g en art. 441b Sw. Hierdoor worden op algemene wijze bepaalde spionagetechnieken in hoofde van overheid en burger geïncrimineerd.[105] Niet alleen het afluisteren en heimelijk opnemen

---

[99] Zie de analyses op basis van het werk van M. Foucault, S. Cohen, G. Deleuze en G.T. Marx, alsook de referenties in S. Gutwirth, *Waarheidsaanspraken in recht en wetenschap, o.c.*, 192-223, 490-523, 611-722.
[100] Een systeem om 's nachts dienstdoende apotheken te beschermen, door eventuele klanten te verplichten zich eerst te identificeren bij een nachtpost van de politie, leidde tot een gevoelige vermindering van het aantal delicten tegen apothekers, maar ook tot een vermindering van het aantal personen dat een apotheker wenst te contacteren (Antwoord van de minister van Binnenlandse zaken op een parlementaire vraag (nr. 969), *Vragen en Antwoorden* Belgische Kamer van Volksvertegenwoordigers, 1994-1995, 14659.
[101] Zie ook B. Hulsman en P. Ippel, 'Privacy in arbeidsverhoudingen. Waakhonden gevraagd', *Rechtshulp*, 1995, 1, 2.
[102] Hoge Raad, 9 januari 1987, *Computerrecht*, 1987, nr. 2, 111.
[103] Dit heeft ongetwijfeld te maken met het veranderend tijdsklimaat dat we hoger reeds hebben beschreven. Zie ook het persbericht dat onder de titel 'Privacy versus veiligheid' opgenomen is in *NJB*, 11 februari 1994, 209.
[104] Vermelden we hierbij nog dat camera's naast de privacy, al naargelang de context van hun plaatsing, nog een reeks andere fundamentele rechten en vrijheden dreigen te schenden. Zie hiervoor o.m. in S. Gutwirth, 'Nineteen Ninety-Five ! Hoog tijd om cameratoezicht te beperken' (Redactioneel), *Recht en kritiek*, 1995/1, 3-11.
[105] Wet van 7 april 1971 houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer, *Nl. Stbl.*, 1971, nr. 180 (van kracht sedert 23 april 1971). Eveneens: de art. 372-375 Sw. en 441a Sw. (verbod op het aanprijzen van apparatuur). Over deze wet o.a. J. Silvis, 'Heimelijk afluisteren en opnemen in strafrecht strafvordering', *Computerr.,* 1989, 3, 135.

van gesprekken en telefoongesprekken komt aan bod, maar ook het ongevraagd nemen van foto's (139f-g Sw.) ter bescherming van in woningen vertoevende personen.[106] Een lichtere strafmaat is voorzien voor het heimelijk fotograferen van aanwezigen in winkels en horecagelegenheden (441b Sw.). Met deze wetgeving werd niet op alle vragen over heimelijk filmen opgelost.[107] Onder meer over de rechtmatigheid het filmen van cliënteel en personeel in winkels bleven er bepaalde twijfels. Er waren stemmen om in deze kwesties zoveel mogelijk ruimte als mogelijk aan werkgevers en eigenaars te geven 'omdat privacy niet in het voordeel mag werken van dieven',[108] en, voor ons niet toevallig, er werd hierover geen duidelijk antwoord gegeven in de vele geschriften die het Cbp over deze kwestie uitbracht.[109] Volledig terecht heeft de wetgever in deze kwestie recent gekozen voor een duidelijk antwoord, ditmaal in het belang van de gefilmde persoon door een aanscherping van de bestaande strafbepalingen.[110] Als gevolg van de aanscherping moet het cameratoezicht waarmee personen in de gaten worden gehouden op *alle* voor het publiek toegankelijke plaatsen, zoals bijvoorbeeld in banken, stations, casino's, bussen, musea, uitgaansgebieden of stadions, in ieder geval steeds voor de burger kenbaar moeten zijn. Dit geldt ongeacht of met de camera's al dan niet beelden worden vastgelegd. Wanneer de aanwezigheid van dergelijke camera's niet op duidelijke wijze kenbaar is gemaakt en er sprake is van een aangebrachte camera met het oogmerk om afbeeldingen van personen te maken, wordt in beginsel een overtreding begaan.[111] In de memorie wordt op duidelijke en voorbeeldige wijze aangegeven hoe het nu verder moet met candid camera's, camera's in pashokjes, beveiliging van de woonomgeving en cameratoezicht op de werkvloer. Luidens de memorie van toelichting was er behoefte om 'de norm dat het gebruik van camera's voor de burger kenbaar moet zijn, duidelijk in de wet te verankeren'. Het initiatief geeft aan dat de wetgever terecht van oordeel was dat die duidelijkheid niet werd gegarandeerd met de Wbp. Over de relatie strafrecht en Wbp valt weinig te lezen in de memorie van toelichting. Wel leert dit document dat het Cbp heeft geadivseerd en heeft bijgedragen tot een ruime terminologie zodat ook webcams onder de reikwijdte van de wet vallen.[112]

Het verhaal van de wetgevingsinspanningen m.b.t. cameragebruik in Nederland stopt niet bij het voorgaande. Ook heeft de Nederlandse wetgever naar aanleiding van het IRT-schandaal, ten dele aangezt door het falen van de rechtspraak om de grondrechtenaspecten van visuele opsporingstechnieken ernstig te nemen,[113] de bevoegdheden terzake verduidelijkt in de Wet Bijzondere opsporingsbevoegdheden (Wet BOB).[114] Door zo'n keuze wordt een evenwichtige

---

[106] Hoge Raad, 25 juni 1974, *N.J.*, 1974, 455; J. Doomen, *De hollende kleurling*, Contact, Amsterdam, 1991, 41. Over art. 139f Sw.: J.A.W. Knoester, 'De verborgen camera van Crime Time in een juridisch zoeklicht', *AA*, 1994, 9, 562 et seq.

[107] De oorspronkelijke strafbaarstelling in art. 441b Sr had immers alleen betrekking op winkels en horecagelegenheden en zweeg bijgevolg over andere voor het publiek toegankelijke plaatsen, waaronder ook de openbare weg. Zie over de keuze tot strafbaarstelling van de wetgever in 1971: Memorie van toelichting, Kamerstuk 2000-2001, 27732, nr. 3, Tweede Kamer, 2 & 3 met verw. naar het oorspronkelijk wetsvoorstel.

[108] L. Bergkamp, 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy', *Computer Law and Security Report*, 2002, Vol. 18 no. 1, 31-47.

[109] We doelen onder meer op het rapport *In Beeld gebracht* (Registratiekamer, 1997).

[110] Wet van 8 mei 2003 tot wijziging van de artikelen 139f en 441b van het Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht), *Staatsblad*, 2003, nr. 198.

[111] Memorie van toelichting, Kamerstuk 2000-2001, 27732, nr. 3, Tweede Kamer, 8. Door de opname van het bestanddeel «wederrechtelijk» in artikel 441b Sr en artikel 139f Sr. wordt aangegeven dat cameragebruik ten behoeve van de opsporing of de nationale veiligheid en ten behoeve van de vrije nieuwsgaring aan de strafbaarstelling kan ontsnappen. Zie Memorie van toelichting, Kamerstuk 2000-2001, 27732, nr. 3, Tweede Kamer, 6 en 12.

[112] Memorie van toelichting, Kamerstuk 2000-2001, 27732, nr. 3, Tweede Kamer, 3-4.

[113] Zie onze analyse van de rechtspraak van de Hoge Raad: P. De Hert & S. Gutwirth, 'Cameratoezicht, veiligheid en de Wet Persoonsregistraties. Juridische denkoefeningen naar aanleiding van de Franse wet van 21 januari 1995 inzake veiligheid', *Recht en kritiek*, 1995/3, 218-250.

[114] Deze wet is op 1 februari 2000 in werking getreden. De Wet BOB is een uitbreiding op het Wetboek van Strafvordering (Sv) die de volgende opsporingsbevoegdheden regelt: stelselmatige observatie; het opvragen van verkeersgegevens; het opnemen van telecommunicatie (tappen); het opnemen van vertrouwelijke communicatie (direct afluisteren); het betreden van een besloten plaats; de drie 'undercoverbevoegdheden' infiltratie, pseudo-koop of pseudo-dienstverlening en het stelselmatig inwinnen van informatie. Aanleiding van de toenemende belangstelling voor opsporingsmethoden was de 'opsporingscrisis' van midden jaren negentig. De parlementaire enquête over de opsporing stelde misstanden in een aantal grote drugsonderzoeken aan de kaak. Dit betrof met name het doorlaten van verdovende middelen onder regie van politie en justitie en een gebrek aan grip op (criminele) burgerinformanten/infiltranten. Belangrijke aanbevelingen van de parlementaire-enquêtecommissie onder leiding van Van Traa waren onder meer: bijzondere opsporingsmethoden van een wettelijke basis voorzien, de verantwoordelijkheden van verschillende diensten en functionarissen op het terrein van opsporing verduidelijken en de positie van het Openbaar Ministerie

grondrechtenpolitiek in de hand gewerkt.[115] Sluitstuk vormt het eind 2002 bekend gemaakte wetsvoorstel cameratoezicht in de openbare ruimte.[116] Gemeenteraden krijgen in het voorstel de mogelijkheid vaste toezichtcamera's te plaatsen voor het handhaven van de openbare orde en de veiligheid in de openbare ruimte. Dat mag alleen waar dat nodig is; er moet sprake zijn van een gebied waar zich in de praktijk onveilige situaties voordoen of met enige regelmaat wanordelijkheden plaatsvinden. Ook moet vaststaan dat het niet mogelijk is om met minder ingrijpende instrumenten de veiligheid te verbeteren. Het is de taak van de burgemeester om het besluit van de gemeenteraad uit te voeren. In overleg met de officier van justitie stelt de burgemeester de periode vast waarin de camera's daadwerkelijk gebruikt worden. De politie krijgt de operationele regie over het cameratoezicht. Het wetsvoorstel heeft alleen betrekking op cameratoezicht door de overheid in openbare ruimtes als wegen, pleinen, parken en winkelpassages. Voor cameratoezicht door private organisaties in bijvoorbeeld winkels, postkantoren, parkeergarages of gemeentehuizen blijft de Wet bescherming persoonsgegevens van kracht, aldus de tekst bij het voorstel. Gegevensbescherming wordt alzo geëxpliciteerd waarbij ten dele wordt gegrepen naar de logica van begrenzing.[117]

12. Afronding

In deze bijdrage hebben we ons gebogen over een de grondslagen van een evenwichtige grondrechtenpolitiek in een klimaat van grote veiligheidszorg. Onze focus lag daarbij op het inzicht dat wat ook de bereikte balans is tussen grondrechten en veiligheid, het resultaat alleszins helder moet worden opgebouwd. Onze zorg ging daarbij uit naar het signaal dat de huidige privacyregulering alleen te begrijpen valt door juristen, zodat de burger wordt uitgesloten bij het debat.
Vertrekkend vanuit het inzicht dat macht in de democratische rechtsstaat tegelijkertijd wordt begrensd en gekaderd door onderscheiden instrumenten, hebben we geargumenteerd dat bij de balans van moderne privacyvraagstukken denkoefening moet plaatsvinden die verder denkt dan *data protection*. Gegevensbescherming is immers zelf niet meer dan een instrument en is in hoofdorde geconstrueerd voor de omkadering van macht via transparantie. Dit noodzakelijk instrument en de muzikanten die het bedienen (de *data protection officials*) worden aangemaand tot bescheidenheid. Nadat transparantie is gerealiseerd of nadat de schijnwerpers zijn geplaatst op niet gekanaliseerde machtsuitoefening teneinde deze te problematiseren vangt het echte werk aan, met name het beoordelen van de opportuniteit van het trekken van grenzen. Het resultaat van dit werk kan juridisch uiteenlopende vormen aannemen: grondwetsverrijkingen, wetten, gemeentelijke wetgeving, nieuwe Europese richtlijnen, ja zelfs uitspraken van (grondwettelijke) hoven. Het betreft stuk voor stuk juridische instrumenten met grote democratische legitimiteit en in de meeste gevallen geven ze vorm aan een via de meerderheidsregel bereikte keuze in kwesties waarin goed of fout en pro of contra niet altijd eenvoudig aan te wijzen zijn.[118]

---

versterken. De commissie-Van Traa benadrukte daarbij het belang van de integriteit van de opsporing. Rechtspraak van de Hoge Raad uit die periode (Charles Z.) richtte zich op de vraag in hoeverre toegepaste opsporingsmethoden inbreuk maakten op grondrechten, in het bijzonder het recht op privacy. Beide gezichtspunten, enerzijds integriteit en beheersbaarheid van het opsporingsapparaat en anderzijds inbreuk op grondrechten, zijn van belang geweest bij het vormgeven van de Wet BOB.

[115] De memorie van toelichting (MvT)geeft de volgende drie uitgangspunten van het Wetsvoorstel BOB weer:
1 *Codificatie van opsporingsmethoden*. Opsporingsmethoden dienen naar inhoud en procedure goed geregeld te zijn. Opsporingsmethoden die risico's meebrengen voor de integriteit van de opsporing of inbreuk maken op grondrechten van burgers dienen hun basis te hebben in het Wetboek van Strafvordering.
2 *Centrale autoriteit bij de opsporing is de officier van justitie.* Het gezag over de opsporing ligt op grond van artikel 148 Sv bij de officier van justitie. Bij bijzonder ingrijpende bevoegdheden is echter toestemming van de rechter-commissaris vereist.
3 *Controleerbaarheid van de opsporing.* Van gebruikte opsporingsbevoegdheden dient verslag te worden gedaan en deze dienen in principe ter zitting te kunnen worden verantwoord.

[116] Cf. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Persbericht ministerraad, 20 december 2002

[117] Meer begrenzing kan ook worden bereikt via andere instrumenten. De denken valt aan het civielrecht (bijv. zwembaden verbieden het bij zich hebben van digitiale camera's en telefoontoestellen met een cameraoptie) of via het administratief recht (bijv. het fotoverbod Eikenhorst van de gemeente Wassenaar). De tekst van dit besluit, d.d. 30 juni 2003, alsmede de reacties, kunnen geraadpleegd worden via recht.nl.

[118] Over het belang en de kracht van de meerderheidsregel om in controversiële kwesties de minderheid te brengen tot aanvaarding, leze men het zesde hoofdstuk 'the physics of consent' in Jeremy Waldron, *The Dignity of Legislation*, Cambridge, Cambridge U.P., 1999, 151-166.

Uit onze aanbeveling om bij het beleid het dubbele spoor van begrenzing en kanalisering te volgen, kan zonder twijfel een aanbeveling worden afgeleid om een de heersende gegevensbeschermingslogica steeds te toetsen aan de bruikbaarheid en meerwaarde van een privacylogica en beide logica's in de gevallen dit nodig blijkt te laten samen gaan. Volgt hier nu uit dat elk Nederlands politicus dag na dag de adviezen van het Cbp moet aanhoren en de door het Cbp verstuurde brieven moet lezen, om vervolgens uit te maken voor zichzelf of er wettelijke bijsturing via een privacylogica nodig is? Waarschijnlijk wel, of misschien toch niet. De gegevensbechermingslogica heeft een bedwelmend karakter en is in staat om het kritisch en intuïtief vermogen te verslappen. Het kan geen kwaad om een alarmfunctie aan de bevolking te geven[119] en de wetgever alleen te laten reageren op deze signalen waarbij hij handelt naar eigen inzicht wat de keuze van de instrumenten tot actie betreft. De respectievelijke taken van het strafrecht, het grondwettelijk recht, het privaatrecht, het arbeidsrecht en het administratief recht mogen niet verwaarloosd worden louter op grond van het gegeven dat aan de Wbp een ruim, bovensectoraal karakter toekomt. Een grondrechtenpolitiek is belangrijk en behoeft meer dan alleen procedurele rechtvaardigheid.

[119] Deze aanbeveling is o.i. niet in strijd met de observatie dat onzichtbare of geheime privacybeperkende maatregelen minder snel door de publieke opinie worden gepercipieerd. Dat is nu eenmaal de aard van het beestje, denken we dan. Aan het verschijnsel dat de wetgever zonder discussie repressieve wetgeving produceert valt niet altijd veel efficiënte weerstand te bieden. Het is zoals vaak wachten op misbruiken en schandalen naar aanleiding van geheime bevoegdheden om het publieke debat op gang te trekken.