Digitale grondrechten en de Staatscommissie: op zoek naar de kern

PROF.DR. B.J. KOOPS*

1. Inleiding

Het rapport van de Staatscommissie Grondwet, dat eind 2010 werd gepubliceerd onder de beeldende titel *Rapport Staatscommissie Grondwet*, besteedt conform haar opdracht ook aandacht aan grondrechten in het digitale tijdperk. In deze bijdrage bespreek ik wat de commissie daarover zegt (en niet zegt), in aanvulling op de bespreking van Luc Verhey elders in dit nummer. Waar Verhey de voorstellen vooral bespreekt vanuit het perspectief van grondrechten, zal ik de voorstellen meer benaderen vanuit het perspectief van het digitale tijdperk. Ons verschil in benadering laat zich goed illustreren aan de hand van de plaats van digitale grondrechten in de taakopdracht: waar Verhey met enige verrassing constateert: 'Zonder zichtbare aanleiding verscheen het thema in de opdracht van de Staatscommissie Grondwet', zou ik eerder stellen: zonder zichtbare aanleiding verdween het thema in de opdracht van de Staatscommissie Grondwet.

De vraag is immers waarom het thema 'grondrechten in het digitale tijdperk' nogmaals – nadat er al door de Commissie-Franken in 2000 over was geadviseerd – door een officiële commissie moest worden behandeld, en zo ja, of déze Staatscommissie daar dan een geschikte commissie voor was. Wat het eerste betreft: er was al een rijkdom aan voorstellen en standpunten voorhanden.[1] Er zijn twee goede redenen om opnieuw een Staatscommissie voorstellen te laten doen: ofwel de bestaande voorstellen zijn verouderd en behoeven actualisering in het licht van nieuwe ontwikkelingen, ofwel er is onvoldoende eenheid te ontwaren in de voorstellen en er is behoefte aan een nieuw, gezaghebbend advies. Beide redenen hadden in dit geval enige relevantie. De voorstellen van de Commissie-Franken waren in 2000 adequaat, maar ze waren niet bijzonder vooruitkijkend naar nieuwe technische ontwikkelingen.[2] Dat is des te relevanter nu in het afgelopen decennium de contouren en gevolgen van het digitale tijdperk op zijn minst flink zijn aangescherpt, maar misschien ook wel

* Prof.dr. B.J. Koops is hoogleraar regulering van technologie, Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg. De auteur dankt Jasper Sluijs en de redactie voor hun commentaar op een eerdere versie van dit artikel

1 Zie onder meer Rapport Commissie Grondrechten in het digitale tijdperk, Den Haag, mei 2000; E.J. Dommering , 'De nieuwe Nederlandse Constitutie en de informatietechnologie', *Computerrecht* 2000, p. 182-183; J. Nouwt e.a., 'Grondrechten in het digitale tijdperk', *Nederlands Juristenblad* 2000, p. 1321-1327; L. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, diss. Amsterdam (UvA), Amsterdam: Otto Cramwinckel 2003.

2 B.J. Koops, Hanneke van Schooten en Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004.

ingrijpend zijn veranderd. Daarnaast is er een gebrek aan eenheid te zien in het moeizame traject met betrekking tot de grondrechten in het digitale tijdperk (hierna naar praktisch spraakgebruik 'GDT' genoemd). Na het echec van het wetsvoorstel om art. 13 Gw aan te passen,[3] bracht de Commissie-Franken niet het gehoopte momentum – de op haar rapport gebaseerde wetsvoorstellen werden in 2004 door de Raad van State afgeserveerd, en het thema verdween vervolgens in de ijskast. Een rechtsvergelijkend onderzoek in opdracht van BZK[4] kon het thema niet ontdooien. Dat het thema vervolgens in 2009 aan deze Staatscommissie werd meegegeven, samen met een stapel andere – en meer politiek populaire – onderwerpen, kwam op mij dan ook vooral over als een vertragingstactiek: het thema uit de ijskast halen en langzaam laten ontdooien achterin de koelkast. Desondanks heeft de commissie het onderwerp serieus opgepakt en voorstellen gedaan om grondrechten in het digitale tijdperk te actualiseren en te stroomlijnen.

In deze bijdrage stel ik de vraag of deze voorstellen van de Staatscommissie adequaat zijn voor het digitale tijdperk. Ik doe dat aan de hand van een algemeen voorstel van de commissie: het idee om de kern van grondrechten bijzonder te beschermen (par. 2). Vervolgens bespreek ik de gegevensbescherming (par. 3), het communicatiegeheim (par. 4), de vrije meningsuiting (par. 5) en de toegang tot overheidsdocumenten (par. 6), alsook enkele onderwerpen die helaas niet in het rapport zijn te vinden (par. 7). Ik sluit af met een conclusie (par. 8).

artikelen

2. De kernrechtgedachte

De Staatscommissie kreeg onder andere de vraag voorgelegd of de beperkingssystematiek van de grondrechten aanpassing behoeft. De commissie meent dat over het algemeen de systematiek en de bestaande beperkingsformuleringen gehandhaafd kunnen blijven, maar stelt in aanvulling een algemene beperkingsclausule voor (p. 55):

> 1. Beperkingen van grondrechten gaan niet verder dan het doel van de beperking vereist.
> 2. De kern van grondrechten wordt niet aangetast.

Het tweede lid, de 'kernrechtbepaling', is vooral bedoeld als waarschuwing en motiveringsplicht voor de wetgever. Het gaat volgens de commissie (p. 55-56) daarbij om

> 'de onaantastbaarheid van de wezenlijke kern ('*the very essence*', '*das Wesensgehalt*') van het recht dat in de desbetreffende bepaling bescherming vindt. Zij geeft hiermee de uiterste grens van beperking aan: zelfs als beperking van een grondrecht het enige middel is om een bepaald doel te bereiken, en zelfs als dit doel van zwaarwegend belang is, is zo'n beperking niet aanvaardbaar voor zover zij de kern van het grondrecht aantast.'

3 Zie *Kamerstukken II* 1998/99, 25 443, nr. 40d en voorgaande stukken.

4 Ronald Leenes, Bert-Jaap Koops en Paul De Hert (red.), *Constitutional rights and new technologies: a comparative study*, The Hague: T.M.C. Asser Press 2008.

Deze kernrechtbepaling is een interessant maar ook verstrekkend voorstel. Het kan de normatieve werking van de Grondwet – een van de leidende gedachten voor de commissie – versterken: tot hier en niet verder. Maar door te stellen dat de kern van het grondrecht absoluut is, maakt de commissie het vrijwel onmogelijk om hieraan normatieve werking te ontlenen. Welke onderdelen van grondrechten zijn zó fundamenteel dat ze onder geen omstandigheid mogen wijken voor andere belangen? De wetgever zal in bijna alle gevallen gaan beargumenteren dat een bepaalde inbreuk niet de kern van het grondrecht raakt. Daarover valt vervolgens wel te discussiëren, maar dan verschuift de discussie over de wenselijkheid en toelaatbaarheid van een inbreuk naar een semantische discussie over de kern van het grondrecht. Materieel schieten burgers daar denk ik weinig mee op. Het is beter om de op zich waardevolle kernrechtgedachte in te voeren in de vorm van een kern met daaromheen één of meer schillen van afnemende beschermwaardigheid, waarbij naarmate men dichter bij de kern komt de ruimte voor inbreuken afneemt en de motiveringsplicht navenant zwaarder wordt.
In die vorm kan een kernrechtbepaling een interessante aanvulling zijn op onze grondrechtensystematiek. Het veronderstelt wel dat voldoende duidelijk is wat de kern van een grondrecht is. Bij sommige grondrechten is dat duidelijker dan bij andere. We kunnen de proef op de som nemen en kijken of de commissie zelf voldoende helderheid schept in het aanduiden van de kern van de door haar voorgestelde grondrechten.

3. Gegevensbescherming

De commissie stelt unaniem (het feit dat ik, met Verhey, geneigd ben om hier een uitroepteken achter te zetten is veelzeggend) voor om de bescherming van persoonsgegevens af te splitsen van het grondrecht op privacy. Dat is winst. In de literatuur is overtuigend beargumenteerd dat privacy en gegevensbescherming weliswaar verwant maar ook principieel verschillend zijn,[5] en inmiddels is met het Handvest van de Grondrechten van de EU ook een internationaalrechtelijke basis voor deze splitsing voorhanden.
Maar dan. Als we het erover eens zijn dat het beschermen van persoonsgegevens als zelfstandig grondrecht vormgegeven moet worden, hoe moet het er dan uitzien? Hier biedt de Staatscommissie weinig houvast. De toelichting is summier, en met maar liefst drie (!) voorstellen kunnen we vele kanten op. Nu is het zo dat twee van de voorstellen een minderheidsstandpunt bettreffen van hetzelfde lid, Overkleeft-Verburg, en dat het vast niet de bedoeling is dat haar voorstel in de hoofdtekst (p. 84) afwijkt van dat in de bijlage met toelichting (p. 148). Mijn indruk is dat het voorstel in

5 Zie eerst en vooral Peter Blok, *Het recht op privacy*, diss. Tilburg, Den Haag: Boom Juridische uitgevers 2002.

de hoofdtekst uit een eerdere versie afkomstig is (dat spreekt van het atypische 'Eenieder' en 'bij en krachtens de wet') waar de bijlage een latere versie betreft, maar dat is speculatie.
In elk geval biedt deze redactionele misser een prachtig domein voor tekstanalyse. In de tekstvarianten komt bijvoorbeeld een cruciaal aspect naar voren: moet gegevensbescherming worden vormgegeven als subjectief (afweer)recht – zoals de commissie in meerderheid voorstelt –, of als regelopdracht (zoals in het huidige art. 10 Gw)? Het is een teken aan de wand dat het minderheidsstandpunt in één versie (p. 84) het derde lid – kennisneming en verbetering – vormgeeft als regelopdracht, en in de andere versie (p. 148) als subjectief recht. Nog subtieler is het verschil in het tweede lid: 'De verwerking van persoonsgegevens wordt geregeld bij en krachtens de wet' respectievelijk 'Persoonsgegevens worden verwerkt ingevolge bij de wet te stellen regels'. De eerste variant klinkt als een regelingsopdracht, terwijl de tweede variant iets meer klinkt als een subjectief recht met regelingstrekjes. Het meerderheidsvoorstel is veel explicieter als subjectief recht geformuleerd: Ieder heeft recht op bescherming van zijn persoonsgegevens (lid 1), die alleen voor welbepaalde doeleinden en op toestemmings- of wettelijke grondslag mogen worden verwerkt (lid 2), en ieder heeft recht op inzage, kennisneming en correctie (lid 3). Het is opmerkelijk dat de keuze voor een subjectief recht, dat daarin sterk afwijkt van de huidige regelingsopdracht in art. 10 Gw, niet wordt gemotiveerd of toegelicht. Slechts terloops wordt op p. 49 aangestipt dat, mocht het wetsvoorstel-Halsema over constitutionele toetsing worden aangenomen, het nieuwe grondrecht op gegevensbescherming aan de catalogus zou kunnen (moeten?) worden toegevoegd; saillant is immers dat dit wetsvoorstel art. 10 lid 2-3 (niet zijnde een afweerrecht) niet noemt als toetsingsgrondrechten.
Evenmin besteedt het rapport aandacht aan de horizontale werking van het voorgestelde afweerrecht. Nu het niet meer als regelopdracht (waarbij redelijk vanzelf ook de private sector wordt meegeregeld) maar als subjectief recht, en dus primair tegenover de overheid, wordt vormgegeven, rijst de vraag in hoeverre het recht inroepbaar is tegen verwerking door private partijen. Nu kent art. 8 EVRM flinke positieve verplichtingen en ligt het voor de hand dat een nieuw artikel ruimhartig horizontale werking zal worden toegekend, maar dat had dan wel even mogen worden geëxpliciteerd. Ik zie overigens ook uit naar de vele rechtszaken die we tegemoet mogen zien wanneer de overheid zich onvoldoende kwijt van haar taak om in wetgeving en rechtspraktijk de bescherming te waarborgen van consumenten tegen verwerking van hun persoonsgegevens door Google, Facebook en Amazon. Het kan nog druk worden bij de constitutionele rechter.

Op zich valt er veel te zeggen voor een subjectief grondrecht op gegevensbescherming. De ontwikkeling van het gegevensbeschermingsrecht heeft duidelijk constitutionele trekken, getuige niet alleen Verdrag 108 van de Raad van Europa[6] en art. 8 van het Handvest, maar ook de EHRM-rechtspraak over art. 8 EVRM.[7] In de literatuur wordt regelmatig een recht op informationele zelfbeschikking ingeroepen, meestal onder verwijzing naar het Duitse *Volkszählungsurteil*.[8] Maar nog los van de vraag of zo'n recht op informationele zelfbeschikking ook feitelijk bestaat (*de jure*, anders dan *de desiderione*), wat ik sterk betwijfel, is het onduidelijk wat een subjectief recht op bescherming van persoonsgegevens dan precies moet behelzen. Wat is de kern van dit grondrecht?

Dit wordt niet uitgelegd in het rapport, dus we moeten hier zelf iets op vinden. Men zou kunnen stellen dat het grondrecht het hele 'dataprotectie-acquis' omvat, wat naar redelijke consensus min of meer uit Verdrag 108, de OESO-richtlijnen[9] en Richtlijn 95/46/EG bestaat. Maar het is enigszins de omgekeerde wereld om een nieuw grondrecht in te vullen aan de hand van bestaande richtlijnen en niet-constitutionele wetgeving. De Wet bescherming persoonsgegevens (gebaseerd op Richtlijn 95/46) moet de Grondwet volgen, niet omgekeerd. Bovendien is de Richtlijn complex en veelomvattend. Is het bijvoorbeeld een constitutioneel recht dat, wanneer een instantie bij een betrokkene persoonsgegevens opvraagt, de instantie daarbij informatie verstrekt 'of men al dan niet verplicht is om te antwoorden en de eventuele gevolgen van niet-beantwoording' (art. 10 lid c Richtlijn)? Is het, constitutioneel gesproken, verplicht om het verzet tegen verwerking van persoonsgegevens voor direct marketing kosteloos te kunnen doen (art. 14 Richtlijn)? Is de meldingsplicht bij toezichthouders voor dataverwerkers constitutioneel van aard? Ik betwijfel eerlijk gezegd of het de bedoeling kan zijn van een grondrecht op bescherming van persoonsgegevens om dergelijke details uit lagere wetgeving binnen te halen.

Het ligt meer voor de hand aan te sluiten bij de meer abstracte algemene beginselen van dataprotectie, die redelijk compact zijn geformuleerd in Verdrag 108 en de OESO-richtlijnen. Maar ook dit is twijfelachtig, nu enkele van deze beginselen apart worden gespecificeerd in leden 2 (doelbinding en grondslag) en 3 (kennisneming en correctie) van het voorstel, terwijl andere beginselen niet expliciet worden vermeld, zoals het beveiligingsbeginsel, het datakwaliteitsbeginsel of het verantwoordingsbeginsel.[10] Moeten we de rechten uit het tweede en derde lid zien als verbijzonderingen van het algemene recht uit het eerste lid en zo ja, wat rechtvaardigt dan deze aparte vermelding – behoeven deze beginselen meer bescherming dan andere, of zijn ze zelfs een aanduiding van de kern van het grondrecht? Dat laatste zal wel niet; als doelbinding een absolute kern

6 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 108, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG>.

7 Paul De Hert en Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action', in: Serge Gutwirth e.a. (eds), *Reinventing Data Protection?*, Berlin: Springer 2009, p. 57-71.

8 BVerfG 15 december 1983, *BVerfGE* 65, 1.

9 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, beschikbaar via <http://www.oecd.org>.

10 Zie ibid.

van gegevensbescherming zou uitmaken, dan kunnen de politie en de AIVD hun bevoegdheden om gegevens bij derden op te vragen vergeten, en dat kan niet de bedoeling zijn. Ik weet ook niet waarom deze beginselen meer of explicietere bescherming zouden behoeven dan de niet genoemde algemene dataprotectiebeginselen. Ik zou ofwel kiezen voor een algemene verwijzing, ofwel voor een aanduiding van álle beginselen. Wat de verwijzing naar een grondslag voor gegevensverwerking in lid 2 betreft moet nog worden opgemerkt dat het voorstel van de commissie vragen oproept: verwerking mag alleen 'a) hetzij met toestemming van de betrokkene, b) hetzij op grond van bij de wet te stellen regels'. Hiermee lijkt de commissie te suggereren dat toestemming primaat heeft boven andere grondslagen, en wellicht ook dat toestemming wettelijke grondslagen kan doorbreken (bijvoorbeeld als de wet zegt dat het voor bedrijven verboden is om ras- en geloofsgegevens te verwerken voor marketingdoeleinden, dan zou het bedrijf dat alsnog kunnen doen als het toestemming van consumenten vraagt en krijgt). De belangrijke grondslag van contractuele verplichting (art. 8 onder b Wbp) lijkt verdwenen te zijn (tenzij je gekunsteld redeneert dat 'bij de wet te stellen regels' ook het contractrecht omvat, maar dat is dan een vage grondslag voor concrete verwerkingen). Bovendien is het, voor een subjectief en dus klassiek afweerrecht, misleidend om toestemming vooraan te zetten, omdat juist verwerkingen door de overheid van gegevens van burgers vaker op basis van wettelijke verplichtingen dan op basis van toestemming plaatsvinden. Het zou kortom beter zijn, als je per se de grondslag specifiek wilt vermelden in het grondrecht, om algemeen te verwijzen naar 'rechtmatige grondslag', waaronder dan alle grondslagen vallen die art. 7 Richtlijn en art. 8 Wbp noemen.

Een ander mogelijk houvast bij de zoektocht naar de kern van het voorgestelde recht op bescherming van persoonsgegevens is de inkleuring van het grondrecht. Volgens de commissie (p. 81) maakt verzelfstandiging van het recht duidelijk dat gegevensbescherming niet alleen raakt aan privacy, maar ook aan vrijheid van meningsuiting en het discriminatieverbod. Ook geeft het uitdrukking aan 'de toegenomen betekenis van de verwerking van persoonsgegevens en de wenselijkheid van een behoorlijke bescherming in de huidige samenleving'(p. 82). De commissie geeft echter niet aan wat er precies beschermd moet worden in de huidige samenleving. Is dat het individu of de economie (die baat heeft bij de vrije uitwisseling van persoonsgegevens in de interne markt, wat één van de twee doelstellingen van Richtlijn 95/46 is)? Gezien de vormgeving als subjectief recht mogen we aannemen dat het gaat om het eerste. Maar welke belangen van het individu beoogt het artikel precies te beschermen? De autonomie? De menselijke waardigheid (wat dat ook mag

zijn)? De informationele zelfbeschikking? En hoe moeten deze abstracte beginselen worden ingekleurd als we moeten beoordelen of een dataverwerker inbreuk mag maken op de gegevensbescherming van een individu? De wetgever en de rechter zullen, op basis van de kernrechtbepaling, moeten weten of een afwijking – van de doelbinding, kennisneming, correctie, het verbod op puur automatische beslissingen – de kern van de bescherming raakt. Zonder zorgvuldig uitgewerkte en gemotiveerde toelichting van de achterliggende gedachte waarom persoonsgegevens in het digitale tijdperk zelfstandige grondrechtelijke bescherming behoeven, valt het grondrecht niet te interpreteren en toe te passen. In een context waarin de Wet bescherming persoonsgegevens al weinig bekend is en als moeilijk hanteerbaar en interpreteerbaar wordt gezien,[11] zal een zelfstandig maar vaag grondrecht op gegevensbescherming eerder afbreuk doen aan de rechtsbescherming, dan dat het de normativiteit van de bescherming versterkt.

Samenvattend kom ik tot de conclusie dat het voorstel om gegevensbescherming als zelfstandig en subjectief grondrecht in te voeren, weliswaar sympathiek is, maar door de afwezige onderbouwing en toelichting een mijnenveld neerlegt voor wetgevers, rechters of rechtsgeleerden die op zoek gaan naar de kern van het grondrecht. Tot hoever het afweerrecht reikt, ook in horizontale verhoudingen, en wat het precies beoogt te beschermen, vergt nog substantiële nadere reflectie vooraleer het rijp is voor opneming in de grondrechtencatalogus. Verder vraagt ook aandacht de verwijzing naar specifieke beginselen naast een algemene bepaling; mijns inziens past of een algemene verwijzing naar de beginselen van behoorlijke gegevensverwerking of een expliciete aanduiding van álle beginselen uit het dataprotectie-acquis.

4. Het (tele)communicatiegeheim

Het brief-, telefoon- en telegraafgeheim is evident aan actualisering toe. Maar hoe? Sinds Hofman in 1995 de toon heeft gezet door te stellen dat het in de kern gaat om bescherming van vertrouwelijke communicatie (en dus niet van niet-vertrouwelijke communicatie),[12] lijkt er haast geen andere benadering meer mogelijk. De commissie-Franken stelde onverdroten een vergelijkbare Hofmaniaanse formulering voor ('Ieder heeft het recht vertrouwelijk te communiceren') als in het voorafgaande wetsvoorstel, dat tot een rampzalige procesgang in Tweede en Eerste Kamer had geleid (wat juist de aanleiding vormde om die commissie in te stellen). Vervolgens kwam het op de commissie-Franken gebaseerde wetsvoorstel met eenzelfde formulering ('Het recht op vertrouwelijke communicatie is

11 G.-J. Zwenne e.a., *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntanalyse*, Leiden: eLaw@Leiden 2007, <http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969>; H.B. Winter e.a. (2008), *Wat niet weet wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Den Haag: WODC, <http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx#>.

12 J.A. Hofman, *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, diss. Amsterdam (VU), Zwolle: W.E.J. Tjeenk Willink 1995.

onschendbaar'),[13] die door de Raad van State was afgeserveerd (waarschuwend 'tegen het zo onbepaald maken van een traditioneel veel strikter omschreven grondrecht').[14] Na deze herhaalde kritiek op 'vertrouwelijke communicatie' als kern van het grondrecht, zou de Staatscommissie zich achter de oren hebben moeten krabben. Gaat het in de kern wel om de bescherming van vertrouwelijke communicatie? De commissie meent van wel:

> 'het belang van de bescherming van het hier aan de orde zijnde grondrecht is dat men in een democratische samenleving vertrouwelijk met elkaar moet kunnen communiceren, zonder de angst dat de overheid meeluistert' (p. 85).

Het gaat daarbij om communicatie die 'objectief gezien als vertrouwelijk moet worden gekwalificeerd en waarbij een redelijke verwachting van vertrouwelijkheid kan bestaan'. Feitelijk komt dit neer op de *Katz*-test zoals die in de VS wordt gehanteerd:[15] het moet gaan om een subjectieve verwachting van vertrouwelijkheid die door de maatschappij ('objectief') als redelijk wordt gezien. De commissie schept meer helderheid dan sommige voorgaande voorstellen door expliciet te stellen dat de bescherming geldt voor de duur van het transport; zodra de communicatie is ontvangen, vervalt de bescherming onder art. 13 en blijft bescherming onder art. 10 of 12 (huisrecht) over. Voor gevallen waarin er nog overlap bestaat tussen transport en ontvangst – een email- of stempostbericht dat in de in-bus van de gebruiker staat maar nog niet is afgeluisterd, het is dan wel ontvangen maar ook nog bij de transporteur – stelt de commissie het bruikbare criterium voor dat het kennisnemen via de transporteur onder art. 13 valt en het kennisnemen via de gebruiker (bijvoorbeeld bij huiszoeking) onder art. 10 of 12 (p. 87). Dat is op zichzelf helder.

Nu lijkt het misschien spijkers op laag water zoeken, maar voor de zoektocht naar de kern moeten we een atypisch voorbeeld bekijken dat niet strookt met het voorgestelde criterium. Wat als iemand een brief schrijft aan de kinderen om te lezen na het overlijden en dit in een dichtgeplakte envelop met opschrift 'Aan mijn nabestaanden' in het dressoir opbergt? Dit is een duidelijk geval van vertrouwelijke communicatie, lijkt me. Er is echter geen sprake van transport, althans in dit geval valt de transporteur samen met de gebruiker. Valt bij een opsporingsdoorzoeking deze brief nu onder de bescherming van art. 10 en 12 of (ook) onder art. 13? Volgens de commissie is art. 13 niet van toepassing: de overheid neemt immers kennis van de inhoud 'bij de verzender of de ontvanger'. Maar als dat zo is, moet men zich afvragen of het voorgestelde art. 13 wel echt bedoeld en geschikt is om vertrouwelijke communicatie te beschermen. Als het idee

13 *Kamerstukken II* 1996/97, 25 443, nrs. 1-2.
14 Advies Raad van State 24 januari 2002, bijgevoegd bij brief van de Minister aan de Koningin d.d. 29 oktober 2004, kenmerk 0000018194.
15 *Katz* v. *United States*, 389 US 347 (1967).

is dat iemand vertrouwelijk moet kunnen communiceren zonder dat de overheid meeluistert, dan zou ook de brief aan de nabestaanden op deze grondslag moeten worden beschermd. Waarom zou wel het gesprek met de buurman over de heg en een muurberichtje aan vrienden op Facebook onder art. 13 – met de sterke rechtsbescherming van rechterlijke controle – vallen, maar niet de veel vertrouwelijker communicatie die op andere manieren dan communicatietransport of een 'live gesprek' wordt gevoerd? Ik zie ook niet goed in waarom vertrouwelijke communicatie principieel bescherming tegen overheids-meeluisteren verdient tijdens transport maar niet voor of na het transport. Als de kern is het beschermen van vertrouwelijke communicatie *als zodanig*, zou het principieel niet moeten uitmaken of de overheid een brief in beslag neemt bij de postbode of bij de gebruiker, evenmin als het uitmaakt of de brief nog gesloten en ongelezen is of gelezen en opgeborgen. De vertrouwelijkheid van de communicatie tegen een meelezende overheid is in deze gevallen evenzeer in het geding. De keuze voor vertrouwelijke communicatie als kern en tegelijk beperking voor de duur van transport is dus inconsistent.

Het minderheidsstandpunt, wederom van Overkleeft-Verburg, kiest voor een fundamenteel andere benadering: de kanaalbescherming. Zij herformuleert art. 13 als een brief- en telecommunicatiegeheim en een recht op vrijwaring van heimelijke opneming van mondeling[16] gevoerde gesprekken. Haar toelichting (p. 149-153) is aanzienlijk scherper en overtuigender dan het nauwelijks toegelichte meerderheidsvoorstel. Terecht wijst Overkleeft-Verburg op een spanningsveld tussen de bedoeling van de commissie – het uitbreiden van art. 13 met Internet- en live-communicatie – en de formulering die in plaats van trajectbescherming de nadruk legt op vertrouwelijke communicatie. Een probleem van dat laatste – naast de hierboven aangestipte problemen – is dat niet-vertrouwelijke communicatie tijdens het transport in principe niet beschermd zou moeten worden, maar dat het veelal onmogelijk en ook onwenselijk is dat transporteurs gaan differentiëren tussen vertrouwelijke en niet-vertrouwelijke communicatie.

Een andere ontwikkeling die in de discussie moet worden betrokken is dat de communicatie-infrastructuur leidt tot substantieel andere patronen van omgang met informatie. *Cloud computing* is momenteel het sleutelbegrip: het aanbieden van diensten voor informatieopslag en -verwerking onafhankelijk van locatie – denk aan diensten als Google Docs[17] waarbij je tekstbestanden, rekenbladen, foto's of referentiebibliotheken op afstand opslaat (in 'de cloud', wat aanduidt dat het onbekend en ook irrelevant is waar de servers staan waarop de informatie wordt opgeslagen). Mensen

16 Het is een detail, maar men zou kunnen nadenken over een formulering die ook 'live' gesprekken in gebarentaal afdekt, als we art. 1 Gw recht willen doen.

17 <http://docs.google.com>.

gebruiken dit zodat ze vanaf elke plaats bij hun bestanden kunnen. Het opslaan van bestanden in de *cloud* is functioneel equivalent met het opslaan van bestanden op de thuiscomputer, wat weer een equivalent is van het bewaren van fotoalbums, plak- en dagboeken en administratiemappen in de kast. Nu vallen deze laatste dingen onder de bescherming van het huisrecht. In de *cloud* opgeslagen gegevens doen dat niet; dat is misschien terecht omdat de redelijke privacyverwachting kleiner is als je bestanden voor opslag aan een derde toevertrouwt (zeker als die derde Google is), maar het roept wel enige vragen op over hoe het huisrecht vormgegeven moet worden in het digitale tijdperk waarin veel klassieke binnenhuiselijke activiteiten zoveel buitenhuiselijke effecten hebben. Dat is andere materie. Waar het hier om gaat is dat het transport van bestanden tussen huis (of waar dan ook) en *cloud* ook bescherming behoeft, en dat daarvoor klassiek het transportgeheim van art. 13 Gw bedoeld is. Maar het gaat niet om communicatie als zodanig.

Het begrip 'communicatie' wordt niet uitgelegd in het rapport, en ook in voorgaande discussies nauwelijks toegelicht.[18] Men kan voor de interpretatie aanhaken bij de definitie in de strafvordering: 'de uitwisseling van berichten tussen twee of meer personen'.[19] Iemand die extern bestanden opslaat, net zoals iemand die telewerkt en daarbij bestanden tussen huiscomputer en werkserver uitwisselt, is echter niet aan het communiceren maar bestanden aan het opslaan. Nu kun je redeneren dat iemand met zichzelf 'communiceert' of met een computer communiceert, maar dat is een gekunstelde interpretatie van het begrip 'communicatie'. Juist hier wringt de keuze van de commissie om 'vertrouwelijke communicatie' als kern van de bescherming aan te duiden: in het digitale tijdperk is veel van wat er over het telecommunicatienetwerk gaat feitelijk geen communicatie, terwijl het uit het oogpunt van rechtsbescherming wel bescherming verdient tegen afluisteren of opnemen door de transporteur of de overheid. Daarom zou de kern van de bescherming in art. 13 Gw mijns inziens niet vertrouwelijke communicatie *als zodanig* moeten zijn, maar uitwisseling van gegevens *die aan een derde voor transport worden toevertrouwd*. Dat wordt gevat onder het klassieke post-, telegrafie- en telefoongeheim, dat van oudsher transportbescherming biedt en dat daarom in het digitale tijdperk het best kan worden geformuleerd als een post- en telecommunicatiegeheim.[20] Deze benadering, om transport te beschermen tegen onderscheppen door de overheid, ongeacht de inhoud van wat er wordt getransporteerd, is zuiverder en beter af te bakenen dan de benadering om communicatie, laat staan vertrouwelijke communicatie, als zodanig te beschermen. Het minderheidsstandpunt verdient dus de voorkeur boven het meerderheidsstandpunt.

18 Zie B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, p. 40-42.

19 *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 36.

20 De mogelijke kritiek dat 'telecommunicatie' een (te) techniekafhankelijke formulering zou zijn, deel ik niet. Het is een abstract begrip dat, letterlijk, communicatie op afstand aanduidt; het kan alle technische verschijningsvormen daarvan omvatten en hoeft niet noodzakelijk gekoppeld te zijn aan het striktere begrip uit de Telecommunicatiewet.

De vraag of het 'live-gesprek' ook beschermd moet worden en zo ja, hoe, moet mijns inziens worden losgekoppeld van de vraag hoe het brief-, telefoon- en telegraafgeheim moet worden herzien. De reden hiervoor is gelegen in de historische achtergrond van art. 13 Gw als een transportgeheim. Er zijn denk ik goede redenen om onmiddellijke communicatie (zoals ik het liever zou noemen, ter onderscheiding van de middellijke vormen van communicatie, die een communicatiekanaal gebruiken) grondrechtelijk te beschermen, nu op afstand afluisteren simpel en onzichtbaar kan plaatsvinden. Bescherming via art. 13, zoals het minderheidsstandpunt voorstelt, is mogelijk, maar laten we ons daar niet op blindstaren. Het gaat mijns inziens om een ander type kwetsbaarheid dan bij het transportgeheim aan de orde is. Bij dit laatste speelt dat gegevens aan een derde worden toevertrouwd – waarmee beschikkingsmacht uit handen wordt gegeven – terwijl het bij onmiddellijke communicatie meer gaat om heimelijke observatie. De kwetsbaarheid van heimelijke observatie speelt eveneens bij het huisrecht (infrarood- en terahertzcamera's) en bij lichamelijke integriteit (infrarood- en mobiele bodyscanners), evenals bij niet-communicatieve uitingen zoals heimelijke observatie van privégedrag. In plaats van bescherming van onmiddellijke communicatie bij art. 13 onder te brengen, zou men ook kunnen overwegen een zelfstandig artikel te creëren dat bescherming biedt tegen alle vormen van (directe)[21] heimelijke observatie, als nieuwe verbijzondering van het algemene privacyrecht.

Tot slot nog het vraagstuk van verkeersgegevens. De commissie vindt deze beschermwaardig, maar niet in bijzondere mate. In lijn met de keuze voor bescherming van de inhoud van communicatie als zodanig, vindt de commissie dat het algemene recht van art. 10 Gw of het nieuwe grondrecht op gegevensbescherming voor verkeersgegevens volstaat. Het minderheidsstandpunt wil ze wel als zelfstandige categorie beschermen in art. 13, maar de argumentatie daarvoor (p. 152-153) is minder overtuigend dan het de rest van het minderheidsvoorstel op dit terrein. Het feit dat verkeersgegevens in allerlei regelgeving worden beschermd en gevoelige informatie bevatten en dat regelgeving (Richtlijn 2002/58/EG) ook bedrijfsverkeersgegevens beschermt (welke gegevens niet onder het grondrecht op gegevensbescherming vallen), geeft mijns inziens onvoldoende basis om deze gegevens als zelfstandige categorie te beschermen.[22] Bedrijfs(verkeers)gegevens verdienen geen constitutionele bescherming, terwijl verkeersgegevens qua gevoeligheid niet kwetsbaarder zijn dan veel andere soorten gegevens (zoals financiële, seksuele of etnische). Als men vindt dat gevoelige gegevens aanvullende bescherming behoeven, gezien de ruime beperkingsclausules in art. 10 en het grondrecht op gegevensbescherming, dan kan men beter in die grondrechten een

21 Ter onderscheiding van de observatie via derden, die bij het communicatietransportgeheim aan de orde is.

22 Het enige steekhoudende argument om verkeersgegevens wél in art. 13 te vermelden, noemt het rapport niet; dat is het argument van de Amsterdamse school dat verkeersgegevens zodanig samenhangen met het gebruik van een communicatiekanaal dat ze gezamenlijk beschermd moeten worden; anders zou bijvoorbeeld het kennisnemen van verkeersgegevens een verkillend effect kunnen hebben op de mogelijkheid om vertrouwelijk te telecommuniceren. Zie Asscher 2003, p. 245; W. Steenbruggen, *Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk*, diss. Amsterdam (UvA), Amsterdam: Otto Cramwinckel 2009, p. 57.

aanvullend lid opnemen dat zwaardere eisen stelt aan kennisneming en verwerking van gevoelige persoonsgegevens in het algemeen.[23]

5. Vrijheid van meningsuiting

Art. 7 Gw. is vermoedelijk het meest ingrijpend aan vernieuwing toe, en de commissie besteedt dan ook evenveel pagina's aan art. 7 als aan art. 10 en 13 gezamenlijk. Er spelen diverse vraagstukken: niet alleen de actualisering van de pre-digitale 'drukpers' maar ook of en, zo ja, hoe ontvangst en garing, radio en televisie, minderjarigen en handelsreclame apart vermelding behoeven. Daarnaast speelt het vraagstuk van pluriformiteit van de media, dat de Commissie-Franken al aansneed. Opmerkelijk is dat over het hoofdpunt – de herformulering van het algemene recht in lid 1 – de commissie een unaniem standpunt inneemt, terwijl over de overige onderwerpen vaak verschillend wordt gedacht. Over al deze onderwerpen valt veel te zeggen, maar ik laat de discussie daaromtrent over aan specialisten op dit terrein.

Hier wil ik mij beperken tot het algemene punt van wat de kern is of zou moeten zijn van het grondrecht op vrijheid van meningsuiting in het digitale tijdperk. Volgens de commissie biedt art. 7 historisch 'een verbod voor de overheid om van burgers te eisen dat zij voorafgaande toestemming van de overheid vragen voor het uiten van gedachten en gevoelens (het openbaren)' (p. 71), waarop de commissie zoveel mogelijk wil aansluiten, behoudens het terechte vervangen van 'gevoelens' door 'meningen'. Waar het artikel voorheen primaat gaf aan openbaring via de drukpers, stelt de commissie dat er in het digitale tijdperk 'nieuwe categorieën van voor vrije meningsuiting geschikte media, zoals die welke gebruik maken van internet' (p. 70) zijn bijgekomen, en stelt daarom een geheel mediaonafhankelijke formulering voor. Deze formulering drukt een algemeen openbaringsrecht uit, ongeacht medium.

De commissie lijkt er hier van uit te gaan dat de opkomst van de zogeheten 'nieuwe media' simpelweg een aanvulling zijn op het medialandschap dat vroeger bestond uit drukpers, radio en tv. Daarom volstaat zij met een primair wetstechnische herformulering die geen inhoudelijke reflectie biedt op de kern van de bescherming. Daarmee miskent de commissie dat het Internet en de daarmee samenhangende 'nieuwe media' niet alleen een uitbreiding zijn van het arsenaal aan uitingsmogelijkheden, maar ook gepaard gaan met fundamentele maatschappelijke veranderingen in communicatie en gedrag.

Fortuyn voelde enkele jaren geleden de tijdsgeest haarfijn aan met zijn adagium 'Ik zeg wat ik denk en ik doe wat ik zeg.' Dit Fortuynisme gaat ervan uit dat je eerst iets denkt en dat vervolgens zegt. Sommige blogs

23 Daarmee is overigens niet gezegd dat (bepaalde categorieën) verkeersgegevens geen aanvullende bescherming behoeven in *lagere* wetgeving; zie daarover A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006; J.C. Fischer, *Communications Network Traffic Data. Technical and Legal Aspects*, diss. Eindhoven, Eindhoven: TU/e 2010.

wekken echter de indruk dat er niet altijd een verband bestaat tussen zeggen en denken. Ook het laatste deel van het adagium wordt inmiddels regelmatig omgedraaid in het Twittertijdperk: niet 'ik doe wat ik zeg' maar 'ik zeg wat ik doe'. Kijk naar tweets als 'Pff, de verwarming in de trein is wel heel erg opgestookt' of 'Op thuiswerkdag nu even in wachtkamer van mondhygiëniste. Moet helaas ook gebeuren'.[24] Zijn dit 'gedachten' of 'meningen' in de zin van het voorgestelde art. 7 lid 1 Gw? Zonder definitie of nadere omschrijving van deze begrippen – waar de commissie niets over zegt – heeft de rechter veel interpretatievrijheid om de begrippen 'gedachte' en 'mening' al dan niet van toepassing te achten op dergelijke uitingen in het web 2.0-tijdperk. Misschien gaat het bij een deel van wat er op nieuwe media te lezen, te zien en te horen valt, niet zozeer om een functioneel equivalent van de oude drukpers, maar eerder om een functioneel equivalent van de rondzendbrief, waarbij het niet primair gaat om het *openbaren* van een uiting maar meer om het *communiceren* van een uiting naar een (meer of minder bepaalde) groep volgers. In web 2.0 liggen publieke communicatie en niet-publieke communicatie dicht tegen elkaar aan. Het feit dat een uiting publiek *beschikbaar* is, wil niet per se zeggen dat het ook een publieke *functie* heeft. Asscher merkt op dat het niet vaststaat dat art. 7 ook van toepassing is op 'niet-openbaar bedoelde communicatie'.[25] Wie voorstelt om het censuurverbod medianeutraal te formuleren, zal in dat licht op zijn minst nader moeten aanduiden wat moet worden verstaan onder 'gedachten', 'meningen' en 'openbaren' en hoe deze van toepassing zijn op nieuwe media.[26]

Als men nu kiest voor een ruim toepassingsbereik van het 'openbaren van gedachten of meningen' – waar veel voor te zeggen valt, omdat het moeilijk is een afbakeningslijn te trekken – zal er, de kernrechtgedachte indachtig, wel iets moeten worden gezegd over wat tot de kern en wat tot de periferie van het censuurverbod behoort. Ook hier laat de commissie een steek vallen, door nauwelijks aan te duiden waar we de kern moeten zoeken. Daarmee heeft de rechter geen houvast om de proportionaliteit te kunnen beoordelen van inbreuken op de vrije meningsuiting. Wanneer de wetgever het medianeutrale voorstel van de commissie overneemt, zal hij in de toelichting hopelijk uitgebreider en scherper dan de commissie ingaan op wat de kern van de vrije meningsuiting is. Wat mij betreft gaat het bij de vrije meningsuiting in de kern om het publieke belang dat gedachten en meningen vrijelijk kunnen worden geuit, waarmee het publieke debat kan worden verrijkt, verbreed en verscherpt. Dat is geen absoluut onaantastbare kern, maar wel een kern waar de motiveringsplicht voor censuurmaatregelen het zwaarst, en de rechterlijke toetsing van proportionaliteit van die maatregelen het scherpst is.

24 Twee tweets van Valérie Frissen op 11 resp. 28 januari 2011, <http://twitter.com/vfrissen>.

25 Asscher 2003, p. 236.

26 Vgl. over de complexe toepasbaarheid van het begrip 'openbaarheid' op Internet: S. van der Hof e.a., *Openbaarheid in het internettijdperk. De invloed van ICT op juridische concepten van openbaarheid*, Den Haag: Sdu 2006.

6. Toegang tot overheidsdocumenten

Er valt veel te zeggen over de vraag of en in hoeverre er een grondrecht moet komen op toegang tot (of openbaarheid van) overheidsinformatie of, iets beperkter maar wel relevanter, overheidsdocumenten. Daar is weinig ruimte voor binnen het bestek van deze bijdrage – evenals bij de commissie die dit niet in haar taakopdracht zag. Een driepersoonsminderheid stelt een grondrecht voor op toegang tot bestuurlijke documenten, in aanvulling op art. 110 Gw (p. 90-91). Ik deel de gedachte van de minderheid dat een dergelijke toegang de kern raakt van de mogelijkheid het openbaar bestuur te controleren en dat de pers de publieke taak om aan deze controle bij te dragen alleen kan uitvoeren als de overheid voldoende transparant is. Over de kern van waartoe dan toegang moet kunnen worden verkregen, evenals misschien over de constitutiewaardigheid van dit belang, is verdere discussie nodig.

In het verlengde van mijn betoog over de vrije meningsuiting wil ik ten behoeve van die discussie in elk geval meegeven dat hier óók moet gaan over de rol die Internet speelt in de huidige samenleving. WikiLeaks is nu nog in het (eerste) hypestadium, maar het idee achter WikiLeaks is fundamenteel en blijvend. Daar waar overheden te veel neigen tot geheimhouding, zal vroeg of laat, via een server in Buðardálur of Breda,[27] gelekt worden naar de openbaarheid. De vraag is of de overheid een Internetoorlog wil aangaan door veldslagen te voeren met WikiLeaks en zijn toekomstige opvolgers, of dat de overheid de transparantie-extremisten een stap voor is – de aanval is de beste verdediging – door proactief en serieus werk te maken van openbaarmaking van overheidsdocumenten. Uit zichzelf is de overheid daar niet bijzonder toe geneigd, zo leert de ervaring. Met een grondrecht op toegang tot overheidsdocumenten kan veel beter dan momenteel het geval is een balans worden bereikt tussen transparantie waar mogelijk en afscherming waar nodig. Daarmee verdwijnt WikiLeaks niet geheel uit beeld – er zullen altijd transparantie-extremisten blijven – maar er is dan wel een dusdanig betere controle op de overheid door de pers mogelijk, dat er minder noodzaak is voor bezorgde ambtenaren om via lekken aan WikiLeaks de klok te luiden.

7. Wat er niet in het rapport staat

De commissie had, wat digitale grondrechten betreft, een beperkte opdracht en heeft ervoor gekozen (in dit opzicht) niet buiten die opdracht te werken. Dat valt de commissie niet te verwijten. Toch staat er daardoor het nodige *niet* in het rapport, waar tenminste wel over gedebatteerd zou moeten worden in het kader van de discussie over grondrechten en tech-

27 In navolging van IJsland krijgt ook Breda een eigen WikiLeaks, zie *Binnenlands Bestuur* 9 december 2010, <http://www.binnenlandsbestuur.nl/breda-krijgt-eigen-wikileaks.487374.lynkx>.

nologie. Ik stip hier een aantal onderwerpen aan die hopelijk in het vervolgtraject opgepakt kunnen worden in de discussie.
Drie grondrechten buiten de taakopdracht zijn qua formulering of inhoud mogelijk niet toegesneden op het digitale tijdperk. Het petitierecht (art. 5 Gw) spreekt van 'schriftelijke verzoeken', wat geen urgent probleem is nu de minister elegant maar enigszins creatief 'schriftelijk' heeft geïnterpreteerd als ook 'elektronisch' omvattend.[28] De techniekafhankelijke (fysieke) formulering van het huisrecht in art. 12 Gw ('binnentreden') verdient aanpassing tot een algemene formulering (bijvoorbeeld 'de woning is onschendbaar'). Ook is het recht op lichamelijke integriteit wellicht toe aan herinterpretatie nu van buitenaf heimelijk op of in het lichaam kan worden gekeken (denk aan bodyscanners, of aan de infraroodcamera's die bij de SARS-epidemie op vliegvelden werd ingezet). Dit laatste roept ook de vraag op of, vergelijkbaar met art. 12 Gw, een notificatieplicht nodig is voor burgers op wier grondrechten inbreuk is gemaakt als zij daarvan niet uit de aard der zaak op de hoogte zijn. Verhey merkt al op dat de commissie geen aandacht besteedt aan notificatie bij art. 13 Gw, terwijl dat juist bij alle voorgaande voorstellen een gemeenschappelijke aanbeveling was. Ook voor andere vormen van heimelijke observatie valt er veel te zeggen voor een notificatieplicht. Wellicht kan in de algemene beperkingsclausule een lid worden opgenomen dat bepaalt dat burgers in kennis worden gesteld wanneer hun grondrechten heimelijk zijn beperkt; daarbij kan desgewenst een uitzondering worden opgenomen, zoals in art. 12 lid 3 Gw, dat de notificatie volgens bij wet te stellen regels kan worden uitgesteld in het belang van de strafvordering of de nationale veiligheid.
In de tweede plaats kan bekeken worden of er *nieuwe* grondrechten nodig zijn in het digitale tijdperk. In de literatuur wordt vooral nagedacht over een recht op vergeten.[29] Nu het collectieve digitale geheugen onverbiddelijk is – wat eenmaal op Internet staat krijg je niet of nauwelijks meer weg – kunnen mensen meer en meer geconfronteerd met hun uitspraken of gedrag in het verleden, ook waar het opmerkingen betreft die vroeger terloops over de heg of in de kroeg vervlogen maar die nu, geblogd en getwitterd, opgeslagen worden voor wie weet hoe lang. Wellicht moet een grondrecht worden geformuleerd dat mensen beschermt tegen onredelijke confrontatie met jeugdzonden en oude koeien (en kalfjes) uit de digitale sloot. Dat is zowel relevant in de relatie overheid-burger, bijvoorbeeld bij vergunningverlening en in het (bestuurs)strafrecht, als in horizontale verhoudingen, bijvoorbeeld in het arbeidsrecht en het privaatrechtelijke privacyrecht. Nadere discussie is welkom of een eventueel recht op vergeten meer past bij een grondwettelijke regelopdracht tot gegevensbescherming of dat een zelfstandig afweerrecht zou moeten worden geformuleerd.

28 *Kamerstukken II* 2004/05, 27 460, nr. 3, p. 1-2.
29 V. Mayer-Schönberger, *Delete : the virtue of forgetting in the digital age*, Princeton: Princeton University Press 2009.

Voorts kan men aan de regering meegeven dat zij zich, bij het streven de Grondwet actueel te houden in het licht van technische ontwikkelingen, niet moet blindstaren op het digitale tijdperk. Zoals Buruma terecht opmerkte: waar de twintigste eeuw de eeuw was van de ICT (met *1984* als paradigma voor discussie), zo wordt de eenentwintigste eeuw de eeuw van de biotechnologie (met *Brave New World* als paradigma voor discussie).[30] Deze ontwikkeling vraagt evenzeer als het digitale tijdperk om fundamentele bezinning op de grondrechtencatalogus, die niet kan wachten tot de regering in 2047, als de bio-revolutie is uitgekristalliseerd, een Staatscommissie Grondrechten in het bio-tijdperk instelt. Humane biotechnologie is, in de woorden van NJV-preadviseur Bovenberg, '*au fond* een manifestatie van het eeuwige streven van de mens om grip te krijgen op het begin, het verloop, de kwaliteit en het einde van zijn leven.'[31] Als er ergens grondrechten relevant zijn, dan is het wel hier. Het zou treurig zijn als onze Grondwet niet is toegerust om mede richting te geven aan de manier waarop in de komende eeuw dit streven naar greep op het leven vorm krijgt. De enkele verwijzing naar 'menselijke waardigheid' in de door de commissie voorgestelde algemene bepaling (p. 40-42) zal in elk geval niet in staat zijn om enige richting te geven aan wetgeving en praktijk rond biotechnologie; het concept 'menselijke waardigheid' is daarvoor te vaag en te multi-interpretabel.[32] Wat dan wel nodig is, moet binnen afzienbare termijn worden bediscussieerd. Aanzetten daarvoor bestaan al.[33] Het is aan de regering om nu een proactief beleidstraject over grondrechten in het bio-tijdperk uit te zetten.

8. Conclusie

Ik heb de GDT-voorstellen van de Staatscommissie besproken om te bekijken of ze adequaat zijn voor het digitale tijdperk. Ik stelde in de inleiding dat er twee redenen kunnen zijn voor de regering om, na de veelheid van eerdere voorstellen, opnieuw een commissie over GDT te laten adviseren: een gezaghebbend eenduidig advies en actualisering in het licht van nieuwe ontwikkelingen.

Helaas is de Staatscommissie in beide opzichten niet goed in haar opdracht geslaagd. Van stroomlijning van eerdere voorstellen tot een gezaghebbend advies is weinig terechtgekomen, door de verdeeldheid van de commissie die zichtbaar is in de minderheidsstandpunten – ook op kernonderdelen van de materie – en eveneens in de summiere toelichting die, zoals Verhey terecht stelt, lijkt te wijzen op onderlinge meningsverschillen over hoe het advies geïnterpreteerd moet of kan worden.

Wat actualisering betreft wordt een goede poging gedaan voor art. 7 (vrije meningsuiting), art. 10 (privacy en gegevensbescherming) en art. 13

30 Y. Buruma, 'Brave New World 2009', *Nederlands Juristenblad* 2009, p. 1.

31 J.A. Bovenberg, 'Het Antoni van Leeuwenhoek-recht: pleidooi voor een nieuw grondrecht', in *Handelingen Nederlandse Juristen-Vereniging* 2009-I, p. 61-96, op p. 95.

32 Vgl. D. Beyleveld en R. Brownsword, *Human dignity in bioethics and biolaw*, Oxford , New York: Oxford University Press 2001.

33 Bovenberg 2009; B.J. Koops, 'Over "mensen" en "mensen"-rechten. De maakbare mens bezien vanuit het perspectief van grondrechten', in: B.J. Koops e.a. (red.), *De maakbare mens*, Amsterdam: Bert Bakker 2009, p. 279-310.

(post- en telecommunicatiegeheim), maar de poging strandt wat mij betreft halverwege door het gebrek aan doordenken van wat het digitale tijdperk behelst. Positief is dat een zelfstandig grondrecht op gegevensbescherming wordt voorgesteld, maar het lijkt in de kern niet goed doordacht: wat betekent de vormgeving als subjectief (afweer)recht voor het verwerken van persoonsgegevens in een informatiesamenleving en -economie? Wat beoogt het precies te beschermen, welke dataprotectiebeginselen vallen er wel of niet onder, en hoe werkt dit door in horizontale verhoudingen?

Vooral wat de communicatiegrondrechten betreft, toont het rapport een beperkte visie op de betekenis van het digitale tijdperk. Het lijkt erop alsof de commissie vooral een wetstechnische exercitie heeft doorlopen om de in art. 7 en 13 genoemde 'oude media' uit te breiden met 'nieuwe media' en dat vervolgens 'medianeutraal' te formuleren. Daardoor wordt de reikwijdte van beide artikelen heel breed, maar daarmee vervaagt ook de kern van wat deze grondrechten precies beogen te beschermen. Zoals Asscher opmerkt, biedt een techniekneutrale formulering alleen rechtszekerheid als 'voor de wetgever en de rechter buiten kijf staat wat de inhoud is van het recht',[34] en daarvoor bieden de commissievoorstellen te weinig houvast.

Bij art. 13 stelt de commissie communicatie *als zodanig* centraal, waarmee de primaire koppeling vervalt met transport via de communicatie-infrastructuur. De commissie lijkt geen oog te hebben voor de functie die deze infrastructuur in het digitale tijdperk heeft: het gaat niet alleen meer om communicatie, maar ook om opslag van eigen gegevens bij *cloud-computing*. Daarbij komt dat commissie inconsistent is om vertrouwelijke communicatie als zodanig als beschermingskern aan te wijzen en tegelijk de bescherming te beperken voor de duur van transport; ook communicatie buiten transport zou in deze benadering bescherming tegen een meelezende overheid moeten bieden. Zowel vanuit historisch als vanuit inhoudelijk oogpunt valt er veel voor te zeggen het communicatiegeheim in het digitale tijdperk als kanaalbescherming te blijven vormgeven.

Waar het huidige art. 7 openbaring van gedachten en meningen tegen censuur beschermt gekoppeld aan de drukpers, stelt de commissie een algemeen openbaringsrecht voor, ongeacht medium. Nu in het web 2.0-tijdperk publiek beschikbare uitingen niet alleen een openbaringsfunctie kunnen hebben maar ook een (niet-publieke) communicatiefunctie, vraagt de medianeutrale formulering om een nadere toelichting van de begrippen 'gedachten', 'meningen' en 'openbaren'. Wanneer daarbij een ruim toepassingsbereik wordt gekozen, is vervolgens meer toelichting nodig dan de commissie biedt – met het oog op de kernrechtgedachte – wat tot de kern van het censuurverbod behoort. De wetgever zou in de

34 Asscher 2003, p. 242.

toelichting bij een medianeutraal art. 7 lid 1 Gw wellicht kunnen aanknopen bij het publieke belang van het *openbaar* maken van een uiting, bijvoorbeeld in het kader van het publieke debat.
Door de nadruk op wetstechnische aanpassingen en onderbelichting van de functie van de grondrechten in het digitale tijdperk, raakt de kern van deze grondrechten uit beeld. Dat is des te spijtiger, nu de commissie in de voorgestelde kernrechtbepaling stelt dat de kern van grondrechten onaantastbaar moet blijven. Waar de commissie er zelf niet in slaagt om een helder beeld te schetsen van waar we de kern van art. 7, 10 en 13 Gw moeten zoeken, zullen wetgever en rechter niet uit de voeten kunnen met deze kernrechtbepaling.

Het is al met al geen gelukkige zet geweest van de regering om zich te laten adviseren over grondrechten in het digitale tijdperk door deze commissie. De samenstelling van grotendeels staatsrechtgeleerden heeft ertoe geleid dat er geen samenhangende visie is ontwikkeld op de betekenis van grondrechten in het digitale tijdperk. Het enige lid in de commissie dat vermoedelijk met het oog op dit onderwerp in de commissie is benoemd, geeft wel blijk van enig begrip van actuele technische ontwikkelingen, maar het feit dat we dit moeten lezen in bijlagen met minderheidsstandpunten geeft aan dat zij de andere leden niet heeft kunnen overtuigen. Anders dan de commissie lijkt te denken, gaat het in het digitale tijdperk niet simpelweg om een vervanging van oude technologie door nieuwe technologie – vroeger drukte je een stencil, nu stuur je een tweet. Het digitale tijdperk gaat gepaard met fundamentele maatschappelijke veranderingen in communicatie en gedrag. De grondrechten moeten daarom niet zozeer techniekneutraal worden geherformuleerd, maar veeleer opnieuw worden doordacht in hun betekenis voor de burger in een veranderde maatschappelijke context.[35]
En overigens ben ik van mening dat art. 12 Gw aangepast moet worden.[36]

35 Zie ook ibid., p. 238-240.
36 Koops e.a. 2004.