

Digitale grondrechten

De Nederlandse staatsburger hoeft weinig te verwachten van zijn Grondwet waar het aankomt op de verdediging van zijn vrijheden in het digitale tijdperk. Het is, zo betoogt de auteur, in veel opzichten een verouderd en dood instrument. Het zou met onze vrijheden snel bergafwaarts gaan als het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) onze Grondwet niet zo vaak de jure en de facto zou overstijgen. We mogen onze Europese zegeningen wel tellen.

Er bestaan geen digitale grondrechten. Er bestaan wel grondrechten, rechten van burgers die de grens van de overheidsmacht markeren. Een aantal daarvan gaat over informatieprocessen. Dat is al zo sinds de Grondwet werd opgesteld. Maar wat nieuw is, is dat die rechten steeds gemakkelijker zijn uit te oefenen en te beperken. En dus zijn ze ook makkelijker naar twee kanten te misbruiken: in het gebruik (bijvoorbeeld schelden op internet) en in de beperking (zoals door het op grote schaal af luisteren van vertrouwelijke communicatie). Over deze informatiegrondrechten zal ik het hier hebben.

Laten we bij het begin beginnen: de grondrechten in de Nederlandse Grondwet. Ze staan in het eerste hoofdstuk van de Grondwet. Je zou zeggen: dat is mooi. Dat is het natuurlijk ook, maar het is toch minder mooi dan het lijkt, want die grondrechten kunnen maar in beperkte mate door de Nederlandse rechter worden toegepast, namelijk niet als het om daden van wetgeving gaat. Dat heet in het staatsrechtelijke jargon: het toetsingsverbod, wat wil zeggen dat de rechter wetten niet aan de Grondwet mag toetsen. Of zoals het zo plechtig in artikel 120 van de Grondwet staat: ‘De rechter treedt niet in de beoordeling van de grondwettigheid van wetten en verdragen.’

De rechter, die in de trias politica bij uitstek degene is die burgerlijke vrijheden moet beschermen tegen de wetgevende en uitvoerende macht (‘Le pouvoir arrête le pouvoir’, zoals Montesquieu het zo mooi zei in *De l’esprit des*

lois), staat dus buitenspel op een van de belangrijkste gebieden waar overheidsmacht wordt uitgeoefend. In het systeem van de Grondwet zou dat vacuüm moeten worden opgevuld door de wetgever zelf, immers degene die in hoofdstuk 1 wordt aangesproken. Dat betekent, zo is de staatsrechtelijke gedachtegang, dat de wetgever in dit hoofdstuk kan opzoeken wat de grenzen van zijn macht zijn. In de praktijk komt daar natuurlijk weinig van terecht, want hij heeft wel wat anders aan zijn hoofd: hoe houd ik steeds wankelere coalities bij elkaar, hoe krijg ik een sluitend budget, hoe druk ik de punten van het regeerakkoord erdoor, enzovoort. Burgerlijke vrijheden, kom op zeg, het politieke bedrijf is al ingewikkeld genoeg. Dat is dus het eerste nadeel van dat toetsingsverbod.

Het tweede nadeel is dat de formulering van de grondrechten ge-

Is de pc een drukpers, een telefoon of een brief?

dateerd is. Hoe zijn ze dan geformuleerd? Als ik de term ‘digitale grondrechten’ vertaal naar de zinnvollere term ‘informatiegrondrechten’, moeten we voor de huidige informatietechnologie kijken naar ten minste acht artikelen: de artikelen 6 tot en met 13. Artikel 6 gaat over godsdienst en gewetensvrijheid en daar is geen woord techniek bij. De artikelen 8 en 9, over de vrijheid een vereniging op te richten en de vrijheid om te demonstreren, zijn ook nog redelijk techniekneutraal. Maar bij de vrijheid van meningsuiting in artikel 7 gaat het mis, want daarin ligt het accent op de drukpers. Artikel 10 gaat over privacy. Aha, denkt de burger van vandaag, dat is belangrijk, maar hij komt bedrogen uit. In het artikel staat eigenlijk niet meer dan dat de wetgever het ‘recht op eerbiediging van de persoonlijke levenssfeer’ en ‘het vastleggen en verstrekken van persoonsgegevens’ in verband daarmee moet regelen. Dat is dus geen beperking, maar een carte blanche voor de wetgever. De artikelen 11 en 12 beschermen fysieke privé-cirkels: het menselijk lichaam en het eigen huis. Maar die

cirkels zijn met bodyscanners en DNA-analyses, telelizen en richtmicrofoons volkomen doorzichtig geworden. En is het hacken van een privécomputer huisvredebreuk? Dan komt artikel 13, dat zegt dat het briefgeheim en het telefoon- en telegraafgeheim onschendbaar zijn. Maar vraag een facebooker-tje van vandaag wat een ‘telegraaf’ is en die zal in het beste geval antwoorden dat het een ochtendkrant is.

Daarin schuilt nu het tweede nadeel van het toetsingsverbod: er is geen rechter die de grondrechten naar de eisen van de tijd mag vertalen.

Als je dit verbrokkelde en gedateerde geheel over de netwerksamenleving van vandaag heen legt, is wel duidelijk dat ze niet op elkaar passen. Een pc wordt voor privé- en openbare communicatie gebruikt. Is die een drukpers, een telefoon of een brief? Bij iedere communicatie in een netwerk produceert een gebruiker een wolk van gegevens die meer over de zender en de ontvanger zeggen dan de inhoud van de boodschap zelf. Dat zijn de zogenaamde metadata (adres- en locatiegegevens) waarover bij de NSA-affaire zo veel te doen is. Vallen die gegevens nu onder het telefoon- of het briefgeheim? De veiligheidsdiensten menen over het algemeen van niet. De grenzen van het privéleven zijn steeds vager, evenals die tussen waarnemen en vastleggen. Het draait steeds meer om te interpreteren data. De reken- en combinatiekracht van computers is zo sterk dat ook uit ver van een individu verwijderde gegevens tot de persoon herleidbare data zijn te destilleren. De Big Data-beweging heeft het onderscheid tussen algemeen toegankelijke (tot het publieke domein behorende) gegevens en tot de persoon herleidbare (en af te schermen) gegevens weggevaagd. De burger van vandaag zit gevangen als een vliegje in een web.

Is er dan helemaal geen bescherming van grondrechten in Nederland? Jawel, en dat komt paradoxaal genoeg door diezelfde Grondwet. Artikel 94 van de Grondwet opent namelijk een doorgeefluik voor internationale regels die voor burgers bindend zijn. Als nationale regels strijdig zijn met internationale, geeft het artikel voorrang aan de laatste. Dankzij die

bepaling moet de Nederlandse rechter de internationale mensenrechtverdragen toepassen, waarvan het EVRM het belangrijkste is. Dat Verdrag is zo belangrijk omdat er een Hof voor de Rechten van de Mens is dat voor de lidstaten bindende interpretaties van de in het verdrag gegarandeerde rechten geeft en ook beginselen formuleert voor de proportionele beperking daarvan, waar nationale autoriteiten zich aan moeten houden.

En zo passeert de Nederlandse rechter het grondwettelijke verbod om wetten aan de Grondwet te toetsen, met dank aan de grondwettelijke plicht wetten aan verdragen te toetsen. Deze tamelijk absurde situatie is alleen uit te leggen door juristen die in het staatsrecht hebben doorgeleerd, maar fortuinlijk is het in ieder geval wel. Vanuit de problematiek van deze bijdrage heeft het twee voordelen. Ten eerste is de formulering van de grondrechten in het Verdrag tamelijk techniekneutraal, zodat de verdragstekst eenvoudig aan nieuwe technische en sociale situaties is aan te passen. Bovendien hanteert het Hof de leer van het ‘living instrument’, wat wil zeggen dat het verdrag mee moet evolueren met nieuwe opvattingen en met ontwikkelingen op het sociale en technische vlak. Langs deze twee wegen is het Hof er steeds in geslaagd het privacyrecht, het communicatiegeheim en de vrijheid van meningsuiting te beschermen tegen erop ingrijpende ontwikkelingen in de informatietechnologie, in zekere zin dus om deze rechten te ‘digitaliseren’.

Het moge duidelijk zijn dat dit doorgeefluik en de grote invloed van het Europese Hof de Thierry Baudetjes van deze wereld niet aanstaat, omdat het soevereiniteit afsnoept van de nationale staten. Maar we moeten eerder blij zijn dat het zo gelopen is, omdat het er voor de grondrechtelijke bescherming in Nederland anders slecht had uitgezien. De dikwijls bepleite route van ingrijpende aanpassing van de Grondwet is overigens illusoir. Tot tweemaal toe hebben grondwetscommissies de afgelopen jaren voorstellen gedaan om het toetsingsverbod op te heffen en de informatiegrondrechten up-to-date te maken, maar met heel weinig succes. Met de steeds krapere en vaker wisselende politieke meerderheden is de zware besluit-



Verschillende communicatiesatellieten

vorming (tweederde meerderheid in twee lezingen voor een wijziging van de Grondwet) over ieder enigszins controversieel onderwerp nagenoeg onmogelijk geworden. We kunnen dat internationale doorgeefluik dus maar beter open houden!

DE DIGITALE WERELD

Wat zijn nu de problemen bij de digitalisering van de informatiegrondrechten? Ik tel er vijf: twee algemene en drie specifiek informatierechtelijke die betrekking hebben op de openbare communicatie, privécommunicatie en de afbakening en overlap tussen die twee. We beginnen met de drie specifieke problemen.

Bij de openbare communicatie zijn we gaandeweg een vergaande bescherming gaan toekennen aan een institutie als de pers. De pers heeft grote vrijheid een robuust openbaar debat te voeren en te entameren, en geniet voorrechten in de vorm van bronbescherming. Ook kan zij toegang tot informatiebronnen eisen. Het Europese Hof heeft bij zijn uitleg van artikel 10 van het Verdrag (dat over vrijheid van meningsuiting handelt) de rol van de pers als waakhond van de democratie zwaar aangezet. Daarbij leunt het sterk op de na de Tweede Wereldoorlog in de VS in zwang gekomen theorie van de *social responsibility* van de pers, omdat het in artikel 10 niet alleen gaat over de vrijheid maar ook over 'duties and responsibilities' bij de uitoefening daarvan. De pers heeft in de visie van het Hof de plicht te goeder trouw en in overeenstemming met een journalistieke ethiek te handelen.

Dit hele normatieve institutionele gebouw dreigt in het internettijdperk om te vallen. De verzwakking van de oude 'trusted media' en de proliferatie van nieuwe individuele – maar openbare – media heeft het normatieve kader van deze vrijheid aanmerkelijk verzwakt. De zwakke feitelijke basis waarop er op internet vaak nogal ruige aanvallen op personen worden gedaan, zijn er een voorbeeld van. Die lijken vaak minder op nieuws dan op de lastercampagnes die we kennen uit zeventiende- en achttiende-eeuwse pamfletten. Om een ander, beschaafder, voorbeeld te noemen: een digitale 'krant' als *De Correspondent*, die zichzelf als nieuw kwaliteitsmedium boven de andere in-

ternetmedia wil plaatsen, geeft geen enkel uitsluitel over wat het al dan niet beschouwt als zijn journalistieke verantwoordelijkheden. Op de website staat een rondkend missiestatement, maar daar blijft het bij. Onderschrijft het medium een journalistieke code? Is er een klachteninstantie? Is er een ingezonden-brievenrubriek? Is er een opiniepagina? Of blijft het bij opiniërend gebabbel met een reactieknop eronder? Waar is de uitgever gevestigd? Is die eigenlijk wel (juridisch) aanspreekbaar (volgens zijn website doet hij in boekbesprekingen)? Waarom is een 'correspondent' eigenlijk een journalist die ik als democratisch burger te woord moet staan als daarom gevraagd wordt?

Het tweede probleem betreft de vermenging van privé- en open-

Veel gebruikers weten niet of zij op internet privé of openbaar communiceren

bare communicatie, zowel aan gebruikers- als aan verspreiderskant. Veel gebruikers weten niet of zij op internet privé of openbaar communiceren. Het uit de hand gelopen Facebook-verjaardagsfeestje Project X in Haren is een extreem voorbeeld van wat een iets te onnadenkend ingedrukte verzendknop voor maatschappelijke gevolgen kan hebben. Het monitoren van e-mailverkeer voor reclamedoeleinden is een ander voorbeeld. Aan de kant van de verspreider is er een identiteitsconflict tussen de rol van telecommunicatieaanbieder – die zich op het telefoongeheim beroept omdat hij niet op de inhoud van de boodschappen die hij verspreidt wil worden aangesproken ('het telefoongeheim is onschendbaar') – en de rol van media-aanbieder, die verantwoordelijkheid aanvaardt voor de informatie die hij publiceert. Voor rechters is het nog steeds moeilijk om de grens tussen die twee vrijheden te trekken. Moeten zij het telefoongeheim beschermen of de vrijheid van meningsuiting?

Het derde probleem zit hem in de vervaging van begrippen als 'persoonlijke communicatie', 'per-

soonsgegeven' en 'algemene data'. Ik stipte dat hierboven al aan toen ik het over metadata en Big Data had. Het object van het grondrecht van het telefoongeheim placht de inhoud van de communicatie te zijn. In de klassieke wereld van de post- en de telecommunicatie waren inhoud en adressering goed te scheiden. Het adres stond op de enveloppe, de brief met inhoud zat erin, en het telefoongesprek en de adressering van het gesprek verliepen via gescheiden kanalen. Dat is niet meer zo. De adresregel van een e-mailbericht loopt over in de inhoud van het bericht. Maar dat is niet alles: metagegevens zeggen vaak zelfs meer over iemands privéleven dan de daadwerkelijke inhoud van diens mededelingen; beheersing van grote hoeveelheden anonieme gegevens maken privégedragingen zichtbaar, ja zelfs voorspelbaar.

DIGITALE MIST

De twee meer algemene problemen hebben betrekking op verlies van plaats en verlies van proportionaliteit. Met het eerste bedoel ik dat communicatie op internet en de daaruit voortvloeiende opslag van data 'overal en nergens' plaatsvinden. De NSA-affaire heeft ons van dat feit en de implicaties ervan recentelijk nog eens hardhandig doordrongen: de Amerikaanse overheid claimt jurisdictie over buitenlandse burgers omdat hun communicatie via servers in de VS verloopt en daar in databanken wordt opgeslagen. De sterkere bescherming die het Europese recht biedt, wordt daarmee opzijgezet. Europese dataautoriteiten heffen machteloos de handen ten hemel.

Verlies van proportionaliteit uit zich op verschillende, elkaar versterkende, manieren. Allereerst is er de drang om alles wat technisch mogelijk is ook werkelijk te doen. Daarnaast is er de drang om zo veel mogelijk data te verzamelen en te bewaren. Alleen met zo veel mogelijk gegevens kan het reken- en associatiepotentieel van Big Data optimaal tot zijn recht komen, en alleen als het nu opgeslagen wordt, kunnen nieuwe technieken later alsnog op de nu al opgebouwde dataverzamelingen toegepast worden. Dan is er nog de druk die uitgaat van de diffusiteit van 'de dreiging'. Iedereen kan een terrorist zijn, dus is iedereen een potentiële

verdachte. Ooit was de norm dat er een concreet vermoeden moest bestaan dat iemand een strafbaar feit had gepleegd, voordat daadwerkelijk overgegaan kon worden tot tijdelijke beperking van zijn of haar grondrechten (bijvoorbeeld door het aftappen van een telefoon voor een bepaalde tijd). Dat lijkt nu vervangen door een algeheel vermoeden tegen de hele bevolking, met algemene beperkingen over langere perioden tot gevolg. In wezen is de gerichte individuele aansprakelijkheid en strafbaarheid op dit digitale terrein zo goed als vervangen door een permanente collectieve aansprakelijkheid.

De 'overal en nergens'-dimensie en de trend van disproportionaliteit doen zich niet alleen gelden in onze privécommunicatie, maar zijn ook voelbaar in de openbare. Dat communicatie – die immers 'overal en nergens' bestaat – in een groot aantal landen opgevist kan worden, leidt tot 'forumshopping': het verlangen én de mogelijkheid om te procederen in het land waar de mediaregels het strengst zijn. Disproportionaliteit betekent in deze internationale context dan dat staten en/of bedrijven de verspreiding van bepaalde, voor hen gevoelige, openbare communicatie kunnen verhinderen door clandestien (of in ieder geval ongemerkt) druk uit te oefenen op knooppunten in het internet (Internet Service Providers, platforms, browsers, betaalservices – denk aan WikiLeaks en de Egyptische Revolutie). Ook hier ontstaat dus in wezen een tendens richting collectieve aansprakelijkheid.

De eerste drie (specifiek informatierechtelijke) problemen kunnen we herleiden tot de vervaging van het object van het grondrecht (het aanknopingspunt voor bescherming). In combinatie met verlies van plaats, tijd en proportionaliteit zien we dat de grondrechten in een digitale mist dreigen op te gaan. Wij, eenentwintigste-eeuwse aardbewoners, zijn boven alles digitale datasubjecten. Als wij vrije staatsburgers willen blijven, zullen wij ons moeten wijden aan het op orde brengen van onze datahuishouding. Alleen dan kunnen wij onze eigen koers in het wereldwijde digitale netwerk zelf blijven bepalen.

