Privacy in het post NSA-tijdperk: tijd voor een fundamentele herziening?

van der Sloot, B.

Published in:
Nederlands Juristenblad

Privacy in het post NSA-tijdperk

Tijd voor een fundamentele herziening?

Bart van der Sloot[1]

De recente NSA-affaire heeft een brede technologische ontwikkeling blootgelegd waarin zeer grote hoeveelheden persoonsgegevens worden verzameld, opgeslagen en verwerkt, zonder dat dit een vooraf en helder bepaald doel heeft. Alhoewel dit evidente privacyproblemen met zich meebrengt, lijken de meeste privacydoctrines, waarvan in Europa de belangrijkste artikel 8 EVRM is, niet toegesneden op deze nieuwe ontwikkeling.

1. Introductie

De gegevensverzameling door de NSA staat in een bredere tendens die ook wel Big Data wordt genoemd.[2] Hierbij worden zo veel mogelijk persoonsgegevens verzameld, door middel van onder meer camera's, telefoontaps, GPS-systemen en internetmonitoring, opgeslagen in grote databases en geanalyseerd door computeralgoritmes. De gegevens worden geaggregeerd, tot groepsprofielen verwerkt en geanalyseerd op basis van statistische verbanden en wiskundige patronen. De profielen worden vervolgens gebruikt om personen die aan een bepaald beeld voldoen te individualiseren, ook wel profiling genoemd. Deze techniek wordt voor steeds meer doeleinden toegepast, zoals de strijd tegen terrorisme, waarbij een persoon kan worden gevolgd of afgeluisterd als hij, geheel of gedeeltelijk, aan een bepaald profiel voldoet (bijvoorbeeld man, moslim, Arabische afkomst en vakantiebestemming Jemen). Evenzo gebruiken banken en verzekeraars risicoprofielen van klanten en baseren daarop (deels) hun beslissingen en benutten internetbedrijven als Google en Facebook dergelijke profielen voor reclamedoeleinden. Als een persoon bijvoorbeeld voldoet aan het profiel "Man, hoger opgeleid, woonachtig te Amsterdam" dan kan dit worden gekoppeld aan een reclame voor het concertgebouw of het nieuwste boek van Umberto Ecco.[3]

Bij dit proces is er derhalve geen redelijk vermoeden nodig om iemand te individualiseren. Zelfs al is er maar 1% kans dat iemand een zeer duur luxeproduct zal aanschaffen of een terroristische activiteit zal ontplooien, dan nog kan het de moeite lonen deze persoon er uit te lichten. Ook wordt in dit proces niet met de gegevensverzameling aangevangen nadat hiervoor aanleiding is gevonden, maar worden er gegevens verzameld waarvan het eventueel nut pas in een later stadium duidelijk wordt. Daarnaast is er in principe geen afbakening in persoon, tijd en ruimte, maar kan simpelweg iedereen aan het gegevensverwerkingsproces worden onderworpen en blijven de verzamelde data niet noodzakelijkerwijs direct gekoppeld aan één persoon, maar worden ze vaak gebruikt om algemene groepsprofielen en statistische verbanden mee te genereren.

Alhoewel het evident is dat Europese burgers niet in rechte kunnen opkomen tegen de door Edward Snowden onthulde afluisterpraktijken van de Amerikaanse National Security Agency (NSA), legt deze zaak wel een al langer gaande ontwikkeling bloot die maakt dat de huidige bescherming van het recht op privacy, dat in Europa primair volgt uit artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM), steeds meer aan relevantie dreigt te verliezen. Het belang van dit artikel met betrekking tot big-datasystemen, die ook door de Nederlandse veiligheidsdienst worden gebruikt, is des te groter gezien het toetsingsverbod[4] en de uitzondering in de Wet bescherming persoonsgegevens voor gegevensverwerking door veiligheidsdiensten.[5] Ook is de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 mede tot stand gekomen omdat de voorloper daarvan uit 1987 in 1994 door de Raad van State in strijd werd geacht met artikel 8 EVRM.[6]

Dit artikel vormt dan ook de kern van twee belangrijke rechtszaken die momenteel aanhangig zijn. De eerste is een zaak aangespannen tegen de Britse overheid door drie Britse rechtspersonen en één natuurlijk persoon woonachtig in Duitsland aangaande NSA-gelijke gegevensverzamelingen door de Britse inlichtingendiensten. Het Europese Hof voor de Rechten van de Mens (EHRM) heeft de partijen de volgende vragen voorgelegd: 1. Vallen de klagers aan te merken als slachtoffer van een privacyschending? 2. Hebben de klagers de nationale rechtsmiddelen uitgeput alvorens een klacht bij het EHRM aan te brengen? 3. Is het verzamelen en verwerken van persoonsgegevens door de Britse inlichtingendiensten voorgeschreven bij wet en noodzakelijk in een democratische rechtsstaat?[7]

In Nederland is een rechtszaak aangespannen over de activiteiten van de Nederlandse inlichtingendiensten, de

Algemene Inlichtingen- en VeiligheidsDienst (AIVD) en de Militaire Inlichtingen- en VeiligheidsDienst (MIVD).[8] Plasterk heeft vervolgens besloten meer openheid van zaken te geven, om zich zo in de juridische procedure teweer te kunnen stellen, dit tegen de gebruikelijke geheimhouding omtrent de werkwijze van de inlichtingendiensten in.[9] Daaruit bleek onder meer dat de Nederlandse inlichtingendiensten zelf Nederlandse burgers afluisteren en de verkregen informatie vervolgens doorspelen aan, onder andere, de Amerikaanse diensten als onderdeel van de roemruchte 'nine-eyes' samenwerking,[10] en niet andersom, zoals Plasterk eerst leek te suggereren.[11] Tevens is duidelijk geworden dat het vermoedelijk gaat om 1,8 miljoen meta-data die per maand worden verzameld,[12] maar ook dat het daarbij niet gaat om 1,8 miljoen afgeluisterde (telefoon)gesprekken, aangezien per gesprek meerdere 'brokjes' meta-data kunnen worden verzameld (bijvoorbeeld de deelnemers aan een gesprek, de duur van het gesprek en de locatie van de gesprekspartners). Hierop volgde een kamerdebat en een oppositiebreed (met uitzondering van de kleine Christelijke partijen) gesteunde motie van wantrouwen,[13] gezien het feit dat Plasterk eerder wist dat zijn aanvankelijke uitlatingen incorrect waren, maar daar de Kamer niet onmiddellijk over had ingelicht.[14]

Terwijl de twee rechtszaken ten tijde van het schrijven van dit artikel nog onder de rechter zijn, zal hier worden geprobeerd daaruit drie kernpunten te destilleren ten aanzien van de vraag of het huidige privacy paradigma nog geschikt is voor de 21ste eeuw, waarin big-dataprocessen een steeds belangrijkere positie zullen innemen. Het huidige recht op privacy onder het EVRM is globaal gebaseerd op drie principes, waarin steeds het individu en zijn belangen centraal staan. Ten eerste kent het een individueel klachtrecht toe aan een natuurlijk persoon. Ten tweede beschermt het individuele belangen, gekoppeld aan autonomie, waardigheid of persoonlijke vrijheid. Tot slot vindt er een belangenafweging plaats tussen het private en het publieke belang die met een inbreuk zijn gemoeid om te beoordelen of deze onrechtmatig is. Aangezien het persoonlijke element in big-datasystemen juist naar de achtergrond verdwijnt komen deze principes steeds meer onder druk te staan. Alhoewel het EHRM op elk van deze punten bereid is tot enige flexibiliteit is het de vraag of dit voldoende is om aan de nieuwe eisen van deze tijd te voldoen. In de laatste paragraaf van dit stuk wordt voorgesteld om het huidige paradigma aan te vullen met een privacybeschermingsstelsel dat is gebaseerd op de plicht van de overheid, die de basale legitimiteit en effectiviteit van de staat waarborgt en als absolute minimumvoorwaarde voor elke democratische rechtsstaat geldt.

Dit artikel analyseert deze drie punten met een verwijzing naar de jurisprudentie van het EHRM. Er wordt derhalve niet stilgestaan bij vragen zoals of in big-datasystemen (als gebruikt door inlichtingendiensten) van een 'legitimate aim' sprake is, of de eventuele inbreuken voorgeschreven zijn bij wet en of de Nederlandse overheid een positieve plicht had om eventuele gegevensverzamelingen door buitenlandse diensten tegen te gaan, zoals aangevoerd is in de Nederlandse rechtszaak. Het artikel neemt als aanleiding de NSA-affaire en de twee rechtszaken die nu aanhangig zijn, maar tracht vooral meer breed iets te zeggen over de onderliggende kernprincipes van het huidige recht op privacy. Hierbij zullen artikel 8 EVRM en de jurisprudentie van het EHRM als primair referentiemateriaal dienen; op één punt verschilt de Nederlandse rechtspraak, waarvoor uiteraard extra aandacht zal zijn.

2. Individueel klachtrecht

Bij de totstandkoming van het EVRM kozen de verdragsopstellers er voor om het klachtrecht slechts in beperkte mate te stoelen op het individuele belang van een natuurlijk persoon. Het EVRM kent twee klachtenprocedures, namelijk voor interstatelijke en individuele klachten. Bij een interstatelijke klacht staat niet een persoonlijk belang van de klager centraal, immers een staat die niet zelf is getroffen, maar de beoordeling van het overheidshandelen van de aangeklaagde staat als zodanig, vaak gerelateerd aan misbruik van macht. Daarnaast staat het individuele klachtrecht behalve voor natuurlijke personen, ook open voor rechtspersonen (met uitzondering van overheidsorganisaties) en groepen. Kenmerkend aan de laatste twee categorieën is dat er wederom geen persoonlijke schade van de klager hoeft te worden aangetoond. Een juridisch persoon kan hoogstens getroffen zijn in zijn belangen in verband met de uitvoering van zijn (bedrijfs) activiteiten, maar kan geen persoonlijke schade lijden. Wederom staat bij een dergelijke klacht doorgaans de onbehoorlijkheid of onrechtmatigheid van het overheidsoptreden als zodanig centraal. Daarnaast moet de mogelijkheid om als groep een klacht in te dienen worden gezien tegen de achtergrond van de Tweede Wereld Oorlog, waarbij groepen stelselmatig werden gediscrimineerd

Auteur

1. Mr. B. van der Sloot is onderzoeker aan het Instituut voor Informatierecht (IViR) van de UvA. Dit onderzoek is verricht in het kader van het NWO gefinancierde project: *Privacy as virtue*. Voor een benadering van deze en andere punten vanuit een filosofisch perspectief: B. van der Sloot, 'De NSA-affaire en de grenzen van de macht, of naar een wederkerige begrip van privacy', *Filosofie en Praktijk*, nog te verschijnen.

Noten

2. V. Mayer-Schönberger en K. Cukier, *Big data: a revolution that will transform how we live, work, and think*, Boston: Houghton Mifflin Harcourt 2013.
3. B. Custers, T. Calders, B. Schermer en T. Zarsky (eds.), *Discrimination and privacy in the information society: Data Mining and profiling in Large Databases*, Heidelberg: Springer 2013.
4. Artikel 120 GW.
5. Artikel 2 Wbp.
6. *ABRS* 16 juni 1994, *AB* 1995/238. Zie verder: <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002/b-20546-webeindversie.pdf.
7. https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter_from_ecthr_to_uk_gov.pdf.
8. http://bureaubrandeis.com/wp-content/uploads/2013/11/Dagvaarding-Burgers-tegen-Plasterk-bureau-Brandeis.pdf.
9. http://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/groot_deel_oppositie_zegt_vertrouwen_in_plasterk_op.jsp.
10. https://decorrespondent.nl/525/over-five-eyes-en-third-parties-met-wie-werkt-de-nsa-samen/25565925-b5edb16e.
11. http://nieuwsuur.nl/video/569130-plasterk-over-de-nsa-en-afluisteren.html; http://pauwenwitteman.vara.nl/media/302465.
12. http://pauwenwitteman.vara.nl/media/308955.
13. https://zoek.officielebekendmakingen.nl/kst-30977-82.pdf.
14. Ook de Commissie Stiekem achtte zich niet geïnformeerd. http://nieuwsuur.nl/onderwerp/613075-commissie-stiekem-niet-geinformeerd.html.

en gestigmatiseerd.[15] De verdragsopstellers gaven met het groepsklachtrecht een persoon of een groep personen het recht om voor de belangen van de groep op te komen, zonder dat zij noodzakelijkerwijs zelf en individueel getroffen waren door een bepaalde praktijk die de groep waartoe zij behoren als geheel treft.[16] Tot slot werd, gezien de serieuze vrezen voor een te grote stroom aan klachten door individuen,[17] door de verdragsopstellers besloten tot een twee-stappensysteem, waarbij de klachten eerst op ontvankelijkheid worden getoetst door de Europese Commissie voor de Rechten van de Mens (een taak die sinds 1998 aan een aparte kamer van het Hof is toebedeeld) en pas daarna een inhoudelijke beoordeling krijgen van het Hof. Kenmerkend is dat aanvankelijk individuen wel klachten onder de Commissie mochten brengen, maar niet onder het Hof, zelfs al was hun zaak ontvankelijk verklaard. Slechts de Commissie zelf of een betrokken lidstaat kon hiertoe besluiten.

De praktijk van het Hof heeft zich echter steeds meer toegespitst op de klachten van natuurlijke personen die een individueel belang kunnen aantonen. Ten eerste is gaandeweg besloten om individuen wel toe te staan klachten direct voor het Hof te brengen.[18] Daarnaast zijn de andere klachtenmogelijkheden (vrijwel) van geen waarde gebleken. Sinds het van kracht worden van het EVRM zijn er slechts zo'n twintig interstatelijke klachten ingediend,[19] het groepsklachtrecht is door het Hof beperkt tot de mogelijkheid van verschillende individuen, die allen door dezelfde wet of praktijk zijn geraakt, om hun klacht te bundelen en het Hof heeft bepaald dat rechtspersonen in principe geen beroep kunnen doen op artikel 8 EVRM. Toen bijvoorbeeld een kerk klaagde over een schending

van haar privésfeer door de politie in relatie tot strafrechtelijke procedures stelde de Commissie dat '[t]he extent to which a non-governmental organisation can invoke such a right must be determined in the light of the specific nature of this right. It is true that under Article 9 of the Convention a church is capable of possessing and exercising the right to freedom of religion in its own capacity as a representative of its members and the entire functioning of churches depends on respect for this right. However, unlike Article 9, Article 8 of the Convention has more an individual than a collective character [..]'.[20] Alhoewel in de recente jurisprudentie een lichte versoepeling op dit punt valt te ontwaren,[21] blijft het uitgangspunt van het Hof dat er een individueel belang en persoonlijke schade moeten zijn aangetoond door de klager, zodat rechtspersonen in principe geen of slechts in beperkte mate een recht op privacy kunnen inroepen.

Een gevolg van de nadruk op het individuele belang en persoonlijke schade is dat zogenoemde *in abstracto* claims, waarbij wordt geklaagd over een wet of praktijk als zodanig, zonder dat deze toegepast is of anderszins een effect heeft gehad op de klager zelf, niet-ontvankelijk worden verklaard, wat ook geldt voor een zogenoemde *actio popularis*, waarin een persoon, groep of maatschappelijke organisatie opkomt tegen een wet of bepaalde praktijk, niet uit persoonlijk oogpunt maar in het maatschappelijk belang, en voor hypothetische klachten en zogenoemde *a priori* claims, waarbij er wordt geklaagd over een mogelijke en in de toekomst liggende inbreuk door de staat, zonder dat er reeds schade is opgetreden.[22]

Dit brengt een evident probleem met zich mee voor klachten gerelateerd aan grootschalige dataverzamelingen, of die nu door veiligheidsdiensten worden geïnitieerd of door grote bedrijven, nu personen vaak simpelweg niet weten dat zij zijn gefilmd, door cookies worden gevolgd of onderworpen zijn aan internetmonitoring door veiligheidsdiensten, en slechts weinigen een rechtszaak zullen voeren als zij niet vermoeden dat dit inderdaad het geval is. Bovendien verdwijnt het persoonlijk belang in dit soort processen steeds meer naar de achtergrond, aangezien niet één individu of enkelen specifiek worden getroffen, maar een zeer grote groep personen. Het punt is niet dat die of deze persoon geraakt is door big-datasystemen, maar dat simpelweg iedereen dat zou kunnen zijn. Daarbij komt dat waar bij klassieke privacyvraagstukken, zoals met betrekking tot een huiszoeking, het individuele belang redelijk duidelijk en afgebakend is en een causaal verband heeft met de gepleegde inbreuk, de eventuele individuele schade die voortvloeit uit gegevensverzamelingspraktijken vaak een tamelijk hypothetisch karakter draagt, aangezien de verzameling zelf doorgaans weinig effect heeft op de persoonlijke autonomie of menselijke waardigheid van een individu. De schade die zou kunnen ontstaan vloeit voort uit de mogelijkheid van bijvoorbeeld een datalek of misbruik door een toekomstig en kwaadwillend regime, waarvan onduidelijk is of dit zal geschieden en welke consequenties dit zal hebben.

Om deze problemen te ondervangen accepteert het Hof soms een lichte versoepeling van het vereiste van individuele schade en persoonlijk belang van de klager.[23] Zo oordeelde het Hof ten aanzien van een mogelijke afluisterpraktijk waarover geen openheid van zake werd gegeven, dat het onaanvaardbaar is dat 'the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation.'[24] Ook is het Hof bereid tot een ruimere interpretatie ten aanzien van klachten omtrent zeer breed en algemeen geformuleerde surveillance-wetgeving, door te stellen dat '[t]he mere existence of the legislation entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for correspondence'.[25]

Het punt is niet dat die of deze persoon geraakt is door big-datasystemen, maar dat simpelweg iedereen dat zou kunnen zijn

Ook zaken waarin de klager niet weet of hij is geraakt door een bepaalde praktijk of waarin hij slechts geraakt wordt door het enkele feit dat hij een burger is die mogelijkerwijs zou kunnen worden getroffen door een bepaalde algemeen opgestelde wet kunnen derhalve onder omstandigheden ontvankelijk worden verklaard. Toch geldt ook hier dat het in principe aannemelijk moet zijn dat iemand onderwerp is geweest van een bepaalde praktijk, onderdeel uitmaakt van een specifiek in de wet aangeduide groep personen of activiteiten ontplooit die aanleiding zouden kunnen geven tot het afluisteren van een persoon. Zo wordt er geen klachtrecht geaccepteerd op basis van vage vermoedens en het horen van mysterieuze klikgeluiden tijdens het telefoneren, maar wel op basis van het feit dat klagers lid zijn van een groep die actief campagne voert tegen nucleaire kruisrakketen.[26] Het Hof erkent dan ook als principieel uitgangspunt dat er een 'reasonable likelihood'

15. A.H. Robertson, *Collected edition of the 'travaux préparatoires' of the European Convention on Human Rights.* Vol. 1, The Hague: Nijhoff, vol. 1, p. 160-162.
16. Robertson, vol. 2, p. 270.
17. Ibid, p. 188-192.
18. Zie als tussenfase: <http://conventions.coe.int/Treaty/en/Treaties/Html/140.htm>.
19. http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#{"article":["33"],"documentcollectionid2":["JUDGMENTS","DECISIONS"]}.
20. ECRM, *Church of Scientology of Paris vs. Frankrijk* (19509/92), 09/01/1995.
21. Zie o.a.: EHRM, *Stes Colas Est e.a. vs. Frankrijk* (37971/97), 16/04/2002.
22. Zie o.a.: ECRM, *Tauira e.a. vs. Frankrijk* (28204/95), 04/12/1995.
23. De Nederlandse dagvaarding verwijst o.a. naar: EHRM, *Kennedy vs. GB* (26839/05), 18 mei 2010.
24. EHRM, *Klass e.a. vs. Duitsland* (5029/71), 06 september 1978, §36.
25. EHRM, *Lordachi e.a. vs. Moldavië* (25198/02), 10 februari 2009, §34.
26. ECRM, *Matthews vs. GB* (28576/95), 16 oktober 1996.

moet bestaan dat de klagers zijn geraakt door de afluister- of monitorpraktijk waarover zij klagen.[27]

Er is derhalve geen eenduidig antwoord te geven op de vraag of de klachten omtrent big-dataprocessen, al dan niet ingezet door veiligheidsdiensten, succes zullen hebben. Niet alleen blijft er het uitgangspunt dat er een individueel belang moet worden aangetoond, althans de aannemelijkheid van individuele schade, er blijft tevens een praktische drempel voor burgers die niet weten of zij zijn geraakt door een bepaalde praktijk, aangezien, indien hier geen aanwijzingen voor zijn, weinig burgers het initiatief zullen nemen tot een rechtszaak. Zelfs al zou deze kennis wel bestaan en al zou de individuele schade wel kunnen worden aangetoond, dan blijft staan dat met de technologische ontwikkelingen en de toenemende gegevensverwerkingsprocessen door niet alleen staten, maar ook bedrijven en burgers, het niet onwaarschijnlijk is dat het in de toekomst voor een individu simpelweg ondoenlijk wordt om bij te houden wie er gegevens over hem verwerken, voor welk doel en op welke wijze en om daar in rechte tegen op te komen bij een vermoedelijke misstand. Het individueel klachtrecht als zodanig dreigt daardoor zijn praktisch nut te verliezen. Daarbij komt dat het de vraag is of stichtingen uit een algemeen belang een succesvol beroep onder artikel 8 EVRM kunnen doen.

Als de rechter de staat op dit punt zou volgen, ontstaat er een stelsel dat fundamenteel lijkt te verschillen van het systeem onder het EVRM

Op dit punt verschilt de Nederlandse rechtspraktijk, zoals bleek uit de recente uitspraak van het Gerechtshof Den Haag in de zaak omtrent de uitgifte van nieuwe paspoorten, aangespannen door stichting Privacy First en een aantal natuurlijke personen. Daarin werden de natuurlijke personen door de rechtbank niet ontvankelijk verklaard omdat zij eerst een bestuursrechtelijke klacht hadden moeten indienen en werd Privacy First door de rechtbank niet ontvankelijk verklaard omdat het geen eigen belang zou hebben. 'Zij komt uitsluitend op voor een belang dat voortvloeit uit de bundeling van de privacybelangen van – naar zij zelf stelt – alle Nederlanders boven de twaalf jaar die een paspoort of identiteitskaart aanvragen. Al deze personen kunnen echter zelf opkomen tegen de verplichting tot het verstrekken van biometrische gegevens, zodat het door Privacy First gestelde belang uitsluitend een bundeling van belangen van die personen betreft. Bovendien betreft dit door Privacy First gestelde algemene belang, te weten de bescherming van de privacy van alle Nederlanders, een zuiver ideëel belang. Naar vaste rechtspraak kan het enkele ideële belang niet gelden als een voldoende belang in de zin van artikel 3:303 BW [..]'.[28] Het Gerechtshof verklaarde de stichting in hoger beroep echter wel ontvankelijk mede omdat Privacy First niet slechts de gebundelde belangen van specifieke individuen vertegenwoordigt, maar voor het algemeen belang opkomt.[29]

Opmerkelijk genoeg wordt soortgelijks ook betoogd door de staat in zijn conclusie van antwoord ten aanzien van de zaak die is aangespannen met betrekking tot de activiteiten van de Nederlandse inlichtingendiensten. Deze klacht is ingediend door een aantal natuurlijke personen, maar ook door vier rechtspersonen, namelijk de Nederlandse Vereniging voor Strafrecht Advocaten (NVSA), de Nederlandse Vereniging voor Journalisten (NVJ), de Internet Society Nederland en Stichting Privacy First. Alhoewel de staat in de conclusie van antwoord meent dat de NVSA en de NVJ niet ontvankelijk moet worden verklaard aangezien de belangen die deze verenigingen zich blijkens hun doelstellingen aantrekken andere zijn dan de belangen waarin zij in deze procedure bescherming zoeken en dat Internet Society Nederland tevens niet ontvankelijk moet worden verklaard aangezien deze rechtspersoonlijkheid ontbeert, stelt hij ten aanzien van Privacy First dat zij moet worden geacht een voldoende belang te hebben. Opmerkelijk is dat de staat juist meent dat de vijf natuurlijke personen die mede de klacht hebben ingediend niet ontvankelijk zouden moeten worden verklaard.[30] Als de rechter de staat op dit punt zou volgen, ontstaat er een stelsel dat fundamenteel lijkt te verschillen van het systeem onder het EVRM.

3. Afbakening van het recht op privacy

Artikel 8 EVRM beschermt eenieders privé- en familieleven, woning en correspondentie, kortom het recht op privacy. Het beschermt echter in principe niet tegen grootschalige gegevensverwerkingsprocessen, wat onder het zogenoemde dataprotectierecht valt. Om het verschil tussen deze twee rechten duidelijk te maken kan worden verwezen naar het Handvest van de Grondrechten van de Europese Unie dat in artikel 7 bepaalt dat eenieder recht heeft op eerbiediging van zijn privé, familie- en gezinsleven, zijn woning en zijn communicatie en in artikel 8 het gegevensbeschermingsrecht vastlegt: '1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens. 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan. 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.' Dit laatste recht is een van privacy gescheiden doctrine en wordt in de EU beschermd door de Richtlijn bescherming persoonsgegevens en in Nederland door de daarop geënte Wet bescherming persoonsgegevens.

Alhoewel er op een aantal punten duidelijk overlap bestaat tussen deze twee rechten is er ook een belangrijk onderscheid. De materiële reikwijdte van het recht op privacy onder artikel 8 EVRM wordt gekoppeld aan de bescherming van persoonlijke belangen als de menselijke waardigheid, individuele autonomie en persoonlijke vrijheid en strekt zich derhalve in principe niet uit tot de verzameling van publieke en niet privacygevoelige gegevens: 'private life does not necessarily include all information on identified or identifiable persons. However, data protection covers exactly this information. This wider scope results from the definition of personal data in the Data Protection

Convention and the Data Protection Directive'.[31] Het begrip 'persoonsgegeven', een begrip dat centraal staat in het dataprotectierecht, ziet niet slechts op privé of privacygevoelige gegevens, maar op elk gegeven waarmee iemand mogelijkerwijs zou kunnen worden geïdentificeerd. 'Zelfs bijkomstige informatie, zoals "die man met een zwart pak aan", kan iemand identificeren temidden van voorbijgangers die bij een stoplicht staan te wachten.'[32] Het gegevensbeschermingsrecht ziet dan ook niet slechts op de bescherming van de privébelangen van specifieke individuen, maar ook, en misschien wel vooral, op procedurele waarborgen en zorgvuldigheidsnormen, zoals ten aanzien van de transparantie van het gegevensverwerkingsproces, het feit dat persoonsgegevens correct en up to date moeten worden gehouden en dat er maatregelen moeten worden getroffen om de gegevens te beveiligen tegen datalekken.

Ondanks het feit dat er dus grote en belangrijke verschillen bestaan tussen de twee rechten heeft het Hof er in toenemende mate voor gekozen de gegevensbeschermingsrechtelijke principes ook te garanderen onder het EVRM, meer specifiek het recht op privacy,[33] onder meer door te bepalen dat de opslag van persoonlijke data, zoals transcripties van telefoongesprekken, foto's, ziekenhuisdossiers en lichaamsmateriaal, ook wordt beschermd onder het recht op privacy.[34] Ook is door het Hof bepaald dat er een legitieme verwerkingsgrond moet zijn voor de verwerking van persoonsgegevens, dat er terughoudendheid moet worden betracht bij het doorgeven van persoonlijke data aan derden en dat gegevens, indien mogelijk, moeten worden vernietigd als zij niet langer ter zake dienend zijn,[35] stuk voor stuk kernprincipes uit het gegevensbeschermingsrecht, en dat de overheid de plicht heeft om adequate gegevensbeschermingsregels neer te leggen in haar nationale wetgeving.[36] Daarbij stelt het EHRM dat het niet uitgesloten is dat ook het verzamelen en verwerken van meta-data onder bepaalde omstandigheden onder artikel 8 EVRM kunnen vallen.[37]

Toch blijft het Hof ook in deze zaken vasthouden aan het principe dat er een persoonlijk belang centraal moet staan, zoals de schending van de autonomie van een persoon.[38] Als er bijvoorbeeld weinig persoonsgegevens worden opgeslagen, deze gegevens slechts triviale informatie bevatten, zoals naam en adres, of als de gegevensverzameling onderdeel vormt van een alledaagse praktijk dan valt een klacht doorgaans buiten de materiële reikwijdte van het recht op privacy.[39] Ook is door het Hof bepaald dat als data worden verzameld in het openbaar, maar niet worden opgeslagen of wel worden opgeslagen, maar voor niemand toegankelijk zijn, dit niet onder het recht op privacy valt.[40] Privacyexperts wijzen er dan ook op dat de garantie van gegevensbeschermingsprincipes onder artikel 8 EVRM vrij beperkt is en dat het onderscheid tussen privacygevoelige gegevens en niet-privacygevoelige gegevens, dat in het gegevensbeschermingsrecht is vervallen, blijft gehandhaafd in de jurisprudentie van het Hof. 'A closer reading shows that the old distinction between 'data that merits protection' and 'data that does not' is still at work and that processing of data is excluded from the privacy scope when (1) the data as such are not considered as private, (2) when there are no systematically stored images or sound recordings, or other data, (3) when the data are not systematically stored with the focus on the data subject, and (4) when the data subject could reasonably expect the processing.'[41]

Wederom is het derhalve onzeker of het huidige privacypardigma geschikt is voor de nieuwe technologische ontwikkelingen. Er lijkt zich een aantal problemen voor te doen bij de toepassing van artikel 8 EVRM op big-dataprocessen. 1. Veel van de data die worden verzameld zijn niet privé maar openbaar en bovendien ziet de verwerking vaak op zogenoemde meta-data, zoals gegevens over de duur van en deelnemers aan een telefoongesprek, maar niet over de inhoud van communicatie.[42] 2. Daarnaast worden niet altijd de persoonsgegevens zelf opgeslagen, maar worden deze vaak gebruikt om geaggregeerde groepsprofielen mee te vervaardigen. 3. De gegevensopslag heeft in dit soort grootschalige gegevensverzamelingsprojecten doorgaans nu juist geen focus op een specifiek datasubject, maar betreft in principe eenieder. 4. In zekere zin vormen dergelijke grootschalige gegevensverzamelingssystemen reeds onderdeel van de alledaagse praktijk en is de verwachting dat dit zeker in de toekomst zo zal zijn. Ook op dit punt is het derhalve sterk de vraag of het recht op privacy onder het EVRM adequate bescherming biedt in relatie tot big-datasystemen en blijft het fundamentele punt staan dat de focus op het individuele belang ten aanzien van de menselijke waardigheid, indivi-

27. Zie o.a.: EHRM, *Kennedy vs. GB* (26839/05), 18 mei 2010.

28. http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2011:BP2860.

29. http://bureaubrandeis.com/wp-content/uploads/2014/02/20140218-arrest-Hof-Den-Haag-geanonimiseerd.pdf.

30. http://bureaubrandeis.com/wp-content/uploads/2014/02/Conclusie-van-antwoord.pdf.

31. J. Kokott en C. Sobotta, 'The Distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR', p. 89, in: H. Hijmans en H. Kranenborg (eds.), *Data Protection anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014),* Intersentia, 2014.

32. Werkgroep29, 'Advies 4/2007 over het begrip persoonsgegeven', 20 juni 2007, p. 13.

33. Aanvankelijk golden ook andere artikelen als fundament voor gegevensrechtelijke principes: P. De Hert, *Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955-1997, Jaarboek ICM 1997,* Antwerpen: Maklu, 1998.

34. Zie verder: EHRM, *Leander vs. Zweden* (9248/81), 26/03/1987. EHRM, *Amann vs. Zwitserland* (27798/95), 16/02/2000. EHRM, *Rotaru vs. Roemenië* (28341/95), 04/05/2000.

35. Zie voor klassieke gegevensbeschermingszaken o.a.: EHRM, *Perry vs. GB* (63737/00), 17 juli 2003; EHRM, *Copland vs. GB* (62617/00), 3 april 2007; EHRM, *Halford vs. GB* (20605/92), 25 juni 1997; EHRM, *Peck vs. GB* (4467/98), 28 januari 2003.

36. EHRM, *Köpke vs. Duitsland* (420/07), 05 oktober 2010.

37. EHRM, *Malone vs. GB* (8691/79), 2 augustus 1984; EHRM, *P.G. & J.H. vs. GB* (44787/98), 25 september 2001.

38. Zie verder: F. Nardell, 'Levelling up: Data Privacy and the European Court of Human Rights', in: S. Gutwirth, Y. Poullet en P. De Hert, *Data Protection in a Profiled World,* Dordrecht: Springer, 2010; G. G. Fuster en S. Gutwirth, 'Opening up personal data protection: a conceptual controversy', *Computer Law & Security Review*, 2013-29.

39. Zie o.a.: ECRM, *Murray vs. GB* (14310/88), 10 december 1991.

40. ECRM, *Herbecq vs. België* (32200/96 & 32201/96), 14 januari 1998.

41. P. de Hert & S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', p. 26, in: S. Gutwirth, Y. Poullet, P. de Hert, J. Nouwt en C. De Terwangne (eds), *Reinventing data protection?*, Dordrecht: Springer Science, 2009.

42. Ook dit kan overigens veelzeggend zijn: <https://decorrespondent.nl/502/metadata-het-meest-onderschatte-woord-van-het-jaar/24445894-48eae1d8>.

duele autonomie of persoonlijke vrijheid zich principieel slecht verhoudt tot deze nieuwe technologische ontwikkelingen, waarin het individu juist niet centraal staat.

4. Belangenafweging

Zelfs al zou de gegevensverwerking in big-dataprocessen, zoals onder meer ingezet door veiligheidsdiensten, onder artikel 8 EVRM vallen en al zou de burger een individueel klachtrecht toekomen, dan nog is het de vraag of het Hof dit in zijn voordeel zal overwegen. Artikel 8 lid 2 laat immers toe dat staten de privacy van burgers beperken indien dit bij wet is voorgeschreven en noodzakelijk is in verband met, onder andere, het garanderen van de nationale veiligheid en openbare orde. Het uitgangspunt van de verdragsopstellers was hierbij aanvankelijk dat er primair naar de noodzakelijkheid van een inbreuk moest worden gekeken, dat wil zeggen naar de effectiviteit, proportionaliteit en subsidiariteit van de inbreuk. Alhoewel deze intrinsieke test niet helemaal is verdwenen, is zij wel meer naar de achtergrond verdwenen en wordt zij aangevuld door een belangenafwegingstest. 'This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest.'[43] Er vindt derhalve een afweging plaats tussen de schade die aan het individuele belang is gedaan door een specifieke maatregel en de mate waarin deze het algemeen belang, bijvoorbeeld in relatie tot veiligheid, bevordert.

Het probleem met een belangenafwegingstest voor big-datavraagstukken is tweeërlei. Ten eerste lijkt de noodzakelijkheidstest veel beter geschikt voor de problemen die de NSA-affaire en soortgelijke gevallen met zich meebrengen. Hierbij is simpelweg de vraag of zo'n grote gegevensverzameling betreffende zoveel mensen over zo'n lange tijdsspanne überhaupt wel noodzakelijk en proportioneel is met het oog op de veiligheidsbescherming, nog los van het eventuele individuele belang dat daarmee is gemoeid, en of er geen minder belastende alternatieven voor handen waren. Daarnaast wordt ook de effectiviteit van dergelijke projecten betwijfeld. 'Some agency insiders now believe that NSA is only able to report on about 1 percent of the data that it collects, and it is getting harder every day to find within this 1 percent meaningful intelligence. Senior Defense and State Department officials refer to this problem as the "gold to garbage ration," which holds that it is becoming increasingly difficult and more expensive for NSA to find nuggets of useful intelligence in the ever-growing pile of garbage that it has to plow through.'[44]

Anderzijds wordt het in dit soort big-datasystemen steeds lastiger om een goede belangenafweging te maken. Een belangenafwegingstest ligt voor de hand bij de toetsing van klassieke privacyproblemen, bijvoorbeeld een huiszoeking van een persoon in het kader van een strafrechtelijk onderzoek, waarbij de inbreuk duidelijk in persoon, tijd en ruimte is beperkt en zowel het daaruit voortvloeiende individuele belang als het publieke belang, bijvoorbeeld gerelateerd aan het oplossen van een moordzaak, een zeer concreet karakter dragen. Bij big-datasystemen is echter enerzijds het publieke belang hypothetisch en abstract en is het vaak onduidelijk in hoeverre een specifieke gegevensverzameling een bijdrage zal leveren aan het streven naar bijvoorbeeld veiligheid en draagt anderzijds het individuele belang tevens een abstract en hypothetisch karakter, aangezien de data vaak moeilijk tot een bepaald persoon zijn te herleiden en de schade, zoals eerder gesteld, niet zozeer direct verband houdt met de gegevensopslag zelf, die vaak weinig effect zal hebben op het leven van een specifiek individu, maar moet worden gezocht in bijvoorbeeld eventueel toekomstige datalekken of misbruik van gegevens door kwaadwillende regimes. Beide belangen zijn weinig concreet en derhalve moeilijk tegen elkaar af te wegen.

Om aan deze problematiek tegemoet te komen is het Hof bereid om zich in dit soort zaken voornamelijk te richten op de intrinsieke kwaliteiten van wettelijke kaders en overheidsprojecten.[45] 'The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.'[46] Ook is bepaald dat personen, waar mogelijk, in ieder geval naderhand op de hoogte moeten worden gesteld van het feit dat zij onderwerp zijn geweest van afluisterpraktijken, moeten er goede democratische controlemogelijkheden bestaan voor bijvoorbeeld het parlement om de activiteiten van veiligheidsdiensten te kunnen beoordelen en ook moet er voor individuen die mogelijkerwijs geraakt zijn door de afluisterpraktijken een effectieve rechtsgang openstaan.[47]

Beide belangen zijn weinig concreet en derhalve moeilijk tegen elkaar af te wegen

Ook op dit punt is het echter de vraag of het huidige paradigma voldoende waarborgen kan bieden ten aanzien van big-dataprocessen. Ten eerste moet er op worden gewezen dat het Hof zich hier voornamelijk op procedurele voorwaarden richt, namelijk op toegang tot een rechter en democratische controle en in mindere mate op de noodzakelijkheid, proportionaliteit en subsidiariteit als zodanig. Daarbij geldt dat als de nationale rechter of wetgever besluit dat de praktijken inderdaad noodzakelijk en proportioneel zijn, het Hof hun oordeel in principe zal volgen. Het Hof stelt dan ook dat in het geval van inlichtingendiensten en surveillancesystemen 'the margin of appreciation available to the respondent State in assessing the pressing social need [..] and in particular in choosing the means for achieving the legitimate aim of protecting national security, [is] a wide one.'[48] Daarenboven accepteert het Hof dat zowel geheimhouding ten aanzien van de aard en het doel van de activiteiten van bijvoorbeeld inlichtingendiensten als de terughoudendheid bij het informeren van specifieke personen over het feit dat zij onderworpen zijn geweest aan afluisterpraktijken in principe legitiem zijn aangezien deze vertrouwelijkheid onderdeel is van de effectiviteit van de activiteiten. Hoe dan ook blijft ook hier het fundamentele punt staan dat de belangenafwegingstest simpelweg niet geschikt lijkt voor dit soort big-datasystemen.

Er is vaker op gewezen dat grondrechten wellicht beter primair als grondplichten van de staat kunnen worden gezien

5. Analyse

Privacy, zoals beschermd door artikel 8 EVRM, is thans geformuleerd als een individueel klachtrecht, dat persoonlijke belangen beschermt, die in concrete zaken worden afgewogen tegen algemene belangen. Door ontwikkelingen op het gebied van big data komen deze principes onder druk te staan. Het Hof probeert aan deze uitdagingen tegemoet te komen door een zekere flexibiliteit, maar het is de vraag of dit voldoende is om een adequate bescherming te bieden. Hoe dan ook blijft er een fundamenteel spanningsveld tussen de focus op het individu en zijn belangen en de technologische ontwikkelingen. De vraag rijst of niet voor een principieel andere benadering van privacyregulering moet worden gekozen, ter vervanging van of als aanvulling op het huidige paradigma.

Ten eerste kan worden afgevraagd of het vereiste van persoonlijke schade nog moet worden gehandhaafd. Het probleem met dit principe is dat klachten over gegevensverzamelingsprocessen vaak een hypothetisch en een abstract karakter dragen, maar daarom niet minder belangrijk zijn. Alhoewel de kans dat bijvoorbeeld een kwaadwillend regime de macht grijpt en de gegevens misbruikt voor kwaadaardige doeleinden bijzonder klein is, overstijgen de mogelijke gevolgen in veelvoud het belang dat met een doorsnee privacyschending als een huiszoeking is gemoeid. Het doel van dit principe lijkt er in te zijn gelegen te waarborgen dat niet iedereen zomaar kan opkomen tegen een vermeende misstand, maar dat slechts zij dit kunnen doen die daar direct belang bij hebben. Het is echter zeer de vraag of het loslaten van het principe van persoonlijke schade zal leiden tot een grotere stroom aan klachten. Het toestaan van een *actio popularis* kan er voor zorgen dat een bepaalde maatschappelijke misstand als zodanig wordt aangepakt, zodat individuele schade en een myriade aan klachten kan worden voorkomen of in ieder geval gebundeld. Ook zorgt het toestaan van claims *in abstracto* er niet alleen voor dat mogelijke toekomstige schade kan worden voorkomen en daarmee de eventuele schare aan klachten, maar ook dat het eventuele oordeel van de rechter substantieel beknopter wordt nu er geen analyse hoeft te worden gemaakt van de omstandigheden van het geval, de persoonlijke situatie van de klager en het causale verband tussen de wet of praktijk en de schade aan het individuele belang.

Ten tweede kan worden afgevraagd of het recht op privacy slechts en alleen nadruk moet hebben op het persoonlijk belang van de klager ten aanzien van zijn waardigheid, autonomie of vrijheid, of dat de onderliggende waarde en daarmee de materiële reikwijdte van privacy ook zou kunnen worden geformuleerd als publiek belang. Er is vaker op gewezen dat grondrechten wellicht beter primair als grondplichten van de staat kunnen worden gezien,[49] wat in ieder geval zeker geldt voor privacy. Zo werd het recht op privacy in de Universele Verklaring voor de Rechten van de Mens, waarop artikel 8 EVRM is gestoeld, aanvankelijk simpelweg 'Freedom from wrongful interference' genoemd en specifieerde het: Freedom from unreasonable interference with his person, home, reputation, privacy, activities, and property is the right of every one.[50] Privacy was dan ook aanvankelijk primair een plicht van de staat die zag op het maatschappelijk belang ten aanzien van het tegengaan van misbruik van overheidsmacht en niet noodzakelijke en proportionele inmengingen in de privésfeer. Mogelijk is om hier hernieuwde nadruk op te leggen, wat aan zou sluiten bij het loslaten van het schade-vereiste nu de primaire normadressant van privacy de staat wordt die een plicht heeft onafhankelijk van een door het individu geclaimd subjectief recht.

Ten derde zou ervoor kunnen worden gekozen om een noodzakelijkheidstest toe te passen zonder dat er persoonlijke schade is opgetreden en zonder dat er een individueel belang op het spel staat, maar er simpelweg wordt geklaagd over het arbitraire of onrechtmatige optreden van de overheid als zodanig. Deze nadruk zou niet slechts kunnen worden toegepast op grote gegevensverzamelingsprocessen, maar ook op meer klassiek privacyvraagstukken omtrent huiszoekingen en telefoontaps, waar tevens de primaire vraag zou kunnen zijn of de inbreuk noodzakelijk, proportioneel en subsidiair is, los van een eventuele afweging van de daarmee gemoeide belangen van het individu. Dit ligt zeker in het kader van veiligheidsbeleid voor de hand aangezien indien een huiszoeking, telefoontap of gegevensverwerking noodzakelijk en effectief is in het kader van dit belang, het vaak simpelweg irrelevant is of en in hoeverre een burger daar door wordt getroffen aangezien het veiligheidsbelang vrijwel altijd zal prevaleren boven het individuele belang. Ook op dit punt zou het dus aanbeveling verdienen te beoordelen in hoeverre het subjectieve element in de huidige privacydoctrine zou kunnen worden losgelaten ten faveure van een meer objectieve en op intrinsieke waarden gebaseerde test. •

43. C. Ovey en R.C.A. White, *European Convention on Human Rights,* Oxford: Oxford University Press 2002, p. 209.
44. M.M. Aid, *The secret sentry: the untold history of the National Security Agency,* New York: Bloomsbury Press 2009, p. 304.
45. Zie verder: EHRM, *Kruslin vs. Frankrijk* (11801/85), 24 april 1990; EHRM, *Huvig vs. Frankrijk* (11105/84), 24 april 1990; EHRM, *Weber and Saravia vs. Duitsland* (35623/05), 29 juni 2006; EHRM, *Uzun vs. Duitsland* (35623/05), 02/09/2010. EHRM, *Telegraaf Media e.a./Nederland* (39315/06), 22/11/2012. EHRM, *S. and Marper vs. GB* (30562/04 & 30566/04), 04 december 2008; EHRM, *Liberty e.a. vs. GB* (58243/00), 01 juli 2008.
46. Klass, §50.
47. Zie o.a. EHRM, *Eimdzhiev vs. Bulgarije* (62540/00), 28 juni 2007.
48. EHRM, *Leander vs. Zweden* (9248/81), 26 maart 1987, §59.
49. C.A.J.M. Kortmann, 'Zijn grondrechten subjectieve rechten', http://repository.ubn.ru.nl/bitstream/2066/15362/1/15362.pdf.
50. Document: E/HR/3.