De noodzaak om privacy als publiek belang te herformuleren

Privacy wordt tegenwoordig geformuleerd als individueel recht dat bescherming biedt aan persoonlijke belangen. Deze benadering is echter niet langer houdbaar in Big Data-processen, die niet op specifieke individuen zijn gericht, maar potentieel eenieder betreffen. Privacy zou dan ook moeten worden geherformuleerd als maatschappelijke waarde. Een dergelijke benadering ondervangt de knelpunten van het huidige privacyparadigma en kan voorkomen dat grootscheepse gegevensverzameling door inlichtingendiensten en instellingen elementaire rechtsbeginselen schendt.

door *Bart van der Sloot*

De auteur is onderzoeker aan het Instituut voor Informatierecht (IViR) van de Universiteit van Amsterdam en coördinator van het Amsterdam Platform for Privacy Research (APPR) van dezelfde universiteit.

PRIVACY IS THANS GEBASEERD OP DRIE PRINCIPES waarin steeds het individu en zijn belangen centraal staan.[1] In de eerste plaats is privacy een recht van een natuurlijk persoon – dit in tegenstelling tot bijvoorbeeld het recht op vrijheid van meningsuiting of de vrijheid van religie, waarbij rechtspersonen als mediaorganisaties of kerken een centrale rol bekleden. Een natuurlijk persoon kan een klacht indienen als hij kan aantonen dat hij persoonlijk schade heeft geleden door een privacyschending. Dit heeft bijvoorbeeld onder het Europees Verdrag voor de Rechten van de Mens (EVRM) tot gevolg dat drie soorten klachten niet-ontvankelijk worden verklaard. Ten eerste zaken waarin een groep of een maatschappelijke organisatie opkomt tegen een wet of een bepaalde praktijk, niet uit persoonlijk oogpunt,

maar in het maatschappelijk belang (classaction). Ten tweede zaken waarin wordt geklaagd over een wet of praktijk als zodanig, zonder dat deze is toegepast of anderszins een effect heeft gehad op de klager (in-abstracto-klachten). Ten derde zaken waarbij wordt geklaagd over een mogelijke en in de toekomst liggende inbreuk, zonder dat er reeds schade is opgetreden (hypothetische klachten of a-priori-claims).

Privacy is, in de tweede plaats, een instrumentele waarde die is gekoppeld aan individuele belangen als menselijke waardigheid, persoonlijke autonomie en individuele vrijheid. Niet alleen zijn dit persoonlijke waarden, het zijn ook waarden die verwant zijn aan de meest basale voorwaarden voor een menselijk bestaan en voor de persoonlijke ontwikkeling. Het recht op privacy wordt dan ook vaak geformuleerd als een persoonlijkheidsrecht, dat bescherming biedt aan de 'persoon als persoon'. Privacy ziet derhalve slechts op individuele belangen – dit wederom in tegenstelling tot andere rechten, zoals de vrijheid van meningsuiting, waar naast de mogelijkheid tot persoonlijke ontplooiing en zelfexpressie ook de zoektocht naar waarheid en het vrije debat als onderdeel van de democratische rechtsstaat centraal staan.

Tot slot is privacy een waarde die vrijwel altijd conflicteert met andere, voornamelijk maatschappelijke, waarden. Dit wordt ook gereflecteerd door de structuur van het EVRM. Daarin is een aantal rechten vervat die nimmer mogen worden beperkt, zoals het recht om niet te worden gefolterd of aan onmenselijke of vernederende behandelingen te worden blootgesteld, en een aantal rechten die wel mogen worden beperkt, maar slechts in geval van nood (artikel 15 EVRM). Artikel 8 EVRM mag echter ook in niet-uitzonderlijke gevallen worden beperkt, namelijk als een inperking is voorgeschreven bij wet, noodzakelijk is in een democratische samenleving, en instrumenteel is aan het waarborgen van een maatschappelijk belang, zoals de nationale veiligheid, het gemeenschappelijk economisch welzijn of de volksgezondheid. Hierbij wordt de uitkomst van een zaak door het Europees Hof voor de Rechten van de Mens (EHRM) doorgaans bepaald door het met een privacyinmenging gemoeide individuele belang en het daarmee gemoeide publieke belang tegen elkaar af te wegen.

PROBLEMEN MET HET HUIDIGE MODEL

Er is echter een aantal problemen met de toepassing van deze benadering op de privacyproblemen die met Big Data-processen zijn gemoeid. Zo is het vaak onduidelijk voor personen of zij onderworpen zijn aan dergelijke Big Data-processen en of hun persoonlijke data zijn verzameld. Tot op de dag van vandaag is er bijvoorbeeld geen zekerheid over wie precies

onderwerp zijn geweest van de afluisterpraktijken van de NSA, over welke periode en betreffende welke activiteiten. Kennis omtrent een mogelijke schending ontbreekt derhalve, wat logischerwijs een drempel met zich meebrengt voor het indienen van een klacht. Daarnaast moet worden bedacht dat de NSA niet de enige organisatie is die op grote schaal persoonsgegevens verzamelt – veel overheidsdiensten, zowel binnen- als buitenlandse, doen hetzelfde; bedrijven als Google en Facebook hebben een businessmodel dat is gebaseerd op het op grote schaal verzamelen en verwerken van persoonsgegevens van hun gebruikers; en vrijwel iedere burger kan met kinderlijk gemak via zijn mobiele telefoon foto's en filmpjes maken en die op internet plaatsen, zonder dat de gefilmde of gefotografeerde daar noodzakelijkerwijs erg in heeft. Het lijkt in deze constellatie van zeer wijdverbreide gegevensverzameling en -verwerking voor iemand schier onmogelijk om alle natuurlijke en juridische personen die in het bezit zijn van zijn persoonsgegevens in kaart te brengen, hun handelwijze op rechtmatigheid te controleren en om indien dit niet het geval is, een klacht in te dienen om zodoende via juridische weg zijn recht op privacy af te dwingen.

Daarbij komt dat het lastig zal zijn om de concrete schade aan de persoonlijke belangen van de klager aan te tonen. Niet alleen is het onduidelijk of iemand is opgenomen in een database, maar zelfs als dit wel bekend is zal het lastig zijn om een specifiek persoonlijk belang aan te tonen, aangezien dergelijke databases vaak gegevens over duizenden of soms zelfs miljoenen personen bevatten. Terwijl bij traditionele privacyschendingen, zoals huisvredebreuk, de schending en de gevolgen daarvan in tijd, ruimte en persoon waren afgebakend en het daaruit voortvloeiende persoonlijk belang derhalve redelijk concreet was, heeft de eventuele individuele schade die voortvloeit uit gegevensverzamelingspraktijken vaak een tamelijk hypothetisch karakter, aangezien de verzameling zelf doorgaans weinig effect heeft op de persoonlijke autonomie of menselijke waardigheid van een specifiek individu. De schade die zou kunnen ontstaan vloeit voort uit de mogelijkheid van bijvoorbeeld een datalek of misbruik van de gegevens door een toekomstig en kwaadwillend regime, waarvan onduidelijk is of dit zal geschieden en welke consequenties dit zal hebben.

Misschien wel belangrijker is dat in dit soort grootschalige gegevensverwerkingsprocessen simpelweg een andere waarde op het spel lijkt te staan dan de persoonlijke vrijheid, autonomie of waardigheid. Bij een klassieke privacyschending, die specifiek gericht is op één persoon of een afgebakende groep (bijvoorbeeld een huiszoeking), is het primaire belang dat op het spel staat een individueel belang, bijvoorbeeld een vorm van negatieve vrijheid. Nu gegevensverwerkingsprocessen juist niet zijn gericht op één

persoon of een afgebakende groep maar simpelweg (potentieel) iedereen betreffen, rijst de vraag of een paradigma waarin de kernwaarde die men tracht te beschermen een aan een persoon verbonden belang is, niet op gespannen voet staat met deze nieuwe ontwikkelingen.

Wat veeleer op het spel lijkt te staan bij Big Data-processen zijn algemene en maatschappelijke belangen. Bij de NSA-affaire is dat bijvoorbeeld de effectiviteit van overheidsbeleid. '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.'[2] Daarmee kan niet alleen de vraag worden gesteld welk nut het verzamelen van zoveel persoonsgegevens dan heeft, maar ook of dit wel noodzakelijk, proportioneel en subsidiair is, dat wil zeggen of de overheid geen minder belastende alternatieven heeft om dezelfde doelstellingen te verwezenlijken. Wat hierbij derhalve op het spel lijkt te staan is simpelweg de vraag of de overheid haar macht misbruikt en of zij daarmee niet de basale legitimiteit van de democratische rechtsorde als zodanig ondermijnt.

Wat op het spel staat is de vraag of de overheid haar macht misbruikt en of zij daarmee niet de basale legitimiteit van de democratische rechtsorde als zodanig uitholt

Anderzijds wordt het in dit soort Big Data-systemen steeds lastiger om een goede belangenafweging te maken. Een belangenafweging ligt voor de hand bij de toetsing van klassieke privacyproblemen, bijvoorbeeld een huiszoeking bij een persoon in het kader van een strafrechtelijk onderzoek, waarbij de inbreuk duidelijk in persoon, tijd en ruimte is afgebakend en zowel het daaruit voortvloeiende individuele belang als het publieke belang, bijvoorbeeld gerelateerd aan het oplossen van een moordzaak, een zeer concreet karakter draagt. Bij Big Data-systemen 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 heeft anderzijds, zoals eerder gesteld, het individuele belang ook een abstract en hypothetisch karakter. Beide belangen zijn weinig concreet en derhalve moeilijk tegen elkaar af te wegen.

Daarnaast is het de vraag of privacy, in de zin waarin die bijvoorbeeld bij de NSA-affaire centraal staat, wel een relatieve waarde zou moeten zijn. Als het klopt dat het hier niet langer gaat om de schending van de individuele autonomie of de menselijke waardigheid van deze of die persoon, maar om een structureel probleem met een daaraan verbonden maatschappelijk belang, namelijk de basale legitimiteit en effectiviteit van de rechtsorde,

dan is het de vraag of het hier niet simpelweg om de basale minimumvoorwaarden voor een democratische rechtsstaat gaat. Als dit inderdaad het geval is, dan gaat het niet langer om een relatieve waarde, die de belangen van het individu beschermt, maar om een absolute waarde, die door elke democratische rechtsstaat moet worden gerespecteerd.

PRIVACY ALS CONSTITUTIEVE WAARDE VOOR ALGEMENE BELANGEN

Het is dus zaak om een alternatieve benadering te formuleren. Deze kan worden gestoeld op het maatschappelijk belang dat privacy vertegenwoordigt. Het koppelen van de privacybescherming aan algemene en publieke waarden staat in een lange traditie.[3] Zo formuleerde Spiros Simitis het recht op privacy al in 1987 als 'a constitutive element of a democratic society'.[4] Ruth Gavison argumenteert in gelijksoortige bewoordingen: 'In the absence of consensus concerning many limitations of liberty, and in view of the limits on our capacity to encourage tolerance and acceptance and to overcome prejudice, privacy must be part of our commitment to individual freedom and to a society that is committed to the protection of such freedom. Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy.'[5] Natuurlijk is ook bekend dat voor Habermas mensenrechten, privacy en autonomie wederzijds constitutief zijn aan democratie: de democratie is gebaseerd op respect voor mensenrechten, en mensenrechten zijn van hun bestaan en bescherming afhankelijk van democratische rechtsstaten.[6] Als privacy als voorwaarde voor het democratische proces of als minimumeis voor een democratische rechtsstaat wordt beschouwd, richten privacyschendingen zich niet slechts op individuele belangen, maar ondermijnen zij de democratie en de rechtsstaat als zodanig.

Een gelijksoortig betoog kan ook worden geconstrueerd ten aanzien van het elektronisch patiëntendossier (epd), het Landelijk Schakelpunt of soortgelijke systemen in de medische sector. Net als veel andere door de publieke en semipublieke sector geïnitieerde IT-projecten is men zich pas in een laat stadium bewust geworden van eventuele privacygevaren. Er is, zoals wel vaker, voor gekozen om het bestaande systeem op een beperkt aantal punten aan te passen, maar geen structurele wijzigingen door te voeren. Voor een dergelijke aanpak wordt wel meer gekozen, bijvoorbeeld bij de ov-chipkaart – de privacygevaren blijven dan bestaan en de systemen blijven zeer inbreukgevoelig. Bij elektronische systemen in de gezondheidszorg wordt er vaak voor gekozen om de burger zelf te laten kiezen of hij akkoord gaat met de opname van zijn persoonsgegevens in dergelijke gevoelige systemen. Deze benadering is om twee redenen onzalig.

Ten eerste is deze keuze geen echte keuze te noemen. De burger wil immers van het openbaar vervoer gebruikmaken, en van de gezondheidszorg evenzo. Als de NS of de dokter suggereert dat de opslag van zijn gegevens bijdraagt aan de levering van de dienst, blijkt dat veel burgers hiermee instemmen uit vrees dat zij de dienst anders niet zullen krijgen. Zelfs als de keuze 'vrij' zou zijn, dan nog berust zij niet op informatie. Het is immers ondoenlijk voor elke burger om na te gaan welke gegevens in welke systemen zijn opgeslagen, waartoe dit dient, welke gevaren hiermee zijn gemoeid, wat de kans is dat deze gevaren zich materialiseren, en welke nadelige effecten eruit zouden kunnen voortvloeien als dat zou gebeuren. De eventuele toestemming van de patiënt, reiziger of burger in elke andere hoedanigheid is derhalve nietszeggend.

Ten tweede, en belangrijker, is wat hier op het spel staat wederom niet (slechts) een individueel belang, maar een maatschappelijk belang, aangaande het vertrouwen van het publiek in de overheid en de goede werking van de gezondheidszorg. Systemen als het elektronisch patiëntendossier of het Landelijk Schakelpunt dreigen bijvoorbeeld de vertrouwelijkheid tussen patiënt en arts te ondermijnen; niet alleen de huisarts van een persoon kan immers toegang krijgen tot zijn patiëntendossier, ook derden kunnen die krijgen. Nog los van het grote gevaar op toegang door onbevoegden (die gebruikmaken van mazen in het systeem) wordt de vertrouwelijkheidssfeer opgerekt tot verscheidene artsen, specialisten en waarschijnlijk hun assistenten binnen en waarschijnlijk ook buiten de woonregio van de patiënt. Het gevaar is dat een dergelijke afbreuk van de arts-patiëntrelatie en de bijbehorende vertrouwelijkheid het gezondheidssysteem als zodanig ondermijnt; dit is een publiek belang.

IT-systemen als het elektronisch patiëntendossier of het Landelijk Schakelpunt dreigen de vertrouwelijkheid tussen patiënt en arts te ondermijnen

'First, confidentiality encourages seeking medical care. Individuals will be more inclined to seek medical attention if they believe they can do so on a confidential basis. It is reassuring to believe others will not be told without permission that one is unwell or declining, has abused illegal drugs, been unfaithful to one's partner, obtained an abortion, or enlarged one's breasts. [...] Second, confidentiality contributes to full and frank disclosures. Individuals seeking care will be more open and honest if they believe the facts and impressions reported to health providers will remain confidential. It may be easier to speak freely about embarrassing symptoms if one believes the content of what one says will not be broadcast to the world at large.'[7]

Anita Allen, internationaal vermaard privacyexpert, stelt in het voorgaande

citaat dat de vertrouwelijkheid tussen arts en patiënt waarborgt dat burgers naar artsen toestappen als zij gezondheidsklachten hebben en dat zij eerlijk en open zijn over hun ziektebeeld en de eventuele oorzaken daarvan. Zij voegt daar nog aan toe dat een gebrek aan privacy in de gezondheidszorg leidt tot hogere kosten, aangezien vroege diagnoses en behandelingen en preventieve maatregelen vaak kostenbesparend zijn. Het gevaar is derhalve dat het epd of soortgelijke IT-systemen afbreuk zullen doen aan de vertrouwelijkheid tussen arts en patiënt. Als deze afbreuk zich daadwerkelijk voordoet of als er in de perceptie van burgers een reëel gevaar is dat deze vertrouwelijkheid (bevoegd of onbevoegd) wordt geschonden, zal niet alleen het individuele belang van de patiënt in gevaar komen (bijvoorbeeld doordat er ruchtbaarheid wordt gegeven aan een bepaald ziektebeeld waarop een stigma rust), maar komt daarmee ook een maatschappelijke waarde onder druk te staan, namelijk de effectiviteit en doelmatigheid van de gezondheidszorg als zodanig.

VOORDELEN VAN EEN DERGELIJK MODEL

Op deze punten lijkt een herformulering van privacy als maatschappelijk belang derhalve de reële situatie het best te benaderen. Daarbij biedt een dergelijke benadering een mogelijke oplossing voor de drie eerder gesignaleerde knelpunten.

Ten eerste wordt in een dergelijk model het respect voor privacy niet zozeer het subjectieve recht van de burger als wel de plicht van de staat als onderdeel van zijn wederkerige relatie met de burger. Als de staat de voornoemde privacybelangen ondermijnt, ondermijnt hij immers zijn eigen fundamenten – de voorwaarden voor een democratische rechtsstaat. Hiermee vervalt ook de correlatie tussen persoonlijke schade en een persoonlijk klachtrecht en wordt de weg vrijgemaakt voor een actio popularis, een rechtszaak in het algemeen belang. Daarin wordt een klacht simpelweg gerelateerd aan het feit dat de staat niet voldoet aan de randvoorwaarden voor het gebruik van zijn macht, en daarmee wordt de eerste van de bezwaren ten aanzien van het huidige paradigma ondervangen: individuele schade hoeft (nog) niet te zijn opgetreden. Dit opent ook de deur voor hypothetische klachten en in-abstracto-claims.

Ten tweede wordt de grootschalige verzameling van metadata en de opslag en het gebruik van geaggregeerde informatie en groepsprofielen, zoals gebruikelijk is in Big Data-processen, niet langer gekoppeld aan het individuele belang en de autonomie en waardigheid van de burger. Het belang dat hiermee is gemoeid wordt veeleer een maatschappelijk belang, gekoppeld aan de vraag of zulke systemen überhaupt noodzakelijk, proportioneel en effectief zijn. Een klacht over Big Data-processen hoeft dan

ook niet zozeer te gaan over welke schade zulke systemen doen aan een specifiek individu, maar veeleer over de vraag of zij de basale legitimiteit en effectiviteit van de staat niet ondermijnen, of zij de minimumvoorwaarde voor een goed en doeltreffend zorgsysteem niet eroderen, enzovoort. Een dergelijk argument kan natuurlijk eveneens worden gemaakt met betrekking tot de vertrouwelijkheid tussen cliënt en advocaat en tot de geheimhouding van journalisten ten aanzien van hun bronnen. Niet voor niets zijn ook de Nederlandse Vereniging voor Journalisten en de Nederlandse Vereniging voor Strafrechtadvocaten partij bij een rechtszaak tegen de Nederlandse staat – in verband met de gegevensverzameling door binnen- en buitenlandse inlichtingendiensten en de uitwisseling van gegevens tussen deze diensten.[8]

Ten derde, en tot slot: alhoewel de belangen van het individu worden meegenomen, geschiedt de beoordeling van regelgeving en beleid in deze nieuwe benadering niet door deze tegen het algemeen belang af te wegen, maar worden wetten en regels op hun intrinsieke kwaliteit beoordeeld. Hierdoor wordt een alternatief aangedragen voor de afweging van belangen, die nu prominent is in privacyzaken, maar faalt als het gaat om Big Data-processen. Daarbij komt dat er minimumprincipes voor de rechtsorde of andere instituten kunnen worden geïntroduceerd die nimmer mogen worden geschonden, ook niet als dit uit een afweging tussen het individuele en het algemene belang zou volgen. Dit zou een oplossing kunnen bieden voor het feit dat de gegevensverzameling door de inlichtingendiensten en het installeren van systemen die de vertrouwelijkheid tussen arts en patiënt, advocaat en cliënt, en journalist en bron ondermijnen, maatschappelijke en niet (slechts) individuele belangen raken.

Noten

1 Het onderzoek voor dit artikel is verricht in het kader van het door NWO gefinancierde project 'Privacy as Virtue'. De bijdrage stoelt deels op: B. van der Sloot, 'Privacy in het post NSA-tijdperk. Tijd voor een fundamentele herziening?', *Nederlands Juristenblad* 89 (2014), nr. 17, pp. 1172-1179; en B. van der Sloot, 'De NSA-affaire en de grenzen van de macht. Naar een wederkerig begrip van privacy', *Filosofie & Praktijk* 35 (2014), nr. 2, pp. 49-66.

2 M.M. Aid, *The Secret Sentry: The Untold History of the National Security Agency*. New York: Bloomsbury, 2009, p. 304.

3 Zie onder andere P.M. Regan, *Legislating privacy. Technology, social values, and public policy*. Chapel Hill: University of North Carolina Press, 1995, p. 213.

4 S. Simitis, Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review* 135 (1987), nr. 3, pp. 707-746.

5 R. Gavison, 'Privacy and the Limits of Law', *Yale Law Journal* 89 (1980), nr. 3, p. 455.

6 J. Habermas, *Between facts and norms*. Cambridge: MIT Press, 1996.

7 A.L. Allen, *Unpopular privacy. What must we hide?* Oxford: Oxford University Press, 2011, p. 112.

8 Zie http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:8966.