B.J. Koops (2014), 'Privacy, informatieveiligheid en een onzichtbare medaille', in: S. Kok e.a. (red.), *Informatieveiligheid*, Taskforce Bestuur & Informatieveiligheid Dienstverlening, p. 57-73

Privacy, informatieveiligheid en een onzichtbare medaille

Bert-Jaap Koops
Hoogleraar regulering van technologie, Universiteit van Tilburg

1. Inleiding

Informatieveiligheid beschermt informatie (of eigenlijk breder: gegevens), privacy beschermt persoonsgegevens (of eigenlijk specifieker: persoonsinformatie). Informatieveiligheid en privacy hebben daarom veel met elkaar gemeen. Is privacy (bescherming *persoons*gegevens) misschien een deelverzameling van informatieveiligheid (bescherming van *alle* gegevens)? Dat nu ook weer niet. Vaak gaan privacy en informatieveiligheid hand in hand, maar soms ook niet. Kijk bijvoorbeeld naar de vragen die rijzen binnen de 3D-operatie van decentralisatie van jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen. Enerzijds is decentralisatie een geschikte techniek binnen informatieveiligheid: je spreidt risico's door gegevens in veel kleine vergaarbakjes op te slaan; deze zijn immers een minder aantrekkelijk doelwit voor hackers dan één grote vergaarbak, en de schade is kleiner als er toch wordt ingebroken. Anderzijds ontstaan zorgen voor de privacy door decentralisatie: zullen gemeenten voldoende zorgvuldig omgaan met deze vaak gevoelige persoonsgegevens? En in welke mate mogen persoonsgegevens worden gedeeld binnen gemeentelijke netwerken om dienstverlening te verbeteren? Uit het oogpunt van informatieveiligheid moet je terughoudend zijn met het delen van informatie: meer kopieën bij een veeltal van actoren betekent meer schakels en meer kwetsbaarheden. Uit het oogpunt van privacy lijkt terughoudendheid met delen op het eerste oog ook gewenst, maar bij nadere beschouwing hoeft dat niet zo te zijn: de privacywetgeving staat—binnen de grenzen van proportionaliteit—delen toe als er een goede grondslag voor is, mede omdat het mogelijk leidt tot een adequater beeld van iemand, waardoor zorgvuldiger beslissingen mogelijk worden.

Het is daarom interessant om nader te beschouwen hoe privacy en informatieveiligheid zich tot elkaar verhouden. In dit essay onderzoek ik in welke mate ze samengaan, als twee kanten van een medaille, en in hoeverre ze uit elkaar lopen als mogelijk conflicterende belangen.

Uit mijn argumentatie zal blijken dat er vooral een synergie bestaat, en dat die synergie ons iets vertelt over waarom beide belangrijk zijn in de informatiemaatschappij. Privacy en informatieveiligheid hebben in elk geval gemeen dat de overheid op beide vlakken, al dan niet terecht, geen al te beste reputatie heeft. Een beter begrip van de ratio van privacy kan helpen om het belang van informatieveiligheid beter te onderkennen en daarmee serieus te nemen, en omgekeerd kan een goed begrip van informatieveiligheid de overheid helpen om beter te begrijpen waarom privacy belangrijk is in het informatietijdperk.

2. Begripsbepaling

2.1. Wat is informatieveiligheid?

Informatieveiligheid is een relatief helder begrip: het duidt aan dat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie (of gegevens) moet worden gewaarborgd. Daarmee zijn de belangen die ten grondslag liggen aan informatieveiligheid duidelijk: informatie moet niet (zonder reden) op straat komen te liggen, je moet kunnen vertrouwen op informatie en je moet bij informatie kunnen. Dat zijn basisvoorwaarden voor een goede informatiehuishouding en dus bestaansvoorwaarden voor de informatiesamenleving.

Dat wil overigens niet zeggen dat het altijd duidelijk is hoe informatieveiligheid vorm moet krijgen. We leven in een aanzienlijk complexere—meer vernetwerkte en verknoopte—wereld dan een paar decennia terug, toen informatieveiligheid op de kaart werd gezet. Toen heette het overigens nog informatie*beveiliging*. Nu zijn veiligheid (*safety*) en beveiliging (*security*) nauw verwante begrippen, maar ze leggen wel een verschillende nadruk. Beveiliging ziet meer op bescherming tegen schade ontstaan door (vaak opzettelijke maar mogelijk ook niet-opzettelijke) handelingen van mensen, terwijl veiligheid meer te maken heeft met bescherming tegen schade

ongeacht de oorzaak, dus ook schade door niet-menselijke oorzaken zoals natuurrampen. In die zin is veiligheid een ruimer begrip dan beveiliging. En hoewel bescherming tegen natuurlijke oorzaken (overstromingen, kabels doorknagende knaagdieren) ook wel tot informatiebeveiliging werd gerekend, lag de nadruk in het verleden toch meer op maatregelen tegen menselijke aanvallen of falen. In dit opzicht is informatieveiligheid ook complexer geworden, omdat het een integrale vorm van veiligheid van informatie suggereert. Wil men informatie voldoende veiligstellen, dan vergt dat een integrale risicoanalyse van alle mogelijke oorzaken van schade aan informatie, binnen de hele, complexe context van risico's waaraan informatie in de netwerksamenleving blootstaat.

Hoewel informatieveiligheid aldus een complexer vraagstuk is geworden, doet dat niet af aan de relatieve duidelijkheid van het begrip: het gaat nog steeds om het veiligstellen van de onderliggende belangen van vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

2.2. Wat is privacy?

Privacy is een relatief minder helder begrip, en daarom is het goed hier wat langer bij stil te staan voordat we de verhouding tussen privacy en informatieveiligheid bekijken. Het is haast een gemeenplaats geworden om te zeggen dat privacy niet te definiëren valt en dat er talloze definities in omloop zijn. Dat mag waar zijn, maar de meeste definities hebben wel een kern gemeen: privacy duidt een bepaalde privésfeer aan (de 'persoonlijke levenssfeer' van artikel 10 Grondwet) waarbinnen de overheid niet—tenzij met goede redenen en met voldoende waarborgen omkleed—binnen mag dringen. Die privésfeer heeft niet alleen te maken met informatie (de persoonsgegevens die in artikel 10 lid 2-3 Grondwet worden beschermd), maar heeft ook een fysieke dimensie (lichamelijke integriteit, artikel 11 Grondwet), een ruimtelijke dimensie (het huisrecht, artikel 12 Grondwet) en een relationele dimensie (het correspondentiegeheim, artikel 13 Grondwet). Het is daarom te beperkt om privacy alleen te zien als informationele privacy, hoewel in de volksmond (en trouwens ook in de volksvertegenwoordigersmond) 'privacy' en 'bescherming van persoonsgegevens' vaak als synoniemen worden gebruikt. Gezien het onderwerp van dit essay zal ik niettemin aansluiten bij dit spraakgebruik en vooral kijken naar informationele privacy, maar het is goed om in het achterhoofd te houden dat privacy meer facetten heeft: het gaat om alles wat, letterlijk of figuurlijk, 'dichtbij' mensen van vlees en bloed komt, en niet alleen om de digitale representatie van deze mensen.

Dat gezegd zijnde, wat is dan informationele privacy? Wat mij betreft komt het vooral neer op een stelsel fatsoensnormen voor de omgang met persoonsgegevens, die waarborgen dat wanneer mensen niet in de fysieke werkelijkheid (met directe menselijke interactie) maar via digitale representatie worden behandeld, deze behandeling netjes en zorgvuldig plaatsvindt. In databanken heb je nu eenmaal geen sociale omgangsvormen die zich binnen fysieke interacties hebben ontwikkeld, zoals met twee woorden spreken en de juiste persoon aankijken als die aan de beurt is. De digitale fatsoensnormen die zijn vastgelegd in de persoonsgegevenswetgeving zijn (althans in hun basisvorm zoals in de OESO-richtlijnen[1]) relatief simpel: data moeten alleen voor welbepaalde doelen worden verzameld en alleen voor die doelen worden gebruikt; data moeten voldoende accuraat en actueel zijn; ze moeten afdoende worden beveiligd; de verwerking ervan moet transparant en verantwoordbaar ('accountable') zijn; en individuen moeten inzage hebben in hun gegevens en waar nodig om correctie of verwijdering kunnen vragen.

Deze fatsoensnormen hebben niet altijd met de privésfeer te maken: sommige persoonsgegevens zijn breed beschikbaar, zichtbaar, en weinig privacygevoelig. Toch is er een sterke correlatie, en daarom gaat het toch om informationele *privacy*: in sommige contexten kan ook een onschuldig persoonsgegeven—geslacht, leeftijd, haarkleur—invloed hebben op hoe de persoon wordt behandeld, en daarmee kan de privésfeer wel degelijk in het geding zijn. Privacy is een belangrijke onderliggende reden voor een fatsoenlijke omgang met persoonsgegevens. Twee theorieën rond privacy die mij erg aanspreken, kunnen dat illustreren.

Ten eerste heeft privacy te maken met identiteitsontwikkeling. Philip Agre omschrijft privacy als de bescherming tegen onredelijke beperkingen om je identiteit vorm te geven. Privacy

[1] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

betekent dat je moet kunnen zijn wie je zelf wilt zijn (binnen redelijke kaders, je moet niet een serieverkrachter willen zijn), in plaats van een door de omgeving opgedrongen dwangbuis van hoe een ideale burger, consument of werknemer eruit hoort te zien. Wanneer je persoonsgegevens worden gebruikt op een manier dat je niet meer jezelf durft te zijn—bijvoorbeeld als je niet meer een paar glazen alcohol te veel wil drinken omdat je probleempuber dan helemaal het stigma van een risicojongere zou kunnen krijgen—is je privacy in het geding. Let wel: privacy is niet absoluut, en het kan heel legitiem zijn om die persoonsgegevens zo te verwerken (en goed voor je gezondheid en misschien ook voor de probleempuber), maar het illustreert wel dat een inbreuk op je privésfeer een goede grondslag nodig heeft: je moet niet *onnodig* je identiteit hoeven aanpassen.

Een tweede, daarmee samenhangende privacytheorie komt van Jeffery L. Johnson, die zegt dat privacy te maken heeft met bescherming tegen de oordelen van anderen. We worden natuurlijk op allerlei mogelijke manieren beoordeeld in het maatschappelijk verkeer—bijvoorbeeld of we een krediet, subsidie, diploma, lintje of gevangenisstraf verdienen—maar die beoordeling moet wel plaatsvinden op basis van juiste en relevante feiten. Binnen de privésfeer moet je je (binnen redelijke grenzen) kunnen gedragen zonder dat wat je doet—wiet roken, naakt op de keukentafel dansen, vreemdgaan, Donald Duck lezen—invloed heeft op je krediet, diploma of verdenking van een strafbaar feit: het zijn daarvoor namelijk niet relevante gegevens. Deze privacytheorie verklaart daarmee waarom informationele privacy zoveel belang hecht aan dataminimalisatie: je moet alleen gegevens verwerken die echt nodig zijn voor het doel dat je wilt bereiken, zodat je geen irrelevante, verouderde of onjuiste gegevens in de beoordeling van mensen betrekt. Dat is tegenwoordig des te belangrijker, omdat het in de vernetwerkte databankwereld snel gebeurt dat gegevens buiten hun oorspronkelijke context worden verwerkt, en in een andere context kunnen gegevens van kleur verschieten doordat ze in een ander licht komen te staan. Ook decontextualisering levert risico's op voor onterechte beoordelingen, en dat onderstreept het belang van doelbinding.

Tot slot verklaart privacy als ratio voor de bescherming van persoonsgegevens ook waarom de dooddoener 'als je niets te verbergen hebt, heb je toch niets te vrezen' een drogreden is. Privacy staat voor een privésfeer die is onderscheiden van de publieke sfeer. In onze staatsinrichting hebben de publieke autoriteiten de taak gekregen om publieke belangen te behartigen. Waar nodig mag bij de behartiging van publieke belangen ook in de privésfeer worden getreden—maar alleen waar het nodig is. Voor de vraag of privacy in het geding is, maakt het daarom niet uit of je wel of niet iets 'te verbergen' hebt, dus of je al dan niet privacygevoelige dingen aan het doen bent binnen je privédomein; het gaat erom of er vanuit de publieke sfeer in de privésfeer wordt binnengekeken, en wanneer dat het geval is, moet dit binnenkijken worden gelegitimeerd, ongeacht of er iets privacygevoeligs wordt gezien. Ook dit verklaart het belang van dataminimalisatie in de publieke sector: de overheid mag persoonsgegevens van burgers verwerken (en dus in de privésfeer treden), maar alleen voor zover het nodig is voor welbepaalde doelen van publiek belang.

Dat betekent ook dat de vaak geponeerde stelling dat niet het verzamelen maar alleen het gebruiken van persoonsgegevens een privacyinbreuk oplevert, onjuist is. Ook het verzamelen zelf vormt een inbreuk op de persoonlijke levenssfeer die zelfstandig gelegitimeerd moet worden. De verzameling van gegevens kan immers al de beoordeling door de overheid van burgers inkleuren, en dat raakt de vrijheid van burgers zichzelf te kunnen zijn. Ze zouden bijvoorbeeld bij hun vakantie naar Oost-Turkije kunnen afzien van een halal-maaltijd in het vliegtuig, uit angst in een databank van potentiële terroristen terecht te komen. Daarom stellen de bescherming tegen onterechte oordelen en de vrijheid je eigen identiteit vorm te geven grenzen aan ongerichte of ongelegitimeerde dataverzameling door de overheid.

3. De synergie tussen privacy en informatieveiligheid

Als we privacy naast informatieveiligheid zetten, zie ik ten minste drie parallellen. De eerste en belangrijkste is dat de onderliggende beginselen grotendeels vergelijkbaar zijn en soms geheel samenvallen.

Het eerste en voor velen primaire beginsel van informatieveiligheid is vertrouwelijkheid van informatie; dat komt overeen met het onderliggende privacybelang van de bescherming van persoonsgegevens: het afschermen van de privésfeer. Bij beide ligt er een zware nadruk op

bescherming tegen ongeautoriseerde toegang of ongeautoriseerd gebruik van gegevens. Hier zien we dat de belangen van informatieveiligheid en privacy vrijwel naadloos in elkaar overlopen. Privacy wordt gewaarborgd als gegevens adequaat afgeschermd worden volgens de regels van de informatieveiligheidskunst, en privacy staat op het spel als informatie weglekt. Deze parallel is duidelijk te zien in beleidsdiscussies als de meldplicht datalekken (een informatieveiligheidsachtige maatregel die binnen de privacywetgeving wordt vormgegeven) en in dossiers waarin informatiebeveiligingsrisico's in de sleutel van privacy worden gezet, zoals bij slimme energiemeters en elektronische patiëntendossiers, waarbij de beveiligingsrisico's rond gevoelige persoonsgegevens mede reden vormden voor de Eerste Kamer om de desbetreffende wetsvoorstellen af te wijzen. Ook het risico van identiteitsdiefstal is een toenemend aandachtspunt bij de informationele huishouding van de overheid, waarbij privacy en informatieveiligheid hand in hand gaan.

Het tweede beginsel van informatieveiligheid, de integriteit van informatie, is ook, hoewel minder prominent, belangrijk in de informationele privacy. Eén van de acht OESO-privacybeginselen is datakwaliteit: 'Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date' (vgl. art. 11 Wet bescherming persoonsgegevens). De juistheid en nauwkeurigheid van persoonsgegevens komen overeen met de integriteit van informatie. Interessant is wel dat de datakwaliteit bij persoonsgegevens verder gaat dan bij informatieveiligheid: bij het laatste ligt de nadruk op het feit dat gegevens authentiek en niet gemanipuleerd zijn, maar of de gegevens accuraat en 'juist' zijn, maakt in beginsel niet uit. Hier kan de informatieveiligheid mogelijk leren van privacy: voor een goede informatiehuishouding helpt het ook dat gegevens een goede kwaliteit hebben, in de zin van relevantie, accuraatheid en volledigheid, en niet alleen dat ze niet manipuleerbaar zijn.

Ook beschikbaarheid, het derde beginsel van informatieveiligheid, heeft enigszins te maken met het datakwaliteitsbeginsel. Het belang dat je toegang kunt hebben tot informatie wanneer je die nodig hebt, komt ook tot uiting in het belang dat gegevens volledig en actueel zijn, al is de parallel hier wat minder sterk dan bij de eerste twee pijlers van informatieveiligheid. Wellicht kunnen beide velden hier nog iets meer van elkaar leren: voor informatieveiligheid is het ook nuttig dat gegevens volledig en actueel zijn, terwijl voor informationele privacy het belang van beschikbaarheid van gegevens meer zou kunnen worden benadrukt. Pas als alle juiste gegevens voorhanden zijn, kan immers een goede beoordeling worden gemaakt over de betrokken persoon.

De tweede parallel, die vermoedelijk voortvloeit uit het feit dat de onderliggende belangen vaak dezelfde zijn, is dat informatieveiligheid en informationele privacy om een vergelijkbare aanpak vragen. Informatie kan nooit alleen met technische middelen worden beveiligd; de bescherming is gelegen in een passende combinatie van technische, juridische en organisatorische maatregelen. Het gaat daarbij om maatwerk, waarbij op basis van een contextgevoelige risico-inschatting bepaald wordt welke combinatie en welk niveau aan maatregelen nodig is. Dat geldt evengoed voor beveiliging van informatie als voor bescherming van persoonsgegevens. Niettemin kan er wel een accentverschil liggen: bij informatieveiligheid wordt mogelijk in eerste instantie gekeken naar technische maatregelen, die waar nodig worden aangevuld met organisatorische en juridische, terwijl bij persoonsgegevens wellicht eerder wordt uitgegaan van juridische en organisatorische maatregelen (zoals het vastleggen wie voor welk doel gegevens mag verwerken), die worden aangevuld met technische bescherming. Dat lijkt mij een relatief klein verschil: bij beide is bijvoorbeeld een goede regeling van autorisatie (wie heeft toegang tot welke data) essentieel, en of die regeling primair juridisch, organisatorisch of technisch wordt afgedwongen is van ondergeschikt belang.

In de benadering van informatieveiligheid en privacy is voorts een vergelijkbare ontwikkeling te zien, waarbij de aandacht aan het verschuiven is naar een systeembenadering, met nadruk op bescherming bij het begin van de bouw van ICT-systemen in plaats van achteraf, en een voorkeur om waar mogelijk waarborgen in het systeem zelf in te bouwen: *security by design* en *privacy by design*. Het past in een bredere tendens van maatschappelijk verantwoord innoveren (*responsible innovation*), waarbij uitdrukkelijk aandacht is voor de normatieve implicaties van technologische systemen, en waarbij wordt beoogd om deze normatieve implicaties zo vroeg mogelijk te adresseren; als technologieën eenmaal geland zijn in de samenleving, is het immers vaak niet meer mogelijk ze nog wezenlijk te veranderen. Interessant aan de benadering van

maatschappelijk verantwoord innoveren is dat het vooral een procesbenadering is: een reflexief, zelflerend en cyclisch proces waarbij het resultaat—zoals maatregelen genomen in het kader van *security/privacy by design*—doorlopend wordt geëvalueerd en bijgesteld in het licht van gebleken onvolkomenheden, onverwachte neveneffecten of veranderende omstandigheden. Hoewel de tendens naar een systeembenadering, met het inbouwen van waarborgen in systemen zelf, zowel bij informatieveiligheid als bij privacy de laatste jaren waarneembaar is, kan deze tendens nog wel wat versterking gebruiken. Beide velden zouden kunnen leren van ervaringen in andere velden waarbinnen 'responsible innovation' in de praktijk wordt gebracht. Een reflexieve, zelflerende procesbenadering is namelijk geschikter dan een statische benadering om informatie adequaat te beschermen in onze dynamische en complex verknoopte informatiesamenleving.

Een derde parallel die ik zie is de relatieve onzichtbaarheid van informatieveiligheid en privacy buiten de beperkte kring van werknemers die ervoor verantwoordelijk zijn. Het is een probleem waar beide velden mee te kampen hebben: zolang het goed gaat, merk je er niets van, maar wanneer het fout gaat, heb je echt een probleem. Bij informatieveiligheid is een klassieke uitdaging dat het optimale niveau van investeringen in informatieveiligheid moeilijk meetbaar is: het kan altijd beter, maar of meer beveiliging nodig is, weet je pas als het fout gaat (ja, het was nodig)—en dan is het mogelijk te laat: de informatie ligt op straat en de reputatie aan diggelen. Het is een van de redenen waarom informatieveiligheid moeilijk op de directieagenda is te krijgen: het is een kostenpost die geen zichtbaar resultaat oplevert, behalve als er een zwaar incident plaatsvindt (denk Diginotar) dat—achteraf—aangeeft dat het onderwerp voorheen te weinig aandacht heeft gehad.

Evenzo luidt een veelzeggend aforisme dat privacy net is als zuurstof: je merkt het pas als het er niet meer is. In een samenleving met voldoende ruimte voor een privéleven, ben je je nauwelijks bewust dat je kunt zijn wie je wilt; pas als een samenleving autoritaire trekken krijgt, merk je hoe belangrijk levensruimte is om (binnen redelijke grenzen) ongestoord jezelf te kunnen zijn. Maar als die autoritaire samenleving ontstaan is, is het de vraag of er nog een weg terug is: een voortgaande uitholling van privacy zou wel eens onomkeerbaar kunnen zijn. In minder dramatische termen gezegd: het belang van privacy blijft vaak onderbelicht, omdat het weinig zichtbaars oplevert; privacy is smeerolie van maatschappelijke processen doordat het individuen de nodige speelruimte biedt, maar het belang blijkt pas als de maatschappelijke processen spaak lopen. Lang is privacy afwezig geweest als factor in beleids- en bestuursagenda's; pas sinds enkele jaren is privacy weer een factor van betekenis geworden, nu langzamerhand het besef doordringt dat het optuigen van vele databanken met enorme aantallen uitwisselbare persoonsgegevens ook grote risico's oplevert voor het welbevinden van burgers en consumenten, niet in het minst door de Snowden-onthullingen.

Vooral deze derde parallel leert ons dat informatieveiligheid en privacy elkaar nodig hebben om samen sterker te staan: pijnlijke incidenten met informatieveiligheid tonen ook risico's voor privacy aan die vaak pas worden onderkend als het te laat is, terwijl de toenemende aandacht voor privacy ook een toenemende roep betekent om betere bescherming van dataverzamelingen.

4. Waar privacy en informatieveiligheid van karakter verschillen

Hoewel privacy en informatieveiligheid vaak samengaan en vergelijkbare belangen dienen, zijn er ook karakterverschillen. Qua terminologie leggen ze een verschillende nadruk. Waar informatieveiligheid zich richt op informatie, dat wil zeggen *betekenisvolle* gegevens, richt privacy zich op (persoons)gegevens, dus meer de ruwe data ongeacht of deze voor iemand betekenis hebben. Maar dit verschil is klein. Door de ontwikkeling van *data mining* en Big Data convergeren de concepten van gegevens en informatie sowieso: gegevens kunnen altijd informatie bevatten en informatie is weer de grondstof—gegevens—voor andersoortige informatie. Informatieveiligheid gaat in feite over beveiliging van allerlei soorten gegevens, ongeacht hun inhoud, terwijl persoonsgegevens in potentie altijd betekenisvolle gegevens zijn, omdat ze worden verzameld en gebruikt voor bepaalde doelen. Beide gaan dus over de bescherming van gegevens en informatie.

Daarbinnen zien we wel een karakterverschil in het object: informationele privacy beschermt één bepaald type gegevens—persoonsgegevens—vanuit het idee dat daarmee ook de personen over wie het gaat, de zogeheten 'betrokkenen', worden beschermd. Informatieveiligheid is minder eenkennig ten aanzien van het type gegevens: in principe wordt elk type informatie beschermd,

ongeacht waar de informatie betrekking op heeft, en het onderliggende idee is dat daarmee niet alleen de belangen van waar de informatie betrekking op heeft (werking van ICT-systemen, bedrijfsprocessen, klanten, afnemers, koerswaarde) maar vooral ook de belangen van de informatieverwerkende organisatie zelf worden beschermd.

Dat is op zich niet zo interessant, maar relevant is wel dat het gepaard gaat met een karakterverschil in benadering van het object. De privacybenadering is vooral zwart-wit: er is weliswaar discussie over wanneer een gegeven precies een persoonsgegeven is, maar wanneer eenmaal is vastgesteld dát het een persoonsgegeven is, worden alle persoonsgegevens op een tamelijk uniforme manier benaderd, terwijl wat niet als persoonsgegeven wordt gekwalificeerd, helemaal niet wordt beschermd door de privacywetgeving. Informationele privacy kent twee grijstinten: gegevensverwerwerking voor 'huishoudelijk' gebruik is uitgezonderd van de werkingssfeer, terwijl zogeheten 'bijzondere' persoonsgegevens—medische, religieuze of seksuele en andere typisch privacygevoelige gegevens—juist extra worden beschermd. Informatieveiligheid hanteert daarentegen een veel genuanceerdere benadering door de nadruk te leggen op een risicoafweging, die gepaard kan gaan met een rijkergekleurd palet in beschermingsmaatregelen voor verschillende klassen gegevens of gegevensgebruik. In dit opzicht kan informationele privacy denk ik iets wezenlijks leren van informatieveiligheid, want natuurlijk leveren niet alle persoonsgegevens (die buiten de 'huishoud'-uitzondering vallen) altijd dezelfde risico's op voor betrokkenen, en de implicaties van verwerking van 'bijzondere' gegevens kunnen ook enorm verschillen afhankelijk van de context. In de toekomst zal de benadering gelukkig iets genuanceerder worden, aangezien de komende wijziging van de Europese dataprotectiewetgeving aandacht heeft voor gegevensverwerkingen die 'bijzondere risico's' opleveren voor de rechten en vrijheden van betrokkenen, en waarin bovendien voorgesteld wordt om voor gepseudonimiseerde gegevens juist een wat lichter regime te hanteren. Dit zijn goede aanzetten voor een opener, op een risico-inschatting gebaseerde en meer contextafhankelijke benadering om gegevens te beschermen.

Een tweede karakterverschil is de omvang van de bescherming. Informationele privacy hanteert een meer holistische aanpak bij de bescherming van gegevens, met regels voor verzameling, verwerking, opslag, gebruik, doorgifte en vernietiging. Informatieveiligheid heeft ook oog voor de hele cyclus van gegevensverwerking, maar de nadruk ligt toch vaak vooral op beveiliging bij de verwerking en de opslag van gegevens. Hoewel het principe 'select before you collect' wel een vuistregel is binnen informatieveiligheid, zou het meer nadruk kunnen krijgen in beleid en richtlijnen voor een goede informatiehuishouding. De informationele privacy laat immers zien waarom dataminimalisatie—dus vooral ook bescherming bij het startpunt, het verzamelen van gegevens—belangrijk is: het helpt om onterechte beslissingen te voorkomen door vervuiling van het databestand met irrelevante gegevens tegen te gaan.

Omgekeerd is er bij informationele privacy relatief weinig aandacht voor het vraagstuk van toegang en autorisatiecontrole, dat juist een van de belangrijkste pijlers is van informatieveiligheid. Bij privacy wordt uitgegaan van één organisatie die in abstracto als geheel verantwoordelijk is voor de gegevensbescherming; deze organisatie is 'de verantwoordelijke' die rechten en plichten heeft en gegevens op bepaalde manieren mag verwerken. Daarbij blijft in het midden wie binnen de organisatie wat mag doen. Het vraagstuk van toegang en autorisatiecontrole speelt bij privacy eigenlijk alleen een rol bij de verplichting persoonsgegevens adequaat te beveiliging, oftewel het onderdeel informatieveiligheid. De overige aspecten van informationele privacy (bijvoorbeeld voor welke doelen gegevens verwerkt mogen worden, of de kwaliteitseisen voor dataverwerking) gelden in principe voor iedereen binnen de organisatie van de verantwoordelijke. De op een risico-inschatting gebaseerde benadering van informatieveiligheid is fijnmaziger, en laat bijvoorbeeld toe dat sommige afdelingen, of speciaal geautoriseerde medewerkers, meer mogelijkheden (of juist zwaardere kwaliteitseisen) hebben ten aanzien van sommige data uit een dataverzameling dan andere afdelingen of ongeautoriseerde medewerkers.

Een derde, en voor dit essay misschien het meest relevante, karakterverschil is de omgang met het delen van informatie. Bij informatieveiligheid wordt dit in beginsel gezien als riskant: het is zeker niet onmogelijk, maar vaak op zich wel onwenselijk om informatie aan derden te geven. Je verliest daarmee namelijk de controle over gegevens, en dat betekent dat het een bewuste risicoafweging vergt of het doel van delen opweegt tegen het aanvullende risico dat informatie weglekt of wordt gemanipuleerd. Bij het in de inleiding genoemde voorbeeld van de

gedecentraliseerde zorg betekent dit vermoedelijk een uitgangspositie van terughoudendheid bij het delen van informatie binnen gemeentelijke netwerken: je verliest sneller het overzicht wat er gebeurt met informatie waar je als organisatie verantwoordelijk voor bent, en de organisatie heeft een zekere verantwoordelijkheid om na te gaan of gedeelde informatie bij ketenpartners in voldoende veilige handen is.

Bij informationele privacy ligt dat net iets anders: hoewel vaak gedacht wordt dat privacywetgeving een belemmering vormt voor het delen van gegevens, moet het delen niet zozeer worden beschouwd als een extra risico maar eerder als een extra vorm van verwerking die goed geregeld moet worden. Privacywetgeving is niet tegen delen als zodanig (nee tenzij), maar is eerder voor zorgvuldig delen (ja mits). (Merk op dat privacywetgeving twee doelen heeft, niet alleen bescherming van privacy maar ook vrij verkeer van persoonsgegevens binnen Europa—dat laatste wordt wel eens over het hoofd gezien.) Zoals in de inleiding opgemerkt staat de privacywetgeving delen toe als er een goede grondslag voor is en het binnen de grenzen van proportionaliteit plaatsvindt, mede omdat het mogelijk leidt tot een adequater beeld van iemand waardoor zorgvuldiger beslissingen mogelijk worden. Binnen de gedecentraliseerde zorg betekent het daarom niet per se een houding van terughoudendheid om persoonsgegevens te delen, maar eerder een houding van constructief meedenken om in gezamenlijkheid persoonsgegevens adequaat te beschermen. Uiteindelijk verschilt dat misschien niet veel van een benadering ingegeven vanuit informatieveiligheid, die immers ook zou moeten leiden tot adequate bescherming van informatie die waar nodig gedeeld moet kunnen worden, maar het perspectief (een 'nee tenzij'-houding tegenover een 'ja-mits'-perspectief) is net even anders.

Daarbij kan nog wel een kanttekening worden geplaatst. Volgens onderzoek van NRC Handelsblad ('Wie kunnen er straks allemaal je dossier inziens?', 16 augustus 2014) willen de meeste gemeenten het delen van gegevens binnen netwerken legitimeren op basis van expliciete toestemming van burgers. Ongeacht hoe de gegevens verder worden beschermd, is dat niet wat ik zou verstaan onder een zorgvuldige regeling voor het delen van gegevens. Burgers kunnen namelijk maar nauwelijks de implicaties van hun toestemming overzien, daarvoor zijn de netwerken te complex en de mogelijke gevolgen van het delen van informatie veel te diffuus. Bovendien hebben burgers weinig te kiezen—ze kunnen immers moeilijk naar een andere overheid overstappen—zodat toestemming geven feitelijk geen vrije keuze is. In dit opzicht is de benadering van informatieveiligheid beter, die de verantwoordelijkheid voor de beslissing om al dan niet te delen legt waar die thuishoort: bij de instantie die gegevens beheert en die verantwoordelijk is voor een goede informatiehuishouding. Een legitieme grondslag voor het delen van gegevens binnen gemeentelijke netwerken kan worden gevonden in de publieketaakuitoefening van de desbetreffende instanties (artikel 8 onder e Wbp), maar niet in een vorm van toestemming die in hoge mate fictief is.

Misschien is daarom juist de combinatie van beide perspectieven optimaal: het delen van gegevens is goed mogelijk als het zorgvuldig wordt geregeld (het privacyperspectief), maar het blijft wel de verantwoordelijkheid van de delende instantie om duidelijk te maken waarom het delen nodig is en past binnen een goede informatiehuishouding (het informatieveiligheidsperspectief). En dat is denk ik ook de les van de beschouwing van de karakterverschillen tussen privacy en informatieveiligheid: ook waar ze verschillende accenten leggen, vullen de perspectieven elkaar eerder aan dan dat ze in verschillende richtingen wijzen. Ik zie weinig intrinsieke of fundamentele verschillen waardoor het belang van privacy en het belang van informatieveiligheid uiteenlopen; veeleer houden beide belangen elkaar een interessante spiegel voor.

5. De onzichtbare medaille en de beleidsagenda

Zoals ik heb betoogd, hebben privacy en informatieveiligheid veel met elkaar gemeen. Ze dienen vergelijkbare doelen en hanteren vergelijkbare middelen. Hoewel de benadering soms verschilt, komt dit verschil niet voort uit conflicterende belangen maar eerder uit andere perspectieven die verschillende aspecten oplichten en daarmee een spiegel voorhouden. Je kunt privacy en informatieveiligheid dan ook het beste zien als twee kanten van een medaille. Of misschien liever—omdat de overheid nog niet echt een medaille op dit vlak heeft verdiend—als twee kanten van een munt, naar de Engelse uitdrukking 'two sides of a coin'. Die munt drukt uit dat

geïnvesteerd moet worden in een zorgvuldige en fatsoenlijke informatiehuishouding. Informatieveiligheid legt daarbij wat meer nadruk op zorgvuldigheid, privacy wat meer op fatsoenlijkheid; het komt beide neer op een propere informatiehuishouding. Zo'n propere informatiehuishouding kost geld, maar betaalt zichzelf terug omdat voorkomen beter en efficiënter is dan genezen.

Hoewel informatie alleen maar in belang toeneemt in de informatiesamenleving, is de munt van een propere informatiehuishouding toch nog te vaak onzichtbaar op directietafels en in beleidsagenda's. Zowel privacy als informatieveiligheid is vaak een kind van de rekening—de rekening van te weinig en te late aandacht. Zolang het goed gaat, gaat het goed, maar als het fout gaat, is het goed fout.

Ook hier biedt privacy denk ik een waardevolle aanvulling op het perspectief van informatieveiligheid, en omgekeerd. Incidenten rond informatieveiligheid hebben, zeker bij de overheid, al snel een weerslag op privacy, omdat er vaak ook risico's ontstaan voor de privacy van burgers. En waar dat tot enkele jaren gelden soms schouderophalend op de koop toe werd genomen, kan de overheid niet langer onverschillig blijven over privacyrisico's voor burgers. Wat de afgelopen jaren steeds meer blijkt: privacy bijt terug. De slimme meter, patiëntendossiers, centrale opslag van biometrie, verplichte dataretentie van telecomgegevens: steeds vaker blijkt dat een ongebreidelde verzameling en verwerking van persoonsgegevens op weerstand stuit, in de politiek, bij de rechter en, zeker sinds Snowden, in de media en bij het publiek. De overheid kan privacy niet langer als bijverschijnsel zien, maar moet bij elk informatie- en ICT-project zorgvuldig kijken naar de privacyimplicaties. Dit is inmiddels ook geformaliseerd met het uit de iStrategie voortvloeiende toetsmodel Privacy Impact Assessment Rijksdienst, dat standaard wordt toegepast bij de ontwikkeling van wetgeving en beleid waarbij nieuwe ICT-systemen of grote databanken worden voorzien (en hopelijk ook bij maatregelen die gepaard gaan met uitbreiding van bestaande ICT-systemen of databanken).

En dat heeft ook zijn weerslag op de zichtbaarheid van informatieveiligheid: het verzamelen en verwerken van gegevens moet fatsoenlijk gebeuren om rekening te houden met de gevolgen voor burgers (privacy), en moet in het verlengde daarvan ook zorgvuldig worden geregeld (informatieveiligheid). Nu privacy in de publieke discussie zichtbaarder wordt als een belangrijk aandachtspunt bij de opzet en vormgeving van ICT-projecten en gegevensstromen binnen de overheid, komt de andere kant van de munt—informatieveiligheid—vanzelf ook prominenter in beeld. Wil de overheid niet achteraf een gepeperde rekening gepresenteerd krijgen van informatielekken en privacyrampen, dan zal ze tijdig en voldoende aandacht moeten besteden aan de borging van een propere informatiehuishouding.

De combinatie van privacy en informatieveiligheid onderstreept, vanuit de belangen en benaderingen van beiden, waarom een fatsoenlijke en zorgvuldige informatiehuishouding wezenlijk is in de informatiesamenleving. De combinatie zou daarom een winnend team moeten zijn om beide belangen, die elk afzonderlijk vaak te onzichtbaar blijven, prominent op de beleidsagenda te zetten. Dan verdient de overheid toch nog een medaille.