DIF #5

Het collectief belang is heilig verklaard

Een landelijke DNA-databank, cameratoezicht en een elektronisch patiëntendossier: het zijn maar enkele voorbeelden van (nieuwe) ICT-toepassingen waarmee gevoelige persoonsgegevens worden opgeslagen en uitgewisseld. Hoe belangrijk is privacy nog? Een rondgang langs een filosoof, een socioloog en een jurist.

'Privacy' mag een wat wollig begrip zijn, soms wordt het ineens heel tastbaar. Halverwege het gesprek met ICT-socioloog Jan Steyaert, kijkt hij me even strak aan. "Ik weet waar je woont", zegt hij. Ik ben niet onder de indruk, want die gegevens staan gewoon in het telefoonboek. "Ik weet ook", vervolgt hij, "dat je in je vrije tijd met metaaldetectors bezig bent." Dat komt ineens dichtbij. Ik heb de rare gewoonte om met een metaaldetector over een akker te lopen: lekker uitwaaien en tegen beter weten in hopen dat je een pot gouden munten vindt. Prima hobby, maar het is niet iets waar je in een eerste zakelijk contact over zou beginnen. Maar Steyaert had het opgezocht, gewoon via Google. Ik merkte dat ik me even in mijn privacy voelde aangetast. "Mensen zijn naïef in wat er over hen allemaal te vinden is", zei Steyaert nog. "Als je iemand tegenkomt op een feestje, kun je heel makkelijk een profiel van die persoon samenstellen." Hij gaf ook iets van zichzelf prijs: "Als je op mijn naam had gezocht, had je bijvoorbeeld geweten dat ik van requiems houd."
Het zijn onschuldige weetjes, die hooguit een ongemakkelijk gevoel oproepen, maar niet tot schade leiden. Het wordt erger als een potentieel werkgever de gangen van een sollicitant nagaat, berichten tegenkomt op een forum over burnout en het cv van de werkzoekende om die reden maar snel terzijde legt. Maar ja, dat is de eigen verantwoordelijkheid van degene die die berichten post.
Het grootste gevaar op het snijvlak van ICT en privacy, zo betoogt Steyaert, is het secundair prijsgeven van gegevens: dat mensen toegang hebben tot informatie, terwijl ze daar eigenlijk geen toegang toe zouden mogen hebben. "Ik heb er uiteraard geen moeite mee dat mijn huisarts mijn medische gegevens kan bekijken. Het wordt anders als een zorgverzekeraar inzage heeft en mij op basis daarvan uitsluit van een verzekering."

Jurist Bert-Jaap Koops is vooral bezorgd over het gemak waarmee nieuwe opsporingsbevoegdheden in de wet worden opgenomen. "We zijn doorgeschoten. Er is in de wetgeving teveel nadruk komen liggen op veiligheid, te weinig op privacy. Dit jaar zijn de opsporingsbevoegdheden weer verder uitgebreid. Officieren van Justitie mogen gegevens vorderen bij alle bedrijven en instanties, zoals banken, bibliotheken, videotheken en supermarkten. Er worden steeds meer vangnetten uitgegooid, steeds meer gegevens verzameld. De techniek maakt het mogelijk om al die gegevens aan elkaar te koppelen. Er zal steeds meer worden onderzocht zonder dat iemand juridisch gezien verdacht is. Het lenen van bepaalde boeken of video's kan al voldoende reden zijn om camera's te plaatsen en telefoongesprekken af te luisteren. Dat raakt aan de manier waarop we onze maatschappij inrichten." Het woord 'politiestaat' neemt Koops niet in de mond. "Nee, dan schets je een karikatuur. Wat ik mis, is de analyse waarom de huidige bevoegdheden tekort zouden schieten. Zolang men mij niet overtuigt dat nieuwe opsporingsbevoegdheden echt iets substantieels opleveren, ben ik er geen voorstander van."

Interessant was het woordspelletje dat ICT-filosoof Jeroen van den Hoven in ons gesprek introduceerde. “Laten we proberen”, stelde hij voor, “om het woord ‘privacy’ het hele gesprek niet te gebruiken. Dat woord is vaag en wollig, iedereen verstaat er iets anders onder. Het begint een obstakel te worden.”
Van den Hoven wil ver blijven van grote woorden en ideologische begrippen. Concentreer je op de inhoud, dat is wat hij zegt. Praat niet over informatiesystemen in de gezondheidszorg in het algemeen, maar praat zo praktisch mogelijk, bijvoorbeeld over de autorisatiematrix van een ziekenhuisinformatiesysteem. Wie moet toegang hebben tot welke gegevens en waarom? Als je daar de discussie op toespitst, zo stelt hij, kun je wegblijven van het begrip privacy en dan gaat de discussie pas echt ergens over, namelijk over de inhoud. Hij zegt: “Anders dan dogmatische privacyvoorvechters zeg ik: de wereld verandert, structureel. Het is evident dat we informatie over mensen nodig hebben. Die vraag staat voor mij niet ter discussie.”

Socioloog Steyaert was aanvankelijk verbaasd dat ik over het thema privacy ging schrijven. “Het debat rondom privacy is verstomd; het is meer een non-issue geworden. Door betere wetgeving en door de terreurdreiging is er een zekere consensus ontstaan. Toen onlangs de elektronische patiëntendossiers werden gehackt, ontstond een roep om meer *checks and balances*, niet om te stoppen met de dossiers zelf. Die discussie is een gepasseerd station.”
Ook filosoof Van den Hoven vindt een principiële discussie rondom privacy niet zo relevant. “De privacydiscussie gaat mank aan een ongelooflijk geïdeologiseer. Ik bagatelliseer het belang van het beschermen van persoonsgegevens niet, integendeel. Maar ik wil weg van de grote, abstracte thema’s, en terug naar het niveau van beleids- en ontwerpbeslissingen. Twee vragen moeten we steeds beantwoorden bij het ontwerpen van systemen en wet- en regelgeving: zijn de maatregelen die we nemen proportioneel, en zijn er alternatieven? Daar moet de discussie zich op toespitsen.”
Jurist Koops stelt zich strijdbaarder op; hij vindt privacybescherming wel degelijk een issue. Sterker nog, zijn inaugurele rede - afgelopen november - was geheel gewijd aan het thema. Hij pleitte ervoor dat ‘de deksel op de put’ moet, waar het gaat om verdere opsporingsbevoegdheden. “Ik mis de empirische onderbouwing van argumenten. Het gaat mij om de zuiverheid van de discussie, en uiteindelijk om iets veel groters: over de vraag hoe we onze samenleving wensen in te richten.”

Bert-Jaap Koops, hoogleraar regulering van technologie bij het Tilburg Institute for Law, Technology, and Society (TILT) aan de Universiteit van Tilburg

“Ik mis de empirische onderbouwing van argumenten”

“Natuurlijk, burgers moeten altijd een deel van hun privacy afstaan in het belang van de collectieve veiligheid. Maar we zijn doorgeschoten. Er is in de wetgeving teveel nadruk komen liggen op veiligheid, te weinig op privacy. De bevoegdheden van de overheid zijn de afgelopen jaren enorm uitgebreid en nóg verdergaande wetten zijn in de maak. Wat ik mis, is de analyse waarom de huidige bevoegdheden tekort zouden schieten. Zolang men mij niet overtuigt dat nieuwe opsporingsbevoegdheden echt iets substantieels opleveren, ben ik er geen voorstander van.

Enkele jaren geleden is de identificatieplicht ingevoerd. Die was nodig om de handhaving te versterken, zei men. Er was kennelijk een gevoel dat de politie onvoldoende mogelijkheden had. Maar in de praktijk wordt de identificatieplicht vooral toegepast om mensen die door rood licht fietsen dubbel te bekeuren. Het heeft de overheid extra geld opgeleverd, maar of de veiligheid erdoor is verbeterd, betwijfel ik.
Ook van preventief fouilleren kun je je afvragen wat het heeft opgeleverd. Het zal ongetwijfeld het gevoel van angst hebben verminderd bij mensen, maar is dat voldoende reden om zo'n ingrijpende maatregel in te voeren? Want waar komt dat onveilige gevoel vandaan, dát is het echte probleem. Gebeurtenissen als de rampen in Enschede en Volendam zijn ernstige zaken, maar het wordt zó breed uitgemeten in de media dat mensen zich daardoor onveilig gaan voelen. Hetzelfde zie je bij terrorismedreiging. Als je die angsten afzet tegen het statistische risico dat mensen lopen, zijn die angsten disproportioneel in vergelijking met andere risico's. Mensen zullen moeten accepteren dat er altijd risico's zijn in een samenleving, zonder direct aan de overheid te vragen om nóg meer camera's of nóg meer bevoegdheden. De regering gaat te makkelijk mee in die sentimenten.

Dit jaar zijn de opsporingsbevoegdheden weer verder uitgebreid. Officieren van Justitie mogen gegevens vorderen bij alle bedrijven en instanties, zoals banken, bibliotheken, videotheken en supermarkten. Ze kunnen precies zien wat iemand heeft geleend of gekocht en welke transacties hebben plaatsgevonden. Internetbedrijven en telecomaanbieders moeten een half jaar of nog langer alle verkeersgegevens vasthouden. Waar houdt het op?
Er is een nieuwe wet in de maak die de overheid ingrijpende bevoegdheden geeft op basis van 'aanwijzing' in plaats van verdenking. Nu mogen opsporingsbevoegdheden pas worden ingezet bij een concrete verdenking dat iemand een misdrijf heeft gepleegd, gebaseerd op feiten en omstandigheden. Straks is een aanwijzing voldoende, zonder dat duidelijk is wat dat precies inhoudt.
Vroeger, in het 'Saar en Swiebertje'-tijdperk, was het overzichtelijk: er werd een moord gepleegd en die werd vervolgens opgelost. Nu gaan we toe naar een overheid die niet start vanuit een misdrijf. Nee, er worden steeds meer vangnetten uitgegooid, steeds meer gegevens verzameld en al die gegevens worden aan elkaar gekoppeld; de techniek maakt dat mogelijk. Het lenen van bepaalde boeken of video's kan al voldoende reden zijn om camera's te plaatsen en telefoongesprekken af te luisteren. Er zal steeds meer worden onderzocht zonder dat iemand juridisch gezien verdacht is. Dat raakt aan de manier waarop we onze maatschappij inrichten.
Wat daar erg aan is? Het is niet erg als de AIVD dat onderzoek heel bedekt uitvoert en alle gegevens wist op het moment dat blijkt dat er niets aan de hand is. Maar ik betwijfel of je gegevens toch niet ergens in een register blijven staan. De AIVD kan ook zichtbaar onderzoek instellen, bijvoorbeeld door foto's te maken rondom je huis of navraag te doen bij buren. Mensen in je directe omgeving merken dat je in beeld bent, mogelijk door toevalligheden. Dat is ingrijpend, want het beeld van die foute buurman blijft toch hangen bij mensen. In Utrecht hebben we gezien hoe de politie met geweld een woning binnendrong, onterecht bleek achteraf. Hoe meer gegevens de overheid verzamelt, hoe groter de kans dat dit soort fouten optreden. Voor de betrokkenen is dat een zeer ingrijpende inbreuk op de privacy.
Het gaat overigens niet alleen om nieuwe wetten. Door de voortschrijdende techniek maken bestaande wetten veel meer mogelijk dan destijds kon worden voorzien. De wet om telefoongegevens te mogen opvragen dateert van 1926. Destijds had je alleen inzage in wie met wie had gebeld, en hoe lang. Nu kan de overheid onder dezelfde voorwaarden als in

1926 opvragen waar iemand heeft gebeld, welke websites hij heeft bezocht en op welke plaatjes hij heeft geklikt. Hierdoor ontstaat een veel indringender beeld van iemands persoonlijke leven.

Wat ik vooral mis in het huidige debat is de empirische onderbouwing van argumenten. Als je kunt aantonen dat je met een maatregel tien moorden extra oplost, heb je een goed argument. Maar die onderbouwing ontbreekt. Wat is het echte probleem, wat is de echte oplossing? Daar gaat het om. En als een maatregel niet blijkt te werken, draai hem dan terug. Want dat is het lastige: bevoegdheden breiden almaar uit, maar worden in de praktijk nooit teruggedraaid. Bij nieuwe wetgeving zouden horizonclausules moeten worden ingebouwd. Voer na drie jaar een objectieve studie uit: valt de conclusie negatief uit, laat dan de wet vervallen.
Het gaat mij om de zuiverheid van de discussie. En uiteindelijk gaat het om de vraag wat voor samenleving we eigenlijk willen creëren."

Jeroen van den Hoven, hoogleraar filosofie bij de faculteit Techniek, Bestuur en Management aan de TU Delft

"De privacydiscussie gaat mank aan een ongelooflijk geïdeologiseer"

"Het begrip 'privacy' is vaag en wollig; iedereen kan er iets anders onder verstaan. Het begint langzamerhand een obstakel te worden, het moedigt ook intellectuele luiheid aan. Het is daarom beter om het begrip privacy zoveel mogelijk te vermijden. En dat is makkelijker dan het lijkt.
Want waar gaat het om? Je hebt gegevens van mensen, en die wil je beschermen. Waarom wil je dat? Daar kun je verrassend duidelijke antwoorden op geven, zonder het woord privacy te gebruiken. We hebben goede morele redenen om gegevens te beschermen: we willen voorkomen dat mensen schade ondervinden, worden gediscrimineerd, dat informatie wordt gebruikt op plaatsen waar het niet relevant is.
De privacydiscussie gaat mank aan een ongelooflijk geïdeologiseer. Het is de afgelopen dertig jaar door verschillende groepen gemonopoliseerd. Het is de taak van de filosofie om nieuwe concepten te vinden, zodat mensen weer zinvol argumenten kunnen uitwisselen. Ik wil weg van de grote, abstracte, geïdeologiseerde thema's, en terug naar het niveau van beleids- en ontwerpbeslissingen. De discussie moet bijvoorbeeld niet gaan over privacy in *de* gezondheidszorg, maar over een ziekenhuisinformatiesysteem en de bijbehorende autorisatiematrix. Heel concreet: wie moet toegang krijgen tot welke informatie? Mag de portier inzage hebben in medische dossiers? Nee natuurlijk. Een verpleegster? Ja. Mag ze ook printen? Nee. Gegevens wijzigen? Nee, behalve de temperatuurgegevens. Zo ga je te werk en krijg je discussies met focus, waarin argumenten kunnen worden gewisseld. Dat heeft weinig te maken met privacy in een zweverige betekenis. Probeer heldere, morele redenen aan te geven voor concrete beslispunten inzake de bescherming van persoonsgegevens. Juist daardoor kunnen partijen het sneller eens worden over zaken.
Er blijft altijd een residu aan fundamentele verschillen van mening over de relatie tussen individu en samenleving; je hebt individualisten en collectivisten. Maar als ze het niet eens zijn, dan is precies duidelijk waarover ze het niet eens zijn. Zonder dat iemand zich er makkelijk van af kan maken door te zeggen: 'Ja, maar ik vind privacy gewoon belangrijk...'

De wereld is veranderd. Bij de opkomst van het privacydenken in de jaren zeventig stond de autonomie van het individu voorop. Kunnen we dat volhouden? Ik denk het niet. Als je de samenleving draaiende wil houden, moet je niet alleen belasting betalen, maar ook informatiebelasting. Je zult informatie over jezelf moeten prijsgeven.
De vraag is alleen of we het zo radicaal moeten aanpakken. Preventief fouilleren, onbeperkt afluisteren, het vasthouden van internetverkeersgegevens; dat zijn paardenmiddelen. Het zijn natuurlijke reacties op een veranderde omgeving, maar zijn ze ook proportioneel? En zijn ze effectief? Er zijn onderzoeken waaruit blijkt dat het niet altijd even goed werkt, het is vaak symboolpolitiek.
Maar anders dan dogmatische privacyvoorvechters zeg ik: de wereld verandert, structureel. Vroeger, veertig, vijftig jaar geleden, kenden mensen elkaar nog. Het is belangrijk om elkaar te kennen als je interacties aangaat. Die kennis van de ander wordt minder en minder, en dus zoeken we naar middelen om dat kennistekort te compenseren. Dat is een begrijpelijke reactie. Banken willen weten of iemand schulden heeft. Dus checken ze iemands normatieve reputatie in de hoop dat het houvast geeft in de interacties met die persoon. Ik wil het niet op de principiële vraag toespitsen. Het is evident dat we informatie over mensen nodig hebben. De vraag is alleen hoeveel informatie we nodig hebben, en of die proportioneel is. Ook moeten we bedacht zijn op *technology creep*. Het gevaar dat de wil bestaat om, als er eenmaal camera's zijn, de beelden langer te bewaren, om er meer mensen toegang toe te geven, en ze ook voor andere doeleinden te gebruiken.

Het ontwerpen van systemen en wet- en regelgeving moet zodanig gebeuren dat je wel de voordelen hebt, maar niet de nadelen. Neem het kinddossier. Vroeger werkten tientallen instellingen structureel langs elkaar heen, met alle drama's van dien. Dat willen we niet meer. Door informatieketens kunnen gegevens worden uitgewisseld tussen bijvoorbeeld onderwijs-, jeugdzorg- en justitiële instanties. De angst is: op scholen mogen ze niet bij de justitie-informatie komen! En: iedereen schrijft maar in dat kinddossier, je bent als kind zomaar een probleemgeval!
Meteen roepen: 'Dit is privacyinbreuk!', is niet erg behulpzaam. Want waarom willen we een kinddossier? Omdat we willen voorkomen dat er vreselijke dingen gebeuren met kinderen. In dergelijke discussies spelen twee vragen. Zijn de maatregelen proportioneel, en zijn er alternatieven? In het geval van het kinddossier is er geen alternatief. We willen misstanden voorkomen, dat kan alleen door informatie te delen. Waar het in dergelijke discussies steeds om gaat is, dat we moeten zoeken naar manieren om wel de voordelen te hebben, zonder de nadelen. Dat lukt niet met het innemen van vage ideologische standpunten. Dat kan alleen door conceptueel scherp te krijgen wat we willen bereiken, en hoe we systemen moeten ontwerpen die de balans van waarden uitdrukken die we wensen. Voor- en tegenstanders moeten daarvoor dezelfde taal spreken. Het woord 'privacy' hoeft in die taal niet voor te komen."

Jan Steyaert, lector Sociale Infrastructuur en Technologie bij Fontys hogescholen

"Mensen zijn vooral bereid om andermans gegevens weg te geven"

“De grote kentering is gekomen door de aanslagen in New York, Madrid en Londen. Ineens zie je een hoop naïviteit met betrekking tot privacy verloren gaan. Vroeger, tot in de jaren negentig, was de beleving dat privacy iets is dat je voor honderd procent hebt, en dat je alleen maar kan worden afgenomen. Na die aanslagen gingen mensen beseffen dat privacy ook te maken heeft met de veiligheid van de eigen leefomgeving. Om die veiligheid te garanderen moet je iets van je privacy weggeven. Vroeger werd een camera op een metrostation puur gezien als inbreuk op je integriteit; na de aanslagen in Londen geeft het vooral een groter gevoel van veiligheid. Het was dankzij die camerabeelden dat de plegers van de tweede, mislukte aanslag konden worden opgepakt. Het debat rondom privacy is door die aanslagen verstomd; het is meer een non-issue dan tien jaar geleden.
De tijdgeest is veranderd. Toch zie ik een interessante paradox. Enerzijds zijn mensen bereid om gegevens weg te geven, anderzijds zijn ze vooral bereid om gegevens van *anderen* weg te geven. We zijn blij als er een DNA-databank wordt opgericht, maar waar is de wachtrij van mensen die hun eigen DNA-profiel willen aanmelden bij die databank?

In de huidige tijd onderscheid ik twee belangrijke aspecten op het gebied van privacy. Allereerst de naïviteit van de burger over wat er over hem bekend is. We zijn heel vrijgevig. Als je ziet wat Albert Heijn weet van ons, wat banken weten, dat is enorm. Als je googelt op iemands naam, kom je veel te weten. Er zit ook een verschuiving in. Tien jaar geleden was de overheid de grote bedreiging – *Big Brother is watching you* – daarna kwam de bedreiging van het bedrijfsleven. Men sprak van de *glass consumer*, de ‘glazen’ consument waar je doorheen kijkt, waar je alles van weet. Nu, met Google, kun je spreken van een doorkijk-burger, en een glazen collega waar je doorheen kijkt. Als je iemand tegenkomt op een feestje, kun je nadien zo een profiel van die persoon samenstellen. Daar zijn we naïef in.
Een tweede aspect, en dat is ernstiger, heeft betrekking op de controle op het vrijgeven van informatie. Ik heb geen moeite met een elektronisch patiëntendossier, omdat ik weet dat een arts daardoor direct over de juiste informatie beschikt. Het wordt anders als die informatie of de toegang daartoe niet meer controleerbaar is. Bijvoorbeeld als die informatie ingezien kan worden door een zorgverzekeraar of een potentiële werkgever. Kijk, ik wil mijn medische gegevens graag uitlenen aan de huisarts, maar ik wil niet dat het nadien verdergaat. Je ziet dat de discussie zich daarop toespitst: op het secundair vrijgeven van gegevens. Toen onlangs de elektronische patiëntendossiers werden gehackt, ontstond een roep om meer *checks en balances*, niet om te stoppen met de dossiers zelf. Dat is een gepasseerd station.
Het gaat steeds om het evenwicht tussen wat je prijsgeeft en wat je terugkrijgt voor die informatie. Krijg ik voor de videobeelden voldoende veiligheid terug? Krijg ik voor persoonsgegevens voldoende Airmiles terug? En kan ik vermijden dat het ergens fout gaat? Daar zit de crux. De pijn zit bij het secundair prijsgeven. Ik geef informatie aan de huisarts, maar wil niet dat anderen daar inzage in hebben. Ik geef informatie aan een lotgenotengroep, maar wil niet dat de hele wereld daarvan mee kan genieten. Met wetgeving of technologie zou je daarop kunnen toezien.

In de jaren negentig was de aandacht voor privacy op haar hoogtepunt. De toenemende digitalisering was daarvan de oorzaak. De centrale vraag was: hoe kunnen we onze persoonsgegevens zo goed mogelijk beschermen? Er kwam een inhaalslag op het gebied van wetgeving om de privacy te behouden. Het opmerkelijke is dat die privacy daarvoor net zo goed bedreigd werd. Je kon bij wijze van spreken zó bij de sociale dienst binnenwandelen en

de dossierkast opentrekken. Maar door de digitalisering zijn we gevoeliger geworden voor schending van de privacy en hebben we een beter instrumentarium ontwikkeld om de privacy te bewaken. Dat is de winst van de jaren negentig.
In de discussie rondom privacy spelen de media een rol, actiegroepen, de overheid, en burgers zelf. Eens in de zoveel tijd zie je in die discussie rustpunten ontstaan. Nu, door betere wetgeving en door de terreurdreiging is er een zekere consensus. Maar hoe die consensus er over tien jaar uitziet is moeilijk te voorspellen. Als de terreurdreiging afneemt, als het veiligheidsgevoel toeneemt, dan zal er snel weer protest komen tegen cameratoezicht, centrale databanken of het uitdoen van je schoenen op het vliegveld. Die beweging terug is heel wel mogelijk. Ik zou niet weten waarom de houding ten opzichte van privacy lineair zou zijn. Het kan zo maar omslaan."