

## JAN STEYAERT LECTOR SOCIALE INFRASTRUCTUUR EN TECHNOLOGIE BIJ FONTYS HOGESCHOLEN



'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 wat 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 ze de plegers van de tweede, mislukte aanslag konden oppakken. 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 doorkijkburger 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 een zorgverzekeraar of een potentiële werkgever die informatie kan inzien. Kijk, ik wil mijn medische gegevens graag uitlenen aan de huisarts, maar ik wil niet dat het nadien verder gaat. Je ziet dat de discussie zich daarop toespitst: op het secundair vrijgeven van gegevens. 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? 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 kan meegenieten. 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.'