Column
PUBLIC EYE

THEO DE VRIES

Op 9 mei 2007 krijg ik het volgende persbericht van de gemeente Leiden onder ogen: 'De gemeente Leiden heeft als eerste gemeente in Nederland gegevens geleverd aan het Digitaal Klant Dossier (DKD). Het DKD is een virtueel dossier met relevante informatie uit de databases van verschillende organisaties op het gebied van werk en inkomen zoals UWV, CWI, en Sociale Diensten. De gegevens worden automatisch aangeleverd, samengevoegd en zijn direct op het beeldscherm te zien. Van de financiële situatie van de klant tot onder meer voertuigbezit, werkervaring, polisadministratie, uitkeringen en reïntegratie. Het DKD ontsluit hiermee een schat aan informatie.'

Klanten hoeven niet langer steeds dezelfde informatie op te geven. Zij kunnen via internet bovendien altijd en overal hun eigen gegevens inzien, zelf informatie of formulieren opvragen en bepaalde gegevens wijzigen. Een prima service. Daar zit mijn probleem niet. Het zit in de mogelijkheid die gegevens te koppelen, al of niet met andere bronnen, en te analyseren. Daarover wordt helaas geen mededeling gedaan. Onduidelijk is ook wie er allemaal bij deze gegevens kan komen.

Een ander voorbeeld. Hier gaat het om veiligheid. Jacob van Kokswijk schrijft in dit nummer van *Liberaal Reveil* dat in Engeland elektronische surveillance zo ver is doorgevoerd dat er 1 camera op 13 inwoners is geïnstalleerd. Dat betekent dat in grotere steden per dag gegevens van heel veel mensen ongevraagd ongeveer 30 keer of meer ergens in een computer worden opgeslagen. Voor bepaalde of onbepaalde tijd. Die camera's zijn vaak onhandig en gelukkig goed zichtbaar. Maar dat verandert snel. Door de nu al waarneembare komst van zeer effectieve herkenningstechnologie, van minuscule camera's en nieuwe generaties computers, is het straks voor overheid en private partijen mogelijk ieders gangen onzichtbaar waar te nemen en te registreren. Goede controle daarop is een illusie. Maar dat niet alleen, de koppeling met al bestaande databanken ligt binnen handbereik.

Nieuwe ontwikkelingen dienen zich in een steeds sneller tempo aan. Zo is het straks mogelijk duizenden minuscule sensors ('smart dust') uit te strooien die vervolgens in een netwerk met elkaar communiceren. Militair gebruik is evident, bij civiel gebruik wordt het mogelijk allerlei beheersprocessen heel efficiënt te laten verlopen. Dat is het probleem niet. Bedenkelijk wordt het pas, als data aan persoonsgegevens wordt gekoppeld.

Vrijwel iedere burger laat bijna dagelijks een indrukwekkende spoor gegevens achter zich. De hoeveelheid daarvan – in digitale vorm – is in de achter ons liggende jaren explosief toegenomen. Die toename gaat onverminderd door, er ontstaat een chaotische databerg waarvan slechts een klein deel effectief en meestal doelgebonden wordt gebruikt. Door middel van nieuwe mathematische modellen, statistische patroonherkenning en algoritmes, tezamen met krachtige computersystemen, kan veel van de datachaos worden getransformeerd in aanzienlijk meer bruikbare informatie voor geheel andere doelen. Zo kunnen bijvoorbeeld medische gegevens bij een zorgverzekeraar verwachtingen over iemands ziektekansen genereren, een soort statistisch DNA; nuttig voor de zorginkoop, dat wel. Of kunnen profielen worden berekend, waardoor criminele tendensen van individuen worden herkend. Onnodig te zeggen dat dit soort activiteiten veel vragen zullen oproepen. Vragen die raken aan de privacy van individuen.

De voorzitter van het College Bescherming Persoonsgegevens (CBP), de heer Kohnstamm, is doordrongen van het gevaar van de snelle technologische ontwikkelingen, zo blijkt uit het jaarverslag 2006 van het CBP. Volgens hem komt de privacy van de burgers daardoor steeds meer in de knel. Probleem is dat de handhaving van de privacy wetgeving rust op een wet uit 2001 – een juridisch werk dat geïnspireerd is door informatie- en communicatietechnologie van aanmerkelijk oudere

datum. Het handhaven van die wet lijkt steeds meer een onbegonnen zaak. Het is illusoir te denken dat dit kan worden opgelost door het verhogen van sancties van 4500 Euro, die bij de komst van de wet als maximale straf is bepaald. Bovendien is de pakkans vrijwel nihil.

Idealiter moet de bescherming van de privacy van burgers aan de voorkant, bij de introductie van nieuwe technologieën, beginnen. Er moet tijdig worden vastgesteld wat de privacyeffecten van een bepaalde technologie of informatiesysteem kunnen zijn – een privacy impact assessment (PIA). Of, zoals geschreven in een rapport (2006) aan de Engelse Information Commissioner, 'Ideally, a PIA tells the story of an information system or technological application: why it exists and how it collects, uses, discloses, and retains personal information. In this process, specific privacy issues are surfaced and can be resolved in a comprehensive manner on the basis of clear thinking and accurate information'.

Een dergelijk PIA zou wettelijk voorgeschreven moeten zijn. Het is ondoenlijk van privacy juristen te eisen, dat zij de gevolgen van nieuwe technologieën kunnen inschatten en adequaat daarop kunnen reageren. Dergelijke nieuwe ontwikkelingen ontsnappen steeds meer aan de juridische denkkaders. Het vooraf bepalen van effecten van nieuwe technologieën vereist daarom een heel andere werkwijze van het CBP. Handhaving van de wet en advies aan de overheid zijn natuurlijk belangrijk. Maar het accent zal meer dan vroeger moeten komen te liggen op visieontwikkeling en op een jaarlijks assessment van nieuwe en toekomstige technologische ontwikkelingen. In het CBP zal daarom structureel plaats moeten worden ingeruimd voor voldoende hoog gekwalificeerde technologen. De huidige taken van het CBP zijn te juridisch getoonzet en bieden daardoor nauwelijks ruimte voor het tijdig inzetten van technologische expertise. Zonodig moet de wet daarom worden aangepast en het budget van het CBP daarmee in overeenstemming worden gebracht. De tijd dringt.

Prof.dr.ir. Th. de Vries is bijzonder hoogleraar Toekomststudie gezondheidszorg aan de Universiteit van Twente en lid van de redactie van Liberaal Reveil.