

Bewijs maar eens je onschuld

Digitaal opgeslagen persoonsgegevens kunnen gestolen en misbruikt worden maar in Nederland is niets aan de hand, vindt onze naïeve overheid.

aan de tafel op het podium schoof een witharige man in gitzwart pak geërgerd op zijn stoel heen en weer. Hij zat daar als ervaren oud-rechercheur, popelend om uit te weiden over de driëntwintig gevallen van misbruik van andermans identiteit die hij alleen al vorig jaar voor een beveiligingsbedrijf had moeten behandelen. Belangrijk voor dit forum over digitale veiligheid. Maar hij werd telkens onderbroken door meer geleerde bespiegelingen. Jammer, want ik wilde zijn voorbeelden van identiteitsroof graag horen. Daarvoor was ik naar de universiteit van Eindhoven gekomen, een technisch omniversum onder de rook van Philips. Er werd veel verteld over beveiligingsmethoden. In een college hoorde ik hoe twee singles met elkaar kennis maken zonder een blauwtje te lopen en zonder hun anonimiteit te verliezen. Een expert liet zien hoe je uit camera-beelden een gezicht kunt herkennen waarbij de privacy van de andere gezichten wordt gewaarborgd. Maar veel veiligheidsexperts hadden kritiek op de nonchalance waarmee de overheid om onze persoonlijke gegevens opslaat en beheert.

Over het belang van privacy en bescherming van persoonsgegevens vallen veel vrome woorden. Maar ze hebben weinig effect. De schade wordt namelijk zelden publiekelijk afgehandeld. Mensen denken dan dat er niets aan de hand is. Tijdens een lezing vroeg een universiteitsdocent naar meer voorbeelden: „Mijn studenten denken dat het zo'n vaart niet loopt omdat ze niets te verbergen hebben. Kan ik hun ook vertellen wat er mis gaat?“, vroeg hij terecht.

Als antwoord komt dan vaak het ombudsmangeval van die ene ongelukkige die was ontslagen en failliet verklaard omdat iemand anders onder zijn naam misdrij-

ven had gepleegd. De dader was een voormalig huisgenoot en dan denk je eerder aan diefstal uit een bureau dan uit digitale bestanden. Dat is anders.

Geen wonder dat veel Nederlanders, onder wie een ruime meerderheid van de Kamer, denken dat brave burgers niets hebben te vrezen. Zoveel mogelijk registreren geldt als veilig, zeker sinds de terreuraanslag van 9/11. Maar massale opslag van intimiteiten kan onveilig zijn dan het denkbeeldige gevaar waar het tegen beschermt. Vijftien jaar geleden nog werd een identiteitsbewijs gezien als *Ausweis* uit de tijd van de Duitse bezetting. Nu is de stemming naar de andere kant doorgeslagen. Bur-



gers worden zonder reden aangehouden en de overheid legt megaregisters aan. Vingerafdrukken in de paspoortdatabank, digitale gegevens in het Elektronisch Patiëntendossier, notities van hulpverleners over het ouderlijk milieu van alle Nederlandse kindertjes in het Elektronisch Kinddossier, reisroutes van de ov-chip in de databanken van vervoersmaatschappijen en centrale registratie van autoritten is in de planning. We moeten erop vertrouwen dat de data kloppen en dat onverlaten geen toegang krijgen.

Voor de ooit zo foute Duitsers is het verbazend. „De digitalisering van het openbaar bestuur en de nauwe verknoping daarvan met het veiligheidsapparaat leiden tot methoden van overheidsdwang die in Duitsland tot nu toe ondenkbaar lijken“, waarschuwde databankspecialist Frank Rieger onlangs over Nederland in de *Frankfurter Allgemeine*.

Volgens Nicole van der Meulen, die op digitale identiteitsfraude promoveert, begon in Amerika het besef van de gevaren in 2005 te

dagen nadat bij de commerciële databank Choice Point 145.000 persoonsgegevens waren gestolen. Dat werd bekend omdat Choice Point het moest melden. Sindsdien is in vrijwel alle Amerikaanse deelstaten zo'n meldplicht voor lekken ingevoerd, waardoor nog meer bekend werd. Maar melden verhelpt het probleem niet. Je moet als burger maar hopen dat na diefstal je identiteit niet wordt misbruikt. De meeste Amerikanen voeren elk kwartaal een credit check op zichzelf uit om na te gaan of iemand anders niet op hun naam schulden aangaat. Ook in Europa gebeurt het. Vorig jaar werd een laptop met 600.000 Britse persoonsgegevens gestolen. Nederland kent geen meldplicht voor diefstal, maar een vrijblijvend meldpunt. We verkeren in de fase van de heilige onschuld.

Na het Eindhovense forum stond ex-rechercheur Wilfred van Roij uit te blazen van ergernis. „Ze denken hier dat het alleen een kwestie is van protocollen“, zei hij. Maar een systeem is zo goed als de mensen die het bestieren. Ook mensen die toegang hebben, zijn ook niet altijd te vertrouwen. Op Van Roij's vroegere politiebureau trokken agenten zich weinig aan van de privacyrichtlijnen. „Ze keken of ze het nieuwe vriendje van hun dochter in het politieregister konden vinden“, zei hij. Met het Elektronisch Patiëntendossier wil hij niets te maken hebben. „Veel mensen kunnen daar inkijken. In het ziekenhuis blijft die computer aanstaan. De secretaresse kan zien of iemand vijftien jaar geleden aan drugs was verslaafd.“

Identiteitsroof gebeurt niet alleen in het buitenland. Een cliënt van Van Roij werd vanuit Vlaanderen gehackt. Daar deed een man in zijn naam zaken. Internet is wereldwijd. De dreiging kan van overal komen: uit China, Rusland of Nigeria. De Britse veiligheids-expert Andy Clark houdt daarom rekening met de feilbaarheid van de mens: „Ontwerp een datasysteem niet op perfectie maar op de mogelijkheid om in te grijpen als het fout gaat.“ Een wijsheid die er bij de Nederlandse overheid nog niet in gaat. Bewijs dan maar eens je onschuld.