Geheimen **Privacy beschermen**

Privé en toch in de databank

Identificatie met irisscan op Schiphol (links). Op de achtergrond de ouderwetse methode. Foto Raymond Rutting de Volkskrant / de Volkskrant

Je kunt persoonsgegevens uit databanken combineren zonder de privacy te schenden, stelt een promovendus. Dan moet je wel zorgen dat alleen bij verdachte personen het kwartje valt.

Door **Michael Persson**

Stel: je vliegt naar New York en bent geen terrorist. Toch heb je liever niet dat de Amerikaanse autoriteiten weten waar je woont, wat je telefoonnummer en creditcardnummer zijn, dat je halal eet en misschien last hebt met plassen. Lukt het om het land binnen te komen zonder deze privé-geheimen prijs te geven?

Nee, volgens de huidige afspraken tussen de Europese Unie en de Verenigde Staten. De Amerikanen hebben het recht om, op zoek naar terroristen, in alle zogeheten Passenger Name Records (PNR's) uit de computers van luchtvaartmaatschappijen te snuffelen.

Ja, in principe wel, beweert daarentegen dr. Wouter Teepe (1977), die donderdag promoveerde bij de afdeling Kunstmatige Intelligentie van de Rijksuniversiteit Groningen. Hij heeft een methode bedacht (proefschrift op www.teepe.com) waarmee het mogelijk wordt informatie uit te wisselen zonder de privacy te schenden. Van onverdachte personen, althans.

'Privacybescherming en terrorismebestrijding zijn goed verenigbaar', vindt Teepe. 'Veel mensen denken dat het gebruik van grote databanken hoe dan ook ten koste gaat van de anonimiteit. Dat is niet zo. Je kunt heel goed databanken doorzoeken en gegevens uitwisselen terwijl de privacy intact blijft.'

Makkelijk is dat niet. Het komt er bij de passagiersgegevens op neer dat twee mensen ieder een geheim hebben, en van elkaar willen weten of dat hetzelfde geheim is. Maar het moet wel geheim blijven.

Zwanger

Teepe geeft een voorbeeld uit de universiteitspraktijk. Een onderzoekster heeft twee collega's afzonderlijk verteld dat ze zwanger is. Maar die moeten dat wel voor zich houden. De twee collega's komen elkaar tegen in de koffiehoek, en willen graag roddelen over het nieuws met mensen die er ook al van op de hoogte zijn. Maar hoe kom je erachter of een ander iets weet wat je, mocht die ander het niet weten, niet wilt verklappen?

De controle van passagiersgegevens door de Amerikaanse autoriteiten is een variant van het roddeldilemma. Het Amerikaanse ministerie van Binnenlandse Veiligheid heeft een lijst met namen van personen die het niet in het land, of zelfs niet in de lucht bóven het land, wil hebben. Die lijst moet wel geheim blijven: anders weet Osama Bin Laden precies wie hij niet naar Amerika moet sturen.

Anderzijds hebben ook de luchtvaartmaatschappijen een lijst die zij geheim willen houden: de passagiersnamen. Het doorspelen van de PNR's is in strijd met Europese mensenrechten, en het is ook niet voor niets dat het Europese hof besloot de overeenkomst tussen de EU en de VS nietig te verklaren. Die trokken zich daar alleen niets van aan, en stelden een nieuw informatie-uitwisselingsverdrag op.

De oplossing van Teepe heet 'kennis-authenticatie'. Niet op basis van gezag krijgt iemand toegang tot gevoelige informatie ('Ik ben van de Amerikaanse douane, geef me al je namen'), maar alleen op basis van kennis ('Ik weet al dat Claudia zwanger is, dus vertel het me maar'). In het geval van de passagiersgegevens betekent dit dat de twee partijen alleen de namen die op beide lijsten staan, aan elkaar bekend maken. Onverdachte passagiers blijven onbekend. 'Zelfs als je de andere partij niet vertrouwt, is die procedure toch betrouwbaar', zegt Teepe.

In woorden lijkt het T-2 protocol, ofwel het tweede protocol van Teepe, bijna triviaal. De twee partijen sturen elkaar alleen onherkenbaar verhaspelde versies van de namen op hun lijsten. Teepe heeft daartoe een zo moeilijke cryptografische functie gebruikt dat het niet mogelijk is uit de verhaspeling de naam in kwestie af te leiden. Alleen wie de verhaspeling herkent omdat die ook op de eigen lijst voorkomt, weet wie erachter schuil gaat.

In de praktijk vereist het protocol een hoop slimmigheden. Codewoorden die alleen de twee partijen kennen, moeten voorkómen dat een van de twee vals speelt. Ook heeft Teepe bedacht dat de twee partijen de verhaspelde namen om beurten in digitale kruimels moeten verzenden. Bit voor bit, dus met één 0 of 1 tegelijk. Een extra veiligheidsmaatregel. Zo kan elke partij met het vergelijken van twee 'namen' stoppen zodra er ook maar één bit afwijkt.

Toepassing

Goed, dat zijn de passagiersgegevens. Maar er zijn nog meer privacygevoelige overheidsplannen die Teepe aan het hart gaan. Want, geeft hij toe, hij heeft dit promotieonderwerp niet alleen gekozen vanwege de theoretische uitdaging. 'Het gaat mij ook om de praktische toepassing.'

Hij heeft iets bedacht voor het veilig koppelen van databanken, een vorm van 'informatieverrijking' waar beleidsmakers en bedrijven veel heil van verwachten. Zo worden met het Burger Service Nummer allerlei persoonsgegevens in handen van de rijksoverheid en gemeenten met elkaar verbonden. En er komt, om meer inzicht te krijgen in de ziektegeschiedenis van patiënten, een zogeheten landelijk schakelpunt, dat gegevens uit huisartsadministraties en apotheken vist om bijvoorbeeld te voorkomen dat een patiënt pillen krijgt voorgeschreven die in combinatie met andere medicijnen gevaarlijk kunnen zijn.

Teepe is daar niet op tegen. 'Natuurlijk kun je de privacy beschermen door geen enkele informatie over individuen uit te wisselen. Maar in de huidige maatschappij is dat onmogelijk. Er zitten te veel voordelen aan het aan elkaar knopen van bestanden. Ik denk dat het mogelijk is om desondanks de privacy te beschermen.'

Alleen, zegt hij, is het correct koppelen van een geboortedatum uit het ene bestand met het adres van dezelfde persoon uit het andere bestand al zo moeilijk gebleken, dat het voor hem geen verrassing is dat privacy en anonimiteit op het tweede plan zijn gekomen.

'Wat ik wil voorkomen, is dat iedereen zo maar kan grasduinen in die databanken', zegt Teepe. 'De huidige oplossing is haast banaal: twee partijen spreken af dat dat niet mag, en dat de persoonsgegevens alleen mogen worden gebruikt voor een beperkt doel. Een houtje-touwtje oplossing.'

Zelf houdt hij meer van technische oplossingen. Net als bij de passagiersgegevens, moeten instanties niet meer de beschikking krijgen over de eigenlijke, 'rauwe' data, maar over *information designators*: etiketjes die verwijzen naar de achterliggende gegevens, zonder die gegevens prijs te geven.

Zo geef je in plaats van een telefoonnummer een andere code aan de luchtvaartmaatschappij waar je je ticket hebt geboekt. Die code verwijst naar je telefoonnummer, en KPN krijgt hem ook. Teepe noemt het een soort schuldbekentenis: de code geeft de ontvanger het recht op een telefoonnummer. 'Maar als dat recht wordt misbruikt, trek ik de code in. Zo houd ik als persoon controle over wat er met mijn persoonsgegevens gebeurt. Ook valt met de code te herleiden hoe een bedrijf dat ongewenste reclame verstuurt, aan je adres kwam.'

Teepe geeft toe dat de methode alleen werkt voor nieuwe databanken. 'Het is niet iets wat je per decreet binnen anderhalf jaar kunt uitvoeren. Ik heb wel wensen en dromen, maar geen illusies.'

Maar technisch is privacybescherming mogelijk. 'De vraag in hoeverre privacy ook daadwerkelijk beschermd moet worden, is uiteindelijk een politieke.'

En het antwoord op die vraag is soms overduidelijk. Zo hebben de Amerikaanse autoriteiten onlangs een systeem opgezet, het Automated Targeting System, waarbij alle vliegtuigpassagiers, of ze nu verdacht zijn of niet, automatisch een risicoprofiel toegewezen krijgen.