

CBP MAAKT ZICH ZORGEN

PRIVACY OP DE HELLING?

Steeds meer gegevens van burgers worden onderling gedeeld en gekoppeld. Om fraude te bestrijden, criminelen op te sporen en de burger beter van dienst te zijn. Kan de overheid werken met big data en tegelijkertijd de privacy waarborgen? Het College Bescherming Persoonsgegevens maakt zich zorgen. 'Door de decentralisaties dreigt het voor zowel burgers als voor de overheid niet meer inzichtelijk te zijn wie welke gegevens verzamelt en gebruikt en met welk doel.'

TEKST PIETER VERBEEK
ILLUSTRATIE YVONNE KROESE

Wanneer je recente big dataprojecten van de overheid tegen het licht houdt, kun je je serieus afvragen in welke mate er rekening wordt gehouden met privacyaspecten. Kijk maar naar het veelbesproken Suwinet, het systeem waarin gemeenten, het UWV en de Sociale Verzekeringsbank persoonsgegevens uitwisselen van mensen in het kader van werk en inkomen. Een beter inzicht in de klant moet leiden tot betere dienstverlening. Uit onderzoek blijkt slechts 4 procent van de gemeenten voldoende maatregelen te nemen om de vertrouwelijkheid van uitgewisselde gegevens te waarborgen. Daarnaast waren in 16 procent van de gemeenten ambtenaren zonder reden in het nieuwe systeem gegevens van Bekende Nederlanders aan het napluizen.

'JE WILT TOCH NIET DAT EEN AMBTENAAR AL JOUW GEGEVENS OP ZIJN SCHERM KRIJGT ZODRA JE EEN RIJBEDIJG AANVRAAGT?'

Of wat te denken van de Belastingdienst, die onlangs – overigens opgelegd door de politiek – gevoelige financiële gegevens deelde met woningcorporaties zodat via de koppeling van data scheefwonen bij huurders aangepakt kan worden? Een ander recent voorbeeld komt van de politie, die zich schuldig maakte aan het delen van informatie voor doeleinden waarvoor het niet is verzameld.

De landelijke eenheid gaf door camera's vastgelegde kentekengegevens, de zogeheten *automatic number plate recognition*, door aan de Belastingdienst om leaserijders te controleren op hun kilometeradministratie.

Kan dit allemaal zomaar? Nee, stelt het College Bescherming Persoonsgegevens (CBP). Het leverde Nederland begin dit jaar ook een officiële waarschuwing op van de Commissie voor Burgerlijke Vrijheden van het Europees Parlement. Nederland moet de privacy van haar burgers beter beschermen.

IN VERKEERDE HANDEN

Het CBP heeft de laatste tijd veelvuldig haar zorgen geuit over het delen van grote hoeveelheden persoonsgegevens door overheden. In het laatste jaarverslag constateerde het college dat overheden steeds vaker persoonlijke gegevens van burgers gebruiken voor andere doeleinden dan waarvoor ze in eerste instantie zijn verzameld. En daarmee overtreedt ze een van de belangrijkste bepalingen in de Wet bescherming persoonsgegevens. Zeker met oog op de decentralisaties, de overheveling van taken naar gemeenten op het gebied van zorg, jeugd en werk, maakt het CBP zich zorgen. 'Door de decentralisaties dreigt het straks voor zowel burgers als voor de overheid niet meer inzichtelijk te zijn wie welke gegevens verzamelt en gebruikt en met welk doel,' legt Wilbert Tomesen, plaatsvervangend voorzitter van het CBP uit. 'Je wilt toch niet dat een ambtenaar al jouw gegevens op zijn scherm krijgt zodra je een rijbewijs aanvraagt?' De risico's van het werken met grote hoeveelheden data zijn enorm, vervolgt hij. 'Ze kunnen in verkeerde handen vallen, of toch voor andere doeleinden worden gebruikt dan waarvoor ze verzameld zijn. Burgers weten niet wat er met hun gegevens gebeurt of, nog erger, overheden weten het ook niet meer. Ik durf de algemene stelling aan dat de grote verwachtingen en ambities rond big data niet gelijk opgaan met de bescherming van de persoonsgegevens.'

Neelie Kroes, als Eurocommissaris verantwoordelijk voor de Digitale Agenda, wuift dit argument weg. Volgens haar wordt de privacy van burgers voldoende gewaarborgd door juridische grenzen en technologie. De angst voor privacyverlies staat de ontwikkeling van big data in de weg, zo zei ze afgelopen november. 'Privacy is essentieel, maar mag geen excuus zijn om niets met big data te

doen.' De meeste big data zijn volgens de VVD-politica bovendien anonieme data. 'We zouden minder huiverig moeten zijn voor het gebruik daarvan.'

Volgens onderzoeksjournalist Brenno de Winter, gespecialiseerd in it-beveiliging en privacy, moet de overheid burgers duidelijk informeren wat ze gaat doen met persoonsgegevens. 'We vertrouwen erop dat overheden en bedrijven het juiste doen,' stelt De Winter. 'Het programma PRISM [van het Amerikaanse National Security Agency, PV] is bijvoorbeeld een big data-project waar we duidelijk zien dat dat niet het geval was. Helaas wordt ons grondrecht om vrij en onbespied door het leven gaan niet goed erkend. We veranderen steeds de spelregels, lijkt wel. We beloven geheimhouding van persoonsgegevens om ze vervolgens met de meest vage redenen toch weer te schenden. Het is bizar om discussie hierover uit te sluiten. We hebben in het verleden al genoeg dure lessen getrokken uit totalitaire regimes die de persoonlijke levenssfeer van burgers schonden. Daar hadden we toch juist regels over gemaakt? Wat is nou de moeite om ons er van te voren over in te lichten?'

Daar is Tomesen van het CBP het mee eens. 'Overheden moeten zich goed realiseren waar ze mee bezig zijn. Privacy moet vanaf het allereerste moment in ogenschouw worden genomen bij het opzetten van een nieuw big data-project. Wat voor gegevens verzamel je? Hoe moet je ze beveiligen? Vanaf het begin moet je helder en consequent zijn. Gelukkig is het huidige kabinet zich hiervan bewust en ziet het de noodzaak in van het belang van het beantwoorden van dit soort vragen, zoals inmiddels gebeurt met de zogeheten *privacy impact assessments*'.

DUIDELIJK DOEL

Het is belangrijk dat er voor een dataverzameling een duidelijk doel is én een goede reden, stelt Sander Klous, teamleider bij KPMG en betrokken bij big data-projecten in de publieke sector en de telecom. 'Er moet expliciet toestemming worden gevraagd voor dat doel. En burgers moeten de mogelijkheid hebben ervan af te zien.' Volgens Klous is het ook belangrijk dat overheden werken met geanonimiseerde data en dat deze alleen in grote hoeveelheden worden getoond als resultaten. 'Dan zijn ze lastiger terug te leiden tot personen.' Om de veiligheid te waarborgen is een verandering van organisatie nodig, stelt Klous. 'Werk meer als een *data driven organization*. Denk goed na hoe je werkt. Waar leg je de verantwoordelijkheden? Zet richtlijnen op om je mensen scherp te houden, zodat ze zorgvuldig omgaan met de data, en om wildgroei te voorkomen. Zo ontstaan er geen ad hoc projecten en zorg je ervoor dat er een beperkt aantal mensen controle heeft over de data.'

Als je onvoldoende kaders stelt, gaat het volgens Tomesen van het CBP mis. Hij doelt op het elektronisch patiëntendossier, rekeningrijden en vingerafdrukken in paspoorten. 'Stuk voor stuk projecten met grote hoeveelheden persoonsgegevens, waarbij privacy onvoldoende een rol speelde. Als je er niet goed over informeert, ontstaat er in de samenleving een unheimisch gevoel wat leidt tot een gebrek aan vertrouwen. Het gaat om



persoonsgegevens. Daar moet je respect voor hebben en zorgvuldig mee omgaan.'

Desondanks speelt privacy in het doorbraakproject Big Data, een initiatief van het ministerie van Economische Zaken (zie pagina 21), nauwelijks een rol. 'Dat doen we bewust,' aldus aanjager Eric van Tol. 'We willen best

'WE Zouden MINDER HUIVERIG MOETEN ZIJN VOOR HET GEBRUIK VAN ANONIEME DATA'

de discussie aan over privacy, maar als ik daar nu heel erg op inzet, krijg ik overal nee te horen. Het houdt innovatie tegen. Veel big data-projecten worden bij voorbaat al getorpedeerd omdat men bezorgd is over de privacy. Wat dat betreft heeft Neelie Kroes gelijk, er heerst een privacyovergevoeligheid.' •

'Ach, ze weten toch al alles van me'

Om veiligheid te creëren moet de overheid je privacy wel schenden. Deze stelling legde jongerenradiozender FunX afgelopen najaar aan haar luisteraars voor. Maar liefst 71 procent van hen was het hiermee eens. Willen burgers eigenlijk wel weten wat de overheid doet met hun gegevens? Ze lijken erg laconiek te zijn rond de schending van privacy. 'Ach, ze weten toch alles al van me,' is een veelgehoorde opmerking. Bovendien zijn veel burgers zelf ook niet al te kritisch met wat ze over zichzelf op het internet plaatsen. Die laconieke houding is echter de makkelijkste manier om ermee om te gaan, stelt Brenno de Winter. Wanneer data tegen je worden gebruikt, zorgt het voor onrust. Het is taak van de overheid om die onrust weg te nemen. Maar ja, als de overheid nu juist de grote privacy-schender blijkt te zijn? Dan zijn er gelukkig andere initiatieven, privacywaakhonden zoals De Winter, Bits of Freedom en de Privacy Barometer. Begin januari ondertekenden 250 academici wereldwijd het manifest *Academics against mass surveillance*. Volgens hen worden we namelijk met z'n allen meer dan ooit tevoren in de gaten gehouden door inlichtingendiensten.