Hergebruik overheidsdata

Een groot gevaar voor onze privacy?

Commercieel (her)gebruik van overheidsdata kan de economie een nieuwe impuls opleveren. "Het is een goudmijn die klaar ligt om te ontginnen", aldus voormalig Eurocommissaris Neelie Kroes.[1] Maar is dit alleen een goudmijn, of liggen er ook gevaren op de loer? Want hoe zit het met onze privacy?

TEKST **MIRJAM ELFERINK**

Door de opkomst van big data-analyse worden nieuwe gebruiksmogelijkheden van overheidsdata mogelijk gemaakt. Een voorbeeld hiervan is *risicoprofiling*. In het recent verschenen boek '*Je hebt wel iets te verbergen. Over het levensbelang van privacy*'[2] schetsen onderzoeksjournalisten Maurits Martijn en Dimitri Tokmetzis waarom het recht op privacy het meest bedreigde mensenrecht van onze tijd is. Zij laten zien dat wij – veelal onbewust – grote hoeveelheden (persoons)gegevens 'weggeven' en welke ingrijpende gevolgen dat voor individuen, maar ook voor de samenleving als geheel kan hebben. Martijn en Tokmetzis vrezen dat door big data-analyse, zoals *profiling*, fundamentele democratische waarden kunnen worden aangetast waaronder de onschuldpresumptie en het non-discriminatiebeginsel.[3] Dat de techniek dit alles mogelijk maakt, brengt natuurlijk enerzijds geweldige mogelijkheden met zich mee, maar roept anderzijds de vraag op of het wenselijk is deze techniek toe te passen op iedere vorm van overheidsdata.

Wat is profiling?

Volgens de definitie in de Algemene Verordening Gegevensbescherming (AVG) is profiling "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of voorspellen."[4]

Persoonsgegevens zijn alle gegevens die direct dan wel indirect te herleiden zijn tot een geïdentificeerde of identificeerbare persoon. Data die op het eerste oog anoniem lijken kunnen door koppeling van verschillende bestanden toch herleidbaar zijn tot een individuele natuurlijke persoon.

Met profiling kan het gedrag van mensen worden voorspeld. Op basis daarvan worden mensen ingedeeld in categorieën. Hoe kunnen terroristen worden herkend? Welke categorieën klanten leveren winst op? Profiling gebeurt met behulp van verschillende technieken die zich in de regel aan het zicht van burgers onttrekken, zoals *tekst- en data-mining*, *risicoscoring* en *machine learning*.

Door big data-analyse kunnen fundamentele democratische waarden worden aangetast

Recht op privacy

Volgens artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: het EVRM) en artikel 10 van de Grondwet moet wetgeving die de bescherming van persoonsgegevens aantast, bepalingen bevatten die regelen welke soorten van gegevens mogen worden verwerkt: de categorieën van personen van wie persoonsgegevens mogen worden verzameld en bewaard, de omstandigheden waaronder dat mag plaatsvinden en de procedures die daarbij moeten worden gevolgd. De overheid heeft derhalve de taak om te zorgen voor wetgeving op basis waarvan persoonsgegevens op een zorgvuldige manier worden verzameld en verwerkt, en moet zich daar ook zelf aan houden. Dit betekent dat de overheid ook zorgvuldig zal moeten omgaan met het verzamelen, opslaan, bewaren en analyseren van overheidsdata die persoonsgegevens bevatten en met de inzet van technieken om big data te analyseren, zoals profiling.

Een voorbeeld van een profilingsysteem is SyRI (Systeem Risico Indicatie). Een systeem dat gegevensbestanden aan elkaar koppelt en analyseert volgens een vooraf vastgesteld risicomodel. Hiermee hoopt de overheid te kunnen voorspellen welke uitkeringsgerechtigde en/of belastingbetaler in de gaten moet worden gehouden.[5] Het College bescherming persoonsgegevens – tegenwoordig Autoriteit Persoonsgegevens – was van mening dat het systeem op een aantal fronten niet voldeed aan aspecten van de Wet bescherming persoonsgegevens.[6]

De overheid dient dus – evenals bedrijven en burgers – te voldoen aan de complexe privacyregelgeving. Het huidige regime daarvoor is vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Verder biedt de Algemene Verordening Gegevensbescherming (AVG), die per 25 mei 2018 rechtstreeks in alle lidstaten van de EU in werking treedt, uitgebreide verplichtingen en concrete maatregelen die moeten worden getroffen teneinde een zorgvuldige omgang met persoonsgegevens te waarborgen.

Zes uitgangspunten

Als de overheid overheidsdata openbaar wil maken en beschikbaar wil stellen voor (commercieel) hergebruik zal de overheid zich moeten houden aan de uitgangspunten van persoonsgegevensverwerking in de Wbp alsmede de AVG, teneinde risico's op onzorgvuldige omgang met persoonsgegevens te voorkomen dan wel te beperken. Hierna bespreek ik enkele van die uitgangspunten.

1 Transparantiebeginsel

Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Uit het reeds genoemde onderzoek van Martijn en Tokmetzis blijkt dat het maar zeer de vraag is of dit bij profiling wel altijd correct gebeurt.

2 Doelbinding

Persoonsgegevens mogen uitsluitend worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder worden verwerkt op een met die doeleinden onverenigbare wijze. Dit is een concreet risico bij toepassing van profiling nu men daarbij data vanuit verschillende bestanden – die zijn verzameld voor diverse doeleinden – aan elkaar koppelt en het maar zeer de vraag is of deze doeleinden van tevoren zijn bepaald én omschreven, en of de betrokkene daar dus steeds van op de hoogte is.

3 Beginsel van dataminimalisatie

Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking'). De crux van big data-analyse en profiling is nu juist dat persoonsgegevens bij voorkeur 'breder' worden verwerkt en het is de vraag of daarbij altijd wordt gehandeld in overeenstemming met de privacyregelgeving.

4 Passende maatregelen bij profiling

De verwerkingsverantwoordelijke – degene die doel en middelen van de gegevensverwerking bepaalt – dient meer maatregelen en waarborgen te treffen ten aanzien van de beveiliging, teneinde onjuistheden van persoonsgegevens te corrigeren en het risico op fouten te minimaliseren. Verder dienen de persoonsgegevens op zodanige wijze te worden bewaard dat rekening wordt gehouden met risico's en belangen van betrokkenen en dat discriminatie of maatregelen met een vergelijkbaar effect worden voorkomen.

5 Waarborgen rechten betrokkenen

Betrokkenen hebben diverse rechten: zoals een inzagerecht, het recht om vergeten te worden en het recht om bepaalde gegevens te laten wissen. Deze rechten dienen ook bij toepassing van profiling te worden gewaarborgd.

6 Inrichting systemen volgens de principes *privacy by design/privacy by default*

Deze principes houden in dat al bij de ontwikkeling en inrichting van geautomatiseerde systemen privacy-verhogende maatregelen worden genomen en dat een zorgvuldige methode van verwerking van persoonsgegevens technisch wordt afgedwongen. Daarnaast wordt in technisch opzicht al rekening gehouden met dataminimalisatie.

Conclusie

Hergebruik van overheidsinformatie, zoals profiling, kan heel veel waardevolle informatie opleveren. In dat opzicht is er inderdaad sprake van een goudmijn. Maar tegelijkertijd is er een keerzijde aan big data-analyse, die heel veel vraagt van de overheid als hoeder van ons fundamentele recht op privacy. Informatiespecialisten houden zich bezig met het verzamelen en beheren van (overheids)informatie, in toenemende mate via digitale processen. Voor hen lijkt een belangrijke taak weggelegd in het mede helpen waarborgen van ons fundamentele recht op privacy. ●

Noten:

1 http://europa.eu/rapid/press-release_SPEECH-11-872_en.htm
2 Maurits Martijn en Dimitri Tokmetzis, *Je hebt wel iets te verbergen. Over het levensbelang van privacy*, De Correspondent, 2016.
3 Maurits Martijn en Dimitri Tokmetzis, *Je hebt wel iets te verbergen. Over het levensbelang van privacy*, De Correspondent, 2016, p. 141-142.
4 Definitie afkomstig uit het richtlijnvoorstel inzake auteursrechten in de digitale eengemaakte markt, EC 14, september 2016, COM (2016), 593 final.
5 https://www.bnr.nl/nieuws/politiek/10008161/overheid-zet-big-data-in-tegen-fraudeurs
6 CBP, Advies conceptbesluit SyRI', brief aan de minister van Sociale Zaken en Werkgelegenheid, 18 februari 2014, p. 3.

Mirjam Elferink
LinkedIn.com/Mirjam Elferink

Mr. dr. M. (Mirjam) Elferink is, advocaat Intellectuele Eigendom, ICT-recht & privacy.

Zie ook www.od-online.nl