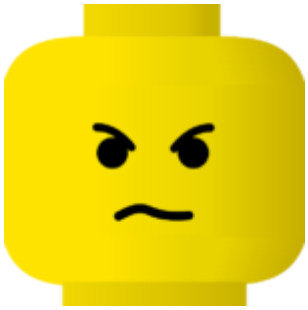
Cumulatief nadeel voor groepen in maatschappij door beoogde big-data-wet(WGS)



Op 31 augustus 2018 schreef ik op deze website een artikel over het wetsontwerp Gegevensuitwisseling door Samenwerkingsverbanden, kortweg WGS. Hiermee wil de overheid een juridische basis creëren voor het grootschalig uitwisselen van data betreffende burgers tussen overheidsinstituties en private partijen. Met de bedoeling deze uitgewisselde data met artificial intelligence(AI) te verwerken en zo (risico)profielen te maken. Door het grootschalig en eigenlijk ongericht gebruiken van deze computertechnologie zal de overheid een sterke toename veroorzaken van sociale stratificatie met een ongelijke verhouding tussen maatschappelijke groepen als gevolg. De Wetenschappelijke Raad voor het Regeringsbeleid(WRR) waarschuwde in april 2016 in de nota "Big data in een vrije en veilige samenleving" voor de grote nadelen en gevaren die verbonden zijn aan het gebruik van big-data-analyse in het publieke domein.

Argumenten

Terwijl de WRR in 2016 goed beargumenteerd waarschuwde zet de overheid thans vol in op big-data-analyse en profiling. Als beslissingen over (groepen van) burgers op basis daarvan genomen worden kan gemakkelijk een cumulatief nadeel (discriminatie en oneerlijke behandeling) ontstaan voor

bepaalde groepen uit de maatschappij. Dat kan doordat op basis van de analyseresultaten burgers uitgesloten kunnen worden van voorzieningen of ontplooiingsmogelijkheden(bijv. onderwijs of baan) zonder dat de burger zicht heeft op het waarom ervan.

Oordeel WRR

De WRR doet in haar rapport een aantal uitspraken die volledig van toepassing zijn op de bevoegdheden die de overheid met de WGS wil verkrijgen. Ze zegt:

*– **Big Data-analyses kunnen leiden tot een toename van sociale stratificatie door de bias te reproduceren en te versterken die in elke dataset zit. Zonder correctie vertaalt zich dit op termijn in discriminatie en oneerlijke behandeling van bepaalde groepen in de maatschappij** (Zarsky 2016: 126-127).*

*– **In het uiterste geval resulteren Big Data-methoden in datadeterminisme.** Daarbij worden individuen beoordeeld op basis van probabilistische kennis (correlaties en inferenties) over wat ze misschien zullen doen, in plaats van wat ze daadwerkelijk hebben gedaan.* Het zou ook afbreuk doen aan de idee van de mens als een autonoom moreel wezen dat in staat is te veranderen en andere keuzes te maken dan die in het verleden “Eens een dief, altijd een dief” is geen onderdeel van ons rechtsstelsel.

WRR vervolgt

*– **Big Data staat op gespannen voet met individuele privacy.** Daarnaast kan Big Data ook privacy als een collectieve invulling van vrijheid aantasten. Het gaat dan niet om de individuele schade van personen – volgens het principe van individual harm dat in het huidige recht voorop staat – maar om schade aan het fundamentele recht zelf, door de veelheid van individuele privacyschendingen.*

*– **Big Data-oplossingen zijn gevoelig voor function creep**, oftewel gebruik van data anders dan het doel waarvoor die data*

zijn verzameld. Function creep is in het domein van het veiligheidsbeleid een punt van zorg vanwege (a) verschillen in bevoegdheid omtrent gegevensverzameling en (b) de ingrijpende gevolgen die aan Big Data-analyses verbonden kunnen worden.

–Big Data-analyses bewerken niet alleen persoonsgegevens, ze genereren ook nieuwe.

Geheimzinnig

De burger mag van de data-uitwisseling en –analyse maar weinig weten. In artikel 7 van het wetsontwerp staat dat de deelnemers aan een samenwerkingsverband jegens derden(dus ook de burgers waarvan data zijn vastgelegd en uitgewisseld) verplicht zijn tot geheimhouding over de gegevens die zij in het samenwerkingsverband verwerken en over de resultaten van de verwerking. Er is ook geen notificatieplicht om de burger te melden dat zijn data in enig samenwerkingsverband gebruikt is dan wel dat er een risicomelding over hem gedaan in een op te zetten register van risicomeldingen. De burger kan slechts als hij/zij er zelf om vraagt binnen de WGS wel vragen of een register van risicomeldingen(op basis van profiling) zijn/haar naam bevat, maar niet wat voor risicomelding over hem gedaan is.

Chilling effect

De grootschalige verzameling, opslag en analyse van data door overheden, waaronder inlichtingen- en veiligheidsdiensten, kunnen ertoe leiden dat mensen het gevoel krijgen dat hun privacy en vrije meningsuiting in gevaar zijn, waardoor zij hun gedrag daarop aanpassen. Dat wordt ook wel het “chilling effect” genoemd.

Panopticum

Het behoeft geen betoog dat de constructie die de overheid op wil zetten met de WGS en nieuwe vorm van een panopticum is. Jeremy Bentham(1748-1832) verwerkte in zijn filosofie over

controle en macht het principe van permanente waakzaamheid en controle. Hij bedacht dat constante observatie van mensen kan helpen om het gedrag van die mensen te corrigeren en te reguleren. Bentham wilde dit idee graag in de praktijk verwezenlijken. Daarom ontwierp de filosoof samen met architect Willey Reveley in 1791 een model voor een gevangenis: het “panopticum”.

Om redenen die in de alinea’s hierboven uiteengezet zijn is ook in het licht van het WRR-rapport de opzet van wat de overheid als extra controlemogelijkheid wil creëren volledig af te wijzen.

W.J. Jongejan, 5 september 2018

Zarsky, T.Z. (2016) ‘The trouble with algorithmic decisions. An analytic road map to examine efficiency and fairness in automated and opaque decision making’, Science, Technology, & Human Values 41, 1: 118-132.