NTM/NJCM-bull. 2018/11

Grootschalige dataverwerkingsprojecten in handen van overheidsdiensten zijn problematisch, ook als er geen concrete nadelige gevolgen voor de burger zijn

Bart van der Sloot, datum 07-03-2018

Datum
07-03-2018

Auteur
Bart van der Sloot[1]

Vakgebied(en)
Internationaal publiekrecht / Mensenrechten

Deze bijdrage plaatst kritische noten bij de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten, en stelt voor een 'non-domination' perspectief te hanteren in plaats van het gangbare 'non-interference' principe. Met behulp van deze republikeinse privacybenadering kan de huidige digitale massaverzameling van privégegevens beter worden gegrepen.

Op 11 juli 2017 werd de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv) aangenomen door de Eerste Kamer.[2] De wet zou nodig zijn in de strijd tegen onder meer terrorisme. Daarom zijn er meer en bredere bevoegdheden toegekend aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen en Veiligheidsdienst (MIVD). Vóór de inwerkingtreding van deze wet mochten de diensten al grote hoeveelheden communicatie onderscheppen als die via de ether liepen, nu mag dat ook voor communicatie die via de kabel loopt, waaronder het meeste internet- en telefoonverkeer.[3] De wet zal in een referendum aan het volk worden voorgelegd, na een succesvol burgerinitiatief,[4] en waarschijnlijk ook voor de rechter worden gebracht.[5] Zorgen zijn er op globaal drie punten. (1) Inlichtingendiensten krijgen zeer ruime bevoegdheden om data te verzamelen, (2) die bevoegdheden kunnen worden ingezet om grote groepen niet-verdachte burgers te volgen en (3) er is vrij minimale parlementaire en rechterlijke controle op de diensten en wat ze met de verzamelde data doen.[6]
Voorstanders van de wet wijzen er op dat dergelijke ruime bevoegdheden nodig zijn in de strijd tegen terrorisme, dat volledige transparantie niet mogelijk is bij inlichtingendiensten, en dat er wel degelijk waarborgen zijn neergelegd, bijvoorbeeld door ministeriële controle, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de nieuw op te richten toetsingscommissie die de inzet van bevoegdheden toetst op rechtmatigheid. Meer fundamenteel wijzen voorstanders er op dat bij bulkinterceptie van gegevens de privacy van burgers niet wezenlijk wordt aangetast. Juist grootschalige gegevensverzamelingsprocessen zijn er niet op gericht om zaken te weten te komen over concrete individuen. Er worden bijvoorbeeld gegevens verzameld over simpelweg alle mensen die in een Amsterdam-West wonen; zo kan worden ontdekt dat er om drie uur 's nachts bovenmatig veel naar Syrië wordt gebeld. Daarop kunnen vervolgens meer specifieke maatregelen worden genomen. De massasurveillance *an sich* doet echter weinig schade aan de burger. Toch gaat dit in tegen een vrij basaal principe dat ook in het dagelijks verkeer wordt gehanteerd, namelijk het vereiste van een voorafgaand doel. Als een onbekend persoon je op straat aanspreekt en vraagt waar je woont dan is vaak de eerste wedervraag: 'Waarom wil je dat weten?' Als blijkt dat dit wordt gebruikt voor bijvoorbeeld een concreet wetenschappelijk onderzoek, dan zullen veel mensen bereid zijn hun gegevens af te staan; als het antwoord echter is: 'We verzamelen gewoon wat data en kijken later of we die ergens voor kunnen gebruiken en zo ja, waarvoor', dan zullen veel mensen weigeren.[7] Een dergelijk basaal principe geldt temeer voor de inzet van overheidsmacht. De overheid mag haar macht in principe alleen gebruiken voor een concreet en legitiem doel en zeker niet willekeurig. Toch is dat precies wat er in toenemende mate gebeurt binnen de Nederlandse overheid – in het geloof dat Big Data de toekomst is, ontplooien inlichtingendiensten, de belastingdienst, de politie en andere organen steeds meer dataverwerkingsinitiatieven, waarbij het vaak van tevoren onduidelijk is welke doelstellingen hiermee worden bereikt en waarom specifieke data nodig zijn.
Daarbij komt de vraag naar effectiviteit. Helpen dergelijke dataverwerkingsprojecten eigenlijk wel en zo ja, is deze inzet van middelen effectiever dan bij bijvoorbeeld kleinschalige gegevensverwerkingsprojecten? Opmerkelijk is dat de regering deze vraag eigenlijk nooit beantwoordt, terwijl onderzoek heeft aangetoond dat deze Big Data-projecten vaak ineffectief zijn. Zo bleek onlangs dat de digitaliseringsslag van de belastingdienst tot nu toe veel meer kost dan dat het oplevert,[8] dat de experimenten met *predictive policing* geen aantoonbaar effect sorteren[9] en er is maar weinig bewijs dat massasurveillance effectief is in de strijd tegen terrorisme.[10] Er wordt derhalve macht gegeven aan inlichtingendiensten om op grote schaal gegevens te verzamelen, zonder dat duidelijk is of dat überhaupt effectief is.[11]
Toch hebben voorstanders van dergelijke initiatieven een punt als zij vragen wat eigenlijk het probleem is, welke last

burgers eigenlijk ondervinden van dit soort dataverzamelingsprojecten. Deze vraag raakt ook aan een basaal uitgangspunt dat zowel in de privacyliteratuur als -jurisprudentie wordt omarmd, namelijk dat burgers alleen een beroep kunnen doen op hun recht op privacy als zij kunnen aantonen direct en individueel geraakt te zijn. Dat wordt in de literatuur wel het 'non-interference' principe genoemd, waaruit volgt dat er bij een 'interference' een inbreuk op een recht is gepleegd. Ook door bijvoorbeeld het Europees Hof voor de Rechten van de Mens (EHRM) ten aanzien van artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM) wordt een dergelijke inbreuk op een individueel recht vereist. Het Hof stelt dat in principe alleen natuurlijke personen een klacht kunnen indienen aangaande het recht op privacy en dat hun klacht alleen ontvankelijk is als zij kunnen aantonen dat zij slachtoffer zijn geweest van een concrete inbreuk. Zogenoemde *in abstracto* klachten, die gaan over een wet of beleid als zodanig, zonder dat de eiser beweert daar zelf hinder van te hebben ondervonden, zijn in principe niet-ontvankelijk.[12] Dat geldt ook voor zogenoemde *a priori* klachten, waarin een zaak wordt aangebracht nog voordat de privacy-inbreuk zich heeft voltrokken,[13] voor hypothetische klachten, over een inbreuk waarvan de klager niet zeker weet of die zich heeft voorgedaan, en voor algemeen belangacties, die bijvoorbeeld worden aangebracht door burgerrechtenorganisaties:

'The Court reiterates in that connection that the Convention does not allow an *actio popularis* but requires as a condition for exercise of the right of individual petition that an applicant must be able to claim on arguable grounds that he himself has been a direct or indirect victim of a violation of the Convention resulting from an act or omission which can be attributed to a Contracting State.' [14]

Dit uitgangspunt komt echter steeds meer onder druk te staan in het tijdperk van Big Data – dataverzamelingsprocessen worden immers steeds groter en het individuele element wordt steeds incidenteler. De meeste traditionele privacyschendingen zijn duidelijk afgebakend in persoon, tijd en plaats. Om zeven uur 's ochtends trad de politie het huis van meneer De Bruijn binnen; van 9 oktober tot 11 november is de telefoon van mevrouw De Wit afgeluisterd. Dit ligt echter anders bij moderne privacyvraagstukken, die vaak draaien om grote gegevensverzamelingsprocessen die nauwelijks in tijd, ruimte en persoon zijn af te bakenen en een structureel en voortdurend onderdeel vormen van de *modus operandi* van overheidsdiensten.
Het probleem van de talloze camera's die op vrijwel elke straathoek van grote steden zijn te vinden is niet dat ze mij als concreet persoon treffen, ze filmen iedereen die zich binnen het bereik van de camera's bevindt overal en altijd. Welke nadelige gevolgen ondervindt een individu eigenlijk als hij gefilmd wordt op straat door een bewakingscamera? Welke concrete schade heeft de gegevensverzameling door de National Security Agency (NSA) gedaan aan de individuele belangen van een gewone Amerikaanse of Europese burger? Het probleem van deze Big Data processen is niet dat ze mij als persoon concreet en individueel treffen, het probleem is gelinkt aan hoe de overheid haar macht inzet en welke waarborgen er zijn om willekeurige, ongerichte machtsinzet tegen te gaan.
Daarom wordt in de literatuur in toenemende mate gesuggereerd dat het liberale 'non-interference' principe moet worden aangevuld met het 'non-domination' principe dat als uitgangspunt wordt genomen in de republikeinse literatuur van onder andere Phillip Petit.[15]

'Contrary to Berlin's account of negative liberty – that a person is free to the extent that no other entity actually interferes with that person's activity – Pettit's neorepublican position does away with the requirement of actual interference, focusing on eliminating the danger (or potential danger) of arbitrary interference from others. Rather than predicating freedom on ideas of self-mastery, autonomy, or a person's ability to act in accordance with their higher-order desires, an account of Berlin's positive liberty, neorepublican theory is more concerned with ensuring the ability of the people to self-govern, by reducing domination and arbitrary interference.' [16]

Om het onderscheid tussen de twee stromingen te duiden wordt vaak verwezen naar slavernij. Vanuit het uitgangspunt van vrijheid als 'non-interference' zal worden verwezen naar fysieke en mogelijke seksuele uitbuiting, geweld en in het algemeen de beperkingen die de slaaf heeft in het uitoefenen van zijn autonomie. Stel echter dat de slavenhouder zijn macht niet gebruikt om de slaven te onderdrukken – de slaven zijn helemaal vrij om te doen en te laten wat ze willen. Wat is dan het probleem? Volgens het republicanisme is deze relatie alsnog problematisch. Ten eerste omdat de machtsrelatie absoluut is en ten tweede omdat er geen waarborgen gelden tegen willekeurig machtsgebruik – de slavenhouder kan op elk moment besluiten om zijn macht toch in te zetten, op elke wijze die hem goeddunkt. Het gaat er dus niet om of de macht wordt gebruikt, maar of de macht *kan* worden gebruikt, en de manier waarop die kan worden ingezet, namelijk *willekeurig,* al naar gelang de grillen van de machthebber.[17]
Als deze theorie wordt toegepast op hedendaagse privacyvraagstukken, dan is de kernvraag niet of er een concrete inbreuk is geweest op een subjectief recht van een individueel persoon, maar of bepaalde macht en bevoegdheden überhaupt moeten worden toegekend aan overheidsdiensten, welke waarborgen er gelden in relatie tot rechterlijke en parlementaire controle en welke garanties er zijn tegen arbitraire machtsinzet.[18] Het republicanisme legt dan ook grote nadruk op de 'rule of law', rechtstatelijke grondbeginselen, ongeacht of er sprake is van individuele schade. [19] Interessant is dat het EHRM bereid lijkt om de nadruk op inbreuken en individuele schade te laten varen en in zaken die draaien om massasurveillance een republikeinse benadering te omarmen. Daarvan kunnen drie voorbeelden worden gegeven.
Ten eerste heeft het Hof al eerder gesteld dat een concrete 'inbreuk' niet alleen moet zijn gestoeld op een wettelijke

grondslag, maar dat ook de ‘quality of the law’ moet zijn gewaarborgd.

‘Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.’ [20]

Ten tweede heeft het EHRM recentelijk aangenomen dat in zaken die draaien om massasurveillance, de vraag naar een concrete inbreuk en individuele schaden kan worden losgelaten.

‘[W]here the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto,* is justified.’ [21]

Niet alleen is hiermee een opening geboden om het slachtoffer-criterium te laten vallen, ook betekent het dat rechtspersonen, zoals burgerrechtenorganisaties ontvankelijk kunnen worden verklaard in zaken die niet zozeer draaien om een individueel, als wel een maatschappelijk belang, gerelateerd aan rechtstatelijke vraagstukken, en dat de ‘quality of the law’ als zodanig kan worden besproken en beoordeeld. [22] Dit sluit aan bij het derde en laatste punt, namelijk dat het EHRM zich steeds meer als constitutionele rechter opstelt, naar voorbeeld van constitutionele hoven in Frankrijk en Duitsland. Het EHRM gebruikt voor dit soort abstracte toetsen van wetgeving dan ook een variant op het woord ‘constitutionaliteit’, namelijk ‘conventionaliteit’. [23] Daarbij toetste het Hof of een nationale wet als zodanig, los van een concrete klacht van een specifiek person, aan de vereisten van rechtmatigheid en rechtsstatelijkheid voldoet.[24] Het is in dit soort zaken zelfs bereid om zaken te behandelen, nog voordat een nationale rechter een oordeel heeft kunnen vellen, juist omdat een kernaspect is of er wel voldoende rechterlijke controle bestaat op nationaal niveau.
Als de Nederlandse Wiv aan het EHRM zal worden voorgelegd, zal dus primair worden bekeken of er voldoende waarborgen zijn getroffen tegen het mogelijk misbruik van macht en potentiële willekeur. Het is niet ondenkbaar dat het Hof juist op deze punten zal oordelen dat de Nederlandse overheid geen afdoende maatregelen heeft getroffen.[25] Met de republikeinse privacybenadering in het achterhoofd en met een verwijzing naar de recente jurisprudentie van het EHRM kan het argument van de overheid in ieder geval niet zijn dat de privacy van burgers niet onredelijk wordt getroffen of dat veiligheid het privacybelang van burgers overstijgt. Privacyschendingen staan in dit soort zaken helemaal niet centraal. Het gaat primair om de vraag of er überhaupt grote en wijde bevoegdheden moeten worden toegekend aan overheidsdiensten, of de middelen überhaupt effectief zijn voor de doelen die worden nagestreefd, of er voldoende waarborgen zijn tegen arbitraire inzet van macht en of er voldoende parlementaire en rechterlijke controle is.

Voetnoten

[1]
Mr. drs. B. van der Sloot is senior onderzoeker aan Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

[2]
Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017).

[3]
Kamerstukken II 2016/17, 34588, 3, p. 100.

[4]
https://nos.nl/artikel/2197088-aftapwet-referendum-op-komst-300-000-handtekeningen-verzameld.html.

[5]
www.privacyfirst.nl/rechtszaken-1/item/1069-concept-dagvaarding-tegen-sleepnetwet-wiv.html.

[6]
https://decorrespondent.nl/7054/vier-redenen-waarom-de-nieuwe-aftapwet-een-slecht-idee-is/216952824-74addb25.

[7]
Het uitgangspunt dat degene die gegevens verzamelt moet aantonen dat dat nuttig en noodzakelijk is, is ook vervat in de Algemene Verordening Gegevensbescherming. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

[8]
https://www.rekenkamer.nl/publicaties/rapporten/2017/10/11/tussenstand-investeringsagenda-belastingdienst.

[9]
https://www.nporadio1.nl/argos/onderwerpen/433715-boeven-vangen-met-algoritmes.

[10]
B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York/Londen:W.W. Norton & Company 2015.

[11]
https://www.360magazine.nl/politiek/6172/longread-op-zondag-een-interview-met-edward-snowden. B. van der Sloot, 'De NSA affaire en de grenzen van de macht', *Filosofie & Praktijk*, 2014-2, p. 49-66.

[12]
EHRM 14 juli 1988, 12763/87 (*Lawlor/Verenigd Koninkrijk*).

[13]
ECRM 4 december 1995, 28204/95 (*Tauira e.a./Frankrijk*).

[14]
EHRM 29 juni 1999, 29121/95 (*Asselbourg en 78 anderen en Greenpeace Association-Luxembourg/Luxemburg*).

[15]
Zijn standaardwerk wat dit betreft is: P. Pettit, *Republicanism: A Theory of Freedom and Government*, Oxford: Clarendon Press 1997.

[16]
B. C. Newell, 'The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe', *I/S a journal of law and policy for the information society* 2014, afl. 2, p. 514-515.

[17]
https://plato.stanford.edu/entries/republicanism/.

[18]
B. C. Newell, 'Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control', *Government Information Quarterly* 2014.

[19]
A. Roberts, 'A republican account of the value of privacy', *European Journal of Political Theory* 2015, vol. 14(3).

[20]
EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*).

[21]
EHRM 4 december 2015, 47143/06, par. 171 (*Roman Zakharov/Rusland*).

[22]
B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities', in: S. Gutwirth, R. Leenes & P. De Hert (red.), *Data Protection on the Move*, Dordrecht: Springer 2016, p. 411-436.

[23]
Zie o.a.: EHRM 11 januari 2005, 66289/01 (*Py/Frankrijk*). EHRM 8 juli 2008, 8917/05 (*Kart/Turkije*). EHRM 17 maart 2009, 37387/05 (*Duda/Frankrijk*). EHRM 13 December 2011, 15297/09 (*Kanagaratnam e.a./België*). EHRM 8 januari 2013, 59677/09 en 1453/10 (*M.N. en F.Z./Frankrijk en Griekenland*).

[24]
Zie verder: EHRM 18 mei 2010, 26839/05 (*Kennedy/Verenigd Koninkrijk*). EHRM 23 juli 2013, 42337/12 (*Suso Musa/ Malta*). EHRM 22 oktober 2009, 17885/04 (*Orchowski/Polen*). EHRM 1 juli 2014, 43835/11 (*S.A.S./Frankrijk*). EHRM 14 januari 2016, 21381/11 (*Duong/Tsjechië*). EHRM 14 januari 2016, 52028/13 (*Maslak en Michalkova/Tsjechië*). EHRM 7 november 2013, 29381/09 en 32684 (*Vallianatos e.a./Griekenland*).

[25]
N. van Eijk, 'Betere waarborgen voor de werkwijze van inlichtingendiensten', *Ars Aequi* juni 2016. https://mensen rechten.nl/publicaties/detail/37322.