

Thema Privacy en nepnieuws

Een nieuwe benadering van het recht op privacy

Hoe het Europees Hof voor de Rechten van de Mens het republicanisme omarmde

Bart van der Sloot

Het recht op privacy komt door een aantal technologische ontwikkelingen steeds meer onder druk te staan. Een voorbeeld is het onderscheid tussen de privé sfeer en de publieke sfeer. Alhoewel dit onderscheid nooit absoluut is geweest, kon globaal een onderscheid worden gemaakt tussen het huis van een persoon, waar het grootste deel van het privéleven plaatsvindt, en de openbare ruimte, waar het publieke en openbare leven zich voltrekt. Beide sferen worden in toenemende mate hybride. In het huis worden steeds meer objecten geplaatst die in constante verbinding staan met het internet en die bestuurd en gecontroleerd kunnen worden van buiten af. Voorbeelden zijn de slimme meter, de slimme koelkast en de slimme televisie. De vraag is wat dit betekent voor het klassieke idee van de bescherming van de woning: vallen deze objecten daar ook onder en zo ja, heeft de eigenaar van de woning dan ook de verantwoordelijkheid voor handelingen die via deze objecten worden verricht, bijvoorbeeld als ze via het internet worden geïnfecteerd en als onderdeel van een botnet worden gebruikt voor onrechtmatige acties?¹

Andersom wordt ook de publieke sfeer steeds meer hybride. Privéhandelingen en privéobjecten zijn steeds vaker in deze ruimte gesitueerd. Een voorbeeld kan zijn de mobiele telefoon, iPad of laptop. Hierop staat een groot deel van het privéleven van mensen en deze apparaten worden meegenomen en benut juist in

1 R. van den Hoven van Genderen, "Privacy and Data Protection in the Age of AI and Robotics", *European Data Protection Law Review* 2017, 3.

de publieke ruimte.² Waarom, zo vragen enkelen zich af, geldt er een flink aantal wettelijke waarborgen tegen politie binnentreden van de woning en niet voor het binnentreden van een smartphone, terwijl voor veel mensen dit als een grotere aantasting van het privéleven voelt?³

1. Data, persoonsgegevens of gegevens

Als voorbeeld van hoe technologische ontwikkelingen het recht op privacy bevragen kan ook worden gewezen op de grootschalige verzameling van persoonsgegevens door zaken als ‘mass-surveillance’, ‘Big Data’ en artificiële intelligentie. Daarom wordt er steeds meer voor gepleit om het recht op persoonsgegevens te verzelfstandigen. In feite gaan veel digitale technologieën om het verzamelen van gegevens over personen en hun gedragingen, los van de bescherming van de woning, privécommunicatie of het lichaam (aspecten die traditioneel onderdeel vormen van het recht op privacy). De gegevens worden vervolgens gebruikt voor data-gedreven toepassingen, zoals ‘predictive policing’, ‘online advertising’ en ‘learning analytics’. Niet alleen zou, naar voorbeeld van het Handvest van de Grondrechten van de Europese Unie,⁴ het recht op bescherming van persoonsgegevens moeten worden losgekoppeld van het recht op privacy, ook zou de vraag moeten worden gesteld of ‘persoonsgegeven’ nog wel een houdbaar begrip is in de digitale context. Aangezien er in toenemende mate ook gebruik kan worden gemaakt van gewone gegevens, die niet direct zijn gekoppeld aan personen, om beslissingen te nemen die een grote impact kunnen hebben op de maatschappij en personen en aangezien de vraag of data aan personen relateren steeds moeilijker eenduidig te beantwoorden is, wordt er steeds meer voor gepleit om simpelweg ‘gegevens’ te reguleren.⁵

Dit zijn meer specifieke vraagstukken die de technologische ontwikkelingen oproepen. Er is echter ook een bredere en meer fundamentele vraag die steeds urgenter wordt. Bij grondrechtenbescherming wordt nu primair gekeken naar de vraag of er een onrechtmatige inmenging van een derde is geweest.⁶ Door

2 Zie aangaande dit vraagstuk ook: Supreme Court *Riley v. California*, 573 U.S. (2014).

3 Een goed voorbeeld is Bert-Jaap Koops die een Vici beurs heeft ontvangen om hier onderzoek naar te doen: <<https://www.tilburguniversity.edu/nl/thema/veiligheid/audio-video/koops-over-huisrecht-en-ict/>>.

4 Handvest van de Grondrechten van de Europese Unie, 2000/C 364/01. <http://www.europarl.europa.eu/charter/pdf/text_nl.pdf>.

5 B. van der Sloot & S. van Schendel, “International and comparative legal study on Big Data”, WRR-rapport, working paper 20, 2016.

6 Zo wordt privacy vaak beschreven als “the right to be let alone”. S. D. Warren & L. D. Brandeis, “The Right to Privacy”, *Harvard Law Review* 4 (1890) 5.

technologische ontwikkelingen wordt het echter steeds moeilijker hard te maken dat en hoe bepaalde data-gedreven toepassingen ingrijpen op aspecten van het recht op privacy. Welke schade er ten aanzien van specifieke individuen is ontstaan of hoe data-gestuurde processen bepaalde belangen hebben ondermijnd is steeds moeilijker te duiden. Daarom heeft een aantal wetenschappers, zoals Bryce Newell en Andy Roberts, gepleit voor een fundamenteel andere benadering van grondrechten in het algemeen en het recht op privacy in het bijzonder. Zij pleiten voor een republikeinse benadering, waarin niet zozeer wordt gekeken naar de concrete impact van al dan niet inbreukmakende activiteiten op het individu, zijn rechten en zijn belangen, maar waarin de machtsverhouding tussen het individu en de ander (de staat, bedrijven of andere burgers) centraal staat. Interessant is dat het Europees Hof voor de Rechten van de Mens (EHRM), in recente jurisprudentie ten aanzien van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM),⁷ waarin het recht op privacy is vervat, deze filosofie reeds gedeeltelijk lijkt te omarmen, terwijl het aanvankelijk juist een sterke nadruk legde op het non-interference principe. Deze omwenteling kan mogelijke gevolgen hebben voor een aantal Nederlandse wetten.

Dit artikel bespreekt het recht op privacy, de technologische ontwikkeling en de leidende jurisprudentie van het EHRM. Paragraaf 2 geeft kort weer hoe het recht op privacy doorgaans wordt benaderd. Paragraaf 3 bespreekt welke spanningsvelden ontstaan door de nieuwe data-gedreven toepassingen, waarin concrete inbreuken en daaruit voortvloeiende schade moeilijk aan te tonen zijn. Paragraaf 4 geeft aan dat een aantal auteurs, gezien deze problematiek, er voor heeft gepleit om een andere benadering van privacy te kiezen, waarbij de nadruk primair ligt op het 'non-domination' principe. Paragraaf 5 bespreekt een deel van de jurisprudentie van het EHRM waarin het hof deze republikeinse benadering reeds lijkt te omarmen. Tot slot bespreekt paragraaf 6 kort welke mogelijke gevolgen dit kan hebben voor de grondrechtenbescherming in het algemeen en de legitimiteit van Nederlandse wetgeving in het bijzonder.

2. Het recht op privacy

Het recht op privacy wordt in Nederlands beschermd door een aantal in de Grondwet vervatte grondrechten, de Wet bescherming persoonsgegevens⁸ en het Europees Verdrag voor de Rechten van de Mens. Omdat Nederland geen

7 <http://www.echr.coe.int/Documents/Convention_NLD.pdf>.

8 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

toetsing van wetten in formele zin aan de grondwet kent⁹ is met name die laatste bron bepalend voor de bescherming van privacy. Artikel 8 uit dat Verdrag bepaalt: “1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.” Zowel de Hoge Raad in de Nederlandse context als het EHRM in de Europese context benaderen het recht op privacy als een primair individueel recht dat bescherming biedt aan primair individuele belangen. Daarbij wordt met name gekeken naar de vraag of er een al dan niet onrechtmatige inbreuk is geweest op dit recht. Dit zal kort worden toegelicht met een verwijzing naar de jurisprudentie van het EHRM.

Het Hof stelt dat in principe alleen natuurlijke personen een klacht kunnen indienen aangaande het recht op privacy. In het algemeen komen interstatelijke klachten, waarbij bijvoorbeeld Nederland een klacht indient tegen Oostenrijk over een schending van één of meer rechten onder het Verdrag, nauwelijks voor.¹⁰ Ook heeft het EHRM geoordeeld dat groepen geen klacht mogen indienen over een schending van één van de rechten uit het verdrag.¹¹ Ten aanzien van rechtspersonen is het EHRM juist bij het recht op privacy aarzelend om hun klachten en zaken in behandeling te nemen.¹² In tegenstelling tot andere rechten, zoals de vrijheid van meningsuiting en de vrijheid van religie waar het Hof wel bereid is om naar de klachten van rechtspersonen te kijken, kunnen rechtspersonen in principe geen beroep doen op artikel 8 EVRM. Rechtspersonen hebben geen privéleven, zo stelt het Hof. “[T]he extent to which a non-governmental organization can invoke such a right must be determined in the light of the specific nature of this right. It is true that under Article 9 of the Convention a church is capable of possessing and exercising the right to freedom of religion in its own capacity as a representative of its members and the entire functioning of churches depends on respect for this right. However, unlike Article 9, Article 8 of the Convention has more an individual than a collective character (...).”¹³

9 Artikel 120 GW.

10 Artikel 33 EVRM.

11 Wel mogen individuen die allen kunnen aantonen door dezelfde inbreuk te zijn geraakt hun klachten bundelen.

12 B. van der Sloot, “Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system”, *Computer Law & Security Review* 2015, 1.

13 ECmHR, *Church of Scientology of Paris v. France*, application no. 19509/92, 09 January 1995.

Dat betekent dat in de praktijk vrijwel alleen natuurlijke personen een klacht kunnen indienen over een mogelijke schending van artikel 8 EVRM. Daarbij komt dat het Hof vereist dat deze personen concrete en daadwerkelijke schade hebben ondervonden van een concrete en specifieke inbreuk. Kan dat niet worden aangetoond, dan worden hun klachten niet-ontvankelijk verklaard. Zogenaemde *in abstracto* klachten, die gaan over een wet of beleid als zodanig, zonder dat de eisers beweren daar zelf hinder van te hebben ondervonden, worden in principe niet-ontvankelijk verklaard. “Insofar as the applicant complains in general of the legislative situation, the Commission recalls that it must confine itself to an examination of the concrete case before it and may not review the aforesaid law *in abstracto*. The Commission therefore may only examine the applicant’s complaints insofar as the system of which he complains has been applied against him.”¹⁴ Ook zogenaemde *a-priori* klachten, waarin een zaak wordt aangebracht nog voordat de privacy-inbreuk zich heeft voltrokken, worden in principe niet-ontvankelijk verklaard. “It can be observed from the terms ‘victim’ and ‘violation’ and from the philosophy underlying the obligation to exhaust domestic remedies provided for in Article 26 that in the system for the protection of human rights conceived by the authors of the Convention, the exercise of the right of individual petition cannot be used to prevent a potential violation of the Convention: in theory, the organs designated by Article 19 to ensure the observance of the engagements undertaken by the Contracting Parties in the Convention cannot examine - or, if applicable, find - a violation other than *a posteriori*, once that violation has occurred. Similarly, the award of just satisfaction, i.e. compensation, under Article 50 of the Convention is limited to cases in which the internal law allows only partial reparation to be made, not for the violation itself, but for the consequences of the decision or measure in question which has been held to breach the obligations laid down in the Convention.”¹⁵

In principe worden zaken derhalve alleen ontvankelijk verklaard als er concrete en daadwerkelijke schade aan het individu is toegebracht door een concrete en specifieke inbreuk door de staat. Dat betekent ook dat hypothetische klachten, over een inbreuk waarvan de klager niet zeker weet of die zich heeft voorgedaan, niet-ontvankelijk worden verklaard, en dat het EHRM geen zaken in behandeling neemt waarin de klagers niet opkomen voor hun eigen belang, maar voor de belangen van anderen of de samenleving in haar geheel. Ook deze zogenaemde algemeen belangacties of groepsvorderingen, *class actions* of *actio popularis*, worden in principe niet-ontvankelijk verklaard.¹⁶

14 ECtHR, *Lawlor v. The United Kingdom*, application no. 12763/87, 14 July 1988.

15 ECmHR, *Taura and others v. France*, application no. 28204/95, 04 December 1995.

16 ECtHR, *Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxembourg*, application no. 29121/95, 29 June 1999.

3. Data-gedreven technologieën

Het recht op privacy is dus primair gekoppeld aan het individu, zijn rechten en belangen. De vraag of dit recht is ondermijnd wordt primair beoordeeld aan de hand van de vraag of er een inbreuk is gemaakt op dit recht. Dit is wat in de literatuur het ‘non-interference’ principe wordt genoemd. Het gaat dan om een concrete en daadwerkelijke inbreuk en concrete en daadwerkelijke schade voor het individu die daaruit voortvloeit. De oorsprong van dit uitgangspunt is te herleiden tot Mill’s beroemde essay *On Liberty*¹⁷ en het daarin besproken schade-beginsel. “Non-Interference formalises some of the fundamental insights of the Harm Principle, namely the idea that society should not interfere with individual choices whenever the latter have no (harmful) effect on others. Mill insists that the reasons for the change in circumstances of the individual (such as neglect, irresponsibility, effort or luck) are not relevant information for social judgements, provided that nobody else is negatively affected.”¹⁸ Een schending van de rechten of belangen van een individu wordt in deze filosofie slechts geconstateerd als daar een concrete inbreuk op is geweest, met concrete schade tot gevolg.

Dit uitgangspunt werkt betrekkelijk goed voor traditionele privacyvraagstukken. Alhoewel het altijd lastig is om schade te materialiseren en te kwantificeren – welke schade volgt uit het binnentreden van een woning als er geen eigendommen worden meegenomen en geen informatie over de inrichting van de woning aan derden wordt doorgegeven? – is het doorgaans relatief eenvoudig om een inbreuk te constateren. De meeste privacy-schendingen 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. Deze zijn nauwelijks in tijd, ruimte en persoon af te bakenen en vormen een structureel en voortdurend onderdeel van de handelingen en gedragingen van overheidsdiensten, bedrijven of burgers. Als voorbeeld kan dienen de talloze camera’s die op vrijwel elke straathoek van grote steden zijn te vinden. Bij dit soort toepassingen wordt het individu incidenteel geraakt – de camera’s filmen niet een specifieke persoon of een specifieke groep mensen. Ze filmen iedereen, overal en altijd die zich binnen het bereik van de camera’s bevinden. Hoe kan een individu in zo’n geval hard maken dat hij specifiek, individueel en concreet is geraakt – welke inbreuk is er geweest en op welk recht?

17 J. S. Mill, *On Liberty and Other Writings*, Cambridge: Cambridge University Press, 1989.

18 M. Mariottiy & R. Veneziani, “The Liberal Ethics of Non-Interference and the Pareto Principle”, <<https://www.st-andrews.ac.uk/~wwwecon/repecfiles/4/1404-ori.pdf>>.

Daarbij komt een praktisch probleem. Het toekennen van individuele rechten aan burgers veronderstelt dat zij primair verantwoordelijk zijn voor de bescherming van hun rechten. Zoals besproken mogen andere burgers of burgerrechtenorganisaties in principe niet opkomen namens de belangen van burgers die dat zelf niet doen. Zulke algemeen belangacties worden niet-ontvankelijk verklaard door het Europees Hof voor de Rechten van de Mens. De moeilijkheid voor individuen om hun rechten te claimen ten aanzien van grote gegevensverzamelingsprocessen is tweërlei. Enerzijds is de burger zich vaak niet bewust van het simpele feit dat er gegevens over hem worden verzameld. Burgers maken foto's en filmpjes van anderen op straat of tijdens feestjes en posten die op Facebook, zonder daarvan alle mensen op de hoogte te brengen, laat staan om toestemming te vragen. Bedrijven verzamelen via het internet grote hoeveelheden data met gebruikmaking van cookies, device-fingerprinting, en zelfs zijn er computerprogramma's die aan de hand van hoe iemand typt op zijn computer met redelijke zekerheid kunnen vaststellen wie het betreft. Overheidsdiensten verzamelen ook grote hoeveelheden data over burgers, zoals middels hittedsensoren, geheime tap-activiteiten door inlichtingendiensten en het opkopen of opeisen van data van bedrijven. Hiervan wordt de burger doorgaans niet op de hoogte gesteld. Als burgers niet weten dat hun gegevens worden verzameld, dan zullen zij doorgaans ook geen beroep doen op hun recht op privacy. Anderzijds zijn er steeds meer gegevensstromen waarin de data van een burger kunnen zijn vervat. Het is voor een burger vrijwel ondoenlijk om bij al deze datastromen na te gaan of zijn gegevens daarin zijn betrokken, wie de gegevens verzamelt, of dit rechtmatig gebeurt en zo niet, om de stap naar de rechter te zetten. Vrijwel alles is tegenwoordig immers data-gedreven.

Meer fundamenteel is het probleem dat zelfs als de burger zich wel bewust zou zijn van alle datastromen waarin zijn persoonsgegevens zijn vervat en zelfs als hij wel de tijd en de energie heeft om bij elk dataverwerkingsproces na te gaan of dit rechtmatig gebeurt en als dat niet zo is, om naar de rechter te stappen, dan nog zal het voor hem lastig zijn om aan te tonen welke inbreuk er is geweest op zijn recht. Middels nieuwe data-gedreven technologieën worden grote hoeveelheden data verzameld over de samenleving als geheel. Door middel van slimme algoritmes worden statistische correlaties ontdekt. Daaruit worden groepsprofielen gedestilleerd die worden gebruikt voor algemene beleidsbeslissingen. Bij dit soort Big Data processen is het individuele belang moeilijk te duiden en is ook moeilijk aan te tonen waar precies een inbreuk op een recht uit bestaat.¹⁹ Welke concrete schade heeft de gegevensverzameling door de National Security Agency

19 Deze problematiek is uitgebreid besproken in onder meer het rapport van de Wetenschappelijke Raad voor Regeringsbeleid. <http://www.echr.coe.int/NR/rdonlyres/E58E405A-71CF-4863-91EE-779C34FD18B2/0/APERCU_19592011_EN.pdf>.

(NSA) bijvoorbeeld berokkend aan de belangen van een gewone Amerikaanse of Europese burger? Waarom is het erg dat Google weet dat van de hoger opgeleide mannen tussen de 30 en 40 woonachtig in Amsterdam 70% geïnteresseerd is in vrijkaartjes voor het concertgebouw? Hoe groter de dataverwerkingsprocessen en hoe algemener de verzamelde gegevens, des te moeilijker zal het zijn voor een individu om zijn belang concreet te maken.

De problematiek die bij dit soort nieuwe data-gedreven technologieën centraal staat is niet zozeer de concrete inbreuk, maar de machtsverhouding die ontstaat. Door de grote hoeveelheden data hebben bedrijven en overheidsdiensten een enorme kennis over het gedrag van burgers en de samenleving in haar geheel; die kennis kunnen zij bijvoorbeeld inzetten om het gedrag van burgers te sturen. Zelfs als zij deze macht niet inzetten of slechts ten goede van de burgers, dan nog is de machtsverhouding een feit. Dit is de eerste problematiek die los staat van de vraag of er een concrete inbreuk is.

De tweede problematiek is het gebrek aan waarborgen tegen de inzet van deze macht. Veel instanties die aan grootschalige gegevensverzameling doen zijn aan minimale restricties gebonden wat betreft de inzet van hun macht. Een goed voorbeeld zijn de inlichtingendiensten, zoals in Nederland de Algemene Inlichtingen en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen en Veiligheidsdienst (MIVD), die zijn uitgezonderd van veel wettelijke en procedurele waarborgen en ten aanzien waarvan vrij minimale juridische en parlementaire controle kan worden uitgeoefend.²⁰ Het enkele feit dat een persoon of organisatie macht heeft en het enkele feit dat deze macht vrij willekeurig kan worden ingezet brengt met zich mee dat burgers zich in hun vrijheid aangetast kunnen voelen en hun gedrag al bij voorbaat beperken uit angst voor mogelijke onbekende gevolgen.²¹

4. Republicanisme

Omdat de problematiek die speelt rond veel moderne data-technologieën slechts gedeeltelijk gaat om concrete inbreuken en meer en meer om machtsverhoudingen als zodanig wordt in de literatuur in toenemende mate betwijfeld of het liberale 'non-interference' principe nog relevant is in deze context. Steeds meer wordt verwezen naar het zogenoemde 'non-domination' principe, zoals dat wordt om-

20 Zie ook de discussie over de herziening van de Wet op de Inlichtingen- en Veiligheidsdiensten, waarover in de laatste paragraaf meer.

21 Dit wordt ook wel het chilling effect genoemd.

armd in het republicanisme en het werk van onder meer Philip Pettit.²² Hij stelt dat liberalen traditioneel vrijheid formuleren in termen van ‘non-interference’, of dat nu als een primair formele vrijheid wordt gezien, zoals de meeste rechtse liberalen doen, of als een vrijheid die ook actieve staatsbemoeienis veronderstelt, zoals de meeste linkse liberalen doen. De kern is het gevrijwaard zijn van inmengingen van derden ten aanzien van rechten en vrijheden. Het kan dan bijvoorbeeld gaan om een verbod op een demonstratie, het terugroepen van een bepaalde publicatie of het binnentreden van iemands zijn woning. Het republicanisme legt niet de nadruk op ‘non-interference’, maar op ‘non-domination’. Het gaat dan niet zozeer om concrete inbreuken op rechten of vrijheden, maar om machtsrelaties als zodanig. “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.”²³

Pettit beschrijft het in zijn boek *Republicanism* als volgt: “[...] advancing someone’s freedom as non-domination is likely to help them escape from uncertainty, strategy, and subordination; certainly, it is more likely to do this than advancing their freedom as non-interference. But something stronger also holds true. Suppose we take steps to reduce a person’s uncertainty about interference, to reduce their need for exercising a strategy of deference and anticipation with others, and to reduce the subordination associated with vulnerability. It is hard to see how we could take such steps without at the same time advancing their freedom as non-domination. Freedom as non-domination appears to be, not just a more or less sufficient instrument for promoting those effects, but a more or less necessarily associated factor. There is no promoting non-domination without promoting those effects; and there is no promoting those effects without promoting non-domination. This may not hold in every possible world, but it certainly seems to hold under plausible assumptions about how the actual world works.”²⁴

Een bekend voorbeeld om het onderscheid tussen vrijheid als non-interference en vrijheid als non-domination te illustreren is slavernij. Zowel liberalen

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

23 B. C. Newell, “The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe”, 10 *ISJLP* 481, 522, p. 514-515.

24 Pettit, p. 90.

als republikeinen zullen uiteraard slavernij verwerpen. Als vrijheid hier wordt gezocht in de vrijheid van inmenging, dan kan worden gewezen op de uitbuiting die plaatsvindt in dit soort machtsrelaties, de eventuele seksuele exploitatie, de povere leefomstandigheden en het fysiek geweld. Ook kan worden gewezen op het gebrek aan keuzevrijheid en autonomie van de slaven; slavenhouders bepalen uiteindelijk of wat een slaaf wil ook mag. Het republicanisme zal zich eerder richten op de machtsrelatie als zodanig. Deze relatie is problematisch om twee redenen. Ten eerste omdat de machtsrelatie absoluut is en ten tweede omdat er geen waarborgen gelden tegen willekeurig machtsgebruik. Een kernvraag die hierbij wordt opgeworpen is: stel de slavenhouder gebruikt zijn macht niet om de slaven te onderdrukken – de slaven zijn helemaal vrij om te doen en te laten wat ze willen en de slavenhouder gebruikt zijn macht niet om de slaven op enigerlei wijze te onderdrukken. Wat is dan het probleem vanuit de theorie van vrijheid als non-interference? Er heeft in zo'n geval helemaal geen concrete inbreuk plaats. Vanuit een republikeins idee is deze situatie nog steeds problematisch omdat een slavenhouder zijn macht *kan* inzetten. Het gaat dus niet alleen om het daadwerkelijke gebruik van macht, maar juist ook om de mogelijkheid daarvan. Daarbij komt dat er in deze relatie geen waarborgen zijn. De slavenhouder kan zijn macht op elk moment inzetten, op elke wijze die hem zint. De slaaf weet dus nooit of en wanneer er macht over hem wordt uitgeoefend, waardoor hij altijd in onzekerheid leeft en in deze zin nooit vrij is.

Er is evenwel flink wat kritiek gekomen op de gelijkschakeling door Pettit en andere republikeinen van het liberalisme en het non-interference principe. Zo benadrukken veel liberale filosofen zeker ook dat onrechtvaardige machtsstructuren een probleem zijn en moeten worden tegengegaan. Een voor de hand liggend voorbeeld is Rawls.²⁵ Het liberalisme impliceert volgens velen ook een machtscheiding en een bestuursrechtelijk verbod van misbruik van macht; in een liberale constitutie is een *recht* van een slavenhouder op een slaaf ondenkbaar, ook als de slavenhouder er in de praktijk van zou afzien van dat recht gebruik te maken. Pettit heeft deze kritiek ter harte genomen. Beter dan het liberalisme en het republicanisme tegenover elkaar te stellen is het dan ook om het non-interference en het non-domination principe tegenover elkaar te stellen, alhoewel ook bij dat scherpe contrast kanttekening zijn te plaatsen.²⁶ Vrijheid als non-domination gaat in op de machtsverhouding en de waarborgen tegen machtsmisbruik als zodanig.

Dergelijke vraagstukken spelen ook in de relatie tussen burger en overheid. Ook hierbij kijkt het republicanisme niet zozeer naar de vraag of de overheid daadwerkelijk haar macht gebruikt en of dit tot een inbreuk heeft geleid, maar naar de vraag hoe groot de macht van de overheid is en of er voldoende waar-

25 J. Rawls, *A Theory of Justice*. Cambridge: Harvard University Press, 1971.

26 <<https://plato.stanford.edu/entries/republicanism/>>.

borgen zijn neergelegd om willekeurig machtsgebruik tegen te gaan. Arbitrair, in deze zin, kan zowel een formele als een materiele kant hebben. “The first defines it procedurally. Power is arbitrary, on this view, to the extent that it is not reliably constrained by effective rules, procedures, or goals that are common knowledge to all persons or groups concerned. To be reliably effective, on this view, constraints must be resilient over a wide range of possible changes or modifications in the relevant circumstances. Roughly speaking, the procedural view equates republican freedom with the traditional idea of the rule of law, provided we are willing to extend the latter idea considerably. Alternatively, we might define arbitrariness substantively: power is arbitrary, on this second view, when it fails to track the ‘welfare and world-view’ of those affected.”²⁷

In deze laatste, materiele zin, is machtsgebruik arbitrair als bevoegdheden worden toegepast zonder rekening te houden met de situatie waarin of de personen waarop deze macht wordt uitgeoefend.²⁸ In negatieve zin legt het republicanisme dus nadruk op de vrijheid van machtsrelaties waarin macht willekeurig kan worden uitgeoefend. In deze zin benadrukken republikeinen de klassieke beginselen van de rechtstaat als zodanig, los van de vraag of er een inbreuk is geweest op een concreet recht van een individu.²⁹ In positieve zin leggen republikeinen de nadruk op de mogelijkheid van burgers om invloed uit te oefenen op de wet- en regelgeving die op henzelf van toepassing is. “Republican rights are not to be understood as pre-political norms – rights that establish the framework within which political decision making takes place. Rather, they are the product of political decision-making processes – processes in which citizens are expected to actively participate.”³⁰

Beide kanten van de republikeinse vrijheid komen onder druk te staan in moderne data-gedreven toepassingen, zonder dat er noodzakelijkerwijs een inbreuk is geweest op het recht op privacy. Burgers hebben niet of nauwelijks invloed op het doen en laten van de grote technologiegiganten als Google, Facebook en Apple. Ook overheidsdiensten die aan grote dataverzamelingen doen, zoals inlichtingendiensten en speciale eenheden van de politie, zijn vaak maar aan beperkte democratische controle onderhevig. Daarnaast bouwen deze instanties grote databases op en vergaren daarmee kennis en dus macht, terwijl de waarborgen tegen arbitraire machtsinzet minimaal is (de procedurele kant van arbitraire machtsinzet) en deze data-technologieën juist worden toegepast op

27 <<https://plato.stanford.edu/entries/republicanism/>>.

28 P. Pettit, *Republicanism: A Theory of Freedom and Government*, Oxford: Clarendon Press, 1997, p. 107.

29 F. Lovett & P. Pettit, “Neorepublicanism: A normative and institutional research Program”, *Annual Review of Political Science* 12, 2009.

30 A. Roberts, “A republican account of the value of privacy”, *European Journal of Political Theory* 14 (2015) 3, p. 337.

een context-blinde wijze (de materiele kant van arbitraire machtsinzet). De NSA verzamelde simpelweg alle gegevens waar het haar hand op kon leggen, camera's op straathoeken filmen iedereen die passeert, Google verzamelt gegevens over iedereen die zich op het web bevindt. Omdat het non-interference principe minder geschikt is voor dit soort vraagstukken stellen steeds meer privacywetenschappers voor om bij dit soort data-gedreven toepassingen ook of met name te kijken naar het republikeinse model van non-domination. “[It] provides valuable insights into how one-sided surveillance powers and control of information vested in states can limit individual freedom. Applying neorepublican political theory in this context represents an important and novel application of these valuable ideas with the capacity to inform future information policy research and the development of better laws and policies related to surveillance, secrecy, and access to information.”³¹

5. Het EHRM als republikeins Hof?

Interessant is dat juist het Europees Hof voor de Rechten van de Mens ontvankelijk lijkt voor dergelijke problematiek. Zoals beschreven in paragraaf 2 heeft dit Hof juist het non-interference principe tot standaard verheven, in die zin dat het vereist dat een klager moet kunnen aantonen expliciet en daadwerkelijke slachtoffer te zijn geweest van een concrete inbreuk. Zaken over een wet of beleid als zodanig, algemeen belangacties en andere zaken die niet direct om individuele schade gaan, worden in principe niet-ontvankelijk verklaard door het EHRM. Steeds meer wordt het Hof echter geconfronteerd met zaken waarin deze schade niet eenduidig is vast te stellen, terwijl er wel evidente knelpunten worden aangekaart. Hierbij gaat het met name om lidstaten die in toenemende mate bevoegdheden toekennen aan politie- en inlichtingendiensten om gegevens te verzamelen over grote groepen individuen en waarbij de macht van deze diensten aan vrij minimale democratische en rechtelijke controle is onderworpen.

Alhoewel het vaak moeilijk is voor individuen om te expliciteren of en zo ja welke inbreuk er heeft plaatsgehad, is het Europees Hof voor de Rechten van de Mens steeds meer bereid om dergelijke klachten ontvankelijk te verklaren. Het ontstijgt daarbij het specifiek individuele belang van de klager in een concrete zaak en kijkt naar klassieke rechtstatelijke principes, naar de controle op machtsuitoefening en waarborgen tegen de arbitraire inzet van macht. Daarbij zijn met name drie punten van belang.

31 B. C. Newell, “Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control”, *Government Information Quarterly* 3, 2014.

Ten eerste is er de zogenoemde drie-stappen toets. Als is vast komen te staan dat het recht op privacy in een bepaalde zaak in het geding was en dat de klagers schade hebben ondervonden van een inbreuk op een recht dan wordt de zaak ontvankelijk verklaard. Dan is onder de systematiek van het Europees Verdrag voor de Rechten van de Mens de tweede vraag of de geconstateerde inbreuk ook onrechtmatig was. Als een beperking (1) is voorgeschreven bij wet, (2) een legitiem doel dient en (3) noodzakelijk is in een democratische rechtstaat, dan is de inperking legitiem en is er geen schending van artikel 8 EVRM. Bij dit eerste criterium gaat het traditioneel om de vraag of de geconstateerde inbreuk op een wettelijke basis stoelt en of aan de in de wet vervatte voorwaarden is voldaan. Zo kan er in de nationale wet als voorwaarde voor het binnentreden van een woning door de politie zijn vereist dat er een huiszoekingsbevel is afgegeven door de rechter-commissaris. Als de politie vervolgens het huis van een burger binnentreedt zonder zo'n huiszoekingsbevel, dan is de inperking op het recht op privacy niet voorgeschreven bij wet en dus onrechtmatig. Gekoppeld aan het criterium van een wettelijke basis is het vereiste dat de wet duidelijk moet zijn, openbaar moet worden gemaakt en dat de gevolgen daarvan voorzienbaar moeten zijn voor burgers.³²

In de loop der tijd heeft het Europees Hof voor de Rechten van de Mens een andere voorwaarde gekoppeld aan het criterium van een wettelijke grondslag, namelijk de 'kwaliteit van de wet'. Interessant is dat het Hof hier juist ingaat op het bestaan van waarborgen tegen arbitraire machtsinzet. Zo heeft het onder meer geoordeeld: "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."³³ De nadruk ligt hier dus op rechtstatelijke aspecten en de rule of law, het al dan niet toekennen van 'unfettered power' aan overheidsinstanties en het bestaan van waarborgen tegen 'arbitrary interference'. Dit 'quality of law' criterium brengt met zich mee dat een wet (1) helder moet beschrijven welke bevoegdheden er worden toegekend, (2) onder welke voorwaarden deze kunnen worden ingezet, (3) welke parlementaire en rechterlijke controle er geldt voor de inzet van deze bevoegdheden en (4) welke middelen de burger toekomt om eventueel machtsmisbruik te voorkomen.

32 <http://ysu.am/files/Davit_Melkonyan-1415702096-.pdf>.

33 ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, 02 Augustus 1984.

Ten tweede is in december 2015 een andere belangrijk omslagpunt geweest in de jurisprudentie van het EHRM. Om toe te komen aan de vraag of de kwaliteit van de wet is gewaarborgd in een specifiek geval, moet het Hof de zaak in ieder geval ontvankelijk hebben verklaard. Zoals gezegd is hiervoor vereist dat er een inbreuk en concrete schade kan worden aangetoond. Zo genoemde *in abstracto* klachten, over de wet of beleid als zodanig worden niet-ontvankelijk verklaard, zo bleek uit paragraaf 2. Uit de lijn van het EHRM zou derhalve moeten volgen dat de klachten ten aanzien van deze nieuwe data-technologieën vaak niet-ontvankelijk zouden moeten worden verklaard, omdat individuele schade en concrete inbreuken vaak lastig zijn aan te tonen. Dat zou betekenen dat overheden die met grootschalige gegevensverzameling en -analyse aan de slag gaan niet onderworpen zouden zijn aan het toezicht van het Europees Hof voor de Rechten van de Mens. Het Hof erkent deze problematiek en heeft daarom het vereiste van schade en het ‘non-interference’ principe laten vallen.³⁴ Dit bleek voor het eerst uit de zaak Zakharov tegen Rusland, aangaande mass-surveillance, uit december 2015.³⁵

“ [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.”³⁶

Niet alleen is hiermee een opening geboden om het slachtoffer-criterium te laten vallen in dit type zaken, ook betekent het dat rechtspersonen, zoals burgerrechtenorganisaties, ontvankelijk kunnen worden verklaard – het gaat in dit soort zaken immers niet om het persoonlijk belang van de klager. Ook kunnen in dit soort zaken maatschappelijke, in plaats van individuele belangen worden meegenomen, namelijk gerelateerd aan rechtstatelijke principes en de machtsrelaties als zodanig. Tot slot mogen er ook *class actions* of groepsvorderingen worden ingediend. In een klein aantal zaken – waar de inbreuk en de daaruit volgende schade niet goed vast te stellen is – is het EHRM dus bereid om alle

34 ECtHR, Szabó and Vissy v. Hungary, application no. 37138/14, 12 January 2016.

35 ECtHR, Roman Zakharov v. Russia, application no. 47143/06, 04 December 2015.

36 Zakharov, § 171.

door hemzelf geformuleerde principes ten aanzien van ontvankelijkheidsvraagstukken over boord te zetten.³⁷

Dit sluit aan bij het derde en laatste punt, namelijk dat het Europees Hof voor de Rechten van de Mens zich steeds meer als een constitutionele rechter opstelt, in plaats van als klassiek mensenrechtenhof. In landen als Duitsland en Frankrijk is de hoogste rechter reeds bevoegd parlementaire wetten en nationaal beleid te toetsen op rechtstatelijke principes als zodanig, los van eventuele individuele klachten of belangen. De toetsing van wetten op ‘constitutionaliteit’ draait om dezelfde aspecten die in de jurisprudentie van het EHRM naar voren komen, namelijk begrenzingsen aan de macht, voorwaarden voor het inzetten van bevoegdheden, controle op de inzet van de macht en de algemene toets op noodzakelijkheid en proportionaliteit van de wet.³⁸

Het EHRM gebruik voor dit soort abstracte toetsen dan ook een variant op het woord ‘constitutionaliteit’, namelijk ‘conventionaliteit’.³⁹ “The abstract review of ‘conventionality’ is the review of the compatibility of a national law with the Convention independently of a specific case where this law has been applied.”⁴⁰ Daarbij is het van belang dat zaken normaal alleen ontvankelijk worden verklaard onder het Europees Verdrag voor de Rechten van de Mens als eerst alle nationale rechtsmiddelen zijn uitgeput (de klager is naar de nationale rechter gestapt, heeft hoger beroep aangekend en is vervolgens naar de Hoge Raad gegaan). Zelfs als dit is gebeurd dan nog zal het EHRM niet optreden als hof in vierde instantie – het zal niet de hele zaak opnieuw in behandeling nemen, maar zal slechts een minimale mensenrechtentoets verrichten. Opmerkelijk is dat ook dit principe overboord wordt gezet in zaken waar het EHRM optreedt als constitutionele rechter – het is dan juist bereid om zaken in eerste instantie te behandelen, dus nog voordat een nationale rechter naar de zaak heeft gekeken. “In other words, the Grand Chamber

37 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 (eds.), *Data Protection on the Move*, Dordrecht: Springer, 2016, pp. 411-436.

38 Michaud, § 73. See also: ECtHR, *Vassiss and others v. France*, application no. 62736/09, 27 June 2013.

39 See for the use of the word also: ECtHR, *Py v. France*, application no. 66289/01, 11 January 2005. ECtHR, *Kart v. Turkey*, application no. 8917/05, 08 July 2008. ECtHR, *Duda v. France*, application no. 37387/05, 17 March 2009. ECtHR, *Kanagaratnam and others v. Belgium*, application no. 15297/09, 13 December 2011. ECtHR, *M.N. and F.Z. v. France and Greece*, application nos. 59677/09 and 1453/10, 08 January 2013.

40 ECtHR, *Vallianatos and others v. Greece*, application nos. 29381/09 and 32684, 07 November 2013.

invests itself with the power to examine *in abstracto* the Convention compliance of laws without any prior national judicial review.”⁴¹

Deze drie stappen zijn niet direct te begrijpen als wordt gekeken naar vrijheid als non-interference. Er is in dit soort zaken immers geen concrete inbreuk op de vrijheid van een persoon, noch is er sprake van concrete schade of nadeel dat daaruit voortvloeit voor de klagende partij. Als vrijheid wordt begrepen als non-domination dan volgen de keuzen van het Europees Hof voor de Rechten van de Mens wel logischerwijs, waarmee uiteraard niet is gezegd dat het Hof inderdaad doelbewust het republicanisme omarmt. Waar het Hof in dit soort zaken naar kijkt is of de wet en het nationale rechtstelsel als zodanige voldoende waarborgen bieden tegen misbruik van bevoegdheden en de arbitraire inzet van macht, nog los van de vraag of dit in concrete gevallen is misgegaan of niet. Het simpele feit dat er geen begrenzingen en kaders zijn waarbinnen overheidsorganen hun macht moeten gebruiken en het simpele feit dat er nauwelijks rechterlijke en parlementaire controle is op dit gebruik is voor het EHRM voldoende om een inbreuk van artikel 8 van het Europees Verdrag van de Mens te constateren.

6. Gevolgen voor de Nederlandse rechtspraak

Uit paragraaf 2 bleek dat het huidige recht op privacy primair wordt gekoppeld aan het individu, zijn rechten en zijn belangen. Een rechtszaak wordt onder het Europees Verdrag voor de Rechten van de Mens slechts ontvankelijk verklaard als de klager duidelijk kan maken dat er een concrete inbreuk is geweest op zijn recht op privacy. Paragraaf 3 beschreef dat het bij moderne data-technologieën steeds moeilijker wordt om concrete inbreuken vast te stellen en daaruit voortvloeiende schade aan te tonen. Dit maakt het steeds moeilijker om in zaken die draaien om grootschalige dataverwerking aan het uitgangspunt van ‘non-interference’ vast te houden. Paragraaf 4 gaf aan dat steeds meer privacy-wetenschappers pleiten voor een andere benadering van privacy, namelijk een republikeinse benadering, waar niet het ‘non-interference’, maar het ‘non-domination’ principe centraal staat. Hierbij gaat het primair om de vraag of er een machtsrelatie is, hoe groot de macht is en of er procedurele en materiele waarborgen zijn die arbitraire machtsinzet tegengaan. Paragraaf 5 gaf aan dat het Europees Hof voor de Rechten van de Mens reeds op een aantal punten lijkt op te schuiven naar een dergelijke benadering. Het laat in zaken die draaien om mass-surveillance van inlichtingendiensten het slachtoffercriterium los en kijkt in plaats daarvan naar

41 ECHR, *Vallianatos and others v. Greece*, application nos. 29381/09 and 32684, 07 November 2013.

de kwaliteit van wetten en oordeelt als een Europees constitutioneel hof over de rechtsstatelijkheid van nationale wetten.

Door deze benadering kiest het Europees Hof voor de Rechten van de Mens in feite voor het beste van twee werelden. Het behoudt in zaken die draaien om meer traditionele privacy-schendingen, zoals het binnentreden van een woning of een lichaam of het aftappen van een telefoongesprek, het non-interference principe. Dit betekent dat het klachtrecht in dit soort gevallen beperkt is tot de personen die ook daadwerkelijk en direct zijn getroffen door de inbreuk, en niet openstaat voor bijvoorbeeld de buurman van degene wiens woning is binnengetreten. Dit heeft als mogelijk voordeel dat het aantal klachten beperkt blijft en er geen abstracte vragen en problemen worden voorgelegd aan het Hof door personen die hebben gehoord van een mogelijke schending van artikel 8 van het Europees Verdrag van de Mens. Tegelijkertijd kiest het EHRM in zaken die draaien om nieuwe data-gedreven technologieën, zoals mass-surveillance door inlichtingendiensten, voor het loslaten van het non-interference beginsel ten faveure van het non-domination beginsel. Zou het dat niet hebben gedaan, dan zou dat hebben betekend dat veel van deze zaken niet-ontvankelijk zouden worden verklaard, omdat het vaak moeilijk is om individuele en concrete schade aan te tonen. Wat dat betreft zou de keuze van het Europees Hof voor de Rechten van de Mens dus kunnen worden toegejuicht, omdat het meer en betere rechtsbescherming biedt en een halt toeroept aan overheden die ongecontroleerde macht toekennen aan overheidsinstanties.

Toch kunnen er ook kanttekeningen bij deze ontwikkeling worden geplaatst, bijvoorbeeld ten aanzien van de vergaande mogelijkheid die het Hof zichzelf toekent (zonder democratische legitimatie) om een abstracte toetsing van nationale wetten en beleid op rechtsstatelijkheid en 'conventionaliteit' te voltrekken. Het toetst deze wetten niet eens als Hof in vierde instantie, maar is onder omstandigheden bereid dat te doen als Hof in eerste instantie. Een klager kan dan dus direct wetten aan het Europees Hof voor de Rechten van de Mens voorleggen, zonder eerst de nationale rechtsmiddelen te hebben uitgeput. Dit zet druk op artikel 120 van de Nederlandse Grondwet, waarin is vervat: "De rechter treedt niet in de beoordeling van de grondwettigheid van wetten en verdragen." De principiële keuze om in Nederland niet de rechter, maar het parlement te laten oordelen over de interpretatie van de grondwet en de rechtmatigheid van wetten wordt door de nieuwe benadering van het EHRM betekenisloos. Opmerkelijk is dat het EHRM zichzelf hiermee een bevoegdheid toekent die niet in het Verdrag zelf is neergelegd. De democratische legitimatie voor deze bevoegdheid ontbreekt dus, wat zich op zichzelf misschien weer slecht verhoudt tot het idee van rechtsstatelijkheid dat het Hof met het concept van 'conventionaliteit' juist placht te beschermen.

Naast dit meer fundamentele punt kan de omslag van het EHRM ook belangrijke gevolgen hebben voor de rechtspraak in Nederland. Om te beginnen kan het betekenen dat er in Nederland meer mogelijkheden moeten komen voor burgers en burgerrechtenorganisaties om in het kader van privacy- en gegevensbescherming algemeen-belangacties in te dienen. Artikel 305a van boek 3 van het Burgerlijk Wetboek biedt nu reeds een kleine opening. “Een stichting of vereniging met volledige rechtsbevoegdheid kan een rechtsvordering instellen die strekt tot bescherming van gelijksoortige belangen van andere personen, voor zover zij deze belangen ingevolge haar statuten behartigt.” Toch blijkt dat dit artikel in privacy-zaken nauwelijks kan worden ingeroepen, onder meer omdat een stichting of vereniging vaak zelf geen direct belang heeft bij de klacht. Dat bleek onder meer toen stichting Privacy First een klacht indiende over de verplichting om een vingerafdruk af te staan ten behoeve van het verkrijgen van een paspoort.⁴² Daarento oordeelde de Hoge Raad: “Onderdeel 1.1 keert zich tegen het oordeel van het hof dat Privacy First ontvankelijk is haar vorderingen, nu zij in deze procedure opkomt voor het algemeen belang van bescherming van het recht op privacy van personen met de Nederlandse nationaliteit. Het onderdeel voert aan dat het te dezen geen verschil maakt of Privacy First optreedt ter bescherming van de gebundelde belangen van individuele personen of ter bescherming van het door het hof genoemde algemene belang. In beide gevallen geldt dat de betrokken individuen de gewraakte maatregelen aan de orde kunnen stellen bij de bestuursrechter, en dat Privacy First daarom niet-ontvankelijk is in haar vorderingen.”⁴³ Als de jurisprudentie van het Europees Hof voor de Rechten van de Mens wordt gevolgd zal er meer opening moeten komen voor individuen en rechtspersonen om zowel op te komen voor de gebundelde belangen van anderen als, met name, het algemeen belang.⁴⁴

Ten tweede kan deze benadering belangrijke gevolgen hebben voor het zogenoemde access-use debat dat ook in Nederland steeds meer woedt. Het huidige gegevensbeschermingsrecht, zoals in Nederland is vervat in de Wet bescherming persoonsgegevens, stelt met name beperkingen aan het verzamelen van gegevens over burgers. De nieuwe Algemene Verordening Gegevensbescherming van

42 Rijkswet van 26 september 1991, houdende het stellen van regelen betreffende de verstrekking van reisdocumenten.

43 R.o. 3.3.1 Hoge Raad, zaaknummer 14/02737, 22 mei 2015.

44 Dit debat is reeds aangewakkerd naar aanleiding van de Uitvoeringswet gegevensbescherming (<https://www.internetconsultatie.nl/uitvoeringswetavg/details>), waarin uitvoering wordt gegeven aan 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 (algemene verordening gegevensbescherming). Daarin is in artikel 80 reeds een opening geboden voor dergelijke acties.

de EU, die in mei 2018 in werking zal treden, behoudt deze nadruk en kent hoge boetes voor schendingen van deze regels. Steeds meer wordt de vraag opgeworpen of dit nog wel houdbaar is. Nieuwe datatechnologieën, zo wordt gesteld, maken het mogelijk om grote hoeveelheden data te verzamelen en te analyseren. De regels staan deze nieuwe toepassingen en data-gedreven innovatie in de weg, zo is het argument. Het verzamelen van gegevens zou moeten worden vrijgegeven en er zouden slechts beperkingen moeten gelden voor het gebruik van de gegevens. Niet alleen de belemmering van de technologische ontwikkelingen is hiervoor een argument, ook speelt de vraag waarom het eigenlijk erg is om persoonsgegevens te verzamelen. Is het niet zo dat alleen bij het eventuele gebruik van data problematische gevolgen kunnen ontstaan voor het individu?⁴⁵ Daarom is er steeds meer druk om alleen het gebruik van gegevens in te kaderen en het verzamelen van gegevens los te laten. Door de nieuwe benadering van het Hof wordt echter duidelijk dat het niet slechts gaat om schade of de gevolgen voor het individu – in dit soort zaken gaat het met name om macht en het gevaar van machtsmisbruik. Juist dat staat op het spel door instanties die toegang hebben tot grote hoeveelheden data over burgers – zij verkrijgen hierdoor kennis van en derhalve macht over het gedrag van burgers. Uit de keuze van het EHRM blijkt dat het niet geoorloofd zal zijn om slechts op de gebruikskant van dataprocessen te reguleren, maar dat altijd ook het verzamelen van gegevens centraal zal staan.

Ten derde en tot slot blijkt uit de jurisprudentie van het Europees Hof voor de Rechten van de Mens dat wetten afdoende waarborgen moeten bevatten tegen machtsmisbruik. Dit betekent onder meer dat er helder in een wet moet zijn neergelegd wanneer bepaalde macht kan worden ingezet, onder welke voorwaarden en welk toezicht er plaats heeft. Juist op deze punten is vaak kritiek, meest recent bijvoorbeeld ten aanzien van de herziening van de Wet op de Inlichtingen- en Veiligheidsdiensten.⁴⁶ Daarin is de mogelijkheid neergelegd voor zogenoemde bulk interceptie op de kabel, die zich nu juist kenmerkt door de arbitraire inzet van macht. Ook wordt er door velen op gewezen dat er nauwelijks parlementaire en rechterlijke controle plaatsheeft op de inzet van de bevoegdheden. Zo schreef professor Van Eijk over de bestaande situatie: “De enige vorm van onafhankelijk toezicht in de Wiv is de CTIVD, die alleen achteraf kan oordelen over het handelen van de activiteiten van de inlichtingendiensten. De CTIVD beschikt niet over handhavingsinstrumenten. Dit toezichtstelsel van de Wiv is onvoldoende, zoals de jurisprudentie bevestigt.”⁴⁷ Terwijl de bevoegdheden van de Algemene

45 Zie over dit debat uitgebreid: B. van der Sloot & D. Broeders & E. Schrijvers (eds.), *Exploring the boundaries of Big Data*, Amsterdam: Amsterdam University Press, 2016.

46 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).

47 N. van Eijk, “Betere waarborgen voor de werkwijze van inlichtingendiensten”, *Ars Aequi* juni 2016.

Inlichtingen- en Veiligheidsdienst (AIVD) enorm worden vergroot, wordt het toezicht slechts in zeer beperkte mate versterkt in de wet, zo menen critici.⁴⁸ Het is dan ook sterk de vraag of deze nieuwe wet stand zal houden als zij ter toetsing aan het Europees Hof voor de Rechten van de Mens zou worden voorgelegd.⁴⁹

Bart van der Sloot is senior Researcher, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Netherlands.

48 <<https://mensenrechten.nl/publicaties/detail/37322>>.

49 Er zijn al plannen in die richting, zie o.a. <<https://www.bof.nl/dossiers/sleepnet/>>.