WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Aan de leden van de vaste commissie voor Justitie en Veiligheid

ons kenmerk 2018/CP/tr	**telefoonnummer** 070 356 4691	
onderwerp Notitie rondetafelgesprek over de ICT van de politie 8 maart 2018 10.00 -12.45	**e-mail** prins@wrr.nl	**datum** 1 maart 2018

Geachte leden van de vaste commissie voor Justitie en Veiligheid,

Als voorzitter van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en tevens hoogleraar recht en informatisering verbonden aan Tilburg University dank ik u voor de gelegenheid om in uw vergadering vanuit de wetenschap iets te mogen zeggen over de ICT-voorzieningen van de nationale politie.

ICT-toepassingen – ik betrek in het onderstaande ook de bredere ontwikkeling van digitalisering - bieden vele kansen voor surveillance, opsporing en handhaving inclusief een meer (pro)actieve betrokkenheid van burgers. Ze faciliteren een voorheen ongekende gegevensuitwisseling tussen een veelheid aan organisaties in het nationale en internationale veiligheidsdomein. Ze stellen de politie in staat om gedetailleerde profielen van burgers en bedrijven te maken en aan de hand daarop handhavend op te treden. En ze geven de politie de mogelijkheid om misdaden snel en precies te reconstrueren. Ontwikkelingen op het gebied van Big Data stellen de politie zelfs steeds in staat om misdaad te 'voorspellen', dat wil zeggen, om van te voren te weten met welke waarschijnlijkheid bepaalde mensen op bepaalde plekken en op bepaalde momenten met een gerede kans de wet gaan overtreden.

Vanwege de alomtegenwoordige inzet van ICT en digitalisering door de overheid betoogde de WRR reeds in 2011 dat er een 'iOverheid' is ontstaan.[1] Kenmerkend voor deze 'iOverheid', aldus de WRR, is niet zozeer de inzet van ICT als zodanig, maar de vele informatiestromen binnen en tussen organisaties die ICT mogelijk heeft gemaakt. Daarmee is een vernetwerkte en wezenlijk andere overheid ontstaan.

[1] WRR, *iOverheid*, Amsterdam: Amsterdam University Press, 2011.

Buitenhof 34, Postbus 20004, 2500 EA Den Haag
telefoon (070) 356 46 00, website: www.wrr.nl, e-mail: info@wrr.nl

We zijn inmiddels zeven jaar verder, en niet alleen het gebruik van ICT door de overheid maar zeker ook de gegevensuitwisseling en het hergebruik van gegevens is alleen maar toegenomen. De politie vormt hierop geen uitzondering. Sterker nog, de politieorganisatie is in de afgelopen jaren misschien wel meer gedigitaliseerd en afhankelijk geworden van informatiestromen dan enig andere overheidsorganisatie. Daarbij wordt intensief gebruik gemaakt van andere partijen. Illustratief is de mededeling (in 2016) van de politie, het ministerie van J&V en de particuliere veiligheidsbranche dat 90% van alle door de politie benutte informatie verkregen via *sensing* (allerhande sensoren zoals camera's, etc.) afkomstig is van private partijen.[2]
Het lijkt mij daarom wel treffend om, naar analogie van de term 'iOverheid', te spreken van het ontstaan van een 'iPolitie'.

Zoals de iOverheid vergaande veranderingen in de relatie tussen burgers en overheden met zich meebrengt, geldt dat evenzeer voor de relatie tussen burgers en de politieorganisatie. De belangrijkste verandering is dat burgers, organisaties en bedrijven bij een goede benutting van digitalisering te maken krijgen met een slagvaardigere, efficiëntere en effectievere politie. Dit kan tot meer veiligheid leiden, of althans tot behoud van het huidige veiligheidsniveau. Digitalisering stelt de politie in staat om bepaalde vormen van criminaliteit effectiever aan te pakken, al dan niet met de inzet van burgers die via sociale media de digitale ogen en oren van de politie zijn. Daarnaast maakt ICT het voor de politie mogelijk om in de digitaliseringswetloop met criminelen een serieus te nemen partij te blijven. Illustratief in dit verband zijn de opsporingsactiviteiten op het zgn. *dark web*. Bepaalde vormen van criminaliteit - en dan met name digitale criminaliteit of criminaliteit waarbij de digitale wereld faciliterend is - kunnen en zullen kortom niet door de politie worden bestreden als de politie niet ook zelf over hoogtechnologische middelen en kennis beschikt en deze middelen blijft ontwikkelen.
Tegelijkertijd brengt het ontstaan van de iPolitie risico's voor burgers met zich mee. Te denken valt hier aan de 'welbekende' risico's op het gebied van privacy, discriminatie en de vrije meningsuiting. Maar ook de democratische controle op de activiteiten van de politie staat potentieel onder druk. In het rapport 'Big Data in een vrije en veilige samenleving' liet de WRR zien dat we niet ver af staan van semiautomatische en geheel automatische besluitvorming, waarbij de uitkomsten van data-analyses sturend zijn voor het handelen van veiligheidsorganisaties zoals de politie.[3] Ik vermeld verder dat er in rechtstatelijke zin nauwelijks een visie is op de opsporing in de digitale wereld, meer in het bijzonder het *dark web* en de hier zo noodzakelijke controle door de zittende magistratuur. Ten slotte noodzaakt onze rechtsstaat tot het doordenken van de rol en ruimte die de politie aan burgers (de samenleving) geeft om de helpende hand te bieden bij de klassieke opsporingstaken van de politie. Waar liggen hier de grenzen?
Wat moet de wetgever met deze inzichten?
ICT biedt ongekende mogelijkheden voor de politie. Maar het digitaliseren van de politieorganisatie mag geen technologische vanzelfsprekendheid zijn. De ICT-uitdagingen worden nog te vaak bezien en beoordeeld vanuit de technologie - de ICT – in plaats van het oogmerk dat in essentie onderliggend is aan de inzet van ICT, namelijk het vergaren, uitwisselen en benutten van **data** - digitalisering.

---

[2] https://www.politie.nl/nieuws/2016/november/10/samenwerking-sensing-voor-veiliger-nederland.html

[3] WRR, *Big Data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press, 2016.

Vaak ook, is er onvoldoende besef dat de inzet van digitalisering en het benutten van de nieuwe digitale wereld door de politie, naast meer slagkracht, ook potentieel verliezen voor de rechtsstaat kan opleveren. Het doordenken en ontwikkelen van de iPolitie vraagt daarom om een systeem van *checks and balances* (mogelijkerwijs ook in digitale vorm) dat in staat is om te gaan met de voortschrijdende digitalisering van de politieorganisatie. Relevant daarbij is wat mij betreft ook het volgende. Politiek en wetgever hanteren met een zeker gemak grote woorden als 'technologie-onafhankelijke en techniek-neutrale wetgeving' en 'wat offline geldt dient ook online te gelden'. Alsof er één eenduidige offline dan wel online wereld bestaat. Alsof er van technologie te abstraheren valt. Maar de inzet van technologie is nooit neutraal. Het verandert onze wereld. Ook de organisatie, rol en positie van de politie. En daarmee verandert de positie van burgers en andere actoren in onze samenleving ten opzichte van de politie. Bovendien: over welke 'offline' wereld hebben we het eigenlijk? De wereld van de politie die in vele opzichten niet zonder het digitale 'wapen' kan? Of de wereld van de rechtsbescherming die nog onvoldoende het digitale been heeft bijgetrokken?[4]
Wil dat been worden bijgetrokken dan zal de wetgever zich - parallel aan de ontwikkeling van de iPolitie - niet alleen moeten richten op instrumentele beginselen zoals veiligheid, efficiency en effectiviteit, maar ook op de rechtsstatelijke tegenwichten van deze beginselen. In het rapport over Big Data dat ik eerder noemde, liet de WRR zien dat de inzet van slimme digitaliseringstoepassingen, met name in het veiligheidsdomein, zonder externe toetsing en controle (door toezichthouder en rechterlijke macht) omwille van diverse fundamentele belangen onverantwoord is.[5] Ook adviseerde de WRR in het kader van Big Data om geautomatiseerde besluitvorming in het veiligheidsdomein achterwege te laten, gegevensverwerking door veiligheidsorganisaties transparanter te maken en om de positie van burgerrechtenorganisaties in juridische procedures te versterken. Meer in het algemeen heb ik eerder al bepleit dat de uitvoerende macht – waaronder de iPolitie - alleen effectief door andere overheidsmachten, zoals de rechter en het parlement, gecontroleerd kan worden als ook deze machten door de wetgever in staat worden gesteld om technologische kansen te benutten.[6] En cruciaal bij dit alles is dat zowel de politie als de wetgever handelen vanuit het besef dat de hedendaagse politie in belangrijke mate een iPolitie is. Om de overgang naar deze nieuwe positie en identiteit vorm en inhoud te geven zal er daarom aandacht moeten zijn voor een aantal noodzakelijke inhoudelijke en institutionele stappen.[7]

De gelijktijdige ontwikkeling en invulling van rechtsstatelijke uitgangspunten in relatie tot de iPolitie is overigens niet alleen een principiële, constitutionele opdracht van de wetgever. Ook in pragmatische zin is er uiteindelijk geen tegenstelling tussen veiligheid en vrijheid, omdat burgers het gebruik van nieuwe ICT en digitalisering alleen zullen accepteren als hun fundamentele rechten en vrijheden daarbij ook gewaarborgd blijven.

---

[4] Zie hierover ook: J.E.J. Prins, 'Bestuursrecht & digitalisering', *Nederlands Juristenblad*, 93 (8) 539. Beschikbaar via: http://www.njb.nl/highlights/bestuursrecht-digitalisering.28127.lynkx

[5] Zie ook: WRR, *Toezien op publieke belangen*, Amsterdam: Amsterdam University Press, 2013.

[6] [6] J.E.J. Prins, 'Digitale (dis)balans binnen de TRIAS', *Nederlands Juristenblad*, 91 (14) 909. Beschikbaar via http://www.njb.nl/njv-jaarvergaderingen/jaarvergadering-2016/artikelen/digitale-(dis)balans-binnen-de-trias.19490.lynkx

[7] Zie voor een aantal voorstellen: WRR, *iOverheid*, Amsterdam: Amsterdam University Press, 2011.

Bovendien zorgen rechtsstatelijke *checks and balances* ervoor dat de politieorganisatie, alvorens zij digitalisering inzet, wordt gedwongen om met andere machten binnen de overheid te delibereren en om, ná het gebruik van digitale middelen, verantwoording af te leggen. Deliberatie en verantwoording zijn essentiële elementen van een gedegen en inclusief veiligheidsbeleid waarbij deskundigen en belanghebbende voldoende invloed en correctiemogelijkheden hebben. Recent legden een aantal internationale auteurs een verband tussen het ontbreken van rechtsstatelijke elementen in het veiligheidsbeleid en zogenaamde 'policy disasters' op dit gebied.[8]

Kortom, het gebruik van ICT-toepassingen en breder digitalisering door de nationale politie biedt vele mogelijkheden, maar kan uitsluitend vruchten afwerpen als de politie in voldoende mate wordt geëquipeerd met iPolitie-kennis en -kunde, op zowel technologisch als rechtsstatelijk vlak en de wetgever de huidige wet- en regelgeving versterkt om fundamentele rechten, deliberatie, rechterlijke toetsing en democratische verantwoording te waarborgen. De WRR is zeker bereid om, mede op basis van eerdere adviezen, daarover met u het nadere gesprek aan te gaan. In ieder geval dank ik u nu voor de mogelijkheid die mij op dit moment daartoe al is geboden.

Hoogachtend,

Prof. mr. Corien Prins
Voorzitter WRR

[8] Zie voor voorbeelden in de Amerikaanse literatuur R. Passchier, 'Als Commander in Chief kan President Trump straks bijna alles', *Nederlands Juristenblad* 2017(1), p. 13.