Politiewerk is … werken in een digitale samenleving

Prof. dr. Wouter Stol is lector Cybersafety aan NHL Stenden Hogeschool en de Politieacademie. Hij is daarnaast bijzonder hoogleraar Politiestudies aan de Open Universiteit.

De politie moet zich sneller aanpassen aan de digitalisering van de samenleving. Waarom gaat dat zo moeizaam? Er is nog steeds een gebrek aan kennis – over digitalisering, cybercrime, gedigitaliseerde criminaliteit, daders van cybercrime, slachtofferschap, cyberspace, opsporing in een digitale omgeving, bevoegdheden, mogelijkheden en nog zo wat. Nog steeds wordt het probleem te veel gezien als iets voor specialisten. Nog steeds is de focus ten onrechte gericht op 'cybercrime'. Ik pleit voor een andere focus.

'*Wat politie en justitie momenteel nog wel het meeste parten speelt is een gebrek aan kennis.*' Zo luidde een conclusie uit het onderzoek *Criminaliteit in cyberspace* bijna twintig jaar geleden (Stol, Van Treeck & Van der Ven, 1999, p, 172). In 2004 was de situatie bij de politie niet beter (Stol, 2004). Acht jaar daarna viel er iets meer te melden: *'Het totaalbeeld dat oprijst anno 2012 is dat van een politie die nog flink wat heeft in te halen op de samenleving die haar omringt, niet zozeer omdat er geen actie wordt ondernomen, maar wel omdat de acties nog pril zijn en te veel het karakter hebben van pionierswerk van enkelen (…). 'Digitaal' is ten onrechte nog geen normaal en integraal onderdeel van de politieorganisatie in de volle breedte.'*(Stol, Leukfeldt & Klap, 2012, p. 37).

Politie en digitale samenleving

De samenleving digitaliseert in rap tempo verder. Niemand bij de politie heeft de keus om daaraan wel of niet mee te doen. Je doet bijvoorbeeld je werk in een wijk – maar die wijk ligt in een digitale samenleving met overal digitale middelen. Er is geen sprake van een wijk én van het web, ze zijn één. Ze vormen samen de digitale samenleving waarin de politie werkt. De marktkoopman? Die is ook actief online, vermoedelijk zelfs tijdens de markt. Een forum voor radicaliserend jongeren? Diezelfde jongeren lopen ook op straat in de wijk en sturen vanaf hun hangplek nieuwe berichten.

Tien jaar na het eerstgenoemde onderzoek voerde ik samen met collega's wederom een verkenning uit naar digitale criminaliteit. De hoofdconclusie luidde dat digitale criminaliteit geen exclusief bezit is van high tech criminelen, maar een alledaags verschijnsel is geworden. Dus moet digitale criminaliteit ook van iedere politiemedewerker zijn. Een aanbeveling luidde derhalve: *'zorg dat voldoende kennis over cybercrime politiebreed aanwezig is'* (Leukfeldt, Domenie & Stol, 2010, p. 266, nadruk toegevoegd).

In 2011 deed ik samen met collega's het eerste landelijke onderzoek naar slachtofferschap van digitale criminaliteit (N=9.163). De aanpak van digitale criminaliteit had wel politieke prioriteit, maar niemand wist hoe vaak mensen eigenlijk daarvan slachtoffer werden. De meest tot de verbeelding sprekende conclusie uit het onderzoek was *'dat Nederland inmiddels kan worden getypeerd als het land van fietsendiefstal (4,8%) en hacken (4,3%)'* (Domenie, Leukfeldt, Van Wilsem, Jansen & Stol, 2013, p. 92).

'De cijfers laten zien dat cybercrime qua prevalentie serieus aanwezig is in het dagelijks leven van burgers. Cybercrime heeft het karakter gekregen van veelvoorkomende criminaliteit, reguliere criminaliteit verweven met het dagelijks leven. Dit betekent dat kennis omtrent het opnemen van aangiften cybercrime en vervolgens aanpakken ervan, serieus aanwezig moet zijn in de volle breedte van de politieorganisatie. Dat is nog niet het geval.' (Ibidem, p.92).

Na 2011 heeft het CBS digitale criminaliteit opgenomen in haar jaarlijkse slachtofferonderzoek en kunnen we in de cijfers zien dat inmiddels in Nederland een groter percentage mensen slachtoffer wordt van hacken dan van fietsendiefstal (Stol & Strikwerda, 2017, p. 188).

» *Wat hacken betreft draagt de politie dus kennis van minder dan het topje van de ijsberg*

Foto: politie.nl

Van de cybercrimeslachtoffers in bovengenoemd onderzoek deed 15% melding bij de politie (Domenie e.a., 2013, p. 95). Het gemiddelde meldingspercentage voor offline delicten was toentertijd 35% (CBS, 2012). Voor hacken lag het meldingspercentage in 2011 op 4%. Wat hacken betreft draagt de politie dus kennis van minder dan het topje van de ijsberg. In een onderzoek naar slachtofferschap van digitale criminaliteit onder MKB-bedrijven vonden we dat 7% van de MKB's die slachtoffer waren geworden daarvan melding maakte bij de politie (Veenstra, Zuurveen & Stol, 2016, p. 95). Ook dat is minder dan het genoemde topje. Door het lage meldingspercentage raakt de digitalisering van criminaliteit de politie dus nog slechts in beperkte mate. Zo valt niet op dat de politie nog niet goed raad weet met het delict dat tegenwoordig het meeste voorkomt!

Hoe wordt de politie digitaal bij de tijd?

Behalve bij specialisten gaat 'digitaal' de politie nog steeds niet goed af. Dat is kwalijk, want zo mist de politie de aansluiting bij de samenleving. Wat is daar aan te doen?

De politie maakt zich de digitalisering niet vanzelf eigen, dus zijn beleidsmaatregelen nodig. Tot ongeveer 2014 was het beleid dat 'digitaal' géén specialisme is (met uitzonderling van het landelijke Team High Tech Crime voor zeer complexe zaken). De politie moet niet voor elke nieuwe criminele ontwikkeling een aparte organisatie inrichten, maar daarmee binnen de bestaande structuren leren omgaan. Met dit 'breedtebeleid' boekte de politie weinig vooruitgang. In 2014 bepaalde de minister daarom hoeveel cybercrimezaken de politie moest draaien.[1] Zij dreigde dat niet te halen en startte met cybercrimeteams (Stol & Strikwerda, 2017, p. 262). Dat leidde tot meer cybercrimezaken en was in die zin een succes.

Het instellen van cybercrimeteams is geen breedtebeleid. Ze gelden als tijdelijk en ze besteden aandacht aan het breder verspreiden van hun kennis en vaardigheden. De cybecrimeteams zijn binnen het breedtebeleid een tijdelijke stimuleringsmaatregel en geen beleidsbreuk. Op een ander punt lijkt wel sprake van een beleidswijziging.

Door in te zetten op het draaien van cybercrimezaken heeft de minister (en daarna de politie) in 2014 de focus gericht op cybercrime. De politie moet echter beter leren werken in een digitale omgeving en dat is een aanzienlijk bredere kwestie dan cybercrimezaken draaien. Digitaal is overal en om alle collega's dat duidelijk te maken kan de politie beter inzetten op het benutten van digitaal bij elk delict en elke taak. Dan kan (en moet) élke collega bijdragen aan het realiseren van het beleid. Nog steeds kunnen dan speciale teams een aanjaagfunctie hebben.

Niemand hoeft nieuw breedtebeleid af te wachten om digitale mogelijkheden te benutten. Er zijn bijvoorbeeld diverse handreikingen online, zoals 'Intake van delicten met een digitale component'.[2] Via intranet kunnen politiemensen ook beschikken over 'Herkennen en veiligstellen van digitale apparatuur' en 'Opsporing in een gedigitaliseerde samenleving.' Ook experts kunnen helpen, allereerst die van de zogenoemde digitale platforms. 'Zo'n digitaal platform bestaat uit mensen met meer dan gemiddelde digitale kennis en vaardigheden en dient binnen de regionale eenheid als extra verbinding tussen TDO en de politiemensen die bij hun zaak technische ondersteuning nodig hebben. Een digitaal platform verleent dus als het ware eerstelijns digitale ondersteuning...' (Stol & Strikwerda, 2017, p. 263). Komen zij er niet uit, dan kunnen zij andere experts inschakelen. Het beste is natuurlijk om te beginnen met jezelf te verdiepen in de materie, bijvoorbeeld met www.internetsporen.nl, een site met tips die bruikbaar zijn in elke zaak.

Hieronder bespreek ik nog drie onderwerpen die relevant zijn voor iedere collega die aan de slag wil met 'digitaal' in de brede zin van het woord.

Het darkweb is een deel van je wijk!

Voordeel van internet is dat het je toegang geeft tot allerlei politie-relevante informatie die voorheen moeilijk te verkrijgen was. Ook – en misschien wel juist – het zogenoemde darkweb hoort bij de voor iedere politiemedewerker relevante werkomgeving. Ook een wijkagent moet thuis zijn op het darkweb. Niet om een darkweb-zaak te draaien, maar wel omdat het de wereld is waarin een wijkagent werkt en de wereld waarin bijvoorbeeld de jongeren in de wijk ook thuis zijn. Een fictieve maar realistische casus:

> **Op een school heeft een leraar een groepje jongens bezig gezien met valse briefjes van twintig. De rector van de school belt de wijkagent, en dat ben jij. Hij nodigt je uit voor een gesprek op school met de leraar en de bewuste jongeren. Voordat je naar dat gesprek gaat moet je natuurlijk wel weten waar en hoe je tegenwoordig aan je valse briefjes van twintig komt anders lachen de jongeren je vierkant uit. Je kijkt dus met je Torbrowser even op het darkweb naar de mogelijkheden en de prijzen.**

Mijn stelling dat iedere politiemedewerker thuis moet zijn op het darkweb ontmoet in politieland nog steeds veel scepsis. Een teamchef vertelde me bijvoorbeeld dat het darkweb gevaarlijk is en dat wijkagenten daar dus niets te zoeken hebben. Een andere leidinggevende vond dat politiemensen al die informatie niet nodig hebben als ze dat niet direct gebruiken in een opsporingsonderzoek.

De opvatting dat de politie niet in een bepaalde omgeving moet komen omdat het daar gevaarlijk zou zijn, is natuurlijk te bizar voor woorden. Het tegendeel is waar. De politie hoort juist daar te zijn waar het gevaarlijk is. Het criminele milieu krijgt een lachkramp als zij hoort dat de politie niet in haar buurt durft te komen omdat zij dat gevaarlijk vindt.

Verder meen ik dat je als opsporingsambtenaar kennis moet hebben over criminaliteit en de laatste ontwikkelingen daarin. Je moet weten wat een gram wiet kost of een illegaal wapen, niet omdat je een drugs- of wapenzaak wil gaan draaien, maar omdat je dergelijke kennis nodig hebt als achtergrondinformatie bij allerlei werk. Vóór het internettijdperk was het lastig om dergelijke informatie te krijgen en bij te houden. Nu ligt het voor het oprapen. Maak er gebruik van: https://www.torproject.org/. Het downloaden en gebruiken van de Torbrowser is overigens legaal en niet per se gevaarlijker dan een andere browser.

De politie mag veel maar niet alles (dus ook niet online)

Omdat internet het zo gemakkelijk maakt om informatie te verzamelen, loop je precies op dat punt het risico dat je doorschiet en verder gaat dan je bevoegdheden toelaten. Online vind je veel informatie over personen in je werkgebied, maar je hebt niet de bevoegdheid om over iemand zomaar alle informatie te vergaren. De grens wordt bepaald door artikel 8 EVRM, dat het recht op eerbiediging van de persoonlijke levenssfeer regelt. Artikel 3 Pw geeft de politie ruimte tot het maken van een niet meer dan geringe inbreuk op iemands privacy (het zgn. Zwolsmancriterium). Gaat het om een verdergaande inbreuk, dan is een speciale bevoegdheid vereist. Bij informatievergaring op internet is dan speciaal te denken aan de bijzondere opsporingsbevoegdheid 'stelselmatige informatie inwinning', zoals geregeld in artikel 126j Sv (BOB-wetgeving).

Bij het googelen van een persoon is dus eerst de vraag wanneer daarmee de grens van 'een niet meer dan geringe inbreuk op de persoonlijke levenssfeer' is bereikt. Daarvoor is geen harde algemene regel. Het Openbaar Ministerie heeft een 'Leidraad bevoegdheden informatievergaring op internet' opgesteld. Deze is niet openbaar, maar in hun 'Handreiking opsporing in een gedigitaliseerde samenleving', waarin herhaaldelijk wordt verwezen naar genoemde leidraad, geven Veenstra, Zuurveen, Kerstens & Stol (2016) politiemensen de volgende richtlijn: '*Bij een herhaalde zoekslag (> 2 keer) die betrekking heeft op personen (hetzij verdachten, hetzij derden die niet worden ver-*

> *» Een teamchef: het darkweb is te gevaarlijk voor wijkagenten*

dacht), geldt dat overleg met de Officier van Justitie vereist is.' (2016, p. 27).

Vervolgens moet worden bepaald of artikel 3 Pw volstaat of dat 126j Sv aangewezen is. De politie beschikt over het hulpmiddel HUIB ('Half Uur Internet Bevraging'), dat beoogt om voor politiemensen het zoeken op internet te structureren. Het is een hulpmiddel dat gebruikt dient te worden binnen de bestaande juridische kaders. Het werken met HUIB verschaft je geen grond om meer te doen dan het Zwolsmancriterium toelaat.

In het kader van de modernisering van het Wetboek van Strafvordering, is een wijziging gepland in de wetgeving aangaande informatievergaring op internet. Nieuw is het voorgestelde artikel 2.8.2.4.1 over stelselmatige vastlegging van persoonsgegevens uit open bronnen. Dit luidt: *'In geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld, kan de officier van justitie bevelen dat een opsporingsambtenaar stelselmatig, met een technisch hulpmiddel, persoonsgegevens uit open bronnen vastlegt.'* Het voert te ver om deze nieuwe bevoegdheid te bespreken. Kortheidshalve verwijs ik daarom naar de dit jaar te verwachten publicatie van Stol en Strikwerda.

Over partners in rechtshandhaving

Rechtshandhaving in een gedigitaliseerde samenleving vraagt om nieuwe kennis en vaardigheden. Een deel daarvan dient iedere politiemedewerker zich eigen te maken, een deel daarvan behoort bij specialisten van de politie en dan zijn er nog specialistische kennis en vaardigheden die berusten bij private organisaties. De politie kan die kennis en vaardigheden bij haar werk betrekken door samenwerking of inkoop.[3]

Het belangrijkste aandachtspunt daarbij is dat politiewerk wordt gereguleerd door wettelijke waarborgen terwijl dat niet op gelijke wijze geldt voor private organisaties. Bij een publiek-private samenwerking (PPS) is het voor de politie dus zaak om na te gaan of zij de informatie die zij betrekt van een privaat bedrijf ook zelf had mogen vergaren als zij daartoe de kennis en middelen had gehad. Is dat laatste niet het geval, dan dient de vraag te worden gesteld of en zo ja in hoeverre de politie de betreffende informatie kan gebruiken.

Een bijzondere partner van de politie in rechtshand-having is de gemeente. Die spelen ten onrechte nog hoegenaamd geen rol in de bestrijding van digitale criminaliteit. Politie en gemeenten kunnen meer samen optrekken. Gemeenten kunnen bijvoorbeeld initiatieven nemen om in hun gemeente de weerbaarheid tegen digitale criminaliteit te vergroten en de samenwerking ter bestrijding van digitale criminaliteit te versterken door partijen bij elkaar te brengen.

Slot

De politie heeft nog steeds flink wat in te halen op de samenleving die haar omringt, niet zozeer omdat er geen actie wordt ondernomen, maar wel omdat de acties nog te veel het karakter dragen van pionierswerk van enkelen. De eerder vermelde conclusie uit 2012 dat 'digitaal' nog geen normaal en integraal onderdeel is van de politieorganisatie in de volle breedte, geldt nog steeds. Sindsdien is wel voortgang geboekt, maar de politie moet zich sneller aanpassen aan de digitalisering van de samenleving en ze kan dus niet volstaan met het draaien van meer cybercrimezaken. Zij moet verlangen dat alle medewerkers digitale mogelijkheden benutten bij al hun zaken en andere taken. «

Literatuur

Domenie, M.M.L., E.R. Leukfeldt, J.A. van Wilsem, J. Jansen & W.Ph. Stol (2013) *Slachtofferschap in een gedigitaliseerde samenleving.* Den Haag: Boom|Lemma.

Leukfeldt, E.R., M.M.L. Domenie & W.Ph. Stol (2010) *Verkenning cybercrime in Nederland 2009.* Den Haag: Boom Juridische Uitgevers.

Stol, W.Ph., E.R. Leukfeldt & H. Klap (2012) Cybercrime en de politie. *Justitiële Verkenningen*, 38, 1, 25-39.

Stol, W.Ph. (2004) Trends in cybercrime. *Justitiële Verkenningen*, 30, 8, 76-94.

Stol, W.Ph. & L. Strikwerda (2017) *Strafrechtspleging in een digitale samenleving.* Den Haag: Boom Juridische Uitgevers.

Stol, W.Ph. & L. Strikwerda (te verwachten in 2018). Online vergaren van informatie voor opsporingsonderzoek: een beknopte evaluatie van voorgestelde wetgeving. *Tijdschrift voor Veiligheid.*

Stol, W. Ph., Treeck, R.J. van, Ven, A.E.B.M. van der (1999) Criminaliteit in cyberspace. Een praktijkonderzoek naar aard, ernst en aanpak in Nederland; met veertig aanbevelingen. WODC.

Veenstra, S., R. Zuurveen, J. Kerstens & W. Stol (2016) *Opsporing in een gedigitaliseerde samenleving. Een handreiking voor het herkennen, vinden en benutten van digitale sporen.* Leeuwarden/Apeldoorn: NHL-Hogeschool/Politieacademie.

Noten

1 Brief van 16 september 2014 van de minister van Veiligheid en justitie aan de Tweede Kamer.

2 https://cybersciencecenter.nl/producten/, geraadpleegd 24 mei 2018

3 De politie kan ook informatie vorderen maar dat vat ik hier niet onder 'samenwerking of inkoop'.