

ARTIKEL

Digitalisering en de politiefunctie: hoe het speelveld verandert en wat dat van de politie vraagt

Wouter Stol, Jurjen Jansen & Wouter Landman

Dit artikel gaat over digitalisering en de politiefunctie. De digitalisering heeft veranderingen teweeggebracht, waardoor het speelveld voor de politiefunctie aanzienlijk is gewijzigd. Vooral actoren buiten de politiefunctie hebben aanvullende mogelijkheden gekregen om de rechtsorde uit te dagen of daaraan bij te dragen. Dit komt door veranderingen in organisatievermogen, informatievermogen en normeringsvermogen. We geven hier voorbeelden van door de invloed van digitalisering op criminaliteit en openbare orde nader te beschouwen. Deze 'nieuwe' werkelijkheid dwingt de politie tot reflectie op haar rol. In dit artikel bieden we daartoe een aantal mogelijke benaderingen, waarmee we het verdere debat willen aanwakkeren over de politiefunctie en de rol die de politie daarin kan of moet vervullen. Deze benaderingen omvatten: 1) samenwerken met burgers en particuliere organisaties, en het reguleren van sociale controle, 2) bewegen van opsporing naar een integrale aanpak en 3) waarborgen van rechtsbescherming door toezicht op het gebruik van nieuwe mogelijkheden door burgers en organisaties. Deze veranderingen vereisen een proactieve aanpak om de effectiviteit van de politiefunctie in het digitale tijdperk te waarborgen en te versterken.

1 Inleiding

In dit artikel verkennen we de gevolgen van digitalisering voor de politiefunctie en wat dat betekent voor de politie. Met digitalisering verwijzen we naar de ontwikkeling dat geautomatiseerde werken op steeds meer plaatsen en op steeds meer manieren een rol spelen in het dagelijks leven (Stol & Strikwerda, 2017). In paragraaf 2 komen de termen 'politiefunctie' en 'de politie' aan bod, alsook het theoretisch perspectief waarin wij deze twee plaatsen. Daarna bespreken we in paragraaf 3 de invloed van digitalisering op criminaliteit en in paragraaf 4 die op openbare orde. Vervolgens gaan we in paragraaf 5 in op het belang van de ontwikkelingen voor de politiefunctie en in paragraaf 6 nemen we stelling in hoe de politie daarop kan reageren.

2 Sociale controle als theoretisch perspectief

De politiefunctie plaatsen we in dit artikel in het theoretisch perspectief van sociale controle (Cachet, 1990; Stol, 1996). Sociale controle is het toepassen van (posi-

tieve of negatieve) sancties met als oogmerk het gedrag van anderen in overeenstemming te houden of brengen met de standaarden die gelden binnen de groep (Stol, 1996). Vanuit dat perspectief gezien houdt de politiefunctie zoveel in als het handhaven van gezamenlijke normen en regels in de samenleving. Kenmerkend voor de politiefunctie is dat het gaat om *formele* sociale controle, wat impliceert dat op basis van rechtsregels dwang kan worden uitgeoefend om handhaving van gezamenlijke normen en regels te bereiken (Heijder, 1989). Tegenover formele sociale controle staat *informele* sociale controle, die steunt op informele sancties in het dagelijks leven (thuis, school, vriendenclub). De politiefunctie heeft dus een bredere strekking dan ‘de politie’ en een smallere dan ‘sociale controle’.

De politiefunctie wordt ook wel gezien als ‘een regulatieve functie bestaande uit toezicht op en handhaving van algemeen geaccepteerde normen en regels en het beschermen van de orde binnen een sociale omgeving – indien nodig met gebruikmaking van drang en/of dwang’ (Van Steden et al., 2009; Van Halderen et al., 2024). In die benadering is de politiefunctie echter niet gekoppeld aan een wettelijke grondslag, waarmee de relatie met rechtsstatelijkheid verloren dreigt te gaan en er geen onderscheid meer lijkt te zijn tussen politiefunctie en sociale controle in welke vorm ook. In onze benadering zijn politiefunctie en sociale controle nadrukkelijk geen synoniemen, juist vanwege de wettelijke grondslag van die eerste.

De politiefunctie wordt uitgeoefend door uiteenlopende partijen (Brodeur, 2010), zoals de politie, bijzondere opsporingsambtenaren, de belastingdienst en GGZ-instellingen voor verplichte zorg. Dit kenmerk wordt in de internationale literatuur ook wel aangeduid als ‘plural policing’ (Bijleveld et al., 2021). De politie is een organisatie voor formele sociale controle en is de organisatie zoals bedoeld in artikel 25 lid 1 Politiewet 2012 (hierna: Polw 2012). De politie heeft van oudsher een unieke positie binnen de bredere politiefunctie, die in het bijzonder verband houdt met de combinatie van haar brede taakopdracht (art. 3 Polw 2012), waarmee zij werkt aan de politiefunctie, haar organisatieomvang, haar zichtbaarheid en haar mogelijkheden om met ingrijpende dwangmiddelen te interveniëren in het domein van individuele burgers en particuliere organisaties.

3 Digitalisering en criminaliteit

In deze paragraaf behandelen we de invloed van digitalisering op criminaliteit. Dit is een beschrijving op hoofdlijnen, waarbij we vooral aandacht besteden aan wat digitalisering betekent voor burgers, private organisaties en de politie.

3.1 Digitalisering en het plegen van delicten

Digitalisering heeft burgers en organisaties de gelegenheid gegeven tot het plegen van online criminaliteit. Dat is criminaliteit waarbij het gebruik van geautomatiseerde werken¹ van cruciale betekenis is voor de uitvoering van het delict. Vanwege

1 We sluiten met dit begrip aan bij artikel 80sexies Wetboek van Strafrecht dat bepaalt: ‘Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.’

de digitalisering zijn nieuwe vormen van criminaliteit ontstaan (cybercriminaliteit) en veel vormen van traditionele criminaliteit hebben een digitale verschijningsvorm gekregen (gedigitaliseerde criminaliteit). Beide vormen en hun mengvormen vatten we alle onder de term online criminaliteit. Online criminaliteit heeft een steeds groter aandeel in de totale criminaliteit (CBS, 2022). Er komen ook steeds nieuwe manieren om langs digitale weg criminaliteit te plegen, denk aan mishandeling door het ontregelen van een pacemaker of hersenimplantaat,² moord door het hacken van een rijdende auto (ENISA, 2017) of aanranding door het virtueel betasten van een avatar.³

De digitalisering biedt burgers en organisaties naast de gelegenheid om nieuwe criminaliteit te plegen ook een dekmantel in de vorm van anonimiteit (Stol, 2003; Van den Berg et al., 2012). Mensen kunnen online eenvoudig hun activiteiten en locaties verhullen door toepassing van encryptie (Jansen et al., 2023). Op het zogenoemde *darkweb* is het verhullen van identiteiten en locaties (IP-adressen) de standaard (Emmen et al., 2023). Ook (criminele) geldstromen kunnen worden verhuuld met digitale valuta (Europol & Eurojust, 2019). Dat een verhulling niet altijd in stand blijft, doet aan deze ontwikkeling op hoofdlijnen niets af.

Online criminaliteit kan tijd- en plaatsafhankelijk worden uitgevoerd. Hoewel de meeste online criminaliteit waarvan mensen in Nederland slachtoffer worden zich binnen de nationale grenzen afspeelt (Roks & Monshouwer, 2022), heeft een deel ervan een internationale dimensie; dader en slachtoffer bevinden zich dan in verschillende rechtsgebieden, waardoor het lastig wordt om deze vorm van misdaad effectief aan te pakken. De zogenoemde de-territorialiteit van online criminaliteit geldt niet enkel voor het doorbreken van nationale grenzen. Ook binnen landsgrenzen kan sprake zijn van een zekere mate van de-territorialisatie, hetgeen in dat geval betekent dat criminele activiteiten zich verspreiden over verschillende regio's, steden of buurten. In alle opzichten nieuw is deze 'binnenlandse de-territorialisatie' overigens niet, eerder een tweede golf. In de jaren zestig constateerden politiechefs onder de titel 'Criminaliteitsbestrijding in een veranderende maatschappij' de eveneens door technologie gedreven eerste golf: 'Niet slechts de zogenaamde beroeps-inbrekers en -oplichters, wier werkterrein vaak het hele land is, maken gebruik van moderne verkeers- en communicatiemiddelen, maar ook de exhibitionisten, aanranders, fietsen- en bromfietsdieven, winkeldieven en -dievegen enz. zijn gemotoriseerd en opereren veelal buiten hun woonplaats' (Haane & Heijboer, 1965: 61-62). De digitalisering doet daar wel scheppen bovenop. Kwaadwillenden kunnen eenvoudig met elkaar samenwerken in wisselende netwerken om hun aanvallen te innoveren (Leukfeldt, 2016; NCTV, 2022), en de voor online criminaliteit gebruikte ICT-infrastructuur kan in verschillende landen staan, bijvoorbeeld door toenemend gebruik van op de cloud gebaseerde opslag en diensten (Europol & Eurojust, 2019). Vooral maakt de digitalisering het mogelijk om delic-

2 www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patientdeath-fears-fda-firmware-update.

3 www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta.

ten op afstand te plegen. De mogelijkheden voor de plegers van delicten zijn dus groot en vergroot.

Voor burgers en bedrijven als potentiële slachtoffers biedt de digitalisering niet in vergelijkbare mate mogelijkheden tot zelfbescherming. Mensen kunnen niet gemakkelijk hun digitale omgeving doorzien en begrijpen, wat leidt tot fouten en kwetsbaarheden (Stol, 2020) en daarmee dus ook tot slachtofferschap. Daarnaast kunnen mensen steeds moeilijker onderscheid maken tussen wat echt/waar en wat nep/onwaar is online (Jansen et al., 2019), wat hen kwetsbaar maakt voor allerlei nieuwe fraudevormen. Een voorbeeld hiervan is ‘voice cloning’, waarbij criminelen een potentieel slachtoffer opbellen met de ‘gekloonde’ stem van een vriend of familielid en de vraag om snel geld over te maken of persoonlijke gegevens te delen (zie Landman, 2023). Ook deepfake video’s illustreren deze ontwikkeling.

Niet alleen burgers en hun organisaties hebben het lastig. Door de digitalisering is de samenleving als geheel afhankelijker geworden van technologisch complexe systemen en daarmee gevoeliger voor uitval, verstoring en aanvallen (NCTV, 2022), wat grote (maatschappelijke) impact met zich mee kan brengen (Prins et al., 2019). Uitval kan een gevolg zijn van een gerichte aanval, maar ook van een zogenaamd cascade-effect, wat wil zeggen dat een individuele (criminele) aanval invloed heeft op de rest van een keten of netwerk of zelfs daarbuiten (Prins et al., 2019).

3.2 Digitalisering en participatie in criminaliteitsbestrijding

Digitalisering geeft burgers en organisaties niet alleen nieuwe mogelijkheden om criminaliteit te plegen, maar ook om sociale controle uit te voeren en criminaliteit te bestrijden. Burgers kunnen zich met digitale technologie organiseren ten behoeve van criminaliteitsbestrijding. Het wijdst verspreid in Nederland is nu vermoedelijk de WhatsApp-buurtpreventiegroep (Lub & De Leeuw, 2019). Specialistischer is Bureau Dupin, dat zich toelegt op het helpen oplossen van vastgelopen moordzaken. Andere voorbeelden zijn het journalistencollectief Bellingcat, dat onder meer onderzoek deed naar het neerhalen van vlucht MH17, en het publicatieplatform voor gelekte informatie Wikileaks (Higgins, 2021). Een mijlpaal in deze ontwikkeling is in Nederland de in 2019 met digitale middelen opgezette organisatie van de familie Faber, gericht op het vergaren van informatie over hun vermiste (en naar later bleek vermoorde) Anne. Dat was meer dan de politie toen deed en de politie heeft daar vervolgens haar voordeel mee kunnen doen (Lam & Kop, 2020). Los van de vraag of een vermist persoon de voorbode is van een delict – het kan ook gaan om bijvoorbeeld weglopen, ongeval of zelfdoding – is het zoeken naar een vermiste een onderwerp waarop digitaal georganiseerde burgers zich richten. Zo zijn er inmiddels het Veteranen Search Team (hierna: VST) en het Coördinatie Platform Vermissing (hierna: CPV).⁴ Ze werken beide officieel samen met de politie. Het VST ontstond in 2017 uit een eenmalig initiatief (VST, 2019) en het CPV ontstond in 2016 vanuit een eenmalige zoekactie via Facebook.

Private partijen kunnen behalve informatie verzamelen ook normeren, interveniëren en sanctioneren dan wel dwang uitoefenen (Svensson & Zouridis, 2004; Stol, 2010). Het kan gaan om correcties door een moderator, maar ook zijn verschillen-

4 Zie resp. www.veteranensearchteam.nl en www.cpv-nl.nl.

de verdergaande mogelijkheden denkbaar, zoals een financiële instelling die een bankrekening opheft waarbij wordt vermoed dat deze voor phishingtransacties wordt misbruikt, een socialenetwerksite die een gebruiker buitensluit van haar dienstverlening omdat de inhoud van een bericht 'normoverschrijdend' is of een provider die een site offline haalt omdat daar vandaan kinderporno wordt verspreid. Ook de mogelijkheden tot sanctioneren middels plagen, pesten en buitensluiten zijn door de digitalisering toegenomen. Toch zijn de sanctioneringsmogelijkheden van private partijen niet onbegrensd, want deze zijn gelimiteerd door rechten van degenen op wie de sancties zijn gericht.

Dat criminaliteit zich nu voor een belangrijk deel online afspeelt, heeft als gevolg dat de partijen die sociale controle kunnen uitoefenen, anders dan voorheen vaak ook private partijen zijn (Svensson & Zouridis, 2004; Bijleveld et al., 2021). Veel van de ICT-infrastructuur, waaronder kabels, servers, datacenters en sensoren, maar ook platformen, diensten, enzovoort, die nodig zijn om online criminaliteit te plegen zijn immers privaat bezit. De eigenaren zijn bijvoorbeeld techreuzen zoals Meta, Google, Apple, Microsoft en Amazon, verzekeraars, energiebedrijven of financiële instellingen. Ook valt te denken aan kleinere bedrijven die zich een positie verwerven dankzij hun digitale informatiepositie (bijv. satellietdata, internetmonitoring). Maar vooral de grote private partijen weten veel van hun eindgebruikers en/of doelgroepen, zoals interesses, voorkeuren en gedragingen (waaronder normafwijkende).

De gevallen waarin burgers digitale middelen aanwenden voor sociale controle staan niet zelden ter discussie vanwege spanning met uitgangspunten van de rechtsstaat. Zo werd in 2009 online-pedojaagster Yvonne van H. veroordeeld wegens smaadschrift.⁵ In 2015 constateert een journalist dat wat in gemeente Aalborg begon als WhatsApp-buurtpreventie, al snel onttaarde in een discriminatoire 'heksenjacht op mensen met een Oost-Europees uiterlijk'.⁶ Politiechef Oscar Dros meldt in 2020 dat de politie geen behoefte heeft aan de 'hulp' van pedojagers, want zij 'plegen strafbare feiten en er ontstaan gevaarlijke situaties'.⁷ De leden van de burgerwacht in Ter Apel werken met een (besloten) Facebookpagina en een WhatsApp-groep waarin zij contact onderhouden. Zij surveilleren en voeren burgerarrestaties uit, waarbij met name dat laatste discussie in de media oproept, vooral wanneer geweld wordt gebruikt.⁸ 'Neem het heft niet in eigen handen', aldus het ministerie van Justitie en Veiligheid.⁹

3.3 Digitalisering, politie en criminaliteitsbestrijding

De digitalisering vraagt van de politie veel aanpassingsvermogen. Zij heeft gaandeweg specialistische teams ter bestrijding van online criminaliteit ingericht en werkt internationaal samen in grote zaken, maar in het generieke politiewerk zoals wordt uitgevoerd aan de basisteams is vooral sprake van een kennistekort. Dit is een con-

5 NRC, 8 mei 2009.

6 *Reformatorsch Dagblad*, 1 oktober 2015; NRC, 23 augustus 2017.

7 www.gelderlander.nl/binnenland/politie-over-pedojagers-dit-zijn-geen-helden-we-zijn-er-klaarmee-a9664741.

8 www.facebook.com/groups/950867156083671/; www.groene.nl/artikel/de-burgerwacht-in-ter-apel.

9 <https://nos.nl/nieuwsuur/artikel/2485941-burgerwacht-in-opkomst-hoe-ver-mag-je-gaan>.

stante bevinding vanaf het begin van de digitalisering (Stol et al., 1999; Jansen et al., 2020; Ruiter et al., 2023). De politie onderneemt wel initiatieven tegen dat kennistekort, maar de inhaalslag verloopt niet vlot. De situatie is nu eigenlijk zo dat de politie de minste kennis bezit over de criminaliteit die het meeste voorkomt, namelijk online criminaliteit. Maar enkel ‘meer kennis’ lost niet alle problemen op waarvoor de digitalisering de politie stelt. Bijvoorbeeld de omvang van online criminaliteit vraagt om capaciteit die schaars is, het *de-territoriale* karakter vraagt om samenwerking tussen verschillende jurisdicties, wat niet altijd eenvoudig is, en de online anonimiteit maakt over de hele linie opsporen lastig (zie ook Jansen et al., 2023).

Verder komen wettelijke kaders die de politie houvast bieden op diverse plaatsen onder druk te staan, hetgeen voor de politie onzekerheid met zich meebrengt. De verweving van mens en machine bijvoorbeeld maakt vormen van criminaliteit mogelijk waarop ons huidige materiële strafrecht nog geen antwoord heeft (Borwell et al., 2021; Van der Wagen, 2018). We noemden eerder al enkele voorbeelden. De digitalisering stelt ook het strafprocesrecht voor nieuwe vragen. Bijvoorbeeld de formele bevoegdheid omtrent stelselmatige informatievergaring (art. 126j Sv) en die omtrent het doen van onderzoek in het lichaam (art. 195 Sv) zijn nu streng gescheiden bevoegdheden. Stelselmatige informatieverzameling kan echter door het vergaren van data uit smartwatches overgaan in onderzoek aan en zelfs in het lichaam (bijv. hartslag, beweging, lichaamstemperatuur, vruchtbaarheidscyclus, slapen/waken).

Natuurlijk biedt de digitalisering de politie ook nieuwe mogelijkheden. Voorbeelden zijn de hackbevoegdheid of de bevoegdheid tot het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke (internet)bronnen.¹⁰ Ook maken politiemensen gebruik van de algemene digitale (informatie)mogelijkheden, zoals Google, en ze leggen informatie vast in politiestructuren die zij naderhand weer kunnen raadplegen. Zo hebben ook politiemensen meer informatie over burgers onder handbereik dan zij ooit hadden, vaak informatie over normafwijkend gedrag. De politie gebruikt informatie uit politiestructuren bij haar optreden op straat of bij het draaien van zaken, maar ook voor bijvoorbeeld *predictive policing*, ofwel analyses die haar moeten helpen criminaliteit te voorspellen om daarop te acteren. We kennen echter geen onderzoek waaruit blijkt dat het gebruik van databestanden of van *predictive policing* tot een vermindering van criminaliteit heeft geleid (zie ook Meijer & Wessels, 2019). Wel weet de politie in internationale samenwerking successen te boeken via het kraken van cryptodiensten, zoals Ennetcom, Encrochat en Sky ECC (o.a. Jansen et al., 2023; Landman, 2023). De Sky ECC-operatie, bijvoorbeeld, leverde zo’n miljard berichten op van 70.000 toestellen, resulterend in honderden opsporingsonderzoeken in alleen al Nederland en België (Oerlemans & Royer, 2023). Het kraken van zulke diensten levert de politie ook kennis op over bijvoorbeeld modus operandi en criminele samenwerkingsverbanden.

10 Dit laatste is onderdeel van de modernisering Wetboek van Strafvordering.

4 Digitalisering en openbare orde

In deze paragraaf gaan we in op de invloed van digitalisering op de openbare orde. Net als bij criminaliteit is dit een beschrijving op hoofdlijnen, waarbij we vooral aandacht besteden aan wat digitalisering betekent voor burgers, private organisaties en de politie.

4.1 Digitalisering en ordeverstoringen

Digitalisering werkt naast criminaliteit ook door in de offline openbare orde. In 1997 organiseerden hooligans per SMS een vechtpartij in een weiland bij Beverwijk, waarbij een dode viel. In 2003 werden de nieuwe digitale mogelijkheden om mensen op de been te brengen in diverse landen ludiek gedemonstreerd met 'flashmobs' (een groep mensen die plotseling op een openbare plek samenkomt, daar iets ongebruikelijks doet en dan snel weer verdwijnt). In 2012 plaatste een 16-jarig meisje een openbare uitnodiging voor haar Sweet Sixteen Party in Haren op Facebook. Via deze uitnodiging, die was gericht aan haar vrienden, werden door een vriend van een vriend meer mensen uitgenodigd en via een sneeuwbaaleffect kwamen er in korte tijd duizenden mensen bij. Het verwijderen van het originele uitnodigingsbericht mocht niet meer baten, want er waren al nieuwe evenementberichten aangemaakt met als terugkerende term 'Project X'. Er kwamen duizenden jongeren naar het 'feest' in Haren, dat eindigde in rellen met de Mobiele Eenheid en het aftreden van de burgemeester (Cohen et al., 2013).

Project X was in essentie niet nieuw, maar een *wake-up call* en daarmee het begin van een fenomeen dat 'online aangejaagde (openbare) ordeverstoringen' is gaan heten: fysieke verstoringen van de openbare orde die online zijn geïnitieerd of online worden versterkt.¹¹ In de jaren na Project X heeft dit fenomeen zich nog veel vaker voorgedaan (Bantema et al., 2020). Het recentste voorbeeld van grootschalige online aangejaagde ordeverstoringen zijn de 'avondklokrellen'. In januari 2021 vormde de invoering van de avondklok de opmaat voor dagen van onrust met rellen in meerdere gemeenten (COT, 2021a, 2021b; Moors et al., 2022). Deze rellen tonen dat de mobiliserende rol van digitale technologie in het fenomeen van 'online aangejaagde ordeverstoringen' zich sterk heeft ontwikkeld: van één digitaal platform naar vele platformen; van een uitnodiging vooraf naar het live verslag doen van rellen; van aanjagen naar aanjagen én coördineren; van zoeken naar vertier en sensatie naar ook het uiten van ongenoegen. In een analyse van de avondklokrellen wordt geconcludeerd: 'De sociale media speelden een rol van grote betekenis. Als een coördinatie- en aanjaagmiddel, dat influencers vanuit groepen met organiserend vermogen doelbewust gebruiken om ervaren onbehagen en boosheid te kanaliseren in protestbewegingen' (Moors et al., 2022: 7).

4.2 Digitalisering en participatie in ordehandhaving

De digitalisering geeft burgers ook nieuwe mogelijkheden actie te ondernemen om de openbare orde te handhaven. In januari 2021 organiseerden 'voetbalsupporters'

11 Naast online aangejaagde ordeverstoringen is er ook online aangejaagd geweld (zie ook Bartelds et al., 2023). Denk aan drillrap-groepen die online versterkte vetes uitvechten op straat.

zich eenvoudig met digitale middelen en gingen de straat op om te voorkomen dat relschoppers in coronatijd de stad zouden vernielen. Zij ontvingen lof van een burgemeester voor deze burgerzin, maar er was ook rechtsstatelijk gemotiveerde kritiek.¹² De politie stond eveneens niet te juichen. Zo'n burgeractie om de orde te handhaven is niet nieuw (al in 1970 veegden mariniers op eigen initiatief De Dam schoon¹³). Het gemak waarmee zo'n actie nu dankzij de digitalisering kan worden geïnitieerd en georganiseerd is dat wel.

De frequentie waarmee dit soort 'burger-ordeteams' ontstaan, is naar onze inschatting minder dan de frequentie waarmee burgers zich mengen in criminaliteitsbestrijding. Er zijn wel in veel wijken buurtvaders en/of -moeders actief die een oogje houden op met name jongeren om de orde in de wijk te bewaren. Maar hun ontstaan en functioneren hangt minder af van digitale middelen. Dergelijke initiatieven ontstaan eerder langs lijnen der geleidelijkheid (idee, overleg, middelen, afstemming met lokale overheid), hoewel in de uitvoering natuurlijk wel smartphones en chatapps worden gebruikt.

4.3 Digitalisering, politie en ordehandhaving

De digitalisering stelt de politie en haar partners in de politiefunctie voor nieuwe vraagstukken waar het ordehandhaving betreft. Om te beginnen zijn er vraagstukken omtrent mogelijkheden en bevoegdheden. Het gaat dan in het bijzonder om de politie die in de afgelopen jaren meer is gaan investeren in het online vergaren van gegevens, in het bijzonder met het oog op de openbare orde en het toenemende 'maatschappelijk ongenoegen' (Landman & Groothuis, 2022). Er zijn echter meer actoren die online gegevens zijn gaan verzamelen in het kader van maatschappelijk ongenoegen en dreigende openbare-ordeverstoringen. In de eerste plaats zijn dat gemeenten. Waar voorheen een gemeente sterk afhankelijk was van de politie voor de informatiepositie op het gebied van dreigende openbare-ordeverstoringen zijn gemeenten in de afgelopen jaren zelf actief geworden op het gebied van 'online monitoring' (Bantema et al., 2021). In 2021 bleek dat ook de Nationaal Coördinator Terrorismebestrijding (hierna: NCTV) met behulp van 'nepaccounts' op grote schaal burgers op sociale media monitorde in verband met mogelijke bedreigingen voor de nationale veiligheid.¹⁴ Daarnaast wordt door onder andere jongerenwerk en de politie gezocht naar manieren om vroegtijdig in de online leefwereld van jongeren aanwezig te zijn en daarin te interveniëren, zodat online aangejaagde ordeverstoringen en/of geweld kunnen worden voorkomen (Bartelds et al., 2023). De vraag is steeds wie welke mogelijkheden heeft en wat juridisch toelaatbaar en ethisch wenselijk is. Het is dan ook niet verrassend dat er op dit terrein veel onzekerheid bestaat over hoe te handelen (Greijdanus et al., 2023).

De ontwikkeling van juridische kaders voor online activiteiten voor openbare-ordehandhaving heeft geen gelijke tred gehouden met de praktijk. De politie werkt bij online gegevensvergarig geregeld in onduidelijk gebied, omdat wetgeving en

12 NRC, 26 januari 2021, www.nhnieuws.nl, 27 januari 2021.

13 NRC, 26 augustus 1970 (NRC-archief: www.nrc.nl/nieuws/1970/08/26/en-minister-president-op-treden-van-mariniers-onuist-kb_000033265-a2898371).

14 www.nrc.nl/nieuws/2021/04/09/nctv-volgt-heimelijk-burgers-op-sociale-media.

jurisprudentie betrekking hebben op het fysieke domein en zich niet een-op-een laten vertalen naar het digitale domein (Bijleveld et al., 2021; Commissie Waarborgen Werken Onder Dekmantel, 2023; Landman & Groothuis, 2022). Dit ‘transferprobleem’ is ook zichtbaar in de zoektocht naar de juridische basis voor wat het ‘online gebiedsverbod’ wordt genoemd (Bantema & Buitenhuis, 2023). Op het gebied van online monitoring zijn er ten behoeve van gemeenten en de NCTV recent maatregelen genomen om activiteiten van meer (juridische) grondslag te voorzien.¹⁵

Naast de juridische/ethische opgave is er sprake van een samenwerkingsopgave. Binnen de politie zijn er steeds meer onderdelen die online gegevens verzamelen en met elkaar zoeken naar de optimale verdeling van taken (Landman & Groothuis, 2022). Tussen de politie en andere actoren is dit proces ook gaande (De Vries & Bantema, 2022). Ook kan worden gedacht aan hoe overheidsinstanties (gaan) samenwerken met online platformen om ongewenste content – in verband met online aangejaagde ordeverstoringen – offline te halen (Bantema & Buitenhuis, 2023). Immers, private partijen nemen de rol op zich van beheerder van de (semi) openbare ruimte. Dat roept dan weer de juridische-ethische vraag op of burgers worden gecontroleerd en ‘berecht’ door een ‘niet democratisch gecontroleerde instantie’ (Bijleveld et al., 2021). De samenwerkingsopgave is dus nauw verbonden met juridisch-ethische kwesties.

5 Conclusies: veranderde posities en de politiefunctie

Het voorgaande toont dat de digitalisering op drie vlakken ingrijpt op sociale controle. Het grijpt in op het organisatievermogen en informatievermogen (Stol, 2020, 2021) alsook op het normeringsvermogen van zowel burgers, private organisaties als overheidsorganisaties, waaronder de politie. ‘Organisatievermogen’, van een individu of collectief, verwijst naar de potentie om acties op elkaar af te stemmen ten gunste van een bepaald doel. ‘Informatievermogen’ verwijst naar informatie als kapitaal en als basis voor actie. Informatievermogen is iets *hebben* en iets daarmee *kunnen*, zoals uitoefenen van sociale controle. Met ‘normeringsvermogen’ doelen we op de mogelijkheden die iemand of een organisatie heeft om opvattingen van anderen en mogelijk ook gedrag dat daarmee samengaat te beïnvloeden. Hierna iets meer over de drie genoemde vermogens.

5.1 Digitalisering en organisatievermogen

Digitalisering creëert organisatievermogen en dat schept vooral nieuwe mogelijkheden voor individuele, elkaar onbekende burgers. Zij kunnen zich dankzij de digitale mogelijkheden nu organiseren en vervolgens gecoördineerd samen optrekken. We zagen zojuist verschillende voorbeelden daarvan. Burgers gebruiken de digitale

15 Voor gemeenten is er sinds oktober 2023 een handreiking voor onlineonderzoek bij het handhaven van de openbare orde. Ten aanzien van de NCTV is de Wet coördinatie terrorismebestrijding en nationale veiligheid relevant, die op 12 december 2023 is gepubliceerd. Deze wet biedt de bevoegdheid om onder verantwoordelijkheid van de minister van Justitie en Veiligheid persoonsgegevens te verwerken, die afkomstig zijn uit publiek toegankelijke bronnen.

mogelijkheden om samen delicten te plegen, demonstraties en rellen te organiseren, dan wel samen te jagen op vermeende criminelen, te zoeken naar vermiste personen of op te treden tegen in hun ogen ordeverstoorders. Niet alleen hebben burgers veel nieuwe mogelijkheden vanwege hun juist verworven organisatievermogen, dit gaat gepaard met een grote flexibiliteit. Zoektochten vanwege vermisingen tonen bovendien dat het ook kan gaan om een grote capaciteit. ‘Meer dan duizend mensen zoeken naar vermiste jongen [...]’, kopt de NOS op 13 januari 2024.¹⁶ De digitalisering biedt natuurlijk ook aan bestaande organisaties extra organisatievermogen, maar hier gaat het niet om een wezenlijke verandering. Mensen in een organisatie wáren immers al duidelijk georganiseerd. Bestaande organisaties zijn vaak gemodelleerd als bureaucratie, ook de grotere commerciële organisaties, en hebben daardoor een veel geringere flexibiliteit (maar vaak wel meer continuïteit en status).

Voor de politie is de verandering vooral dat zij nu te maken heeft met burgers die zich ad hoc en flexibel kunnen organiseren om naar eigen inzicht en op gecoördineerde wijze een uitdaging te vormen voor of juist een bijdrage te leveren aan sociale controle in de samenleving. Zij zijn daarmee geen onderdeel geworden van de politiefunctie (ze missen de formele bevoegdheden die de politiefunctie kenmerken), maar ze plaatsen die functie wel in een ander perspectief. Ze vormen door hun vermogen om gecoördineerd in actie te komen als het ware een nieuw machtsblok ernaast.

5.2 Digitalisering en informatievermogen

Digitalisering schept ook informatievermogen. Dit geeft vooral nieuwe mogelijkheden aan georganiseerde samenwerkingsverbanden. Burgers die zich digitaal hebben georganiseerd, kunnen daarna werken aan het informatievermogen van hun organisatie. Maar informatievermogen floreert pas echt in grotere organisaties met veel informatie.

Informatie over personen is een basis voor het uitoefenen van controle over die personen (Foucault, 1975). Zonder informatie en ‘dossiers’ is er geen corrigerend overheidsingrijpen mogelijk. Wie informatie over burgers heeft, bezit dus een belangrijke grondstof voor de politiefunctie. Van oudsher was het vooral de overheid, waaronder de politie, die beschikte over informatie over burgers. Nu zijn het allereerst (de grotere) particuliere bedrijven die beschikken over veel informatie over de dagelijkse bezigheden van burgers (hun klanten c.q. gebruikers) – informatie die niet zelden van belang kan zijn voor de politiefunctie. Hoewel de politie soms grote hoeveelheden informatie over criminelen weet te bemachtigen, moeten we aannemen dat het informatievermogen in de particuliere sector vele malen meer en sneller is toegenomen dan bij de politie en andere opsporingsinstanties. Particuliere organisaties hadden dertig tot veertig jaar geleden nog nauwelijks informatievermogen en beschikken nu over een niet te schatten hoeveelheid (privacygevoelige) informatie over burgers, ook als we in aanmerking nemen dat onderlinge communicatie tussen gebruikers van communicatieapps zoals WhatsApp en Signal is ver-

16 <https://nos.nl/artikel/2504713-meer-dan-duizend-mensen-zoeken-naar-vermiste-jongen-16-jas-gevonden-in-merwede>.

sleuteld en voor de dienstaanbieder niet is in te zien. Deze organisaties treden hierdoor niet toe tot de politiefunctie, maar zijn partijen geworden met belangrijke grondstof voor die functie en dus ook voor politiewerk, los van de vraag of de politie die informatie zou moeten mogen gebruiken.

Het informatievermogen van organisaties kan ongunstig uitpakken voor individuen wanneer daarmee hun rechten worden aangetast. De samenleving brengt daartegen juridische maatregelen in stelling, in EU-verband bijvoorbeeld werd de General Data Protection Regulation (GDPR) van kracht op 25 mei 2018. Het gaat echter ook om toezicht op de naleving van dergelijke regels. Behalve partijen met voor rechtshandhaving bruikbare informatie zijn organisaties met informatievermogen ook partijen die onderwerp moeten zijn van actief rechtsbeschermend optreden vanuit de politiefunctie.

5.3 Digitalisering en normeringsvermogen

De digitalisering werkt ook door in het normeringsvermogen van met name organisaties, maar ook van individuen. Organisaties of individuen die digitale platformen beheren of modereren, handhaven op het platform bepaalde normen en kunnen sancties toepassen tegen iemand die (te ver) daarvan afwijkt. In het uiterste geval kunnen ze iemand verwijderen van het platform. Ruim twintig jaar geleden lieten Svensson en Van Wijk (2002) reeds zien dat online communities verre van normloos zijn. In online studentengroepen, zo vonden zij, is illegaal kopiëren oké, maar hacken en spammen zijn uit den boze, evenals het verspreiden van computervirussen. Vandaag de dag is volop discussie over algoritmen die voorkeuren van gebruikers bevestigen en versterken. Het gaat vooral om beïnvloeding en niet zozeer om dwang, hoewel soms wel een voorbeeld wordt gesteld, bijvoorbeeld toen Donald Trump werd verwijderd van Twitter (de voorloper van X). Normeringsvermogen ligt van oudsher bij gezaghebbende naasten in iemands alledaagse leefwereld, zoals opvoeders, docenten en peers. Door de digitalisering zijn daar anderen bijgekomen, zoals influencers en organisaties die algoritmen beheren (zie ook Schuilenburg, 2023).

Actoren in de politiefunctie zijn eveneens normerend. De taak van de politie in dit verband is om de in de wet vastgelegde normen te bekrachtigen als die geschonden worden, desnoods met geweld op basis van wettelijke bevoegdheden. De digitalisering heeft daaraan niet iets wezenlijks veranderd. Wel zijn nieuwe gedragingen strafbaar geworden (bijv. hacken), waardoor nu op die gedragingen oude bevoegdheden van toepassing zijn (bijv. aanhouden) en ook zijn vanwege de digitalisering nieuwe bevoegdheden geïntroduceerd (bijv. op afstand een computer binnendringen). Nieuw is het door de digitalisering ontstane normeringsvermogen van individuen en organisaties en hun mogelijkheden om dat met (dreigen met) sancties kracht bij te zetten. Tussen de informele normering in de alledaagse leefwereld van mensen (door bijv. ouders, docenten, vrienden) en de formele normering door de politiefunctie (de staat) heeft zich vanwege de digitalisering een groep ontwikkeld van mensen en organisaties met een normerende rol en sanctionerende mogelijkheden. Met name de opkomst van algoritmen heeft die middengroep versterkt. Gezien vanuit de politiefunctie is door het ontstaan van deze middengroep het maatschappelijk weefsel van sociale controle complexer geworden.

5.4 Digitalisering: gewijzigde maatschappelijke verhoudingen

Hoewel onze analyse beknopt is, leidt zij tot de conclusie dat de maatschappelijke verhoudingen zijn gewijzigd. Individuen en particuliere organisaties hebben nieuwe mogelijkheden gekregen tot normafwijkend gedrag en tot sociale controle. Voor individuen is dat allereerst het vermogen om zich snel ad hoc te organiseren. Politie mensen hebben die optie in theorie ook, maar in de praktijk niet, want zij werken in overeenstemming met hun reeds bestaande organisatie. Voor organisaties houden de nieuwe mogelijkheden vooral verband met informatievermogen. Hoewel de politie meegaat met haar tijd, is ze nu niet langer dé organisatie die beschikt over gevoelige informatie over burgers. Ze heeft zelfs praktisch gesproken niet langer het monopolie op het organiseren van handhaving of van opsporingsonderzoek, zelfs niet op het verzamelen van opsporingsrelevante informatie. De politiefunctie betreft sociale controle en dus het handhaven van normen. De politie kan daarbij van oudsher als enige organisatie, en als *ultimum remedium*, geweld gebruiken. Maar zij heeft niet het monopolie op negatieve sancties en al helemaal niet op het bekrachtigen van normen. Door de digitalisering is het normeringsvermogen van individuen (die dan *influencers* worden) en organisaties vergroot, en zijn de mogelijkheden van organisaties om sancties toe te passen toegenomen. De consequentie van de veranderingen in organisatie-, informatie- en normeringsvermogen is dat de politiefunctie in een ander krachtenveld moet worden vormgegeven (zie ook Van Halderen et al., 2024). Voor de politie betekent dit dat zij haar positie ten opzichte van burgers en bedrijven met hun nieuw verworven vermogens opnieuw moet bepalen. We doen enkele aanzetten voor de discussie die hierover dient te worden gevoerd.

6 Discussie: opdracht voor de politie in het veranderde speelveld van de politiefunctie

6.1 Nieuwe machtsblokken in een veranderd speelveld

Het speelveld waarin de politie haar werk doet, is aanzienlijk veranderd: burgers en private organisaties hebben mogelijkheden die zij eerst niet hadden en gebruiken die ook volop. Zij zijn daarmee geen onderdeel van de politiefunctie geworden, maar wel plaatsen ze de politiefunctie in een geheel andere omgeving. Burgers en private organisaties vormen door hun vermogen om gecoördineerd in actie te komen als het ware een nieuw machtsblok waartoe de politiefunctie, en dus de politie, zich moet verhouden. Private organisaties zijn met hun informatievermogen een partij geworden met belangrijke grondstof voor de politiefunctie en dus voor politiewerk, en dus moet de politie zich tot die organisaties verhouden. Tussen de klassieke informele sociale controle in ieders alledaagse leefwereld en de formele sociale controle door de politie is een nieuwe groep voor sociale controle ontstaan, bestaande uit moderators, influencers en algoritmen. Ook zij vormen een nieuw machtsblok in het speelveld van de politiefunctie. De ontwikkelingen negeren is geen optie en dus roepen ze de vraag op hoe de politiefunctie, en speciaal de politie, zich tot de nieuwe groepen en posities dient te verhouden. In deze afsluitende dis-

cussie geven we, voortbordurend op wat we naar voren brachten, enkele aanzetten die kunnen dienen als stof voor verder debat.

Eerst over de rol van de politie. De politie is de organisatie die namens de overheid en indien nodig met geweld, belast is met de handhaving van rechtsregels. Bij haar berust het geweldsmonopolie. De politie voert (formele) sociale controle uit op basis van rechtsregels. Ze werkt in ondergeschiktheid aan het bevoegd gezag en legt aan het gezag verantwoording af over haar werk. Democratisch gekozen volksvertegenwoordigers kunnen het bevoegd gezag ter verantwoording roepen. Anders gezegd: de politie controleert de samenleving en een vertegenwoordiging van die samenleving controleert weer de politie. Essentieel in politiewerk is de balans tussen staatsmacht en burgerrechten. Dezelfde wet die de politie machtsmiddelen geeft, beschermt burgers tegen ongewenste schending van hun rechten. De politie hoort te waken over zowel rechtshandhaving als rechtsbescherming; zij waakt over de juiste verhouding tussen die twee, en wat de juiste verhouding is moet steeds opnieuw worden vastgesteld. Vele anderen in de samenleving werken continu aan de handhaving van rechtsregels. Zo bezien is de rol van de politie beperkt en vaak ook enkel aanvullend, maar – als sluitstuk met doorzettingsmacht en met aandacht voor de balans tussen rechtshandhaving en rechtsbescherming – niet van minder belang.

Ook waar de samenleving door digitalisering verandert, is de politierol in essentie zoals in de vorige alinea geschetst. Zoals gezegd heeft de digitalisering er echter toe geleid dat het speelveld van de politiefunctie is veranderd, en wel zodanig dat de politie daarop moet reageren. Niet zozeer om in een machtsstrijd haar eigen positie veilig te stellen, maar om de politierol en de onderlinge verhoudingen in onze rechtsstaat mee te laten groeien met haar tijd. Drie thema's vragen daarbij primair aandacht: samenwerken, een integrale aanpak van online criminaliteit en waken over de rechtsbescherming.

6.2 Samenwerken

Samenwerken verwijst om te beginnen naar samenwerken met burgers en organisaties vanwege hun toegenomen mogelijkheden in rechtshandhaving (organisatie-, informatie- en normeringsvermogen). Lam en Kop (2020) pleiten naar aanleiding van de Anne Faber-casus voor een samenwerkingsmodel dat zowel burger- als politieparticipatie omvat. Die ontwikkeling is gaande. De politie staat open voor samenwerkingen, maar heeft ook reserves vanwege principes op het vlak van democratische controle en fatsoen in de rechtshandhaving, en terecht, want dat is haar rol. Een cruciale vraag is hier of de politie enkel ad hoc moet samenwerken met afzonderlijke groepen burgers en organisaties of dat zij het veld wil reguleren. Dat laatste lijkt misschien wat vreemd in een schijnbaar chaotisch krachtenveld, maar is zeker ten dele een realistische optie. Wanneer de politie samenwerkt met een bepaald initiatief voor rechtshandhaving, en het initiatief mede daardoor een structureel karakter krijgt, werkt dat kanaliserend voor gelijksoortige initiatieven die daarna volgen. De politie werkt bijvoorbeeld samen met de twee genoemde organisaties voor burgerzoekacties bij vermissingen (het VST en het CPV) en het lijkt daarom onwaarschijnlijk dat er nog meer van dergelijke permanente organisaties zullen ontstaan. Het VST en CPV roepen beide ook op om nieuwe burgerinitiatie-

ven bij hen te melden en werken aldus aan regulering. De politie dient dus beleid te ontwikkelen over of en zo ja hoe zij vanuit haar rol het veld van en rondom de politiefunctie wil reguleren als reactie op initiatieven op het vlak van rechtshandhaving.

Het thema samenwerken is tevens verbonden aan samenwerking met organisaties voor rechtshandhaving uit andere landen en aan nationale dan wel internationale samenwerking met private organisaties met informatievermogen. Voor de politie is daarbij allereerst van belang dat zij de geldende principes van rechtsbescherming handhaaft. Het verwijt van *jurisdiction (s)hopping* moet niet kunnen worden gemaakt en de samenwerking met private bedrijven moet voldoen aan de heersende normen voor rechtsbescherming.

Over samenwerken merken we tot slot op dat de politie weliswaar samenwerkt met de overal in de samenleving aanwezige WhatsApp-buurtpreventiegroepen, maar in de regel niet deelneemt aan de groepen zelf, maar contact onderhoudt met de groepsbeheerders. Hiervoor zijn goede redenen, zoals dat deelname aan een groep de suggestie kan wekken dat elk bericht die in de groepsapp wordt gedaan daarmee officieel ter kennisname van de politie is gebracht. Ook capaciteitsgebrek speelt een rol. Tegelijk is er reden om deze beleidskeuze eens goed te evalueren. Ze staat namelijk op gespannen voet met het principe van kennen en gekend worden. Het huidige systeem geeft de politie een gezicht bij de beheerder, maar zij blijft anoniem voor alle andere deelnemers, en dus voor het gros van de wijkbewoners.

6.3 Integrale aanpak

Online criminaliteit is veelvoorkomende criminaliteit (VVC) en vermoedelijk zelfs, als we alle online delicten zouden kunnen tellen, ‘de meest voorkomende criminaliteit’. Het bestrijden van online criminaliteit door ‘digi-zaken’ te draaien is een heilloze weg. Kop (2012) pleit voor een beweging van opsporing naar criminaliteitsbestrijding. Dat laatste is dan nadrukkelijk inclusief het aan de voorkant aanpakken van de problematiek. Dat gaat in eerste instantie om preventiebeleid, waarbij diverse publieke en private actoren een belangrijke rol spelen. Preventie omvat weerbaarheid bij potentiële slachtoffers, zowel in kennis en gedrag als in organisatorisch en technisch opzicht. Ook met behulp van wet- en regelgeving (vanuit EU) wordt hier aandacht aan besteed, bijvoorbeeld door te regelen dat in het ontwerpproces van technologie al rekening moet worden gehouden met privacy en security.¹⁷

Criminaliteitsbestrijding gaat naast preventie ook over relatief nieuwe strategieën, zoals verstoring van criminaliteit. Het Team High Tech Crime (hierna: THTC) van de politie werkt in dat verband met analyses die zijn gericht op het detecteren van knooppunten in of cruciale services voor het plegen van online criminaliteit, om die vervolgens aan te pakken – en daarmee niet enkel één zaak te draaien, maar tegelijk door verstoring van het systeem nieuwe delicten te voorkomen (zie ook Van den Eeden et al., 2021). Sinds enige tijd kent het THTC een Cyber Offender Prevention Squad (COPS). Zaken draaien is niet afgeschafte, maar de specialisten zetten duidelijk meer dan voorheen in op preventie van daderschap en verstoring

17 Zie bijv. <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.

van de criminele infrastructuur. Terwijl de specialisten dus andere wegen zoeken wordt, paradoxaal genoeg, tegelijk van districten en basisteams gevraagd om meer (eenvoudige) online criminaliteitszaken te draaien. Voor de politie is het nu zaak om een integrale aanpak van online criminaliteit te ontwikkelen – integraal in de zin van op maat gesneden combinaties van opsporing, preventie (waaronder weerbaarheid) en verstoring, zowel landelijk als in districten en basisteams. Samenwerkingen horen daarbij. Bij preventie en verstoring gericht op rechtshandhaving dient wel steeds rekening gehouden te worden met de grenzen die de rechtsbescherming daaraan stelt.

Preventiebeleid aangaande ordeverstoringen ligt ingewikkelder dan preventie aangaande criminaliteit, omdat bij preventie van ordeverstoring nog eerder dan bij criminaliteit spanning ontstaat met eisen die rechtsbescherming stelt, bijvoorbeeld het beschermen van het recht op privacy, vergaderen en demonstreren. Ons pleidooi voor een integrale aanpak betreft dan ook niet het voorkomen van online aangejaagde ordeverstoringen. Wel dient de politie met inachtneming van de rechtsbescherming en in het verlengde van het adagium ‘kennen en gekend worden’, werkwijzen te ontwikkelen waarmee zij online aangejaagde ordeverstoringen zo goed mogelijk kan zien aankomen. De politie beschikt weliswaar over Teams Openbare Orde Inlichtingen (TOOI), maar die ontvangen momenteel kritiek, omdat zij al spionerend burgerrechten schenden. Er is kennelijk gebrek aan democratische controle op het werk van die teams, aldus bijvoorbeeld de Amsterdamse gemeenteraad.¹⁸ De politie (alook samenleving en de politiek) zal tot op zekere hoogte domweg moeten accepteren dat opstootjes eenvoudiger dan voorheen bij verrassing kunnen voorkomen, want een alwetende politie is geen optie.

6.4 *Waken over de rechtsbescherming*

Als derde thema dat aandacht van de politie vraagt, noemden we bewaken van de rechtsbescherming oftewel van een fatsoenlijke rechtshandhaving. Burgers en organisaties die digitale middelen aanwenden voor het uitoefenen van sociale controle kunnen daarmee de rechten van anderen aantasten en aldus zelf over de schreef gaan. Ze kunnen zelfs zélf onderwerp worden van corrigerende acties. Bijleveld et al. (2021) zien ten aanzien van misdrijven dat alternatieve afdoeningen (civielrechtelijk) vaker lijken voor te komen. Zij vragen zich in dat kader af of deze beweging betekent dat sommige misdrijven ‘de facto straffeloos aan het worden zijn’. Of zijn zij, zo voegen wij daaraan toe, niet straffeloos geworden, maar in behandeling genomen buiten het formele strafrechtelijke systeem.

Stol (2021) benadrukt dat, juist ook in relatie tot digitalisering, de politie tot taak heeft te zorgen voor een fatsoenlijke rechtshandhaving. Wij noemden dat het waken over de balans tussen rechtshandhaving en rechtsbescherming. Gezien alle initiatieven die burgers en organisaties zoals techreuzen vanwege de digitalisering en hun daardoor verworven vermogens kunnen nemen, is meer aandacht vereist voor het bewaken van de rechtsbescherming. Activiteiten die burgers en organisaties dankzij hun nieuwe vermogens kunnen nemen, zijn niet onderworpen aan een bevoegd gezag en een democratische controle zoals in de strafrechtspleging gebrui-

18 NRC, 24 januari 2024, p. 8.

kelijk is. Wie bijvoorbeeld van een socialemediaplatform wordt geweerd, kan naar de rechter stappen en wie door een burgerwacht van zijn vrijheid wordt beroofd kan aangifte doen. Maar een politie die dit alles aankijkt en niet acteert, staat wel erg afwachtend langs de zijlijn. Een proactievere houding is te prefereren, want het gaat om essenties van onze rechtsstaat. De politie dient, kortom, het voortouw te nemen in de openbare discussie omtrent digitalisering en rechtsbescherming.

Literatuur

- Bantema, W. & M. Buitenhuis (2023) Burgemeester: Sheriff van het internet? *Het Tijdschrift voor de Politie*, (2), 42-45.
- Bantema, W., S. Westers, M. Hoekstra, R. Herregodts & S. Munneke (2021) *Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk*. Den Haag: Sdu.
- Bantema, W., S. Westers & S. Munneke (2020) *Niet bevoegd, wel verantwoordelijk? Handhavingmogelijkheden bij online aangejaagde ordeverstoringen*. Den Haag: Boom bestuurskunde.
- Bartelds, A., S. de Vries, L. Postma, W. Bantema & H. Greijdanus (2023) *Preventie van online aangejaagd geweld. Een praktijkverkenning naar de online werkwijze van jongerenwerkers en politie in Amsterdam Zuid-Oost*. NHL Stenden Hogeschool/Rijksuniversiteit Groningen.
- Berg, E. van den, C. Hermans & J. Quast (2012) *Politiefunctie in perspectief: Instrumenten voor toekomstgericht denken over de maatschappelijke functie van de politie*. Den Haag: Ministerie van Veiligheid en Justitie (Directe Strategie).
- Bijleveld, C., R. Salet, A. Damstra & D. Stéfanovic (2021) *Politiefunctie in een veranderende omgeving*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid.
- Borwell, J., J. Jansen & W.Ph. Stol (2021) Comparing the victimization impact of cyber-crime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, 3(3), 85-110.
- Brodeur, J.-P. (2010) *The policing web*. Oxford University Press.
- Cachet, A. (1990) *Politie en sociale controle*. Arnhem: Gouda Quint.
- CBS. (2022) *Veiligheidsmonitor 2021*. Den Haag: Centraal Bureau voor de Statistiek.
- Cohen, M.J., G.J.M. Brink, O.M.J. Adang, J.A.G.M. van Dijk & T. Boeschoten (2013) *Twee werelden: You Only Live Once*. Commissie 'Project X' Haren.
- Commissie Waarborgen Werken Onder Dekmantel. (2023) *Waarborgen voor heimelijk werk: Onderzoek van de commissie Waarborgen Werken Onder Dekmantel*. Pencilpoint.
- COT. (2021a) *Ongekende ongeregelheden: Leerevaluatie naar aanleiding van de ongeregelheden in Eindhoven van 24 januari 2021*. COT.
- COT. (2021b) *Een machteloos gevoel: Leerevaluatie naar aanleiding van de ongeregelheden in Den Bosch op 25 januari 2021*. COT.
- Eeden, C.A.J. van den, J.J. van Berkel, C.C. Lankhaar & C.J. de Poot (2021) *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum.
- Emmen, B., C.J. de Poot & W.Ph. Stol (2023) Politieoptreden op het darkweb. *Tijdschrift voor de Politie*, 85(2), 32-35.
- ENISA. (2017) *Cyber security and resilience of smart cars*. European Union Agency for Cybersecurity.

- Europol & Eurojust (2019) *Common challenges in combating cybercrime*. Verkregen via: www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime.
- Foucault, M. (1979 [1975]) *Discipline and Punish; the Birth of a Prison*. New York: Vintage Books.
- Greijdanus, H., T. Postmes, A. Bartelds, L. Postma, S. de Vries & W. Bantema (2023) *Interventies in de cyclus van online aangejaagd geweld: Inzichten uit een literatuurreview*. Rijksuniversiteit Groningen/NHL Stenden Hogeschool.
- Haane, Th.H. & H.J. Heijboer (1965) Criminaliteitsbestrijding in een veranderende maatschappij. *Tijdschrift voor de Politie*, 26(3), 61-74.
- Halderen, R.C. van, R. Tjoelker & R. Spithoven (2024) Met gezag online. Online schadelijk gedrag, publieke waarden en de politiefunctie. *Cahiers Politiestudies*, nr. 70, 185-200.
- Heijder, A. (1989) *Management van de politiefunctie*. Lochem en Arnhem: Van den Brink en Gouda Quint.
- Higgins, E. (2021) *Wij zijn Bellingcat. Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden*. Amsterdam: Het Spectrum.
- Jansen, J., T. van Valkengoed, S. Veenstra & W.Ph. Stol (2020) *Level-Up! Kennis voor politiewerk in een digitale samenleving*. Leeuwarden: Cybersafety Research Group.
- Jansen, J., S. Westers, W. Schreurs, M. Berkenpas, G. Alpár & W. Stol (2023) *De rol van encryptie in de opsporing. Belemmeringen en mogelijkheden*. Leeuwarden: Cybersafety Research Group.
- Jansen, J., S. Westers, S. Twickler & W.Ph. Stol (2019) *Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing*. Den Haag: Sdu (Politie en Wetenschap).
- Kop, N. (2012) *Van opsporing naar criminaliteitsbeheersing. Vijf strategische implicaties*. Den Haag: Boom Lemma uitgevers.
- Lam, J. & N. Kop (2020) *Schouder aan schouder: Burger- en politieparticipatie tijdens de vermissing van Anne Faber. Leerpunten uit de samenwerking tussen burgers en politie*. Apeldoorn: Politieacademie.
- Landman, W. (2023) *Politiewerk aan de horizon: Technologie, criminaliteit en de toekomst van politiewerk*. Den Haag: Sdu Uitgevers.
- Landman, W. & S. Groothuis (2022) *Politiewerk op het web: Een verkennend onderzoek naar online gegevensvergaring door de politie*. Den Haag: Sdu Uitgevers.
- Leukfeldt, E.R. (2016) *Cybercriminal networks: Origin, growth and criminal capabilities*. Den Haag: Eleven International Publishers.
- Lub, V. & T. de Leeuw (2019) *Politie en actief burgerschap: een veilig verbond? Een onderzoek naar samenwerking, controle en (neven)effecten*. Den Haag: Sdu Uitgevers.
- Meijer, A. & M. Wessels (2019) Predictive policing: review of benefits and drawbacks. *International Journal of Public Administration*, 42(12), 1031-1039.
- Moors, H., L. Klarenbeek, E. Berger, M. Dückers, M. van Duin, G. Kist, M. Luesink, T. Schrijvenaars & M. van der Wijngaart (2022) 'Avondklokrellen': lokale dynamiek in een mondiale crisis. *Analyse van de voedingsbodem van de ordeverstoringen in vier Noord-Bra-bantse steden*. EMMA.
- NCTV. (2022) *Cybersecuritybeeld Nederland (CSBN) 2022*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- Oerlemans, J.J. & S. Royer (2023) The future of data-driven investigations in light of the Sky ECC operation. *New Journal of European Criminal Law*, 14(4), 434-458.
- Prins, J.E.J., E.K. Schrijvers, R. Passchier & M. de Visser (2019) *Vorbereiden op digitale ontwijking*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid.

- Roks, R. & N. Monshouwer (2020) F-gamers die 'mapsen', 'swipen' en 'bonken': Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële verkenningen*, 46(2), 44-58.
- Ruiter, S., M. van Leuken, T. van Ruitenburg, J. Schiks & R. Leukfeldt (2023) *In- en doorstroom van online criminaliteit in de strafrechtketen*. Amsterdam: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.
- Schuilenburg, M. (2023) Big data policing. Schets van de belangrijke vraagstukken, partijen en nieuwste trends in de praktijk. In: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (red.), *Big data policing* (pp. 53-70). Gompel & Svacina.
- Steden, R. van, M. Roelofs & M. Heijnen (2009) *Pluriforme politiefunctie Inventarisatie van en burgerpercepties over beveiligers, toezichhouders en handhavers* (uitgave 14 in de serie Dynamics of Governance). Vrije Universiteit Amsterdam.
- Stol, W.Ph. (1996) *Politie-optreden en informatietechnologie: Over sociale controle van politiemensen*. Lelystad: Koninklijke Vermande.
- Stol, W.Ph. (2003) Sociale controle en technologie. De casus politie en kinderporno op het internet. *Amsterdams Sociologisch Tijdschrift*, 30(1/2), 162-182.
- Stol, W.Ph. (2010) *Cybersafety overwogen: Een introductie in twee lezingen*. Den Haag: Boom Juridische uitgevers.
- Stol, W.Ph. (2020) Digitalisering en criminaliteit: Een beknopte inleiding op cybercrime. In: C. de Poot, E. Lievens, W. Stol & L. De Kimpe (red.), *Cahier Politiestudies*, nr. 56, 13-22.
- Stol, W.Ph. (2021) Digitalisering en de rol van de politie: Naar een 'autoriteit fatsoenlijke rechtshandhaving'. *Panopticon*, 42(2), 161-168.
- Stol, W.Ph. & L. Strikwerda (2017) *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom Juridisch.
- Stol, W.Ph., R.J. van Treeck & A.E.B.M. van der Ven (1999) Criminaliteit in cyberspace: Een praktijkonderzoek naar aard, ernst en aanpak in Nederland. Elsevier.
- Svensson J.S. & A.Ph. van Wijk (2002) *Informeel sociale normering op het internet*. Enschede/Apeldoorn: IPIT/NPA.
- Svensson, J.S. & S. Zouridis (red.) (2004) *Waarden en normen in de virtuele wereld: Twee verkennende studies met discussie*. Enschede: IPIT.
- Vries, S. de & W. Bantema (2022) *Aanpak in kaart: Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen*. NHL Stenden Hogeschool.
- VST. (2019) *Stichting Veteranen Search Team. Jaarverslag 2018*. Verkregen via: www.veteranensearchteam.nl.
- Wagen W. van der (2018) *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory* (diss. Groningen).