

OPSPOREN OF PRIVACY VERLOREN?

E-magazine

Jaargang 7
Editie 2
2020-2021



LISA Law & ICT
Students' Association

Brinkhof

NORD
ADVOCATEN

Redactie

Hoofdredacteur

Sylvia Chan

Redacteur | Secretaris

Lotte Derksen

Redacteur

Bart Pastoor



Vormgeving

Sanne Barzilay

Harun Hubanic

Annika Winkel

Laura Weide

Voorwoord

Hoofdredacteur

Geachte lezer,

Hierbij presenteer ik u de tweede editie van het e-magazine voor dit collegejaar. De redactiecommissie heeft hier de afgelopen weken hard aan gewerkt en wederom een mooie editie weten neer te zetten. Bij deze wil ik mijn mede-commissieleden van harte bedanken voor hun inzet! Ook de mediacommissie heeft niet stilgezeten en heeft ook deze editie weer mooi vormgegeven, waarvoor dank!

We zitten op dit moment nog steeds in een lockdown vanwege het coronavirus, waardoor de digitale omgeving van onmiskenbaar belang blijft. Dit heeft ook gevolgen op het gebied van het straf(proces)recht. Zoals u in dit e-magazine zult lezen, is het aantal gevallen van cybercriminaliteit gestegen als gevolg van de coronacrisis. Deze verplaatsing van fysieke strafbare feiten naar de digitale wereld levert uitdagingen op voor de politie en het OM. Kan de politie bijvoorbeeld toegang krijgen tot berichten van een verdachte die via Telegram Messenger zijn verstuurd? Ook buiten coronatijd waren de ontwikkelingen rondom digitale opsporingsmiddelen overigens al in volle gang. In dit e-magazine komen twee van deze ontwikkelingen aan bod: het gebruik van drones en het gebruik van bodycams door de politie. Daarnaast bevat dit e-magazine een interview met mr. dr. Erik Gritter, universitair docent straf(proces)recht aan de Rijksuniversiteit Groningen en tevens onderzoeker op het gebied van cybercrime en nieuwe opsporingstechnieken.

Oftewel, een e-magazine boordevol interessante ontwikkelingen, des te meer voor de studenten die op dit moment de vakken Strafrecht 3 en Strafrecht en IT volgen. Ik wens u veel leesplezier toe!

Namens de redactiecommissie,

Sylvia Chan
Hoofdredacteur



Inhoudsopgave

Voorwoord	2
Telegram als spil bij cybercrime	4
Interview met mr. dr. Erik Gritter	10
Big Brother is watching you	15
Bodycams onder de loep	21

Cybercriminaliteit viert hoogtij dankzij de coronacrisis.¹ Naast een stijging in het aantal gevallen van cybercriminaliteit, weten criminelen met nieuwe tactieken in te spelen op de coronacrisis. Denk bijvoorbeeld aan oplichting via WhatsApp, waarbij criminelen zich voordoen als de zoon, dochter of goede vriend die, al dan niet vanwege de coronacrisis, dringend geld nodig heeft. Het betaalverzoek dat de crimineel vervolgens stuurt, is in werkelijkheid een phishinglink. Wanneer het slachtoffer de toegangscode van zijn of haar bankrekening invult, wordt deze automatisch doorgestuurd naar de crimineel. Op deze manier kan de crimineel toegang krijgen tot de bankrekening, het geld dat daarop staat overmaken naar andere bankrekeningen en het geld opnemen.²

Dit soort strafbare feiten worden veelal georganiseerd via de berichtendienst Telegram Messenger en ook de wapen- en drugshandel floreren op het platform.³ Zo worden er veel tips en gegevens over het uitvoeren van strafbare feiten gedeeld via het platform.⁴ De gratis berichtendienst Telegram is vergelijkbaar met



Bron: Folder 'Oplichting via WhatsApp: VIN-fraude', politie.nl, 20 oktober 2020.

WhatsApp, maar biedt bovenop de *end-to-end* encryptie,⁵ die beide diensten aanbieden, ook een zelfvernietigingsfunctie aan voor berichten om doorgifte te voorkomen. Tevens maakt Telegram gebruik van het veiligere – althans zo stelt Telegram – MTPROTO Protocol.⁶ Ook biedt Telegram de mogelijkheid om via een zoekfunctie lid te worden van verscheidene groepen. 'Swipe en Bonk',⁷ 'UTRECHT + OMGEVING HANDELS-GROEP 030' en 'The Hustlers Handelgroep' zijn

- 1 'Corona leidt tot geheel nieuwe vormen van criminaliteit', mr-online.nl, 15 januari 2021; E. Schurer, 'Explosieve stijging cybercrime in eerste helft 2020', vpngids.nl, 9 december 2020.
- 2 'Politie start campagne: voorkom oplichting via WhatsApp', rtlnieuws.nl, 15 oktober 2020; 'Grote toename phishing via hulpvraag op WhatsApp', rtlnieuws.nl, 25 januari 2021; Folder 'Oplichting via WhatsApp: VIN-fraude', politie.nl, 20 oktober 2020.
- 3 R. Roks & N. Monshouwer, 'F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger', *Justitiële Verkenningen* 2020/46, afl. 2, p. 51-52; 'Criminelen handelen op berichtenapp: 'Heb je geld? Ik heb een pistool voor 3k'', ad.nl, 10 augustus 2019.
- 4 R. Roks & N. Monshouwer, 'F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger', *Justitiële Verkenningen* 2020/46, afl. 2, p. 52-53.
- 5 Door end-to-end encryptie kunnen enkel de verzender en ontvanger van een bericht de inhoud hiervan inzien. Zelfs de aanbieder van de berichtendienst kan deze informatie niet inzien.
- 6 'Telegram FAQ: Security', telegram.org.
- 7 De term 'swipen' verwijst naar een manier om online producten te bestellen bij webshops en deze te laten leveren, zonder ervoor te betalen. De term 'bonken' verwijst naar het 'gooien' van geld op een bankpas om gestolen virtuele valuta om te zetten in contant geld door zogenaamde 'geldezels'. Zie R. Roks & N. Monshouwer, 'F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger', *Justitiële Verkenningen* 2020/46, afl. 2, p. 53.

enkele voorbeelden.⁸ Al deze functionaliteiten maken Telegram een aantrekkelijk platform voor criminelen om zich te organiseren. Voor de politie is het hierdoor echter lastig om toegang te krijgen tot berichten die via Telegram zijn verstuurd en deze te gebruiken als bewijs tegen een verdachte. De toegang tot het account van de verdachte kan namelijk beveiligd zijn met een wachtwoord en vanwege de *end-to-end* encryptie kan Telegram, ook al zouden ze daartoe bereid zijn, geen medewerking verlenen. Toch biedt het Wetboek van Strafvordering (hierna: Sv) mogelijkheden voor opsporingsambtenaren om beschikking te krijgen over de berichten.

In dit artikel bespreek ik twee opsporingsbevoegdheden op grond waarvan de politie toegang kan krijgen tot het account en de berichten van de verdachte: artikel 126ng Sv en artikel 126nba Sv. Artikel 126ng Sv betreft het vorderen van gegevens over een verdachte en het desbetreffende strafbare feit van de aanbieder van een communicatiedienst. Artikel 126nba Sv is ingevoerd met de Wet Computercriminaliteit III en betreft de bevoegdheid tot het binnendringen in een geautomatiseerd werk, oftewel 'terughacken'. Voor beide opsporingsbevoegdheden zal ik uiteenzetten aan welke voorwaarden moet worden voldaan alvorens van de bevoegdheid gebruik mag worden gemaakt. Daarna komt aan bod op welke manieren de bevoegdheden kunnen worden ingezet. Vervolgens worden beide bevoegdheden geïllustreerd aan de hand van het eerdergenoemde voorbeeld van online oplichting via Whatsapp in de zin van artikel

8 R. Roks & N. Monshouwer, 'F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger', *Justitiële Verkenningen* 2020/46, afl. 2, p. 47.

9 Artikel 126ng lid 1 en 2 jo. 181 Sv.

326 Wetboek van Strafrecht (hierna: Sr), waarbij de verdachte via Telegram informatie heeft uitgewisseld over de oplichting. Tot slot volgt een afweging met betrekking tot welke van beide bevoegdheden het beste kan worden gebruikt in de voorbeeldsituatie.

*"Zelfs wanneer de aanbieder o
voldoen aan de vordering, zoal
Telegram, kan de opsporingsk
grond van artikel 126ng Sv, zij
toegang tot de gegevens be*

Voorwaarden voor inzet opsporingsbevoegdheden

Artikel 126ng Sv

De inzet van artikel 126ng Sv als opsporingsbevoegdheid geschiedt op vordering van de officier van justitie en met machtiging van de rechter-commissaris. Dit is enkel rechtmatig wanneer aan vier voorwaarden wordt voldaan.⁹ Ten eerste mag de vordering van de gegevens geen betrekking hebben op gegevens die bestemd zijn voor of afkomstig zijn van de aanbieder van de communicatiedienst. Deze voorwaarde hangt samen met de tweede voorwaarde, namelijk dat de gegevens klaarblijkelijk afkomstig van de verdachte of voor hem bestemd moeten zijn. Ook moeten de gegevens betrekking hebben op de verdachte en het strafbare feit hebben gediend of klaarblijkelijk zelf betrek-

king hebben op het strafbare feit. Ten derde moet de opsporing zien op een misdrijf waarvoor voorlopige hechtenis is toegestaan op grond van artikel 67 lid 1 Sv en dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Tot slot dient sprake te zijn van een dringend onderzoeksbelang.

Ook niet wil of kan
s in het geval van
bevoegdheid op
het indirect, de
bepoelstelligen."

Artikel 126nba Sv

Ook de inzet van de opsporingsbevoegdheid op grond van artikel 126nba Sv dient te geschieden op vordering van de officier van justitie en met machtiging van de rechter-commissaris. Daarbij is de rechtmatigheid van de inzet afhankelijk van twee voorwaarden die vergelijkbaar zijn met die bij artikel 126ng Sv.¹⁰

Ten eerste moet de opsporing zien op een misdrijf waarvoor voorlopige hechtenis is toegestaan op grond van artikel 67 lid 1 Sv en dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, dan wel een feit waarop een gevangenisstraf van acht jaar of meer staat of bij AMvB aangewezen is. Van welk type misdrijf sprake moet zijn, is afhankelijk van het doel waarvoor de bevoegdheid wordt ingezet. De mogelijke doeleinden, ofwel toepassingen, van de bevoegdheid zullen hieronder besproken worden. Ten tweede dient sprake te zijn van een dringend onderzoeksbelang.

Mogelijke toepassingen van de opsporingsbevoegdheden

Artikel 126ng Sv

Op grond van deze opsporingsbevoegdheid kan de politie gegevens, zoals berichten, over een verdachte of het desbetreffende strafbare feit vorderen van de aanbieder van een communicatiedienst

waar de verdachte gebruik van heeft gemaakt. Deze gegevens kunnen zich namelijk op de server van de communicatiedienst bevinden. Wanneer de verdachte geen medewerking wil verlenen, kan deze bevoegdheid de politie de mogelijkheid bieden om toch toegang tot de gegevens te krijgen. Zelfs wanneer de aanbieder ook niet wil of kan voldoen aan de vordering, zoals in het geval van Telegram, kan de opsporingsbevoegdheid op grond van artikel 126ng Sv, zij het indirect, de toegang tot de gegevens bewerkstelligen.

In een uitspraak van rechtbank Rotterdam heeft de rechter namelijk aangenomen dat artikel 126ng lid 2 Sv in beginsel een voldoende grondslag biedt voor een opsporingsambtenaar om, op vordering van de officier van justitie en gemachtigd door de rechter-commissaris, in te loggen op het Telegram-account van de verdachte en op deze manier beschikking tot de berichten te krijgen. De verdachte in casu werd ervan verdacht malware¹¹ te hebben verspreid waarmee inloggegevens van onder andere bankrekeningen zijn verkregen, waarna geld is weggenomen van deze rekeningen.¹² Op het eerste gezicht lijkt het twijfelachtig of deze constructie van de officier van justitie wel rechtmatig is, aangezien zelf inloggen op het account wezenlijk verschilt van het vorderen van de gegevens via de aanbieder van de communicatiedienst. De rechter-commissaris heeft het verzoek van de officier van justitie in eerste instantie dan ook afgewezen, omdat de officier van justitie het verzoek tot machtiging enkel zou gebruiken ter verkrijging van de goedkeuring van de rechter-commissaris voor het inloggen op het account van de verdachte en niet voor het vorderen van de gegevens via de aanbieder. De rechter-commissaris is van oordeel dat deze werkwijze zijn bevoegdheid op grond van artikel 177 Sv te buiten gaat. Met andere woorden: de rechter-commissaris kan geen onderzoek opdragen aan een opsporingsambtenaar waarvoor deze laatste niet bevoegd is op grond van de wet. Daarnaast is de rechter-commissaris van oordeel dat een doorzoeking van het Telegram-account van de verdachte zonder rechtshulpverzoek niet

¹⁰ Artikel 126nba lid 1 jo. 181 Sv.

¹¹ Software om onder meer phishing mee te bewerkstelligen.

¹² Rb. Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712; artikel 126ng lid 4 jo. 177 jo. 181 Sv.

is toegestaan, omdat deze gegevens zich hoogstwaarschijnlijk op buitenlandse servers bevinden.¹³ De officier van justitie is daarop in hoger beroep gegaan tegen deze beslissing en is daarin door de rechter in het gelijk gesteld.¹⁴

De rechter motiveert deze beslissing grotendeels aan de hand van de wetsgeschiedenis. Bij het opstellen van artikel 126ng Sv is namelijk beoogd om de inzet van de bevoegdheid te toetsen aan de beginselen van proportionaliteit en subsidiariteit en daarmee de grondrechten van de gebruiker van de communicatiedienst te beschermen. Wanneer is voldaan aan de eerdergenoemde voorwaarden voor de inzet van de bevoegdheid is dus ook voldaan aan de proportionaliteits- en subsidiariteitstoets. De rechter is van oordeel dat er in de onderhavige zaak is voldaan aan de voorwaarden en acht de inbreuk op de grondrechten van de verdachte met name gerechtvaardigd vanwege de essentiële rol van het betalingsverkeer in de samenleving en het vertrouwen dat de burger in de veiligheid van financiële- en communicatie dienstverlening moet kunnen hebben.¹⁵

Nu de wetgever met name de belangenafweging tussen het belang van het onderzoek en de grondrechten van de gebruiker voor ogen heeft gehad, is de vorm waarin deze inbreuk, dan wel verstrekking van gegevens plaatsvindt, naar het oordeel van de rechter van ondergeschikt belang. Zowel het inloggen op het Telegram-account van de verdachte als de vordering van de gegevens via de aanbieder leveren een inbreuk op de vertrouwelijkheid van het berichtenverkeer op. Dat deze inbreuk plaatsvindt door in te loggen op het account acht de rechter dus niet van belang voor de rechtmatigheid van deze onderzoekshandeling. Daarbij noemt de rechter nog de omstandigheid dat de wetgever geen re-

kening heeft kunnen houden met de (gevolgen van de toepassing van) *end-to-end* encryptie. Vanwege deze veiligheidsmaatregel kan aanbieder Telegram de berichten niet in leesbare vorm verstrekken aan anderen en is inloggen op het account van de verdachte dus de enige optie.¹⁶

Tot slot heeft bij de beslissing van de rechter meegespeeld dat de Wet Computercriminaliteit III ten tijde van de uitspraak bijna in werking zou treden.¹⁷ Deze wet heeft een aantal bijzondere opsporingsbevoegdheden toegevoegd aan het Wetboek van Sv, waaronder de bevoegdheid tot 'terughacken' die onder de volgende kop besproken zal worden. Deze bevoegdheden zijn nog veel verstrekkender dan het inloggen op het account van de verdachte en het zou mede daarom niet in verhouding staan tot de nieuwe bevoegdheden om het inloggen als onrechtmatig aan te merken.¹⁸

Artikel 126nba Sv

Deze bepaling geeft een opsporingsambtenaar de bevoegdheid om binnen te dringen in een geautomatiseerd werk dat bij de verdachte in gebruik is.¹⁹ 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. Hieronder valt bijvoorbeeld een smartphone of computer, maar ook een usb-stick die in het apparaat zit of *internet of things*-voorwerpen.²⁰ Geautomatiseerde werken van derden kunnen ook onder de reikwijdte van artikel 126nba Sv vallen, nu de bepaling spreekt van een geautomatiseerd werk dat bij de verdachte *in gebruik* is. Eigendom over het geautomatiseerde werk is derhalve niet vereist. Wat betreft het 'binnendringen' heeft de wetgever aansluiting gezocht bij het delict com-

13 Rb. Rotterdam 10 december 2018, ECLI:NL:RBROT:2018:10895, r.o. 2.3-2.5 en 2.8.

14 Rb. Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712.

15 Rb. Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712.

16 Rb. Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712.

17 De Wet Computercriminaliteit III is in werking getreden per 1 maart 2019.

18 Rb. Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712.

19 Artikel 126nba lid 1 Sv.

20 B.W. Newitt, 'Wet Computercriminaliteit III', *Tijdschrift voor Sanctierecht & Onderneming*, 2019/1, p. 29; Artikel 80sexies Sr.

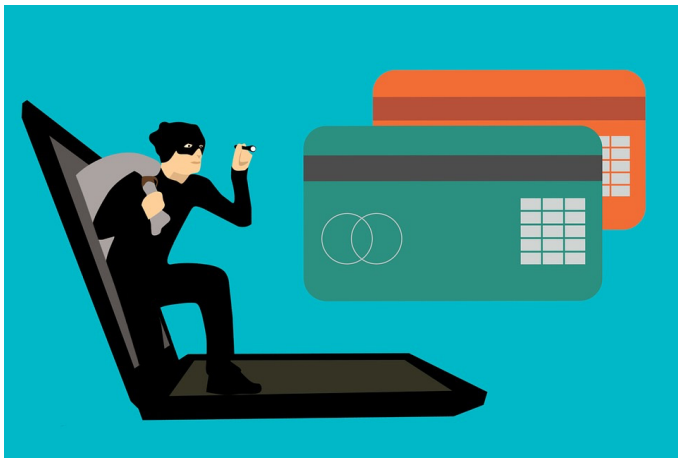
putervredebreuk, oftewel 'hacken'.²¹ Op grond van deze bepaling is in ieder geval sprake van binnendringen, indien de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.²²

Eerder is al aan de orde gekomen dat het vereiste type misdrijf afhankelijk is van het doel waarvoor de bevoegdheid wordt ingezet. Het binnendringen in een geautomatiseerd werk wordt binnen artikel 126nba Sv namelijk onderverdeeld in verschillende gradaties. Zo mag voor een feit waarvoor voorlopige hechtenis is toegestaan worden gehackt met het oog op de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit. Ook mag gehackt worden met als doel gegevens te tappen of een persoon stelselmatig te observeren. Voor misdrijven waarvoor een gevangenisstraf van acht jaar of meer staat, of misdrijven die zijn aangewezen bij het Besluit onderzoek in een geautomatiseerd werk,²³ mag worden gehackt met het oogmerk gegevens die op het geautomatiseerde werk zijn opgeslagen te doorzoeken en te kopiëren, alsmede gegevens ontoegankelijk te maken. Onder dit laatste valt bijvoorbeeld het verstoren van een DDoS-aanval.²⁴

De onderzoekshandelingen die op grond van artikel 126nba Sv verricht kunnen worden gaan dus een stuk verder dan de handelingen waar een opsporingsambtenaar op grond van artikel 126ng Sv toe bevoegd is.

Toepassing op casus

Het in de inleiding genoemde voorbeeld van phishing via WhatsApp, waarbij de organisatie via Telegram plaatsvindt, kan worden aangemerkt als oplichting.²⁵ Dit is een strafbaar feit waarvoor een gevangenisstraf van vier jaar of meer staat en derhalve is voorlopige hechtenis toegestaan op grond van artikel 67 lid 1 sub a Sv. Wanneer ook aan de overige vereisten van een ernstige inbreuk op de rechtsorde en het bestaan van een dringend onderzoeksbelang is voldaan, kan de officier van justitie dus op grond van artikel 126ng Sv vorderen dat op het Telegram-account van de verdachte wordt ingelogd en zo beschikking wordt verkregen over de berichten met betrekking tot het strafbare feit. Ook een vordering krachtens artikel 126nba Sv behoort tot de mogelijkheden, zij het dat op basis van deze bevoegdheid in beginsel enkel vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, het tappen van gegevens en stelselmatige observatie van een persoon is toegestaan. Het gebruiken van malware (artikel 139d lid 1 Sr) staat echter opgenomen in artikel 2 Besluit onderzoek in een geautomatiseerd werk. Wanneer de oplichting dus gepaard gaat met het verspreiden van malware, zoals vaak het geval is bij phishing, dan mogen de gegevens die opgeslagen zijn op het geautomatiseerde werk ook worden doorzocht en gekopieerd door de opsporingsambtenaar, alsmede ontoegankelijk gemaakt. Beide bevoegdheidsgrondslagen bieden dus de mogelijkheid om beschikking te krijgen over de berichten van de verdachte en op grond van artikel 126nba Sv kunnen tevens verdergaande onderzoekshandelingen worden verricht.



21 *Kamerstukken II* 2015/16, 34372, 3, p. 15 (MvT).

22 Artikel 138ab lid 1 Sr.

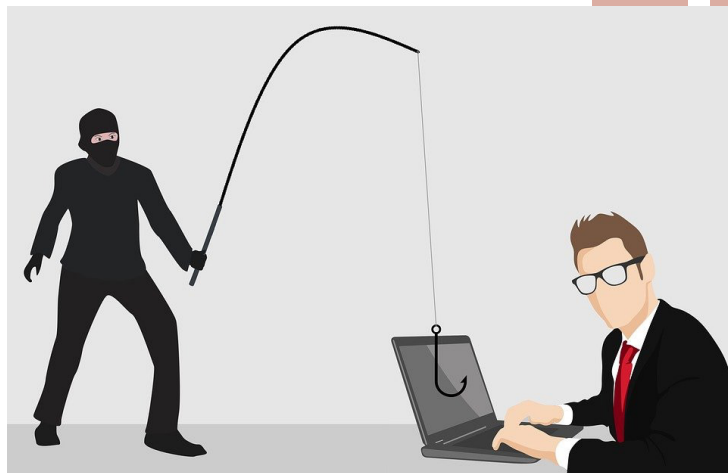
23 *Stb.* 2018, 340.

24 Bij een Distributed Denial of Service (DDoS)-aanval worden grote hoeveelheden data tegelijkertijd naar een server gestuurd, waardoor de server tijdelijk slecht bereikbaar is of zelfs offline gaat; Artikel 126nba lid 1 Sv; B.W. Newitt, 'Wet Computercriminaliteit III', *Tijdschrift voor Sanctierecht & Onderneming*, 2019/1, p. 30.

25 Artikel 326 lid 1 Sr.

Conclusie

In dit artikel zijn twee opsporingsbevoegdheden besproken aan de hand waarvan een opsporingsambtenaar beschikking kan krijgen over Telegram-berichten die een verdachte heeft ontvangen of verstuurd met betrekking tot het plegen van fraude via WhatsApp. De weg van artikel 126ng Sv is daarbij minder voor de hand liggend en is in de rechtspraak tot stand gekomen door middel van een grotendeels wetshistorische interpretatie door de rechter. Met de invoering van Wet Computercriminaliteit III is de relevantie van deze 'omweg' in bepaalde mate verloren gegaan, nu artikel 126nba Sv specifiek voorziet in de bevoegdheid tot 'terughacken'. In de voorbeeldsituatie zijn beide bevoegdheden toepasbaar, maar verdient de bevoegdheid uit artikel 126nba Sv de voorkeur, nu deze voor de delicten genoemd in het Besluit onderzoek in een geautomatiseerd werk verdergaande vormen van onderzoek mogelijk maakt, waaronder het ontoegankelijk maken van gegevens. Hiermee zouden strafbare feiten zoals phishing niet alleen opgespoord kunnen worden, maar ook voorkomen. Wel zou de bevoegdheid voortvloeiend uit artikel 126ng Sv nuttig kunnen blijven bij het onderzoek naar verdenkingen van strafbare feiten waarbij voorlopige hechtenis is toegestaan, maar welke niet in het Besluit onderzoek in een geautomatiseerd werk zijn opgenomen. Artikel 126ng Sv biedt dan immers de bevoegdheid om beschikking over de gegevens te verkrijgen, waar artikel 126nba Sv enkel voorziet in de bevoegdheid tot vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, het tappen van gegevens of stelselmatige observatie van een persoon. Daarbij is het wel nog maar de vraag of het blijven gebruiken van de 'omweg' is toegestaan binnen het systeem van de wet, nu het met Wet Computercriminaliteit III ingevoerde artikel 126nba Sv specifiek ziet op het verkrijgen van toegang tot het systeem van de verdachte, in tegenstelling tot artikel 126ng Sv.





Interview met **mr. dr. Erik Gritter**

Kunt u zich kort voorstellen aan de lezers?

Mijn naam is Erik Gritter. Ik ben universitair docent straf(proces)recht. Ik ben eigenlijk al een behoorlijke tijd werkzaam bij de vakgroep. Vrij kort na mijn studie (privaatrecht en strafrecht) ben ik daar terechtgekomen. Eerst gedetacheerd via de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) om een proefschrift te schrijven en na vier jaar kreeg ik een tijdelijke aanstelling als universitair docent straf(proces)recht. In de tussentijd, in 2003, ben ik gepromoveerd en enige jaren daarvoor ben ik in vaste dienst gekomen. Vanuit die positie heb ik mij als universitair docent en onderzoeker verder ontplooid.

"Mijn dagen zijn gevuld met onderwijs en onderzoek, zoals een universitair docent dat betaamt."

Aanvankelijk heb ik mij gespecialiseerd in het materieel strafrecht en het strafrecht binnen rechtspersonen, denk bijvoorbeeld aan het functioneel ouderschap. Dat is een deel van mijn specialisa-

tie geworden. Tegenwoordig verdiep ik mij ook in cybercrime en het gebruik van nieuwe technieken in de opsporing. Cybercrime sluit mooi aan bij de opsporing, waar ik mij overigens ook reeds veel mee bezig hield.

Welke onderzoeken verricht u dan zoal?

Op dit moment richten mijn onderzoeken zich voornamelijk op opsporing, cybercrime, het onderzoeken van inbeslaggenomen smartphones en het decryptiebevel.

Wist u altijd al dat u zich wilde specialiseren in het strafprocesrecht?

Eigenlijk wist ik dat al vrij snel. Wel heb ik een 'blauwe maandag' economie gestudeerd. Een vriend van mij destijds studeerde rechten en ik keek wel eens in zijn dikke studieboeken over bijvoorbeeld staatsrecht. Dit trok mij erg aan en zo kwam ik uiteindelijk na een overstap bij de studie rechten terecht aan de Rijksuniversiteit. Ook ben ik al snel bij Simon van der Aa terechtgekomen, de studievereniging voor strafrecht en criminologie. Ik heb daar ook in de redactiecommissie gezeten voor het verenigingsblad Asega. Naast strafrecht heb ik ook privaatrecht gedaan, omdat het des-

tijds (de jaren 90, red.) werd geadviseerd er nog een richting naast te doen om je iets breder te oriënteren. Ik weet eigenlijk niet of dat nu echt nodig is. Wat je qua kennis mist bij een bepaalde studierichting leer je gaandeweg wel weer bij een andere richting. Bovendien ontwikkel je algemene juridische vaardigheden die overal van pas komen, ondanks dat je een andere studierichting binnen het recht hebt gedaan.

Dan nu meer over het thema van dit e-magazine. Wat vindt u van de toenemende 'digitale' opsporingsmiddelen en -bevoegdheden? Vindt u dit een gelukkige ontwikkeling?

Uiteindelijk is dat een hele goede ontwikkeling natuurlijk. Qua opsporing moet je als politie en justitie wel blijven. Je kunt niet denken: "Het is allemaal te ingewikkeld, ik negeer het maar". Integendeel, het is de realiteit en de politie moet veel nieuwe dingen leren, net als wij. Je kunt niet achterblijven. Bovendien wil je als politie en justitie eigenlijk altijd een stap voor zijn. Het is in ieder geval goed dat de politie aandacht schenkt aan *smishing* (sms-phishing, red.) en andere cybercrime.

En stelt u zich voor, de politie treft bij een onderzoek naar kinderporno bij de opsporing allemaal kundig versleutelde *harddisks* aan met materiaal. Als je dan de kennis of de bevoegdheden niet hebt, kun je er dan niks mee als politie. Vanuit de wetgever kan er dan een nieuwe bevoegdheid ontstaan voor politie en justitie, zoals bijvoorbeeld de bevoegdheid tot 'terughacken' die ingevoerd is met de Wet Computercriminaliteit III.

De wetgever loopt bovendien eigenlijk altijd wel achter. Men kan denken: we zijn redelijk *up-to-date*, maar ondertussen zijn er allerlei ontwikkelingen op technisch vlak. Het kan dan zijn dat je over een paar jaar weer achterloopt. Die ontwikkelingen zijn wel erg interessant. De vraag of je bevoegdheden techniekneutraal kunt formuleren is ook een interessante. Je kunt niet in de toekomst kijken. Toen ik studeerde, moest ik mijn verslagen nog op papier inleveren. Nu is dat anders. Toen kon je niet weten hoe het er nu allemaal uitziet. Dat is ook zo met ontwikkelingen binnen het

recht.

Bent u van mening dat we naar een 'surveillance maatschappij' neigen met de nieuwe bevoegdheden, zoals terughacken, en als deze vaker worden toegepast?

Dat is een lastige vraag. Enerzijds, voor een bevoegdheid zoals het terughacken, ligt de drempel redelijk hoog. Er moet sprake zijn van de verdenking van een feit waarbij voorlopige hechtenis is toegestaan en er moet meer aan de hand zijn, namelijk een vrees voor een ernstige inbreuk op de rechtsorde. Bovendien moet de inzet van een bevoegdheid altijd de toets van proportionaliteit en subsidiariteit doorstaan. Als inbeslagname van een gegevensdrager niet lukt, dan vind ik terughacken wel legitiem.

Anderzijds moet men wel oppassen voor de surveillance op zich als bijvoorbeeld overal camera's hangen. Ter illustratie een overdreven voorbeeld: China. Als je daar bij wijze van spreke één keer door rood rijdt, wordt je al aangehouden en worden allemaal toeslagen stopgezet. Dat gaat natuurlijk veel te ver, maar de kern is dat je de privéruimte moet bewaren. De afweging van privacy tegenover veiligheid is een lastige discussie, maar ook een interessante. Ik kan mij bijvoorbeeld uit mijn studententijd herinneren dat er een grote discussie was, omdat er camera's bij de Grote Markt werden opgehangen. Er waren toen ook veel protestgeluiden, maar wat bleek? Uiteindelijk kwamen er berichten in de krant dat de politie, door de camera's, tijdig kon ingrijpen bij incidenten. Toen bleek dat de camera's dus ook bij kunnen dragen aan de veiligheid. Nu worden camera's (onder andere op de Grote Markt) geaccepteerd.

De vraag is of de beelden in goede handen zijn, of er op de juiste wijze mee om wordt gegaan en of je die gegevens ook mag delen. Dan komen wij juristen natuurlijk in het spel. Een voorbeeld waar het mis is gegaan betreft het bericht waaruit blijkt dat het Centraal Orgaan opvang Asielzoekers (COA) jarenlang onrechtmatig gegevens had gedeeld met de politie. Het zal een afweging zijn van klassieke grondrechten enerzijds en gegevensbescherming anderzijds.

In dit interview willen we ook graag aandacht besteden aan het onderzoeken van smartphones door opsporingsambtenaren. Heeft u enkele voorbeelden van het onrechtmatig onderzoeken van smartphones in het licht van het arrest Onderzoek Smartphone?

De jurisprudentie is als volgt opgebouwd. Het onderzoeken van een inbeslaggenomen smartphone door een opsporingsambtenaar is toegestaan, mits er sprake is van een beperkte inbreuk op de privacy van verdachte. Een inbreuk, wel beperkt, is dus toegestaan. Een inbreuk is beperkt bij het raadplegen van een gering aantal gegevens. De inbreuk zal meer dan beperkt zijn, indien min of meer een compleet beeld is verkregen van bepaalde aspecten van het privéleven van de verdachte.

Echter, waar de grens ligt, is sterk casuïstisch. Wel geeft de Hoge Raad handvatten, zoals hij vaker doet in arresten binnen het straf(proces)recht. Als het gaat om handmatig een smartphone doorscrollen en er een beperkte inbreuk op de privacy is dan zal het mogen, maar als een smartphone door middel van software helemaal wordt leeggetrokken is het verhaal anders.

Je moet eigenlijk steeds denken aan het eindresultaat: leidt het onderzoek tot een min of meer compleet beeld van bepaalde aspecten van het privéleven van de verdachte? Handmatig scrollen door een smartphone van verdachte kan ook een min of meer compleet beeld geven en met software kun je bijvoorbeeld ook slechts één app leegtrekken. Het min of meer complete beeld van de verdachte moet men trouwens ook niet zonder nuance nemen; het complete beeld kan breed zijn, maar ook ten aanzien van één aspect, bijvoorbeeld enkel iemands uitgaansleven. Er zijn dus meerdere lagen. Het onderzoek moet je daarom niet in hokjes plaatsen. Het is lastig te beoordelen. Er zal nog meer jurisprudentie moeten loskomen. Vaststaat in ieder geval, zoals gezegd, dat

“Het onderzoeken van een inbeslaggenomen smartphone door een opsporingsambtenaar is toegestaan, mits er sprake is van een beperkte inbreuk op de privacy van verdachte.”

de Hoge Raad geen vaste regels geeft. Alleen een kader met buitengrenzen. Het hangt af van de omstandigheden van het geval. Wel is het Smartphone-arrest het uitgangspunt.

Acht u het denkbaar dat de politie, op basis van art. 126nba e.v. Sv, op afstand telefoons of Telegram-groepen waarin illegale handel plaatsvindt gaat terughacken?

Ik kan mij goed voorstellen dat dit binnen art. 126nba Sv past. Helemaal als het gaat om georganiseerde wapenhandel lijkt het me in ieder geval goed logisch dat het kan. Wel moet elke bevoegdheid die wordt ingezet voldoen aan de maatstaven van proportionaliteit en subsidiariteit. Bovendien is een bevel van de Officier van Justitie en een machtiging van de Rechter-Commissaris nodig. Er is dus een dubbele zekering.

Er wordt weleens gezegd dat het onderzoeken van smartphones al snel uit de hand kan

lopen en dat daar nog niet echt een oplossing voor is. Hoe staat u daar in?

Hiervoor moet je weer terug naar de normen van de Hoge Raad, maar je moet ook een blik werpen op de praktijk. De opsporingsambtenaar die een smartphone in beslag neemt, moet een afweging kunnen maken. Hij moet kunnen inschatten hoe ver hij kan gaan. Als hij in de normen van de Hoge Raad te ver gaat, zal een rechter dat uiteindelijk beoordelen. Hij kan dan sancties opleggen.

Aan de andere kant, de drempel voor zware sancties ligt wel hoog. Er is discussie over de vraag in hoeverre dit normerend werkt. Als je in het kader van de sanctionering van vormverzuimen enkel constateert dat er onrechtmatig is gehandeld, dan hoop je maar dat er in het vervolg beter wordt gehandeld.

Dat die onderzoeken snel uit de hand kunnen lopen en dat er nog niet echt een oplossing voor is,

is wellicht een zwakte in het systeem. Een oplossing daarvoor kan zijn dat een opsporingsambtenaar eerst naar de Officier van Justitie moet gaan om te vragen in hoeverre de telefoon onderzocht mag en moet worden. Bovendien zijn de grenzen voor onderzoeken wat vloeierend. Je kunt de onderzoeken niet in beton gieten of in hokjes plaatsen. Zelf heb ik in dit verband wel gepleit voor een grotere rol van de hulpofficier van Justitie.

Naast het onderzoeken van smartphones willen we het in dit interview ook graag hebben over drones als opsporingsmiddel. Wat is precies de wettelijke grondslag voor drones als opsporingsbevoegdheid? Hangt deze grondslag ook af van het doel waarvoor de drone wordt ingezet?

Het voorbeeld van drones is erg interessant en aansprekend om het wettelijke stelsel te schetsen. Tien jaar geleden zou je je drones niet eens kunnen voorstellen en bedenken dat zo'n ding de lucht in gaat met een camera.

De algemene taakstellende bepalingen in art. 3 Politiewet 2012 en art. 141 Sv vormen de algemene bevoegdheidsgrondslag. Als je binnen de grenzen van die bepalingen blijft, voldoe je ook aan het legaliteitsbeginsel (art. 1 Sv en art. 8 EVRM). De inzet van drones, conform de maatstaven van de taakstellende bepalingen en de Hoge Raad, is toegestaan mits er slechts sprake is van een beperkte inbreuk op de privacy. Is er een meer dan beperkte inbreuk, dan voldoen de algemene taakstellende bepalingen niet meer.

Als je gedurende lange tijd een drone in de lucht laat hangen ter observatie van iemand voldoen de algemene taakstellende bepalingen ook niet meer, omdat dan moet worden voldaan aan art. 126g Sv (stelselmatige observatie) wegens het verkrijgen van een min of meer compleet beeld van het privéleven van de verdachte. Bij het mastervak Strafrecht en IT noem ik nog meer technieken waarbij deze kwestie speelt, zoals peilbakens onder auto's. Deze kwestie met camera's kan ook worden geïllustreerd aan de hand van de bodycams die opsporingsambtenaren niet zelden dragen, bijvoorbeeld tijdens oud en nieuw. Dat kan ook op basis

van art. 3 Politiewet 2012, mits er sprake is van een beperkte inbreuk op de privacy. Dat betekent ook dat je de bodycam niet aan mag hebben als je met een politieteam het huis van een verdachte binnenstapt. Er zal dan namelijk al snel een meer dan beperkte inbreuk op de privacy zijn.

Overigens is er ook nog de Wet Politiegegevens die eisen stelt aan hoelang beelden bewaard mogen worden. Dat is eveneens een lastig privacyaspect en betreft de zogenaamde informatieve privacy.

Worden drones al vaak door de politie gebruikt?

Op dit moment nog niet heel erg, heb ik het idee. Wel heeft de politie plannen om dat meer te gaan doen en het 'drone-arsenaal' uit te breiden. Echter, er zijn tegenwoordig drones die zo hoog kunnen vliegen dat je ze niet ziet. Misschien zien we dus zelfs niet eens of ze aan het experimenteren zijn.

Denkt u dat er ook vaker gebruik zal worden gemaakt van drones met een warmtecamera?

Ja, zeker. Er zal doorgaans sprake zijn van een minder grote privacyinbreuk, zo stelt ook de Hoge Raad. Wel is dit afhankelijk van de duur en de intensiteit van het gebruik. Mobiele warmtecamera's worden al voor de opsporing van hennepkwekerijen gebruikt, dus het is goed mogelijk dat drones daar een rol in gaan spelen. De inzet van zulke warmtecamera's is toegestaan, mits er sprake is van een beperkte inbreuk op de privacy. Als je het drie maanden lang stelselmatig en preventief gaat toepassen, dan wordt het mogelijk lastig, maar drones met een warmtecamera kortstondig inzetten om een anonieme tip te verifiëren is goed mogelijk. Onder andere in afgelegen plattelandsgebieden, waar niet zelden kwekerijen of drugslaboratoria worden aangetroffen, kan dit een uitstekend middel zijn.

Denkt u dat het gebruik van drones met warmtecamera's zich vooral zal voordoen om te kijken of ergens een hennepkwekerij is? Of kan het bijvoorbeeld ook worden gebruikt om te kijken hoeveel personen zich in een huis bevinden?

Ja, voornamelijk in de zin van hennepkwekerij-

en, maar wellicht worden zulke drones of camera's ook wel gebruikt bij de instap van een woning. Of als er bijvoorbeeld een (terroristische) dreiging is en de politie weet de locatie van de dreiging, maar niet hoeveel personen zich in een pand bevinden, dan kan ik me voorstellen dat de algemene taakstellende bepalingen de grondslag kunnen zijn voor het inzetten van zulke drones voor tactische doeleinden.

Wat is volgens u voor de rest de kracht of potentie van drones als opsporingsmiddel? Wat voegt het precies toe?

Het kan een mooi middel zijn om op afstand informatie te vergaren. Niet om informatie te vergaren om het informatie vergaren, maar bijvoorbeeld om een anonieme tip te verifiëren. Stel, een opsporingsambtenaar heeft dan die drone of camera niet, dan zou hij gaan binnentreden en dan is de kans dat hij te ver gaat ook weer aanwezig. Een warmtecamera, al dan niet bevestigd aan een drone, kan dan een uitkomst zijn. Zoals gezegd is de drone in afgelegen plattelandsgebieden ook een goed middel om bij een anonieme tip over een kwekerij te kijken of er wel of niet iets aan de hand is.

Wat zijn de voornaamste tegengeluiden?

Voornamelijk *privacy* en *privacy concerns*: het idee dat je bekeken kunt worden. Ook het idee dat je niet weet wat er precies aan de drone bevestigd is, zoals misschien wel een richtmicrofoon, voor zover dat technisch mogelijk is, of dus een camera. Daarnaast speelt ook het feit dat je misschien niet eens weet of je bespied wordt of niet. Ik denk dat dat de voornaamste tegengeluiden zijn. De inzet van drones moet wel transparant blijven en er moeten goede protocollen voor zijn, die op hun beurt ook weer transparant zijn.

Als afsluiter, wat zou u studenten nog graag willen meegeven?

Om met de anekdote te beginnen: ik werk nu meer dan 25 jaar met veel plezier als docent en onderzoeker op het terrein van het strafrecht. Een vak dat nooit saai wordt. Een baan met nog steeds veel uitdagingen die heel goed bij me past. Ik heb over veel strafrechtelijke aspecten gepubliceerd

en ben gepromoveerd. Maar mijn eerste ervaringen met het rechtenonderwijs waren rampzalig. Dramatisch. Ik heb destijds mijn propedeuse Economie nooit kunnen halen, omdat ik maar niet kon slagen voor het eerstejaarsvak 'Recht.' Keer op keer haalde ik een 4 of een 5. Misschien lag het aan de toetsvorm: de tentamens waren multiple choice tentamens. Toch had de materie, veel meer dan de economie zelf, mijn hevige interesse. Ik ben dan ook rechten gaan studeren, in twee richtingen met de toen nog bestaande aantekening advocatuur. Slechts één vak hoefde ik te herkennen. Dat was het vak Zakenrecht en vertegenwoordiging, waarvoor ik eerst een 5 kreeg maar in de tweede kans een 8. Ik ben heel blij dat ik me niet heb laten ontmoedigen!

Misschien houdt mijn 'advies' daar wel mee verband. Kies de studie en de richting waar je blij van wordt. Hou een *open mind* en blijf nieuwsgierig – zeker op latere leeftijd, in een steeds sterker veranderende wereld. Blijf jezelf ontwikkelen, ook op heel andere vlakken, en bedenk, zeker als jurist: denk nooit dat je 'klaar bent' en alles weet. Als het begrip 'life long learning' ergens op van toepassing is, dan is dat de rechtspraktijk en de rechtswetenschap.

Wij als redactiecommissie willen mr. dr. Erik Gritter van harte bedanken voor zijn bijdrage!

Big Brother is watching you

Art. 3 Politiewet 2012 jo. art. 141 Sv als grondslag voor het gebruik van drones als opsporingsmiddel

Geschreven door Bart Pastoor



Big Brother is watching you, aldus George Orwell. Privacy is tegenwoordig een veel besproken onderwerp binnen het recht en de samenleving. Vreemd is dat niet. In de wereld van het recht wordt grote waarde gehecht aan het recht op privacy. Dit recht is als grondrecht onder meer neergelegd in art. 10 Grondwet, art. 8 van het Europees Verdrag voor de Rechten van de Mens en art. 7 en art. 8 van het Handvest van de Grondrechten van de Europese Unie. De bescherming van privacy als grondrecht werkt horizontaal, maar ook verticaal. Burgers onderling mogen geen inbreuk maken op de rechten van een ander, maar ook de overheid mag, in beginsel, de privacy van burgers niet schenden. In beginsel, want onder omstandigheden mogen politie en justitie bij de opsporing van strafbare feiten de privacy van verdachten in bepaalde mate schenden.

In dit artikel staat deze inbreuk op de privacy van burgers, dan wel verdachten, door politie en justitie centraal. Dit wordt bekeken in het licht van de ontwikkeling binnen de politie om haar drone-arsenaal uit te breiden en deze drones vaker in te zetten.¹ 'Met deze uitbreiding neemt het risico op schendingen van privacy toe,' zo vreest Bart Schermer, universitair hoofddocent privacyrecht aan de Universiteit Leiden.² Dit doet de vraag rijzen onder welke omstandigheden de inbreuk op privacy als gevolg van het inzetten van drones als opsporingsmiddel rechtmatig is op grond van de algemene taakstellende bepalingen³ voor de politie: art. 3 Politiewet 2012 (hierna: Polw 2012) jo. art. 141 Wetboek van Strafvordering (hierna: Sv). In dit artikel wordt antwoord gegeven op deze vraag. Eerst zal gekeken worden naar de wettelijke grondslag op grond waarvan opsporingsambtenaren, onder omstandigheden, de privacy van verdachten mogen schenden en in welke mate dit is toegestaan. Deze grondslag zal worden afgezet tegen de omstandigheden waaronder een inbreuk rechtmatig is aan de hand van jurisprudentie. Daarna zal het voorgaande worden toegespitst op de inzet van drones als opsporingsmiddel.

Wettelijke grondslag voor de inbreuk

In de jurisprudentie is aanvaard dat art. 3 Polw 2012 en art. 141 Sv voldoende grondslag bieden voor de inzet van onderzoeksmethoden, opsporingsmethoden en alle handelingen die daarvoor in redelijkheid nodig zijn.⁴ Dit betekent ook dat er een

1 S. Keukenkamp, 'Met de groei van de blauwe dronevloot, neemt ook het aantal vragen over de privacy toe,' 20 november 2020, te vinden op trouw.nl (laatst geraadpleegd op 24 januari 2021).

2 S. Keukenkamp, 'Met de groei van de blauwe dronevloot, neemt ook het aantal vragen over de privacy toe,' 20 november 2020, te vinden op trouw.nl (laatst geraadpleegd op 24 januari 2021).

3 Zo omschrijven Ashouwer en Geurts, F.A.W. Ashouwer en J. Geurts, 'Strafvordering en technologische vooruitgang: de GPS-tracker,' *TPWS* 2017/30.

4 Zie onder meer HR 19 december 1995, ECLI:NL:HR:1995:ZD0328 (*Zwolsman*); HR 1 juli 2014, ECLI:NL:HR:2014:1562 (*IMSI-Catcher*); HR 1 juli 2014, ECLI:NL:HR:2014:1563 (*Stealth Sms*); HR 1 juli 2014, ECLI:NL:HR:2014:1569 (*Stille Sms*); HR 18 april 2017, ECLI:NL:HR:2017:725.

inbreuk gemaakt mag worden op de grondrechten (in het bijzonder de privacy) van verdachten. Dit mag echter niet onbeperkt of zonder grenzen. Er mag volgens de Hoge Raad namelijk niet een meer dan beperkte inbreuk zijn op de grondrechten van een verdachte.⁵ Deze opvatting is, sinds 1995, door de Hoge Raad in stand gehouden.

In het arrest Stille Sms uit 2014 hanteert de Hoge Raad een gelijksoortige opvatting en stelt hij zich op het standpunt dat de algemene taakstellende bepalingen voldoende grondslag bieden voor zover er sprake is van "een wijze die een beperkte inbreuk maakt op grondrechten van burgers en die niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing."⁶ Met deze overweging sluit de Hoge Raad aan bij de parlementaire geschiedenis.⁷ In 2017 voegt de Hoge Raad aan deze opvatting toe dat er voor het inzetten van een bevoegdheid op grond van art. 3 Polw 2012 nog geen verdenking ex art. 27 Sv is vereist.⁸

Omdat er sprake is van een wettelijke grondslag, is hiermee in de woorden van de Hoge Raad ook voldaan aan het strafvorderlijke legaliteitsbeginsel ex art. 1 Sv, zo schrijven Ashouwer en Geurts.⁹ Dit betekent ook dat niet alle opsporingshandelingen van opsporingsambtenaren dienen te berusten op een specifieke grondslag uit het Wetboek van Sv. Bij een beperkte inbreuk op de grondrechten van een verdachte volstaan de algemene taakstellende bepalingen van art. 3 Polw 2012 en art. 141 Sv. Wordt er een meer dan beperkte inbreuk gemaakt, dan is een specifieke grondslag uit het Wetboek van Sv nodig of een andere toereikende bijzondere wet. De vraag die dan rijst is wanneer er sprake is van een beperkte inbreuk op, in het bijzonder, de privacy van een verdachte. Met andere woorden: onder welke omstandigheden is de inbreuk op privacy nog rechtmatig en niet meer dan beperkt?

Inbreuk: onder welke omstandigheden rechtmatig?
Zoals gezegd is een inbreuk op de privacy van een verdachte toegestaan, mits deze inbreuk beperkt is, zo blijkt uit onder meer het arrest Stille Sms.¹⁰ De Hoge Raad merkt in het arrest Stille Sms op dat in het bijzonder de toepassing van een bepaalde opsporingsmethode jegens verdachten of betrokkenen onrechtmatig kan zijn "indien zij in verband met de duur, intensiteit en frequentie ervan geschikt is om een min of meer compleet beeld te verkrijgen van bepaalde aspecten van het persoonlijk leven van de betrokkene."¹¹ Met andere woorden: in die gevallen zal er een meer dan beperkte inbreuk zijn op de grondrechten van verdachte. De Hoge Raad geeft hier een algemene regel die als handvat kan dienen bij de beoordeling of een inbreuk rechtmatig dan wel onrechtmatig is. Omdat deze maatstaf op zichzelf nadere invulling behoeft, zal ik twee arresten bespreken om te concretiseren onder welke omstandigheden de inbreuk op privacy van verdachte dan wel betrokkene rechtmatig is. Opmerking verdient dat de invulling van de maatstaf sterk casuïstisch is en derhalve altijd afhangt van de concrete omstandigheden van het geval.



5 HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, r.o. 6.4.5 (Zwolsman).

6 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.4 e.v. (Stille Sms).

7 Kamerstukken II 1996/97, 25 403, nr. 3, p. 3 respectievelijk p. 9-13.

8 HR 18 april 2017, ECLI:NL:HR:2017:725, r.o. 2.3.

9 F.A.W. Ashouwer en J. Geurts, 'Strafvordering en technologische vooruitgang: de GPS-tracker', TPWS 2017/30; HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, r.o. 6.4.4 e.v. (Zwolsman).

10 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.2.1 (Stille Sms).

11 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.4 (Stille Sms).

“Bij een beperkte inbreuk op de grondrechten van een verdachte volstaan de algemene taakstellende bepalingen van art. 3 Polw 2012 en art. 141 Sv.”

Stille Sms

In het reeds genoemde arrest *Stille Sms* wordt verdachte ten laste gelegd dat hij heeft gehandeld in strijd met onder meer art. 4 Opiumwet. Dit is door het hof bewezenverklaard.¹² Door de opsporingsambtenaren is gebruikgemaakt van een zogeheten ‘stille sms’, waardoor de locatie van verdachte heimelijk kon worden bepaald, zo legt A-G Bleichrodt uit.¹³ De verdediging heeft in het arrest van het hof aangevoerd dat gebruik is gemaakt van een niet wettelijk opsporingsmiddel, namelijk de stille sms.¹⁴ Hierdoor is op intensieve en stelselmatige wijze inbreuk gemaakt op de privacy van verdachte. Dit zou volgens de verdediging moeten leiden tot de uitsluiting van elk onmiddellijk en middellijk bewijs dat als gevolg van deze opsporingsmethode is verkregen.

Het hof oordeelt samengevat dat er inderdaad gebruik is gemaakt van een methode van ‘stil sms’en’, waardoor via het telecommunicatienetwerk globaal de locatie van verdachte kon worden bepaald. Daartoe is in een periode van vijf dagen, gedurende een periode van tussen zes en twaalf uur, om het half uur een ‘stille sms’ verstuurd naar de telefoon van verdachte. Alles is gebeurd onder leiding van en met toestemming van de officier van justitie (hierna: OvJ). Het hof oordeelt dat deze opsporingsmethode geen inbreuk van betekenis heeft gemaakt op de privacy van verdachte, omdat door de ‘stille sms’ slechts zo een beperkt beeld is verkregen van verdachte “dat van een betekenende inbreuk op diens privacy geen sprake was”.¹⁵ Omdat er geen betekenende inbreuk is gemaakt op de privacy van verdachte, stelt het hof dat er voor de

‘stille sms’ geen afzonderlijke wettelijke bepaling nodig is. De algemene taakstellende bepalingen van art. 3 Polw 2012 jo. art. 141 Sv zijn voldoende. Het hof merkt wel op dat indien de frequentie van de sms’jes wordt verhoogd, de uitkomst anders kan zijn. Dan is naar alle waarschijnlijkheid wel een afzonderlijke grondslag nodig, bijvoorbeeld in het Wetboek van Sv.

De Hoge Raad laat het oordeel van het hof in stand. Hij overweegt daarbij dat het oordeel van het hof dat het in dit geval toezenden van ‘stille sms-berichten’ een beperkte inbreuk heeft gemaakt op de grondrechten van verdachte en niet zeer risicovol is geweest voor de opsporing, geen blijk geeft van een onjuiste rechtsopvatting. Er is dus niet sprake van een meer dan beperkte inbreuk ofwel onrechtmatigheid. Of die rechtsopvatting juist is, hangt af van de omstandigheden van het geval.¹⁶ In casu legt de Hoge Raad aan zijn oordeel enkele speerpunten ten grondslag, namelijk de intensiteit en frequentie waardoor slechts een beperkt beeld is verkregen van verdachte, het feit dat er toestemming door de OvJ is gegeven en het feit dat er voldoende duidelijkheid over de inzet is. Met zijn oordeel volgt de Hoge Raad de conclusie van A-G Bleichrodt, die onder punt 30 e.v. schrijft dat hij het oordeel van het hof niet onbegrijpelijk vindt, mede vanwege de globale locatiebepaling door de ‘stille sms’jes.¹⁷

Uit dit arrest kan men de conclusie trekken dat er een beperkte inbreuk is geweest op de grondrechten van verdachte, in het bijzonder de privacy. De algemene taakstellende bepalingen voldoen der-

12 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.2.1 (*Stille Sms*).

13 HR 1 juli 2014, ECLI:NL:HR:2014:1569 (concl. A-G Bleichrodt).

14 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.2.2 (*Stille Sms*); Hof ‘s-Hertogenbosch 14 februari 2013, ECLI:NL:GHSHE:2013:BZ1357, r.o. 4.

15 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.2.2 (*Stille Sms*).

16 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.5 (*Stille Sms*).

17 HR 1 juli 2014, ECLI:NL:HR:2014:1569 (concl. A-G Bleichrodt).

halve als bevoegdheidsgrondslag. De inbreuk is onder meer beperkt vanwege de intensiteit en frequentie waardoor slechts een beperkt beeld is verkregen. Indien de frequentie en intensiteit anders waren geweest, was wellicht wel sprake geweest van een completer beeld van het leven van de verdachte. Dan had aangenomen kunnen worden dat sprake was van een meer dan beperkte inbreuk en had het onderzoek onrechtmatig kunnen zijn. Dit wekt bij mij de indruk dat alles sterk casuïstisch is en afhangt van de omstandigheden van het geval, zoals ook de Hoge Raad stelt ten aanzien van de mate van inbreuken.¹⁸

IMSI-catcher

In een ander arrest van de Hoge Raad staat de IMSI-catcher centraal.¹⁹ Met behulp van dit apparaat kan de globale locatie van een persoon worden bepaald. In het arrest van het hof heeft verdachte als verweer aangevoerd dat de inzet van de IMSI-catcher onrechtmatig was. Er zou geen afzonderlijke machtiging voor de IMSI-catcher zijn afgegeven en de OvJ zou niet hebben bepaald dat dit technische hulpmiddel bij stelselmatige observatie zou worden ingezet. Er zou daarom geen grondslag voor de inzet zijn en dus zou de inzet onrechtmatig zijn. Het hof verwierpt het verweer.²⁰ Hij stelt dat de OvJ wel degelijk toestemming heeft gegeven. Volgens het hof loopt het verweer van de raadsman daarom op dit vlak dus reeds stuk. Voor het overige, het verweer met betrekking tot de grondslag, oordeelt het hof dat er in dit geval slechts sprake is van een beperkte inbreuk op de privacy van verdachte, gelet op de duur van de inzet. Art. 3 Polw 2012 en art. 141 Sv bieden daarom voldoende grondslag, waarmee er wel degelijk een wettelijke grondslag is. Volgens het hof is de duur van de inzet een belangrijk criterium om te bepalen of er sprake is van een beperkte inbreuk of een meer dan beperkte inbreuk op de privacy van een verdachte.

De Hoge Raad oordeelt hieromtrent, net als in het arrest *Stille Sms*, dat art. 3 Polw 2012 en art. 141 Sv inderdaad een voldoende wettelijke grondslag kunnen bieden voor het inzetten van een opsporingsmiddel dat niet nader in de wet is omschreven, mits sprake is van een beperkte inbreuk op de grondrechten van een verdachte. Van een meer dan beperkte inbreuk ofwel onrechtmatigheid is sprake indien het opsporingsmiddel een compleet beeld van het leven van een verdachte doet verkrijgen.²¹

De Hoge Raad laat vervolgens het oordeel van het hof in stand, wat in het onderhavige geval niet onbegrijpelijk is, mede gelet op de korte inzet van de IMSI-catcher en gelet op het feit dat de OvJ toestemming heeft gegeven voor de inzet. Uit de overweging van de Hoge Raad blijkt wederom dat de duur van de inzet van een opsporingsmethode

een belangrijk criterium is voor de beantwoording van de vraag of er sprake is van een meer dan beperkte inbreuk op de grondrechten van een verdachte.

“Zoals gezegd is de uitkomst van de vragen in veel gevallen sterk casuïstisch, waarbij het allemaal afhangt van de omstandigheden van het geval.”

Kort samengevat

Uit het voorgaande kan men de conclusie trekken dat art. 3 Polw jo. art. 141 Sv een voldoende grondslag vormen voor de inzet van een opsporingsmiddel voor zover daarmee niet een meer dan beperkte inbreuk wordt gemaakt op de grondrechten, in het bijzonder de privacy, van een verdachte. Er is geen sprake van een beperkte inbreuk, indien een compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de betrokkene ofwel verdachte. De duur van de inzet, de intensiteit van de inzet en toestemming van de OvJ zijn belangrijke handvatten bij de vraag of er een beperkte inbreuk is of een meer dan beperkte. Bij een meer dan beperkte inbreuk kunnen deze algemene taakstel-

18 HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.5 (*Stille Sms*).

19 HR 1 juli 2014, ECLI:NL:HR:2014:1562 (*IMSI-Catcher*).

20 HR 1 juli 2014, ECLI:NL:HR:2014:1562, r.o.3.2.2 (*IMSI-Catcher*).

21 HR 1 juli 2014, ECLI:NL:HR:2014:1562, r.o. 3.5.2 (*IMSI-Catcher*).

lende bepalingen niet als grondslag gelden; dan is een specifieke grondslag in de wet nodig. Indien het opsporingsmiddel niettemin is ingezet zonder deze specifieke grondslag, dan is dit onrechtmatig. Zoals gezegd is de uitkomst van de vragen in veel gevallen sterk casuïstisch, waarbij het allemaal afhangt van de omstandigheden van het geval.

Drones als opsporingsbevoegdheid

Het zojuist besprokene kan ook van toepassing zijn op drones als opsporingsmiddel. Indien de drone niet op grond van een specifieke wettelijke grondslag ingezet kan worden, kunnen art. 3 Polw 2012 jo. art. 141 Sv een voldoende grondslag zijn. Daarbij gelden de regels die zojuist besproken en toegelicht zijn. De drone kan voorts een technisch hulpmiddel zijn bij stelselmatige observatie in de zin van art. 126g e.v. Sv, waarbij art. 126g Sv in dat geval de grondslag voor de inzet vormt. In dat geval mag er wél een meer dan beperkte inbreuk worden gemaakt op de privacy van een verdachte. Hieronder zal echter de jurisprudentie met betrekking tot art. 3 Polw en art. 141 Sv worden toegepast op drones. Over de drone als technisch hulpmiddel in de zin van art. 126g Sv zal ik niet uitweiden, omdat dit artikel zich richt op de algemene taakstellende bepalingen.

De 'Raven' als opsporingsmiddel: privacyinbreuk?

De 'Raven' is een onbemand vliegtuigje, oftewel een drone, van Defensie dat onder meer bij de opsporing door opsporingsambtenaren ingezet kan worden.²² In dit arrest is verdachte ten laste gelegd dat hij een hennepkwekerij heeft gehad in de periode van december 2012 tot en met juni 2013. Tijdens het opsporingsonderzoek is gebruikgemaakt van de Raven ter ondersteuning van de politie. De drone is ingezet door Defensie. Deze militaire bijstand is aangevraagd door de OvJ, met toestemming van het college van Procureurs-Generaal. Door de inzet van deze drone met een warmtecamera is het huis van verdachte opgevalen vanwege de afwijkende warmte in het huis. Nader onderzoek wees uit dat er sprake was van een hennepkwekerij, zoals ten laste was gelegd.

De verdediging voert als verweer dat de inzet van de drone onrechtmatig is. De drone zou namelijk ingezet zijn zonder dat daarvoor een toereikende wettelijke grondslag bestaat en deze grondslag is in alle gevallen vereist, omdat de inzet van een drone inbreuk maakt op de persoonlijke levenssfeer van burgers.

Het hof is het niet met de raadsman van verdachte eens. Hij verwerpt de stelling dat voor iedere inzet van een drone een specifieke wettelijke grondslag vereist is, omdat iedere inzet van een drone anders kan zijn. Zo kan een drone worden ingezet zonder beeld, met beeld om foto's te maken van een specifiek persoon of een bepaald object, of enkel met een warmtecamera. De duur kan daarbij per inzet ook verschillen. Het hof merkt voorts op dat de inzet van de drone getoetst moet worden aan de rechtsregel die uit onder meer het arrest Stille Sms voortvloeit: is er sprake van een opsporingsmiddel dat slechts een beperkte inbreuk heeft gemaakt op de grondrechten van burgers en is dit opsporingsmiddel niet zeer risicovol geweest voor de integriteit en beheersbaarheid van de opsporing?²³

De inzet van de drone doorstaat deze toetsing. Met andere woorden: het hof beantwoordt de vraag positief. De drone heeft geen opnamen gemaakt van identificeerbare personen of kentekens van auto's. Er zijn enkel opnamen gemaakt van specifieke wijken in Arnhem, waarbij er geen focus ligt op een bepaald object of bepaalde persoon. Bij verdachte is enkel een opvallend warmtebeeld opgemerkt. Het hof acht dat er onder deze omstandigheden geen sprake is van onrechtmatigheid. Bovendien heeft de politie eerder via feitelijke waarneming een opvallendheid op het dak van verdachte geconstateerd: op andere daken lag sneeuw, maar niet op het dak van verdachte. Dit is een aanwijzing voor de aanwezigheid van een hennepkwekerij. Het verweer van de raadsman wordt verworpen.

In het licht van het arrest Stille Sms was er in deze zaak dus een opsporingsmiddel dat een beperkte inbreuk maakt op de privacy van verdachte, waardoor geen specifieke wettelijke grondslag nodig is

²² Hof Arnhem-Leeuwarden 8 november 2016, ECLI:NL:GHARL:2016:8883.

²³ HR 1 juli 2014, ECLI:NL:HR:2014:1569, r.o. 2.4 e.v. (*Stille Sms*).

uit een bijzondere wet. Er is in ieder geval slechts een beperkte inbreuk. Mocht de raadsman subsidair specifiek hebben aangevoerd dat er een meer dan beperkte inbreuk zou hebben plaatsgevonden, dan zou het hof dit fictieve verweer waarschijnlijk alsnog verwerpen, omdat geen opnamen zijn gemaakt van identificeerbare personen, laat staan van verdachte. Enkel zijn dak is opvallend geweest.

Camera

Een vraag die kan rijzen is of het maken van een foto van een persoon een meer dan beperkte inbreuk op de privacy van een verdachte oplevert, in tegenstelling tot het enkele gebruik van een warmtecamera. De Hoge Raad heeft zich in 2017 over deze rechtsvraag moeten buigen.²⁴ Hierbij moet wel worden opgemerkt dat het in dit geval niet om een drone ging. Wel is het arrest illustratief voor de rechtsvraag of het maken van een foto middels een camera een meer dan beperkte inbreuk op de privacy van verdachte oplevert. Het is niet ondenkbaar dat op drones camera's worden geplaatst, zoals ook bij de Raven het geval was, al ging het in dat geval om een warmtecamera. Een extensieve interpretatie van dit arrest kan een antwoord bieden op de vraag of het nemen van een foto van een verdachte middels een drone een meer dan beperkte inbreuk op de privacy van verdachte, oplevert.

Het hof is van oordeel dat in onderhavige geval het nemen van een foto van de verdachte vanaf de openbare weg een geringe inbreuk op de privacy van verdachte oplevert. Waarom er een geringe inbreuk op de privacy is, staat verder in het arrest niet ter discussie.²⁵ De Hoge Raad laat het oordeel van het hof in stand. Uit het arrest volgt dus dat het nemen van een foto van een verdachte een geringe inbreuk op de privacy van de verdachte oplevert. Ik zou voorzichtig durven te stellen dat het nemen van een enkele foto van een verdachte met een camera die aan een drone is bevestigd dan ook slechts een geringe inbreuk op de privacy van de verdachte oplevert. Echter, als met een drone niet enkel een foto van één persoon zou worden genomen,

maar de openbare weg, privéterreinen en andere personen constant gefilmd zouden worden, dan is het aannemelijk dat er wel een meer dan beperkte inbreuk is op de privacy van de betrokkenen in het licht van het arrest over de Raven.²⁶

Conclusie

Het gebruik van drones als opsporingsmiddel op grond van de algemene bevoegdheidsgrondslagen uit art. 3 Polw 2012 en art. 141 Sv is rechtmatig, indien de inzet slechts een geringe inbreuk maakt op de grondrechten, in het bijzonder de privacy, van een betrokkene of verdachte. Voor zover het opsporingsmiddel wordt ingezet op basis van bijvoorbeeld art. 126g Sv kan een grotere inbreuk op de grondrechten van een verdachte geoorloofd zijn. Hierbij zij opgemerkt dat een drone die wordt ingezet om stelselmatig te observeren al snel niet enkel op basis van art. 3 Polw 2012 jo. art. 141 Sv kan worden ingezet, aangezien dan al gauw sprake zal zijn van een meer dan beperkte inbreuk. Hoogstwaarschijnlijk zal er dus in de meeste gevallen een specifieke wettelijke grondslag nodig zijn indien een drone voor stelselmatige observatie wordt gebruikt. Indien de politie haar drone-arsenaal wil uitbreiden en inzetten, zoals aangestipt in de inleiding, dan zal de rechtmatigheid van de inzet derhalve een uitdaging zijn. Er zal per geval goed moeten worden afgewogen of de inzet van een drone rechtmatig is, voornamelijk indien de drone wordt ingezet op grond van de algemene taakstellende bepalingen. Hierbij kan worden gekeken naar de bestaande jurisprudentie hierover, nu deze algemene regels bevat en daarom handvatten biedt voor verschillende omstandigheden, waaronder het gebruik van drones.

24 HR 18 april 2017, ECLI:NL:HR:2017:725.

25 HR 18 april 2017, ECLI:NL:HR:2017:725, r.o. 2.2.4.

26 Hof Arnhem-Leeuwarden 8 november 2016, ECLI:NL:GHARL:2016:8883.

Bodycams onder de loep:

het wettelijk kader voor gebruik en verwerking

Geschreven door Lotte Derksen



Tot slot licht ik toe waar de gevaren liggen en hoe het toekomstperspectief eruitziet voor het gebruik van bodycams door politieagenten.

Voordelen bodycams

Uit onderzoek blijkt dat de bodycams een waardevolle toevoeging zijn bij het politiewerk. Politie medewerkers voelen zich veiliger tijdens het dragen van een bodycam. In meer dan 60% van de gevallen werkt het filmen de-escalerend. Burgers zijn over het algemeen minder agressief,

tonen meer respect voor de politie en gedragen zich coöperatiever.²

'Collega's die de bodycam gebruiken, vertellen dat als de spanning oploopt, het simpelweg helpt om te melden dat het verdere gesprek wordt opgenomen. Alle partijen houden zich dan in,' zo stelt Myria van Lith, voorzitter van de stuurgroep implementatie bodycams.³

Naast het gedrag van burgers, verandert het gedrag van politieagenten ook in positieve zin bij het dragen van de bodycam. Politieagenten gedragen zich bewuster, passen hun taalgebruik aan en geven va-

Al sinds 2017 wordt er door de Nationale ombudsman uitgebreid onderzoek gedaan naar het gebruik van bodycams door de politie. Op verschillende plaatsen in Nederland is hiermee geëxperimenteerd. De Ombudsman kijkt hierbij onder andere naar de informatievoorziening aan de burger, de waarborging van privacy en de bewaartermijnen van de beelden.¹ In dit artikel zet ik eerst de voor- en nadelen van het gebruik van bodycams uiteen. Daarna leg ik uit onder welke wettelijke grondslag het gebruik van bodycams valt. Ook licht ik toe aan welke vereisten de verwerking van de opnames moet voldoen op grond van het Inzetkader Bodycams.

1 'Onderzoek ombudsman naar gebruik bodycams door de politie', nationaleombudsman.nl, 29 april 2019.

2 NHL Stenden, *Evaluatie inzet bodycams: effecten van bodycamgebruik op het operationele politiewerk* 2018, p. 29.

3 'Nieuwe bodycams in zomer 2021 volledig operationeel', 27 oktober 2020, politie.nl.

ker een waarschuwing als de camera draait. De agenten zijn zich meer bewust van hun gedrag en zijn meer geneigd om procedureel correct te handelen.⁴

Een ander voordeel is dat politieagenten serieuzer worden genomen. Dit blijkt uit een onderzoek naar bodycams in Amsterdam, waar de nadruk lag op het gebruik van bodycams in uitgaansgelegenheden. Ouders van jongeren geloofden de agenten veel sneller wanneer ze geconfronteerd werden met beelden waarin alcoholmisbruik onder de jongeren te zien was.⁵

Tot slot zijn de bodycam-opnames een belangrijke toevoeging als ondersteunend bewijs voor het proces-verbaal. Belangrijk om hierbij te melden is dat de opnames enkel als aanvulling op het bewijs dienen. Aangezien de opname maar een deel van de situatie vastlegt, kan het niet als vervangend bewijs dienen in het proces-verbaal. Toch is dit een groot voordeel. Zo zijn er na de zogeheten avondklokrellen, veel mensen opgepakt nadat ze herkend waren op de bodycam-opnames.⁶

Nadelen bodycams

Elk voordeel kent (helaas) zijn nadelen. Zo ook voor de inzet van bodycams. Ten eerste kan het gebruik van bodycams ook escalerend werken. Wanneer wordt medegedeeld dat ze gefilmd worden, besluiten sommige burgers, met name jongeren, zelf ook te filmen. Ook leidt de mededeling van het filmen in sommige gevallen tot ongewenste discussie en/of protest. Ten tweede is een groot nadeel van de bodycams uiteraard dat de privacy van burgers in het geding komt. Het is een inbreuk op de persoonlijke levenssfeer wanneer iemand ongevraagd gefilmd wordt.⁷

Algemene taakstelling: art. 3 Politiewet 2012

Op grond van art. 3 Politiewet 2012 (hierna: Polw) heeft de politie tot taak te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Op grond van art. 141 Sv is de politie belast met de opsporing van strafbare feiten. Deze algemene taakstellende bevoegdheid maakt niet-stelselmatige observatie van een persoon mogelijk, ondanks dat er geen sprake is van een 'verdachte'.

Uit het welbekende Zwolsman-arrest blijkt dat art. 3 Polw jo. art. 141 Sv een toereikende wettelijke grondslag is, indien slechts een beperkte inbreuk op de persoonlijke levenssfeer is gemaakt. Dit begrip zal ik niet nader uitwerken nu dit in het vorige artikel in dit magazine, *"Big Brother is watching you"*, uitvoerig wordt besproken. Het criterium dat hieruit volgt is dus dat de inbreuk beperkt dient te zijn, om de opsporing op art. 3 Polw jo. art. 141 Sv te kunnen baseren.⁸

In het arrest Pseudoverkoop is dit criterium anders opgesteld en aangevuld. Uit dit arrest blijkt namelijk dat de inbreuk op grondrechten van burgers, waaronder het recht op bescherming van de persoonlijke levenssfeer, niet disproportioneel mag zijn. Waar de Hoge Raad in het Zwolsman-arrest het heeft over een absoluut criterium, namelijk het al dan niet beperkt zijn van de inbreuk, laat de Hoge Raad in het Pseudoverkoop-arrest ruimte voor een relatieve toets. Ook voegt de Hoge Raad hier een criterium aan toe. De Hoge Raad stelt namelijk dat de opsporingsautoriteiten alleen bevoegd zijn een opsporingsmiddel in te zetten, indien dit niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing.⁹

4 Politie, *Inzet van bodycams binnen het operationele politiewerk* 2018, p. 18.

5 Politie, *Inzet van bodycams binnen het operationele politiewerk* 2018, p. 17.

6 'Ruim dertig aanhoudingen bij rellen in provincie, bijna helft opgepakt in Haarlem', nhnieuws.nl, 26 januari 2021.

7 Het recht op bescherming van de persoonlijke levenssfeer is opgenomen in art. 10 Grondwet jo. art. 8 EVRM.

8 HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, r.o. 6.4.5.

9 HR 5 maart 2019, ECLI:NL:HR:2019:298, r.o. 4.3.2 (*Pseudoverkoop*).

“Collega’s die de bodycam gebruiken, vertellen dat als de spanning oploopt, het simpelweg helpt om te melden dat het verdere gesprek wordt opgenomen. Alle partijen houden zich dan in.”

Bij het gebruik van een warmtecamera oordeelt de Hoge Raad dat de bevoegdheid op grond van art. 3 Polw jo. art. 141 Sv relatief ver kan gaan. In het Warmtebeeldkijker-arrest werd geoordeeld dat er sprake was van een beperkte inbreuk op de persoonlijke levenssfeer, omdat het ging om kortstondig gebruik met als doel om hennepplantages te spotten. Een split-secondbeeld was al voldoende.¹⁰ De Hoge Raad oordeelde daarom dat deze opsporingshandeling ook onder art. 3 Polw jo. art. 141 Sv valt.

Tot slot blijkt dat de Hoge Raad waarde hecht aan de kenbaarheid van de opsporingshandeling bij burgers. Wanneer burgers er kennis van hebben, kan dit meewegen bij de vraag of een opsporing al dan niet onder de algemene taakstelling op grond van art. 3 Polw en art. 141 Sv valt.¹¹

Algemene taakstelling in verhouding tot bodycams

Het gebruik van een bodycam als vorm van niet-stelselmatige observatie valt onder de algemene taakstelling als genoemd in art. 3 Polw jo. art. 141 Sv, aangezien incidenteel cameratoezicht in het belang van ordehandhaving geschiedt. Bij incidenteel cameratoezicht, zoals bij de bodycams gebeurt, wordt een gebied niet structureel geobserveerd, maar kortdurend en vluchtig.¹² Het filmen is enkel toegestaan op voor publiek toegankelijke plaatsen. Onder het begrip

‘voor publiek toegankelijke plaatsen’ vallen in beginsel de plaatsen die feitelijk toegankelijk zijn voor een onbeperkt aantal personen op grond van art. 1 Wet openbare manifestaties, zoals een restaurant of een museum.¹³ Een lokaal kan hier ook onder vallen, indien het lokaal in beginsel een onbeperkt aantal personen omvat. Denk bijvoorbeeld aan een ruimte die uitsluitend toegankelijk is voor reizigers.¹⁴ Wanneer op een niet voor publiek toegankelijke plaats gefilmd wordt, dan valt dit niet meer onder art. 3 Polw, tenzij er sprake is van omstandigheden die het niet toelaten om te stoppen met filmen.

Bij de beoordeling of de inbreuk op iemands privéleven beperkt blijft, wordt gekeken naar het type bodycam dat is gebruikt, maar ook naar de omstandigheden van het geval zoals de duur, intensiteit, plaats en het doel van de observatie.¹⁵ Er moet hierbij altijd een afweging worden gemaakt aan de hand van de maatstaven van proportionaliteit en subsidiariteit.

De bodycams kunnen worden ingezet ter ondersteuning van de deeltaken van de politie: handhaving van de openbare orde, strafrechtelijke handhaving van de rechtsorde, hulpverlening aan hen die deze behoeven, taken ten dienste van justitie en het waken over de veiligheid van personen. De opnames kunnen daarom aangemerkt worden als politiegegevens

10 HR 20 januari 2009, ECLI:NL:HR:2009:BF5603 (concl. A-G mr. Knigge), NJ 2009/225, m.nt. M.J. Borgers.

11 HR 19 januari 2021, ECLI:NL:HR:2021:80, r.o. 2.5.2.

12 De Jong, 'Incidenteel cameratoezicht in het belang van ordehandhaving', in: S.A.J. Munneke (red.), *De Gemeentewet en haar toepassing (GMT)*, Deventer: Wolters Kluwer.

13 Programma Sensing - Landelijk Project Bodycams, *Inzetkader Bodycams bij operationeel gebruik 2020*, p. 6.

14 *Kamerstukken II 2000/01*, 27732, 3.

15 Programma Sensing - Landelijk Project Bodycams, *Inzetkader Bodycams bij operationeel gebruik 2020*, p. 7.

en de verwerking daarvan vindt plaats op basis van de Wet politiegegevens (hierna: Wpg).¹⁶ De inzet van de bodycams is aan te merken als niet-stelselmatige observatie en valt onder de grondslag van art. 3 Polw en art. 141 Sv. Op de verwerking van deze opnames zijn art. 8 lid 1 en art. 9 Wpg van toepassing. Deze verwerkingsgrondslagen zijn verder uitgewerkt in het Inzetkader Bodycams.¹⁷

Inzetkader Bodycams

In het Inzetkader Bodycams is nader uitgewerkt welke eisen worden gesteld aan het gebruik van de bodycam. Het Inzetkader Bodycams heeft tot doel om te waarborgen dat bodycams zorgvuldig en rechtmatig ingezet worden, dat de opnames rechtvaardig verwerkt worden voor de doelen waarvoor ze zijn verzameld en dat de privacy en rechten van betrokkenen en politiemedewerkers zoveel mogelijk worden gerespecteerd. Het inzetkader is een landelijk beleid dat is opgesteld door het Landelijk Project Bodycams.

Over de verwerking wordt ook het een en ander gezegd. Achtereenvolgens ga ik in op de belangrijkste eisen bij het gebruik van bodycams, namelijk de kenbaarheid van en behoorlijke verslaglegging over het gebruik. Daarna bespreek ik de verwerkingsgrondslagen voor het gebruik van bodycams en de bewaartermijn voor de bodycam-opnames.

Kenbaarheidsvereiste

Een belangrijk element bij het dragen van de bodycams is dat burgers moeten weten dat zij gefilmd worden. De politieagent kan dit mondeling melden, maar een zichtbare communicatie-uiting, zoals een duidelijk zichtbaar oplichtend signaal volstaat ook. Een lampje op de bodycam die aangaat, valt hieronder. Daarnaast moeten de bodycams openlijk en duidelijk zichtbaar gedragen worden.¹⁸

Behoorlijke verslaglegging

In de wet wordt de verslaglegging van verrichtingen en bevindingen in de onderzoeksfase niet genoemd. Toch moet er verslaglegging plaatsvin-

den om controle achteraf mogelijk te maken, zodat altijd teruggegrepen kan worden op wat voorafgaand aan het opsporingsonderzoek is verricht en bevonden. Hierdoor kan doeltreffend worden gereageerd wanneer de rechter in het eindonderzoek om nadere opheldering omtrent bepaalde feiten en omstandigheden verzoekt. De opsporingsambtenaar beschrijft in het proces-verbaal zijn handelen op basis van zijn eigen waarneming op grond van art. 344 lid 1 onder 1 Sv. De agent bekijkt de bodycam-opnames pas nadat zoveel mogelijk informatie in het proces-verbaal is opgemaakt. Worden de beelden van tevoren bekeken, dan wordt dit in het proces-verbaal vermeld. Uit de verslaggeving moet dan beoordeeld worden of een bodycam al dan niet rechtmatig is ingezet, welke opnames hierbij gemaakt zijn en of de inbreuk op de persoonlijke levenssfeer slechts beperkt is. Van belang hierbij is, wanneer de bodycams zijn ingezet, wie de opnames bewerkt hebben en aan wie de gegevens ter beschikking zijn gesteld of verstrekt. De politie kan namelijk niet de integriteit van bewijs- en processtukken garanderen, indien de politie geen duidelijkheid kan verschaffen over de aard, duur en intensiteit van de observatie. Dit kan een vormverzuim opleveren in de zin van art. 359a Sv.

Verwerkingsgrondslagen

Op grond van art. 3 lid 2 Wpg mogen politiegegevens slechts verwerkt worden indien dit rechtmatig is. Ook moeten de opnames ter zake dienend, toereikend, niet bovenmatig en accuraat zijn. Alle handelingen met betrekking tot de opnames vallen onder het begrip 'verwerken'. Hieronder valt bijvoorbeeld ook het verbeteren van beeldkwaliteit, het *blurren* van gezichten en het vervormen van stemmen.¹⁹ In de Wpg zijn vier verwerkingsgrondslagen opgenomen. Ten eerste de uitvoering van de dagelijkse politietaak op grond van art. 8 lid 1 Wpg. Ten tweede de handhaving van de rechtsorde in een bepaald geval op grond van art. 9 lid 1 Wpg. Ten derde het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde bedreigingen van de rechtsorde op grond van art. 10 lid

16 Art. 1 sub a jo. 2 lid 1 Wpg.

17 Brief van de Minister van Justitie en Veiligheid van 14 november 2019, 2734215.

18 Programma Sensing - Landelijk Project Bodycams, *Inzetkader Bodycams bij operationeel gebruik* 2020, p. 9.

19 Programma Sensing - Landelijk Project Bodycams, *Inzetkader Bodycams bij operationeel gebruik* 2020, p. 10.

1 Wpg en tot slot het beheer van en de controle op informanten, infiltranten en beschermde getuigen op grond van art. 12 Wpg. Gegevens die worden verwerkt voor een ander doel dan waarvoor ze oorspronkelijk zijn verkregen, de zogeheten doel-afwijkende verwerking, is alleen toegestaan voor zover de Wpg hier uitdrukkelijk in voorziet.²⁰ De verwerking van bodycam-opnames verzameld door middel van niet-stelselmatige observatie valt vrijwel altijd onder de verwerking in de zin van art. 8 lid 1 of art. 9 lid 1 Wpg.

Bewaartermijnen

Vergelijkbaar met de AVG, gelden er voor bodycam-opnames, oftewel politiegegevens, ook bewaartermijnen. Hierbij geldt dat voor de verschillende verwerkingsgrondslagen ook verschillende bewaartermijnen gelden. Wel geldt voor iedere grondslag dat de gegevens vernietigd moeten worden zodra ze niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld of worden verwerkt.²¹

Bodycam-opnames die in het kader van de dagelijkse politietaken worden verwerkt ex art. 8 Wpg, worden onmiddellijk vernietigd wanneer ze evident onbruikbaar zijn of wanneer ze niet langer noodzakelijk zijn voor de politietaken, interne onderzoeken of de afhandeling van klachten. De opnames worden uiterlijk vijf jaar na datum van de opname verwijderd.²² De politiegegevens die op basis van de algemene taakstelling in de zin van art. 3 Polw jo. art. 141 Sv worden verzameld, zullen onvoldoende waarde hebben om langer bewaard te worden. Na het verwijderen is de opname niet meer zichtbaar en operationeel raadpleegbaar.

De opnames die gemaakt zijn bij onderzoek in ver-

band met de handhaving van de rechtsorde in een bepaald geval, worden niet langer verwerkt dan noodzakelijk voor het doel van het onderzoek op grond van art. 9 lid 4 Wpg. De opnames worden gedurende een periode van maximaal een halfjaar verwerkt. Na dit halfjaar wordt bezien of er aanleiding is tot een nieuw onderzoek.

Voor beide verwerkingsgrondslagen geldt dat de verwijderde politiegegevens gedurende een ter-

mijn van vijf jaar worden bewaard en vervolgens worden vernietigd. Het verschil met verwijderen is dat bij verwijdering van de opnames, deze nog wel bewaard worden met het oog op de afhandeling van klachten en verantwoording van verrichtingen.²³ Bij vernietiging worden ze ook niet meer bewaard.

“Dit is een gevoelig privacy-onderwerp, niet alleen juridisch maar ook naar het gevoel van mensen. Als politie de grenzen overschrijdt, kan je in de toekomst veel kritiek verwachten.”

Moeilijkheden en toekomstperspectief

Wanneer het Inzetkader Bodycams goed nageleefd wordt, lijkt een inbreuk op de privacy van burgers gerechtvaardigd wat betreft het maken van de opnames. Het is daarom van belang dat agenten goed opgeleid worden in het gebruik van de bodycam. Vaak blijkt echter dat de bodycam niet goed wordt ingezet. Maar liefst een op de vier agenten is niet op de hoogte van de regels. Tijdens het onderzoek naar bodycams in Amsterdam is naar voren gekomen dat zes van de tien agenten het geen probleem vinden om bij mensen thuis te filmen, terwijl dit uiteraard een ernstige schending is van de privacy van burgers.²⁴

‘Dit is een gevoelig privacy-onderwerp, niet alleen juridisch maar ook naar het gevoel van mensen. Als politie de grenzen overschrijdt, kan je in de toekomst veel kritiek verwachten’, stelt privacyjurist

20 Programma Sensing - Landelijk Project Bodycams, *Inzetkader Bodycams bij operationeel gebruik* 2020, p. 8.

21 *Kamerstukken II* 2005/06, 30327, 3.

22 Zie art. 8 lid Wpg.

23 Zie art. 14 lid 1 Wpg.

24 ‘Agenten voelen zich veiliger met bodycams maar vergeten de privacy van burgers vaak’, 24 april 2019, trouw.nl.

Dimmen Smolders.²⁵

Om het vertrouwen van burgers te behouden, moeten de bodycams op een zorgvuldige manier worden ingezet. Kennis bij politieagenten is hierbij een voorwaarde. Een mogelijkheid is om hier al aandacht aan te besteden bij de opleiding van nieuwe agenten.²⁶

Daarnaast lijkt het in de praktijk niet altijd goed uitvoerbaar om alleen opnames te maken op plaatsen die voor het publiek toegankelijk zijn, zo stelt ook de Nationale Ombudsman. Wanneer een situatie uit de hand loopt kant het juist belangrijk zijn om de opname door te laten lopen, ook wanneer dat in een woning van een burger gebeurt. Politieagenten moeten goed getraind worden in het handelen met bodycams.²⁷

De voordelen hebben echter de doorslag gegeven, nu bekend is geworden dat bodycams structureel onderdeel gaan uitmaken van de operationele uitrusting van de basisteams. De uitrol van de bodycams in de eenheden is eind oktober 2020 gestart. Het plan is dat tweeduizend bodycams in het tweede kwartaal van 2021 operationeel zullen zijn.²⁸

Conclusie

Er is in de afgelopen jaren veel onderzoek gedaan naar het gebruik van bodycams door politieagenten. Het gebruik kent veel voordelen. Zo voelen agenten zich veiliger, worden ze serieuzer genomen en hebben de bodycam-opnames een belangrijke rol voor het bewijs bij het proces-verbaal. Nadelen zijn dat het filmen ook escalerend kan werken en bijvoorbeeld tot discussies leidt. Een nog groter nadeel is dat de privacy van burgers in het gedrang komt.

Het gebruik van bodycams op voor publiek toegankelijke plaatsen, valt onder de algemene taakstelling van de politie op grond van art. 3 Polw jo. art. 141 Sv. Uit jurisprudentie blijkt dat art. 3 Polw een toereikende wettelijke grondslag biedt, indien het

gaat om een beperkte inbreuk op de persoonlijke levenssfeer. De inbreuk op de persoonlijke levenssfeer mag niet disproportioneel zijn. Van belang bij deze beoordeling is of het gaat om korte opnames en of de burgers er kennis van hebben.

De verwerking van de opnames van de bodycams vindt plaats op grond van de Wpg en is nader uitgewerkt in het Inzetkader Bodycams. Uit het Inzetkader blijkt dat een belangrijk aspect is dat burgers weten dat zij gefilmd worden. Daarnaast moet er sprake zijn van behoorlijke verslaglegging in het proces-verbaal. De opnames mogen enkel verwerkt worden indien deze rechtmatig, ter zake dienend, toereikend, niet bovenmatig en accuraat zijn. De verwerkingsgrondslagen zijn in de Wpg opgenomen. Ook gelden er bewaartermijnen voor bodycam-opnames. Deze verschillen per verwerkingsgrondslag, maar de gegevens dienen in ieder geval vernietigd te worden zodra ze niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld of worden verwerkt.

Het gebruik van bodycams door politie lijkt ideaal. Het gedrag van zowel burgers als politieagenten wordt positief beïnvloed. Daarnaast zijn de bodycam-opnames een belangrijke bijdrage in het bewijs. Een groot nadeel blijkt echter dat politieagenten niet goed opgeleid worden in het gebruik ervan. Ze lijken zich niet altijd bewust van de consequenties wanneer ze met een bodycam een huis binnentreden bijvoorbeeld. Desondanks gaan bodycams structureel deel uitmaken van de operationele uitrusting van de basisteams. Het plan is dat tweeduizend bodycams in het tweede kwartaal van 2021 operationeel zullen zijn.

25 'Agenten voelen zich veiliger met bodycams maar vergeten de privacy van burgers vaak', 24 april 2019, trouw.nl.

26 'Bodycam waardevol voor politie op straat', 24 april 2019, politie.nl.

27 'Onderzoek ombudsman naar gebruik bodycams door de politie', nationaleombudsman.nl, 29 april 2019.

28 'Nieuwe bodycams in zomer 2021 volledig operationeel', 27 oktober 2020, politie.nl.