Artikel

De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel

Mr. C.M. Taylor Parkins-Ozephius, mr. I.N. De Wit, D.A.G. Van Toor PhD LLM BSc en mr. T. Beekhuis*

1. Inleiding

De laatste jaren is er in de rechtspraak,[1] in het wetgevingsproject modernisering van het Wetboek van Strafvordering[2] en in de wetenschap[3] veel te doen over digitale opsporing in het algemeen en het onderzoek naar vergrendelde elektronische gegevensdragers en versleutelde communicatie in het bijzonder. Ondanks dat uit recente rechtspraak van de Hoge Raad blijkt dat het gedwongen ontgrendelen van een elektronische gegevensdrager met een biometrisch kenmerk geoorloofd is[4] en het team *High Tech Crime* van de Nederlandse politie (in samenwerking met buitenlandse collega's) meerdere malen met succes communicatie ontsleuteld heeft,[5] is de toegang tot vergrendelde elektronische gegevensdragers of inzage in versleutelde communicatie geen gegeven. De problemen met vergrendeling en versleuteling kunnen echter worden omzeild als de politie onder dekmantel zelf de elektronische gegevensdragers aan criminelen verstrekt.

Dit briljante idee is blijkbaar de afgelopen jaren ontwikkeld en in werking gesteld. Uit een Amerikaans *affidavit* blijkt dat de *Federal Bureau of Investigation* (hierna: FBI) de ontwikkelaar van de ANOM-*smartphones* heeft opgepakt kort voordat hij in het gat in de markt wilde stappen. Dit gat in de markt was ontstaan na de ontmanteling van de versleutelde communicatieaanbieder *Phantom Secure*, waarvan de ontwikkelaar van de ANOM-*smartphones* distributeur was.[6] In ruil voor strafvermindering ontwikkelde en verspreidde hij de ANOM-*smartphones* als alternatief voor *Phantom Secure* en *Sky* in

* Mr. C.M. Taylor Parkins-Ozephius is verbonden als docent Straf(proces)recht aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht. Mr. I.N. de Wit is verbonden als docent Straf(proces)recht aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht. D.A.G. van Toor PhD LLM BSc is verbonden als universitair docent aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtstaat en Rechtspleging van de Universiteit Utrecht. Mr. T. Beekhuis is verbonden als promovenda aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Utrecht Centre for Accountability and Liability Law (Ucall) van de Universiteit Utrecht.

1. Bijv. HR 9 februari 2021, ECLI:NL:HR:2021:202; Conclusie F.W. Bleichrodt 13 oktober 2020, ECLI:NL:PHR:2020:927; EHRM 25 mei 2021, zaaknrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch* t. *het Verenigd Koninkrijk*).
2. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.
3. Bijv. D.A.G. van Toor, 'Het nemo-teneturbeginsel bij digitale opsporingsbevoegdheden: oproep tot discussie over fundamentele bezinning van de normering van het opsporingsonderzoek in een digitale context', *TBS&H* 2021, 2, p. 89-100
4. HR 9 februari 2021, ECLI:NL:HR:2021:202.
5. www.politie.nl/nieuws/2021/maart/9/nieuwe-klap-voor-georganiseerde-misdaad.html, laatst geraadpleegd 15 april 2021.
6. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 12, laatst geraadpleegd op 8 juni 2021. In dit *affidavit* wordt overigens ook gesteld dat alle verkochte *smartphones* voor criminele doeleinden werden gebruikt.

doi: 10.5553/TBSenH/229567002021007005003

opdracht van de FBI.[7] Uit het *affidavit* blijkt dat de Australische federale politie direct bij *Operation Trojan Shield* is betrokken, vanwege de grote afname van *Phantom Secure-smartphones* aldaar.[8] Kort erna is een ander, niet bij naam genoemd, land betrokken bij het onderzoek door middel van een *Mutual Legal Assistance Treaty*.[9] Uit het *affidavit* blijkt ook waarom 7 juni 2021 bijltjesdag was: de rechterlijke machtiging voor de verrichte opsporingshandelingen – het wordt nog bewust opengelaten welke bevoegdheden hier ingezet zouden zijn – liep op die dag af.[10] Gezien de afname van de ANOM-*smartphones* wereldwijd is het waarschijnlijk dat het derde betrokken land Nederland, Duitsland of Servië is.[11] In deze landen zijn, samen met de Verenigde Staten van Amerika (hierna: Amerika) en Australië, de meeste toestellen verkocht. Uit de berichtgeving van Europol lijkt Nederland, net zoals bij eerdere wereldwijde digitale onderzoeken naar criminaliteit op het *darknet*[12] en naar versleutelde communicatieaanbieders,[13] een sleutelrol te hebben gespeeld.[14]

Met *Operation Trojan Shield* hebben de (Nederlandse) autoriteiten de populariteit van *cryptophones* perfect uitgebuit, mede dankzij de ontmanteling van andere aanbieders.[15] Dit instrumentele succes heeft echter ook een keerzijde: vooralsnog is, naast het eerdergenoemde *affidavit*, niets bekend over de wettelijke grondslag voor de inzet van de opsporingshandelingen. In deze bijdrage wordt onderzocht welke wettelijke grondslag gebruikt zou kunnen zijn, waarbij als uitgangspunten worden genomen dat Nederland inderdaad een sleutelrol heeft gespeeld bij (1) de ontwikkeling van de hardware en de daarop geïnstalleerde software; (2) de verspreiding van de toestellen; (3) het verkrijgen van vertrouwelijke communicatie doordat de toestellen zijn gebruikt; en (4) de analyse van de inhoud van de verstuurde en ontvangen communicatie. De inzet van deze handelingen wordt ten slotte beoordeeld in het licht van het legaliteitsbeginsel zoals dat volgt uit artikel 8 lid 2 EVRM. In deze bijdrage blijft de discussie over de handhavingsjurisdictie met betrekking tot de grensoverschrijdende aard van de operatie buiten beschouwing.

7. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 12, laatst geraadpleegd op 8 juni 2021.
8. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 13, rn. 15 e.v., laatst geraadpleegd op 8 juni 2021.
9. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 13, laatst geraadpleegd op 8 juni 2021.
10. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 18, laatst geraadpleegd op 8 juni 2021.
11. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 19, laatst geraadpleegd op 8 juni 2021.
12. www.politie.nl/nieuws/2018/maart/16/webshops-van-online-drugshandelaren-hansa-market-definitief-gesloten.html, laatst geraadpleegd 15 april 2021.
13. www.politie.nl/nieuws/2021/maart/9/nieuwe-klap-voor-georganiseerde-misdaad.html, laatst geraadpleegd 15 april 2021.
14. www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication, laatst geraadpleegd op 8 juni 2021.
15. In het inmiddels veelvuldig aangehaalde *affidavit* staat dat het aantal gebruikers van ANOM na de (onverwachte) ontmanteling van *Encrochat* en *Sky* van minder dan 3.000 naar ruim 9.000 steeg. Zie: www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 21, laatst geraadpleegd op 8 juni 2021.

2. Het legaliteitsbeginsel

Het is duidelijk dat met *Operation Trojan Shield* een ingenieus idee is uitgewerkt, waarbij de populariteit van *cryptophones* en de wens van criminelen om versleuteld te communiceren perfect zijn uitgebuit. Deze instrumentele waarde heeft echter, zoals reeds eerder werd opgemerkt, ook een keerzijde:[16] met de hierboven beschreven handelingen die zijn uitgevoerd tijdens de operatie wordt een inbreuk gemaakt op de privacy van veel (mogelijk criminele) burgers en dat is volgens het legaliteitsbeginsel alleen toegestaan indien de beperking van een grondrecht in overeenstemming met het recht heeft plaatsgevonden.

Voor die beperking van grondrechten in het licht van het legaliteitsbeginsel dient, ondanks dat (of juist omdat) met *Operation Trojan Shield* een ferme tik is uitgedeeld aan de transnationaal opererende georganiseerde misdaad, aandacht te bestaan. Dat de overheid zich in overeenstemming met het recht dient te gedragen, houdt namelijk een bepaalde kwaliteitsgarantie voor burgers in. Ten eerste door te garanderen dat inbreuken op grondrechten van burgers slechts dan mogelijk zijn na grondige discussie en belangenafweging door de formele wetgever (en niet enkel door de regering bij AMvB of een minister bij ministeriële regeling). Ten tweede leidt de hiervoor genoemde belangenafweging hoogstwaarschijnlijk niet tot vrijbrieven of blanco cheques. In het toekennen van (onbegrensde) macht schuilt het gevaar van grove vrijheidsbeperking van verdachten en derden en eventueel ook van machtsmisbruik (door willekeurig om te gaan met de bevoegdheid). Daarnaast wordt machtsmisbruik tegengegaan door de bevoegdheid geclausuleerd toe te kennen, door te bepalen dat zij slechts door een bepaalde autoriteit, tegen bestemde personen, in bepaalde gevallen en met een specifiek doel mag worden ingezet.

In dit artikel gaat het dan vooral om de waarborgen die in acht moeten worden genomen indien aan de autoriteiten een bevoegdheid wordt toegekend om opsporingshandelingen te verrichten. Onderstaande paragraaf begint daarom met een uiteenzetting van het toetsingskader met betrekking tot het legaliteitsbeginsel als bedoeld in artikel 8 lid 2 EVRM. Immers, alleen *ongerechtvaardigde* inbreuken op artikel 8 lid 2 EVRM leveren een schending van het recht op respect voor privacy op. Een belangrijk onderdeel van die toetsing is dat de inbreuk op het recht op respect voor privacy in overeen-

16. Strafprocesrecht is altijd instrumenteel en rechtsbeschermend. Vgl. R. Foqué & A.C. 't Hart, *Instrumentaliteit en rechtsbescherming*, Arnhem: Gouda Quint 1990, p. 15.

doi: 10.5553/TBSenH/229567002021007005003

stemming[17] met een wettelijke bepaling moet plaatsvinden.

2.1 De rechtvaardigingscriteria uit artikel 8 lid 2 EVRM

Het criterium 'in overeenstemming met een wettelijke bepaling', dat bij meerdere mensenrechten het eerste criterium voor een gerechtvaardigde inbreuk is, kan worden onderverdeeld in drie subcriteria. De inbreuk moet ten eerste op een wettelijke bepaling zijn gebaseerd (*legal basis*).[18] Wat betreft dit criterium is het belangrijk dat er (1) een wettelijke basis is[19] (2) die voor bepaalde (grovere) inbreuken *voldoende specifiek* is.[20] Ten tweede eist het EHRM dat de wettelijke bepaling van *voldoende kwaliteit* is.[21] Ten derde moet de inbreuk op het recht op respect voor privacy *in overeenstemming met* de nationale bepaling hebben plaatsgevonden.[22] Het tweede en derde criterium van 'in overeenstemming met een wettelijke bepaling' kunnen worden samengevat onder de term '*rule of law*'.[23] Hieronder wordt ingegaan op de eisen die voortvloeien uit de *rule of law*-gedachte, zijnde: (1) *toegankelijkheid* van de bepaling; (2) *voorzienbaarheid* van de gedragingen op grond van de bepaling; (3) *waarborgen* tegen willekeurig gedrag op basis van de bepaling en; (4) de *rechtmatigheid* van het overheidsoptreden op basis van de bepaling. De vereisten die volgen uit de voorwaarde *legal basis* laten wij verder buiten beschouwing omdat de eis dat een (specifieke) bepaling moet bestaan – in ieder geval voor het continentaal Europese strafprocesrecht – evident en duidelijk is.

Ten eerste beoordeelt het EHRM of de bepaling waarop de beperking van het recht op respect voor privacy is gebaseerd voor de burger *toegankelijk* is. Burgers moeten een indicatie hebben van welke regels op welk moment gelden.[24] Overigens is het voldoende dat de burger weet waar hij de regels kan opvragen (zonder dat ze zijn gepubliceerd).[25] Derhalve kan van de burger enig initiatief voor het verkrijgen van toegang worden verwacht.

Bij de *voorzienbaarheid* gaat het om de vraag of de wettelijke bepaling voldoende duidelijk en precies is geformuleerd zodat de burger kan voorzien, eventueel met behulp van deskundig advies,[26] welke inbreuk op zijn privacy door overheidsfunctionarissen kan worden gemaakt.[27] De preciesheid en gedetailleerdheid zijn, zoals hierboven kort aangestipt, van belang voor de legitimatie van grovere inbreuken en zijn daarnaast essentieel voor de voorzienbaarheid.[28] De voorzienbaarheid hangt in grote mate af van '*the content of the text in issue, the field it is designed to cover and the number and status of those to whom it is addressed*'.[29] Inhoudelijk hoeft de bepaling niet zo te worden opgesteld dat met zekerheid kan worden beoordeeld welke inbreuken de wet toelaat.[30] Dit zou namelijk leiden tot zeer rigide wetgeving, terwijl de wet gelijke tred moet kunnen houden met veranderende omstandigheden.[31]

Als derde is de kwaliteit van de wettelijke bepaling afhankelijk van de *waarborgen* die gelden bij de toepassing van de bevoegdheid. Wanneer de overheidsfunctionaris een ongelimiteerde bevoegdheid op grond van de wet bezit, kan ten minste ernstig worden getwijfeld aan de kwaliteit van de wet.[32] Grenzen en waarborgen zijn essentieel om te voorkomen dat op arbitraire, willekeurige wijze van de bevoegdheid gebruik wordt gemaakt.[33] Voorts overweegt het Hof in *Kruslin* dat indien in een wettelijke bepaling precies wordt aangegeven *wie* onderworpen mag worden aan de opsporingsmethode en bij *welke strafbare feiten* deze opsporingsmethode mag worden ingezet (hierin zit een proportionaliteitstoets verscholen), dat ook relevante waarborgen tegen misbruik

17. Hier wordt gekozen voor 'in overeenstemming' omdat dit ten eerste de letterlijke vertaling van de Engelse en Franse verdragstekst is en ten tweede omdat deze term beter duidelijk maakt dat het niet alleen noodzakelijk is dat de inbreuk 'bij wet is voorzien' maar dat de inbreuk ook moet geschieden 'in overeenstemming' met hetgeen wettelijk is geregeld. Zie daarover J. Gerards, *EVRM – Algemene beginselen*, Den Haag: Sdu Uitgevers 2011, p. 118.
18. Bijv. EHRM (GK) 10 mei 2001, appl. no. 25781/95, par. 295 (*Cyprus* t. *Turkije*).
19. Bijv. EHRM 12 mei 2000, appl. no. 35394/97, par. 27 (*Khan* t. *het Verenigd Koninkrijk*).
20. Eigenlijk kan deze voorwaarde als *specialis* van de eerste voorwaarde worden gezien. In Nederland kan voor elke privacy-inbreuk artikel 3 Polw 2012 worden gebruikt. Voor stelselmatige inbreuken op het recht op privacy is de bepaling echter niet toereikend omdat zij niet specifiek genoeg is geformuleerd. Zodoende bestaat mogelijk geen wettelijke basis voor grove inbreuken op privacy. Bijv. EHRM 25 september 2001, appl. no. 44787/98, par. 62-63 (*P.G. & J.H.* t. *het Verenigd Koninkrijk*).
21. Bijv. EHRM (GK) 26 november 2013, appl. no. 27853/09, par. 58 (*X.* t. *Letland*). Vgl. D.J. Harris, M. O'Boyle, E.P. Bates & C.M. Buckley, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights*, Oxford: Oxford University Press 2009, p. 400 e.v.
22. Bijv. EHRM (GK) 13 december 2012, appl. no. 22689/07, par. 91 (*De Souza Ribeiro* t. *Frankrijk*).
23. EHRM 25 maart 1983, appl. nr. 5947/72 e.a., par. 90 (*Silver en anderen* t. *het Verenigd Koninkrijk*) en EHRM 18 april 2013, appl. no. 19522/09, par. 28 (*M.K.* t. *Frankrijk*). Zie ook J. Vande Lanotte, *Handboek EVRM – deel 1. Algemene beginsel*, Antwerpen: Intersentia 2005, p. 196-197.
24. EHRM 26 april 1979, appl. no. 6538/74, par. 49 (*Sunday Times* t. *het Verenigd Koninkrijk*).
25. EHRM 28 maart 1990, appl. no. 10890/84, par. 68 (*Groppera Radio AG en anderen* t. *Zwitserland*).
26. Bijv. EHRM 14 maart 2013, appl. no. 24117/08, par. 123 (*Bernh Larsen Holding AS en anderen* t. *Noorwegen*).
27. Bijv. EHRM 2 augustus 1984, appl. no. 8691/79, par. 67 (*Malone* t. *het Verenigd Koninkrijk*) en EHRM 18 april 2013, appl. no. 19522/09, par. 28 (*M.K.* t. *Frankrijk*).
28. A. Galetta & P. de Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance', *Utrecht Law Review* 2014, 1, p. 60.
29. EHRM 28 maart 1990, appl. no. 10890/84, par. 68 (*Groppera Radio AG en anderen* t. *Zwitserland*).
30. EHRM 26 april 1979, appl. no. 6538/74, par. 49 (*Sunday Times* t. *het Verenigd Koninkrijk*).
31. EHRM 14 maart 2013, appl. no. 24117/08, par. 123-125 (*Bernh Larsen Holding AS en anderen* t. *Noorwegen*).
32. Bijv. EHRM 12 januari 2010, appl. no. 4158/05, par. 77 (*Gillan & Quinton* t. *het Verenigd Koninkrijk*). Overigens maakt een ongelimiteerde bevoegdheid het moeilijk voorzienbaar welk gedrag op die bevoegdheid kan worden gebaseerd. Zie daarover EHRM 12 juni 2008, appl. no. 78146/01, par. 125 (*Vlasov* t. *Rusland*).
33. EHRM (GK) 10 maart 2009, appl. no. 4378/02, par. 78 (*Bykov* t. *Rusland*).

doi: 10.5553/TBSenH/229567002021007005003

van de bevoegdheid opleveren.[34] Dit betekent dat een eventuele bevoegdheid geen *carte blanche* mag zijn, maar ook beperkende voorwaarden moet bevatten omtrent onder andere de autoriteit die tot toepassing beslist, bij welke strafbare feiten, bij welke verdenkingsgraad en met welk doel. Een belangrijke rol is daarbij weggelegd voor rechterlijke controle, zeker als het gaat om digitale opsporing zoals een *GPS-tracker* of een telefoontap.[35]

Als vierde moet de inbreuk op het recht op respect voor privacy *overeenkomstig* de wettelijke bepaling hebben plaatsgevonden. Een onrechtmatige handeling op basis van een duidelijke en precieze bepaling is normaliter redelijk onvoorzienbaar en hoogstwaarschijnlijk een arbitraire, willekeurige inbreuk op het recht op respect voor privacy. Het uitgangspunt van de *rule of law* is dat ook de Staat zich aan de geldende regels houdt.

3. De wettelijke grondslag van de ingezette opsporingshandelingen (naar Nederlands recht)

In deze paragraaf wordt bekeken welke wettelijke grondslag voor de handelingen van de politie als winkelier dienst kan doen, alvorens wij in paragraaf vier die grondslag toetsen aan hetgeen hierboven over het legaliteitsbeginsel als toetsingskader is beschreven. Hierbij gaan wij uit van de vroegsporingtitel van de Wet Bijzondere opsporingsbevoegdheden (hierna: Wet BOB), omdat *voorafgaand aan* de verkoop van de toestellen aan een persoon (vaak) (nog) geen (concrete) verdenking ten aanzien van die persoon zal zijn gerezen. Hierbij kan wel de volgende kanttekening worden geplaatst. Bijzondere opsporingsbevoegdheden kunnen in het kader van de vroegsporing worden ingezet op het moment dat nog geen concreet strafbaar feit is gepleegd.[36] Immers, in de vroegsporingtitel wordt gesproken over, kortgezegd, een redelijk vermoeden dat in een georganiseerd verband bepaalde misdrijven worden *beraamd* of gepleegd. Echter, er moet dan wel uit *feiten en omstandigheden* blijken dat sprake is van een *redelijk vermoeden* dat bepaalde misdrijven worden beraamd of gepleegd in georganiseerd verband. Thans is het voor ons, gelet op de beperkte informatie die over *Operation Trojan Shield* bekend is, lastig te beoordelen of aan deze maatstaf is voldaan (zie nader § 3.3).

34. EHRM 24 april 1990, appl. no. 11801/85, par. 35 (*Kruslin* t. *Frankrijk*).
35. EHRM 2 september 2010, appl. no. 35623/05, par. 71-72 (*Uzun* t. *Duitsland*).
36. Vgl. G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers en T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 292-293.

3.1 De ontwikkeling van de ANOM-hardware en de daarop geïnstalleerde software

In het eerder aangehaalde *affidavit* valt te lezen op welke wijze de FBI, met behulp van Australië en mogelijk ook andere landen, de cryptotelefoons heeft laten ontwikkelen.[37] De internationale partners hebben voorafgaand aan de verspreiding van de toestellen een *master key* ontwikkeld en ingebouwd in het op het toestel geïnstalleerde encryptiesysteem. Deze *master key* hecht zich heimelijk aan ieder bericht en maakt het ontsleutelen van deze berichten door de opsporingsinstanties mogelijk. Vanzelfsprekend is dit niet bekend bij, en onzichtbaar voor, de gebruikers van de toestellen. In het geval dat een ANOM-toestel zich buiten Amerika bevindt,[38] wordt ten behoeve van *Operation Trojan Shield* door middel van de *master key* automatisch een kopie van iedere boodschap naar een '*iBot*'-server buiten Amerika verstuurd. Op deze server wordt het bericht direct ontsleuteld en vervolgens weer versleuteld met een FBI-encryptiecode. Het opnieuw versleutelde bericht wordt hierop naar een tweede FBI '*iBot*'-server verzonden waar het opnieuw ontsleuteld wordt en waar de inhoud zichtbaar wordt gemaakt ten behoeve van de opsporing.[39]

Uit deze werkwijze blijkt duidelijk dat de autoriteiten verantwoordelijk zijn voor het toevoegen van een (gewenste) kwetsbaarheid in de toestellen.[40] Hoe dan ook, vanuit een legaliteitsperspectief is er met de ontwikkeling of aanschaf van hardware en software geen probleem. Er staat geen specifieke wettelijke grondslag voor de ontwikkeling van hardware en software in het Wetboek van Strafvordering, en dat is ook niet nodig. Het ontbreken van een wettelijke grondslag voor de hier besproken handeling is acceptabel nu het gebruik van technische hulpmiddelen bij verschillende opsporingsbevoegdheden wel specifiek is geregeld, zoals bijvoorbeeld in artikel 126s Sv. Dus het gebruik van een technisch hulpmiddel is bij sommige bijzondere opsporingsbevoegdheden wettelijk geregeld, maar niet nader is geregeld of deze hulpmiddelen moeten worden aangeschaft of zelf mogen worden ontwikkeld.[41] Met dat laatste kunnen de autoriteiten natuurlijk *tailor made* hulpmiddelen ontwikkelen die perfect passen bij de te onderzoeken situatie.

37. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 13-15, laatst geraadpleegd op 9 juli 2021.
38. Verrassend is dat het territorium van Amerika *geofenced* is tijdens de operatie, waardoor de berichten van gebruikers in Amerika niet konden worden vergaard. Het doel is de ontmanteling van buitenlandse organisaties. De grond ligt waarschijnlijk in het ontbreken van een *search warrant* op basis van het Vierde Amendement, en de problemen in het aanvragen daarvan voorafgaand aan de operatie (vgl. de discussie over het redelijk vermoeden in par. 3.3) Zie over *geofencing*: Redactie, 'Geofence Warrants and the Fourth Amendment: If You Build It, They Will Come', *134 Harv. L. Rev. 2508*.
39. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 13-15, laatst geraadpleegd op 9 juli 2021.
40. Dit wordt in § 4.1 en § 4.2 geproblematiseerd.
41. De gebruikte technische hulpmiddelen dienen wel aan bepaalde kwaliteitseisen te voldoen, deze zijn onder andere terug te vinden in het Besluit technische hulpmiddelen strafvordering van 20 oktober 2006, *Stb*. 2006, 524.

doi: 10.5553/TBSenH/229567002021007005003

3.2 De verspreiding van de toestellen

Na de ontwikkeling en een testfase in Australië zijn de toestellen volgens het *affidavit* verspreid via een door een criminele burgerinformant (*Criminal Human Source*, CHS) opgebouwd, maar niet door de autoriteiten te controleren, distributienetwerk.[42] De CHS die de toestellen heeft ontwikkeld, is ook verantwoordelijk geweest voor de verspreiding van de toestellen.[43] Het gehele distributienetwerk is daarna door andere(n) (criminelen) verder uitgebouwd. Zo heeft een door de Australische autoriteiten als *kingpin* bestempelde crimineel een cruciale rol gespeeld in de verspreiding van de toestellen.[44] Hij heeft de toestellen aangeprezen en anderen hebben de toestellen vervolgens gekocht omdat zij – gelet op de reputatie van deze *kingpin* – ervan uitgingen dat de toestellen goed beveiligd waren.[45] Hieruit blijkt dat de oorspronkelijke distributeur waarmee de FBI een *deal* heeft gesloten slechts de *conditio sine qua non* is voor de gehele operatie, maar dat de distributie vervolgens een eigen leven is gaan leiden via niet-controleerbare andere criminelen.

De vertaling van deze werkwijze naar een Nederlandse bevoegdheid is daarmee niet zo eenvoudig. Dit komt omdat uit het *affidavit* niet blijkt dat de CHS deelneemt aan een criminele organisatie. Daarnaast is het zeer te betwijfelen of het verstrekken van één goed te kwalificeren valt als het verlenen van medewerking aan een criminele organisatie, waarbij meespeelt dat de CHS geen zicht heeft op de distributie aan individuele kopers (en die kopers maken ook nog eens deel uit van veel verschillende criminele organisaties). Ondanks dat de werkwijze iets weg heeft van een infiltratie is het zeker geen standaard geval. Binnen de infiltratie kunnen echter ook andere methoden worden ingezet, zoals de pseudoverkoop, een projectmatige infiltratie en de *frontstore*-operatie.[46]

Een mogelijkheid is dat de toestellen verspreid zijn als onderdeel van een projectmatige infiltratie, waarbij de ANOM-toestellen aan de geïnfiltreerde organisatie zijn geleverd 'teneinde zicht te krijgen op activiteiten en werkwijzen, ten aanzien waarvan concrete aanwijzingen bestaan van gepleegde of nog te plegen misdrijven die tot de georganiseerde criminaliteit gerekend kunnen worden, met als doel het geheel of gedeeltelijk beëindigen van criminele activiteiten'.[47] Het is daarnaast denkbaar dat een *frontstore*-operatie[48] is gebruikt om de toestellen te verspreiden. In *casu* houdt dat in dat een *cover*bedrijf of een structuur van *cover*bedrijven is opgezet of geëxploiteerd door middel waarvan facilitaire ondersteuning in de vorm van de ANOM-toestellen aan criminele samenwerkingsverbanden is aangeboden.[49] Beide beschreven mogelijkheden hebben geen specifieke wettelijke grondslag, maar vallen onder de bredere grondslag van infiltratie.[50]

Toch lijken deze opties, en daarmee de infiltratie, niet passend. Alleen de verspreiding via de CHS is gecontroleerd, maar uit de berichtgeving blijkt dat de CHS andere distributeurs heeft ingezet en daarmee is het volledig oncontroleerbaar aan welke criminelen *casu quo* criminele organisaties de ANOM-toestellen zijn verstrekt. In die zin is het lastig te verdedigen dat de CHS – als infiltrant – medewerking heeft verleend aan (bij hem kenbare) criminele organisaties.

Naast deze verschillende mogelijkheden kan ook de algemene taakstellende bevoegdheid van de politie een rol spelen. Bij het tot stand komen van de Wet BOB heeft de wetgever zich namelijk terdege gerealiseerd dat het opsommen en regelen van allerlei bevoegdheden geen limitatief karakter kan hebben.[51] Bepaalde opsporingshandelingen kunnen, in het geval deze slechts een beperkte inbreuk op de persoonlijke levenssfeer opleveren en geen risico opleveren voor de integriteit van de opsporing, daarom ook gebaseerd worden op artikel 3 Polw 2012. Dit is onder bepaalde omstandigheden het geval bij pseudoverkoop.

In de artikelen 126i en 126q Sv worden pseudokoop en pseudodienstverlening geregeld voor de klassieke opsporing en de vroegsporing. De pseudo*ver*koop ligt hier dicht tegenaan, maar de pseudoverkoop valt niet onder deze wettelijke grondslag.[52] Ook al ontbreekt een specifieke wettelijke grondslag, in de jurisprudentie is wel een aantal gevallen van 'pseudoverkoop' te vinden.[53] De Hoge Raad heeft in 2011 moeten oordelen over een zaak waarin de verdachte telefonisch 1.000 kilogram paracetamol en 400 kilogram cafeïne heeft besteld bij een firma. De farmaceutische grondstoffen zijn vervolgens op verzoek van de autoriteiten geleverd.[54]

De Hoge Raad overweegt dat in *casu* sprake is van een niet in de wet geregelde opsporingsmethode en dat een dergelijke methode alleen mag worden ingezet indien hierbij een beperkte inbreuk wordt gemaakt op grondrechten van burgers of wanneer de inzet van de methode 'niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing'.[55] De Hoge Raad hecht hierbij waarde aan het gegeven dat bij een pseudoverkoop van *niet-illegale* stoffen veel minder kans bestaat dat een ver-

42. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 15, laatst geraadpleegd op 9 juli 2021.
43. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 15, laatst geraadpleegd op 9 juli 2021.
44. news.sky.com/story/anom-alleged-drug-kingpin-told-to-hand-himself-in-after-being-tricked-into-spreading-fake-phone-app-12328192, laatst geraadpleegd op 19 juli 2021.
45. news.sky.com/story/anom-alleged-drug-kingpin-told-to-hand-himself-in-after-being-tricked-into-spreading-fake-phone-app-12328192, laatst geraadpleegd op 19 juli 2021.
46. *Kamerstukken II* 1995/96, 24072, nr. 10, p. 229.
47. *Kamerstukken II* 1995/96, 24072, nr. 10/11, p. 229.
48. *Kamerstukken II* 1995/96, 24072, nr. 10/11, p. 229.
49. *Kamerstukken II* 1995/96, 24072, nr. 10/11, p. 229.
50. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 31.
51. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 9.
52. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 34.
53. Zie bijvoorbeeld HR 5 maart 2019, ECLI:NL:HR:2019:298 en HR 20 december 2011, ECLI:NL:HR:2011:BP0199.
54. HR 20 december 2011, ECLI:NL:HR:2011:BP0199, r.o. 2.3.
55. HR 20 december 2011, ECLI:NL:HR:2011:BP0199, r.o. 2.6.

doi: 10.5553/TBSenH/229567002021007005003

weer met betrekking tot uitlokking kans van slagen heeft.[56] Tevens acht de Hoge Raad het van belang dat de verschillende opsporingshandelingen zijn vastgelegd in een schriftelijke overeenkomst tussen de officier van justitie en de burger zodat dit handelen transparant en achteraf toetsbaar is.[57] De Hoge Raad lijkt in dit geval van mening te zijn dat de verkoop van de middelen op de algemene taakstellende bevoegdheid van de politie (artikel 3 PolW 2012 jo. artikel 141 respectievelijk 142 Sv) kan worden gebaseerd, vanwege de beperkte inbreuk op de grondrechten van de verdachte en gezien de levering van de legale goederen geen groot risico voor de integriteit en de beheersbaarheid van de opsporing met zich bracht.[58]

Op basis van de overwegingen uit het hierboven beschreven arrest kan gesteld worden dat de verspreiding van de ANOM-toestellen mogelijk heeft plaatsgevonden op een vergelijkbare wijze en dus ook berust op de algemene taakstellende bevoegdheid (artikel 3 PolW 2012 jo. artikel 141 respectievelijk 142 Sv). De telefoons zijn op grond van een overeenkomst verspreid door een burger, die als tegenprestatie voor de verspreiding strafvermindering heeft gekregen. Hierbij is het van belang dat alles goed is geverbaliseerd. Zoals uit het beschreven arrest blijkt, hecht de Hoge Raad veel waarde aan de processen-verbaal die het hele opsporingstraject inzichtelijk maken waardoor de handelingen achteraf ook getoetst kunnen worden. Bij de verspreiding van de toestellen lijkt het voorts ook zo te zijn dat het gevaar dat het OM niet of slechts moeizaam kan aantonen dat het *Tallon*-criterium is nageleefd, zich niet voordoet.[59] Immers, een *PGP*-telefoon is een legaal goed,[60] waardoor de verkoop, aankoop en het voorhanden hebben van een *PGP*-toestel geen strafbaar feit oplevert.

3.3 Het verkrijgen van vertrouwelijke communicatie

Zoals eerder genoemd, ondervindt de politie problemen met vergrendeling en versleuteling bij digitale opsporing. Nu de eerder opgedoekte communicatiediensten *EncroChat* en *Sky ECC* populair waren, verwachtte de politie dat criminelen op zoek zouden gaan naar een nieuw communicatiemiddel. Daar heeft de politie met ANOM op geanticipeerd. Sinds oktober 2019 verkreeg de politie communicatie via de ANOM-*smartphones*, in totaal gedurende anderhalf jaar.[61] Deze gang van zaken komt sterk overeen met de handelingen die gebruikelijk zijn wanneer de autoriteiten gebruikmaken van de bevoegdheid om vertrouwelijke communicatie op te nemen. Bij het opnemen van vertrouwelijke communicatie vindt de opname bij de zender of de ontvanger plaats, zoals bij ANOM het geval is. De berichten die worden verzonden, worden direct door de autoriteiten opgeslagen.

Artikel 126s Sv regelt de bevoegdheid tot het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel indien sprake is van vroegsporing. Met de term vertrouwelijkheid wordt bedoeld dat de communicatie in beslotenheid plaatsvindt.[62] De term communicatie gaat verder dan alleen gesprekken; ook berichten en e-mails kunnen hieronder worden geschaard. De uitwisseling van gegevens tussen twee of meer personen volstaat (er is dus interactie tussen twee personen).[63] Ook ziet de bevoegdheid op het onderscheppen van gegevens nog voordat de communicatie plaatsvindt, bijvoorbeeld via een *bug* op een computer voordat gegevens door codering onleesbaar zijn geworden.[64] Het technische hulpmiddel dat wordt ingezet moet voldoen aan de eisen van artikel 126ee Sv en de daarop gebaseerde AMvB.[65]

De bevoegdheid is in werking getreden als aanvulling op de bevoegdheid tot het aftappen van de telefoon. De aftapbevoegdheid zou omzeild kunnen worden door gebruik te maken van *encrypted* elektronische post. Om dit te voorkomen heeft de wetgever de bevoegdheid tot het opnemen van vertrouwelijke communicatie opgenomen: hierdoor kan communicatie worden onderschept voordat encryptie plaatsvindt, aangezien de gegevensinvoer kan worden onderschept voordat er gecommuniceerd wordt.[66] Dit is wat tijdens *Operation Trojan Shield* is gebeurd: de communicatie is direct doorgezet naar een door de autoriteiten beheerde server en daar eerst ontsleuteld en vervolgens, met een andere sleutel, versleuteld opgeslagen.

3.4 De analyse van de inhoud van de communicatie

Uit artikel 126s Sv volgt de bevoegdheid tot het opnemen, het opslaan en het ontsleutelen van vertrouwelijke communicatie. De opgenomen gegevens kunnen zeer bruikbaar zijn voor het opsporingsonderzoek, maar niet als deze gegevens niet geanalyseerd mogen worden. De huidige wet- en regelgeving kent geen expliciete wettelijke grondslag voor de analyse van de inhoud van ver-

56. HR 20 december 2011, ECLI:NL:HR:2011:BP0199, r.o. 2.6.
57. HR 20 december 2011, ECLI:NL:HR:2011:BP0199, r.o. 2.6.
58. Vgl. HR 5 maart 2019, ECLI:NL:HR:2019:298.
59. Dit is vanzelfsprekend afhankelijk van de specifieke omstandigheden van het geval. In het algemeen kan worden gesteld dat de politie enkel een communicatiemiddel heeft verschaft en dat dit middel op zichzelf geen strafbare handelingen uitlokt.
60. Wel wordt in de rechtspraak geoordeeld dat het een feit van algemene bekendheid is dat criminelen vaak gebruikmaken van een *PGP*-telefoon, vanwege de anonimiteit en de versleutelde communicatie. Zie bijv. Rb. Den Haag 7 januari 2021, ECLI:NL:RBDHA:2021:432, r.o. 3.4.4.1 en Rb. Den Haag 1 november 2019, ECLI:NL:RBDHA:2019:14878, r.o. 4.4.
61. nos.nl/artikel/2384211-politie-trots-advocaten-kritisch-na-ongekende-klap-voor-criminelen, laatst geraadpleegd op 9 juni.
62. K. van der Meijde, 'Opnemen vertrouwelijke communicatie met een technisch hulpmiddel (art. 126l Sv en art. 126s Sv)', in: M.F. Attinger e.a./P.A.M. Mevis e.a., *Handboek Strafzaken*, Deventer: Wolters Kluwer 2014, p. 1.
63. T. Blom, 'Opnemen van vertrouwelijke communicatie bij georganiseerde criminaliteit', in: *Tekst en Commentaar Strafvordering*, Deventer: Kluwer 2021, p. 1. Zie ook Aanwijzing opsporingsbevoegdheden, § 2.5.
64. Blom 2021, p. 2.
65. Besluit technische hulpmiddelen strafvordering van 20 oktober 2006, *Stb*. 2006, 524.
66. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35.

kregen gegevens(dragers);[67] dit geldt voor alle in beslag genomen gegevensdragers en ook voor de door de inzet van bijzondere opsporingsbevoegdheden verkregen gegevens.[68]

Uit de Nederlandse jurisprudentie blijkt dat de artikelen 94, 95 en 96 Sv, naast een grondslag voor inbeslagneming, ook een wettelijke basis vormen voor de bevoegdheid om aan in beslag genomen voorwerpen onderzoek te verrichten ten behoeve van de waarheidsvinding, teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen.[69] Opgeslagen gegevens in een *smartphone* zijn daarvan niet uitgezonderd. De bevoegdheid tot inbeslagname is immers niet in het belang van het onderzoek, als de in beslag genomen voorwerpen vervolgens niet geanalyseerd mogen worden.

Hetzelfde geldt voor het opnemen van vertrouwelijke communicatie of het opnemen van communicatie via een telecommunicatiedienst: ook dan volgt de bevoegdheid tot het bekijken en analyseren van de verkregen vertrouwelijke communicatie uit de bevoegdheid tot het opnemen van de communicatie. Dit terwijl de inbreuk op de privacy bij de inzet van deze opsporingshandeling (het bekijken en analyseren van de vergaarde informatie) groter is dan bij de hiervoor genoemde opsporingshandelingen. Pas op het moment dat de *inhoud* van de communicatie wordt bekeken en gewaardeerd, verkrijgen de autoriteiten daadwerkelijk zicht op bepaalde aspecten van iemands privéleven. De hoeveelheid data – in het onderhavige onderzoek zijn in anderhalf jaar tijd 27 miljoen gesprekken en berichten van ca. 9.000 gebruikers verkregen en (gedeeltelijk) geanalyseerd –[70] maakt duidelijk dat de analyse daarvan een grove inbreuk op de privacy maakt. Het is derhalve enigszins vreemd dat naast de verkrijgingshandelingen – zoals de inbeslagname of het opnemen van vertrouwelijke communicatie – de analyse van de verkregen gegevens niet ook een expliciete wettelijke grondslag kent. Al is dat in het geval van het opnemen van vertrouwelijke communicatie minder problematisch gezien de waarborgen van artikel 126s Sv in vergelijking met de afwezigheid van waarborgen bij de inbeslagnamebevoegdheid.

Voor het onderhavige geval betekent dit dat artikel 126s Sv de grondslag biedt voor het opnemen, opslaan en het ontsleutelen van vertrouwelijke communicatie. De rechtmatig opgenomen vertrouwelijke communicatie impliceert de bevoegdheid de verkregen inhoud te analyseren.

67. HR 9 februari 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63, m.nt. Van Toor & Beekhuis; *TBS&H* 2021, 3, m.nt. Beekhuis & Van Toor.
68. Het gaat in onderhavige zaak om de situatie dat de niet in beslag genomen telefoon wordt geanalyseerd a.d.h.v. de verkregen vertrouwelijke informatie. Er wordt in deze paragraaf een lijn getrokken met de inbeslaggenomen telefoon. Wanneer de autoriteiten in onderhavige operatie daadwerkelijk een verdachte hebben opgepakt, kan ook de telefoon in beslag worden genomen. Dan is de hierna genoemde jurisprudentie ook van toepassing. Dit vervolgonderzoek wordt verder buiten beschouwing gelaten.
69. O.a. HR 4 april 2017, ECLI:NL:HR:2017:580, 584, 588 & 592.
70. nos.nl/artikel/2384211-politie-trots-advocaten-kritisch-na-ongekende-klap-voor-criminelen, laatst geraadpleegd op 9 juni.

4. Operation Trojan Shield in het licht van het legaliteitsbeginsel

Hierboven in paragraaf 3 zijn voor de verschillende handelingen van *Operation Trojan Shield* de meest logische wettelijke grondslagen uitgewerkt. Wij komen tot de conclusie dat de ontwikkeling of aanschaf van de toestellen geen specifieke wettelijke strafvorderlijke grondslag behoeft; dat de verspreiding van de toestellen het meest lijkt op pseudoverkoop (artikel 3 PolW 2012) en; dat het opnemen van vertrouwelijke communicatie en de analyse van de inhoud van de communicatie op basis van de daarvoor geldende grondslag uit de Wet BOB kan worden gebaseerd (artikel 126s Sv).

De laatste drie opsporingshandelingen maken allemaal inbreuk op het recht op respect voor privacy. Na de vaststelling dat de privacy op ten minste één onderdeel wordt beperkt, is het noodzakelijk om te beoordelen of deze beperking onder artikel 8 lid 2 EVRM is gerechtvaardigd. Immers, alleen ongerechtvaardigde inbreuken op artikel 8 lid 2 EVRM leveren een schending van het recht op respect voor eenieder zijn privé- en familieleven, zijn woning en zijn correspondentie op. Een belangrijk onderdeel van die toetsing is dat de inbreuk op het recht op respect voor privacy in overeenstemming met een wettelijke bepaling moet plaatsvinden. In paragraaf 2 is dit criterium nader uitgewerkt zodat in deze paragraaf kan worden beoordeeld of de hierboven beschreven opsporingshandelingen artikel 8 lid 2 EVRM schenden. In deze paragraaf komen de voorgaande twee paragrafen samen en worden de verschillende opsporingshandelingen getoetst aan het legaliteitsbeginsel.

4.1 De ontwikkeling van de ANOM-hardware en de daarop geïnstalleerde software en de verspreiding van de toestellen

De ontwikkeling van de ANOM-hardware en de daarop geïnstalleerde software brengt op zichzelf geen inmenging in de privacy van de verdachten met zich. De toestellen zijn op het moment van ontwikkeling immers nog niet in gebruik bij de verdachten en zij hebben zelfs nog geen weet van de komst van de nieuwe ANOM-toestellen. Nu er geen sprake lijkt te zijn van een inbreuk op de privacy, is de ontwikkeling van de toestellen niet problematisch in het licht van het legaliteitsbeginsel.

Deze handeling onttrekt zich hierdoor volledig aan de controle van de rechterlijke autoriteiten. Hoewel dit op dit moment gebruikelijk is voor handelingen die geen inbreuk op de privacy opleveren, kan hier wel kritiek op worden geuit. De ontwikkeling van de toestellen heeft

doi: 10.5553/TBSenH/229567002021007005003

immers als enige doel dat deze ingezet kunnen worden om wél een inbreuk op de privacy van velen te bewerkstelligen. Het is daarom goed verdedigbaar dat de overheidsinstelling niet alleen zou moeten anticiperen op de waarborgen die vanaf het moment dat de inbreuk op de privacy start vereist zijn, maar dat ook gedurende deze stap in het onderzoek al meerdere waarborgen moeten gelden.

Dit zou des te meer wenselijk zijn nu de ontwikkeling van de toestellen, zoals dat volgens het *affidavit* heeft plaatsgevonden, ook risico's met zich brengt. Het gebruikmaken van een zelfontwikkelde opzettelijke kwetsbaarheid is (zeer) risicovol, nu zo'n *backdoor* makkelijker is om uit te buiten door kwaadwillende derden en het schadelijk is wanneer deze uitbuitingspoging slaagt.[71] Daarnaast is het niet bekend of de software volledig zelf is ontwikkeld, of dat er ook gebruik is gemaakt van commerciële software. In het Verslag toezicht wettelijke hackbevoegdheid politie 2020 wordt kritiek geleverd op het gebruik van commerciële software, omdat dit risico's oplevert voor de betrouwbaarheid van het bewijsmateriaal nu er sprake kan zijn van ongecontroleerde toegang tot het bewijs door de leverancier van de software.[72]

Bij het gebruikmaken van *backdoors* en kwetsbaarheden van software binnen de opsporing is het daarom van belang dat rekening wordt gehouden met de aanzienlijke mogelijkheid dat ook anderen misbruik kunnen maken van deze opties.[73] Om dit te voorkomen, dienen er waarborgen tegen deze inbreuken door anderen ingebouwd te worden in het systeem.[74] Indien dit niet het geval is, zal dit gevolgen kunnen hebben voor de waarde van het bewijsmateriaal. Naast de mogelijkheid dat bij het gebruik van commerciële software, de leverancier toegang zou kunnen hebben tot het bewijsmateriaal, is het ongeacht de gebruikte software ook mogelijk dat andere (criminele) burgers zichzelf toegang willen verschaffen. Zo zou het voor rivaliserende criminele organisaties interessant kunnen zijn om gebruik te maken van een kwetsbaarheid van bijvoorbeeld een *PGP*-toestel of de server waar de versleutelde berichten binnenkomen, om de opsporingsambtenaren op het spoor van hun rivaal te brengen door valse berichten te planten en hiermee de competitie uit te schakelen. De mogelijkheid dat er met de berichten en daarmee met bewijsmateriaal is geknoeid, zal een grote uitwerking op de rechtszaak kunnen hebben.[75] Op deze manier komt mogelijkerwijs de betrouwbaarheid van alle communicatie, en daarmee het bewijsmateriaal dat daaruit voort is gevloeid, op het spel te staan. Het gebruikmaken van zelfgecreëerde kwetsbaarheden en *backdoors* brengt aldus risico's met zich, en de inzet hiervan zal dan ook terughoudend moeten worden toegepast. Indien het mogelijk is om een bestaande kwetsbaarheid uit te buiten in plaats van het inbouwen van een nieuwe kwetsbaarheid, zal dat in het kader van een subsidiariteitstoets meegewogen moeten worden.

Bij de ontwikkeling van de ANOM-toestellen zijn deze waarborgen ook van belang, zodat de tijdens de operatie vergaarde bewijsmiddelen niet ter discussie komen te staan. Op basis van bovenstaande beschreven werkwijze lijkt de FBI hier gedurende *Operation Trojan Shield* voldoende aandacht aan te hebben besteed, door gebruik te maken van de ontwikkelde *master key*, de verschillende servers en hun eigen encryptiecodes. Het is wel van groot belang dat bij deze handelingen uit het voortraject, die zich aan het zicht van rechterlijke controle onttrekken, aandacht bestaat voor de eventuele gevaren van de *backdoor* en de aanschaf van hard- en/of software en de consequenties daarvan voor de betrouwbaarheid van het bewijs. Daarom moet ook in dit stadium al transparant worden geverbaliseerd teneinde een toetsing achteraf mogelijk te maken.

4.2 De verspreiding van de toestellen

Indien de verkoop van de toestellen door middel van een pseudoverkoop-constructie heeft plaatsgevonden, zal hierbij de privacy van de verdachten bij enkel de verkoop nauwelijks in het geding zijn gekomen. Het zal dan slechts een transactie zijn geweest, waarbij het toestel door hoogstwaarschijnlijk een (criminele) burger aan een andere (criminele) burger (de latere verdachte) is verkocht. Hierbij wordt uiteraard wel wat informatie over een persoon verkregen; er vindt persoonlijk contact plaats, er wordt een afspraak gemaakt, een ontmoeting geregeld en deze ontmoeting vindt ook daadwerkelijk plaats. Er zijn verder echter geen (persoonlijke) banden tussen de partijen en er is gedurende de transactie op geen enkele wijze een min of meer compleet beeld van het privéleven van een verdachte verkregen, of op enige andere wijze een inbreuk gemaakt op het recht op respect voor privacy van de koper. De algemene taakstellende bevoegdheid uit artikel 3 Polw 2012 jo. artikel 141 respectievelijk 142 Sv is daarom een voldoende grondslag voor deze geringe inbreuk op de privacy. Daarnaast is de door de wetgever uitgesproken zorg dat verweren omtrent het *Tallon*-criterium bij pseudoverkoop moeilijk te weerleggen zijn naar verwachting ook geen pro-

71. S.M. Bellovin et al., 'Going Bright: Wiretapping without Weakening Communications Infrastructure', *IEEE Security and Privacy* 2013, 1, p. 65.
72. www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020, laatst geraadpleegd op 6 augustus 2021.
73. B.J. Koops & J.J. Oerlemans, 'Formeel strafrecht en ICT', in: B.J. Koops & J.J. Oerlemans (red.) *Strafrecht en ICT*, Monografieën recht en informatietechnologie, Den Haag: Sdu 2019, p. 138-139.
74. Enkele waarborgen volgen al uit het Besluit technische hulpmiddelen strafvordering van 20 oktober 2006, *Stb*. 2006, 524. Zo dient bijvoorbeeld op grond van artikel 12 van dit besluit het technische hulpmiddel, dat buiten het zicht van de opsporingsambtenaren wordt gebruikt, zodanig beveiligd te worden dat technische veranderingen achteraf zo veel mogelijk zijn vast te stellen.
75. Hierbij zal het wel van belang zijn dat de verdediging concrete feiten en omstandigheden aanvoert waaruit blijkt dat het bewijsmateriaal niet betrouwbaar is. Vgl. ECLI:NL:GHARL:2020:2261 waarin het hof vooropstelt dat van geen enkel ICT-systeem dat verbinding heeft met het internet uit valt te sluiten dat het systeem kan worden gehackt of dat data op andere wijze door technische omstandigheden zouden kunnen zijn aangetast of door menselijk ingrijpen vervalst zouden kunnen zijn.

bleem. De verkoop van een telefoontoestel, zelfs een bijzonder toestel zoals dit, is geen uitlokking van een strafbaar feit.

De verspreiding van de toestellen met de (hierboven al aangestipte) gewilde kwetsbaarheid zou wel als problematisch in het licht van de integriteit van de opsporing kunnen worden gezien. Volgens de Hoge Raad bieden algemene wettelijke bepalingen alleen dan een toereikende wettelijke grondslag voor opsporingshandelingen als de handeling slechts een geringe inbreuk op een grondrecht maakt *en* zij de beheersbaarheid en integriteit van de opsporing niet aantast. Door het inbouwen van een *backdoor* wordt de situatie gecreëerd dat ook anderen daarvan gebruik kunnen maken. Zeker als rivaliserende organisaties van zo'n *backdoor* gebruik kunnen maken, is dat in het kader van het integriteitscriterium potentieel gevaarlijk. Ook in het licht van deze toets is het derhalve belangrijk dat duidelijkheid over de *backdoor* wordt gegeven.

De inzet van (criminele) burgers bij de verspreiding van de toestellen verdient ook aandacht. Deze burgers hebben een belangrijke rol gespeeld in *Operation Trojan Shield*, wat hen wellicht niet in dank zal worden afgenomen door leden van de criminele organisaties die de toestellen hebben afgenomen. Op welke wijze zal de overheid hen beschermen tegen mogelijke vergeldingsacties? Indien de overheid op de hoogte is van een op hand zijnde situatie waarin het leven van een burger gevaar loopt, heeft zij een inspanningsverplichting om deze burger te beschermen.[76] De Australische autoriteiten roepen daarom een onvindbare crimineel op zich vrijwillig bij de autoriteiten te melden[77] (en daarmee is ook direct het probleem van de onvindbaarheid opgelost).

4.3 Het verkrijgen van vertrouwelijke communicatie

Zoals is opgemerkt in paragraaf 2 verlangt het EHRM dat de wet aan bepaalde kwaliteitseisen voldoet bij een inbreuk op artikel 8 lid 2 EVRM. Het opnemen van vertrouwelijke communicatie is, anders dan de hiervoor besproken handelingen, een duidelijke en vergaande inmenging in de privacy van degenen die deelnemen aan de communicatie. In totaal zijn tijdens *Operation Trojan Shield* in anderhalf jaar tijd 27 miljoen gesprekken en berichten van circa 9.000 gebruikers verkregen. Deze privacy-inbreuk is frequent, intensief en voor een lange duur, maar vindt hoofdzakelijk niet plaats in de privésfeer. De ANOM-*smartphones* werden vermoedelijk voornamelijk 'zakelijk' gebruikt, maar ook zakelijke communicatie valt onder de bescherming van artikel 8 EVRM.[78]

Het EHRM heeft geoordeeld dat criminelen er weliswaar op moeten rekenen dat er een inbreuk op hun privacy wordt gemaakt, omdat er bijvoorbeeld een risico bestaat dat een *undercover*agent bewijs probeert te verzamelen jegens hen, maar dit betekent niet dat criminelen hun recht op respect voor privacy volledig prijsgeven enkel vanwege het feit dat criminaliteit geen rechtens te beschermen belang zou zijn.[79] Daarnaast is het niet ondenkbaar dat een deel van het privéleven van de (criminele) gebruikers zich afspeelt binnen het criminele milieu, en dat daartoe de ANOM-*smartphones* ook zijn gebruikt.[80]

Al met al is het opnemen van vertrouwelijke communicatie, zeker als onduidelijk is op welke wijze het communicatiemiddel wordt gebruikt, een ingrijpende bevoegdheid waar een specifieke wettelijke grondslag voor vereist is. Dit blijkt ook uit de Wet BOB: daarin is namelijk een specifiek artikel met meerdere waarborgen voor het opnemen van vertrouwelijke communicatie opgenomen.

In paragraaf 3.3 is uiteengezet dat artikel 126s Sv de meest waarschijnlijke en logische grondslag voor het verkrijgen van de vertrouwelijke communicatie uit de ANOM-*smartphones* is. De bevoegdheid is expliciet in de wet opgenomen en daarmee in overeenstemming met het door het EHRM gehanteerde *law*-begrip. Een burger kan aan de hand van het artikel voorzien in welke gevallen de overheid de bevoegdheid mag inzetten en dat gebruik mag worden gemaakt van technische hulpmiddelen. Wel kan het voor een burger lastig zijn om te voorzien dat de overheid deze bevoegdheid onder onderhavige omstandigheden inzet. Dit hoeft geen problemen in het licht van het legaliteitsbeginsel op te leveren, gelet op de kwaliteit van de wet. Burgers kunnen inschatten in welke *gevallen* hun vertrouwelijke communicatie opgenomen kan worden en welke *waarborgen* dan gelden.

Dat de vertrouwelijke communicatie *opgenomen moet worden* is een waarborg, daar dit controle achteraf mogelijk maakt.[81] Daarnaast is het opnemen van vertrouwelijke informatie alleen toegestaan door opsporingsambtenaren op (schriftelijk) bevel[82] van de officier van justitie in een geval als bedoeld in artikel 126o lid 1 Sv, zijnde een uit feiten of omstandigheden voortvloeiend redelijk vermoeden dat in georganiseerd verband misdrijven als omschreven in artikel 67 lid 1 Sv worden beraamd of gepleegd die gezien hun aard of de samenhang met

76. EHRM 28 januari 2014, *EHRC* 2014, 144, m.nt. R.S.B. Kool, par. 144 (*O'Keeffe t. Ierland*).
77. news.sky.com/story/anom-alleged-drug-kingpin-told-to-hand-himself-in-after-being-tricked-into-spreading-fake-phone-app-12328192, laatst geraadpleegd op 6 augustus 2021.
78. EHRM, *Guide on Article 8 of the European Convention on Human Rights*, december 2020, p. 23.
79. EHRM 15 juni 1992, nr. 12433/86, ECLI:CE:ECHR:1992:0615JUD001243386, par. 21-40 (*Ludï t. Zwitserland*).
80. *Themastudie Georganiseerde Criminaliteit*, (Analistennetwerk Nationale Veiligheid, bijlage bij *Kamerstukken II* 2021, 29911, nr. 315).
81. Zie ook art. 126c Sv. Daarin wordt (kort gezegd) bepaald dat alle voorwerpen waaraan gegevens ontleend kunnen worden die zijn verkregen door het opnemen van vertrouwelijke communicatie bewaard moeten blijven tot twee maanden na beëindiging van de zaak.
82. Zie voor de inhoud van het bevel art. 126s lid 3 Sv. Bij 'dringende noodzaak' mag het bevel mondeling worden gegeven zolang het bevel dan binnen drie dagen op schrift wordt gesteld. Zie art. 126s lid 6 jo. art. 126g lid 6 Sv. Dit geldt ook voor de aanvulling, verlenging of beëindiging van het bevel, zie art. 126s lid 6 jo. art. 126g lid 8 Sv.

doi: 10.5553/TBSenH/229567002021007005003

andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren. Bij het opnemen van vertrouwelijke informatie moet sprake zijn van een redelijk vermoeden dat een persoon die deelneemt aan de communicatie betrokken is bij het in het georganiseerd verband beramen of plegen van misdrijven en dat deze persoon ook deelneemt aan de communicatie. Daarnaast mag vertrouwelijke informatie pas worden opgenomen indien het onderzoek dit dringend vordert. Met deze eis is de subsidiariteitstoets in de wettelijke bevoegdheid neergelegd.[83] Ook is een schriftelijke machtiging van de rechter-commissaris op vordering van de officier van justitie vereist, zo volgt uit lid 4.[84] Leden 3, 5 en 8 bevatten aanvullende waarborgen, zoals dat het bevel een maximumtermijn heeft van vier weken (exclusief verlenging) en dat van het opnemen ook een proces-verbaal wordt opgemaakt. Deze leden van artikel 126s Sv betreffende de geldigheidsduur, de eisen aan het bevel van de officier van justitie en de gevallen, dragen zowel bij aan de voorzienbaarheid als aan het tegengaan van willekeur. Artikel 126s Sv is allesbehalve een *carte blanche* en *Operation Trojan Shield* zou naar Nederlands recht op dat artikel kunnen zijn gebaseerd. Twee problematische aspecten van *Operation Trojan Shield* in het licht van deze waarborgen zijn (1) het *redelijk vermoeden* dat strafbare feiten worden beraamd of gepleegd en dat de persoon die daarvoor verantwoordelijk is deelneemt aan de communicatie; en (2) de subsidiariteitstoets.

Uit artikel 1260 Sv volgt namelijk dat sprake moet zijn van een redelijk vermoeden dat in georganiseerd verband misdrijven als omschreven in artikel 67 lid 1 Sv worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren. In het *affidavit* is uiteengezet dat de communicatiemiddelen van *Phantom Secure* uitsluitend door leden van criminele organisaties, voornamelijk drugshandelaren, zijn aangeschaft.[85] Ook in de Australische *beta*-fase van *Trojan Shield* zijn de ANOM-*smartphones* alleen voor criminele doeleinden gebruikt.[86] Het derde land dat actief bij *Trojan Shield* betrokken was, en waarvan wij in de inleiding hebben gesteld dat dit Nederland kan zijn, heeft dit niet getest.[87]

83. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35.
84. Uit § 2.5 Aanwijzing opsporingsbevoegdheden blijkt dat de officier van justitie eerst toestemming binnen het OM dient te verkrijgen, voordat hij een vordering bij de rechter-commissaris mag indienen. Voor een wijziging, aanvulling of verlenging van het bevel is ook een machtiging van de rechter-commissaris vereist (art. 126s lid 6 jo. art. 126s lid 8 Sv). Lid 7 voegt hieraan toe dat bij dringende noodzaak de machtiging van de rechter-commissaris mondeling kan worden gegeven. De rechter-commissaris moet zijn machtiging dan wel binnen drie dagen alsnog op schrift stellen.
85. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, p. 5, laatst geraadpleegd op 27 juni 2021.
86. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 15, laatst geraadpleegd op 19 juli 2021.
87. www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record,rn.17, laatst geraadpleegd op 19 juli 2021.

Dit kan problematisch zijn in het licht van de subsidiariteit als de Nederlandse autoriteiten de afweging omtrent de inzet van de ANOM-*smartphones* en met name de opname van de communicatie hebben gemaakt op basis van het gebruik van de toestellen in andere landen. Maar ook op het punt van het *redelijk vermoeden* kan het voorgaande problematisch zijn. Immers, vertrouwelijke communicatie in de vroegsporing kan enkel worden opgenomen als sprake is van het hierboven beschreven vermoeden dat in georganiseerd verband bepaalde misdrijven worden beraamd of gepleegd. Of reeds voldoende informatie aanwezig was waaruit dat kon worden afgeleid voor de Nederlandse situatie, is op dit moment – gelet op de thans beschikbare informatie over de operatie – onduidelijk.

Voorts geldt dat de vertrouwelijke communicatie in het kader van de vroegsporing alleen mag worden opgenomen indien *uit feiten en omstandigheden* een redelijk vermoeden bestaat dat *een persoon die aan deze communicatie deelneemt* ook betrokken is bij het beramen of plegen van misdrijven in het georganiseerd verband.[88] De telefoons zijn in eerste instantie verspreid door een *CHS*, maar daarna ook door anderen (zie § 3.2). De autoriteiten hebben aldus geen zicht gehad op de verspreiding: zij wisten niet aan wie de telefoons zouden worden verkocht (tenzij daar duidelijke afspraken over zouden zijn gemaakt, maar dat lijkt niet voor de hand te liggen). Of dat een persoon was die zelf, of zijn gesprekspartner, voldoet aan het genoemde criterium is dan eveneens niet duidelijk. De vraag of genoeg informatie voorhanden was waaruit de autoriteiten hebben kunnen afleiden dat een persoon die deelneemt aan de communicatie ook betrokken was bij het beramen of plegen van misdrijven in het georganiseerd verband kan nu – op basis van de openbare stukken – dan ook nog niet worden beantwoord.

Hoe dan ook, uit het *affidavit* en de *beta*-fase blijkt dat de ANOM-*smartphones*, als opvolger van de inmiddels in onbruik geraakte versleutelde communicatiemiddelen, enkel door leden van de hierboven genoemde criminele organisaties worden aangeschaft. Grootschalige (internationale) drugs- en of wapenhandel, en het geweld dat daarmee gepaard gaat, zijn bij uitstek misdrijven die de rechtsorde ernstig kunnen schokken door de omvang en gevolgen voor de samenleving.[89] Het verkrijgen van vertrouwelijke communicatie van de ANOM-*smartphones* zal naar verwachting de subsidiariteitstoets doorstaan. Wel zal per geval moeten blijken of er geen meer voor de hand liggende *lichtere* middelen beschikbaar zijn geweest om dergelijke criminele organisaties in kaart te brengen. Dit geldt ook voor het criterium 'redelijk vermoeden': of hieraan is voldaan, kan per geval verschillen.

In het verlengde van het voorgaande kan nog worden opgemerkt dat het ook problematisch kan zijn dat van

88. Art. 126s lid 1 Sv.
89. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 24-25.

alle ANOM-*smartphones* die zijn verspreid in *Operation Trojan Shield* vertrouwelijke communicatie is verkregen. Immers, van alle door derden verspreide ANOM-*smartphones* is de communicatie opgenomen en gedecrypt, zodat inzage kon worden verkregen in de inhoud van de verstuurde berichten. Er heeft – zover wij weten op basis van de thans beschikbare informatie – geen selectie aan de poort plaatsgevonden: noch voor wat betreft de gebruikers, noch voor wat betreft de communicatie. Het was bij de opsporingsautoriteiten op voorhand uiteraard ook niet bekend wie precies deze *smartphones* zouden afnemen. Bovendien was ook na afname van de ANOM-*smartphones* de identiteit van de gebruiker nog niet bekend bij de opsporingsautoriteiten, omdat zij geen zicht hebben gehouden op de verspreiding van de *smartphones*. Wanneer automatisch van alle gebruikers van een bepaald communicatiemiddel de communicatie wordt opgenomen, wordt een grote inbreuk gemaakt op het recht op privacy van de betrokkenen.[90] Daarbij komt ook dat, ondanks dat in het *affidavit* wordt aangegeven dat alleen criminele organisaties van dergelijke *PGP*-telefoons gebruikmaken, tevens niet-criminele burgers het wenselijk kunnen vinden om versleuteld te communiceren. Zo is bijvoorbeeld bekend dat sommige advocaten versleuteld communiceren.[91] Op het moment dat een advocaat gebruik heeft gemaakt van een ANOM-*smartphone* is er informatie verzameld waarop het wettelijk verschoningsrecht van een advocaat van toepassing is. Het verschoningsrecht wordt geschonden op het moment dat derden (waaronder opsporingsambtenaren) inzage krijgen in de communicatie die heeft plaatsgevonden tussen een advocaat en een cliënt.[92] In een dergelijk geval wordt vanwege de bescherming die rust op deze communicatie een extra grote inbreuk gemaakt op het recht op privacy van de betrokkenen. Overigens is hier in de opsporingsoperatie waarin onderzoek werd gedaan naar Ennetcom wel aandacht voor geweest, aangezien het OM een oproep heeft gedaan aan advocaten om zich (anoniem) te melden bij het OM om hun gebruikersgegevens door te geven zodat de vertrouwelijke communicatie tussen een advocaat en een cliënt buiten het strafdossier gehouden kan worden.[93] In een operatie als *Trojan Shield* dient aldus ook aandacht te worden besteed aan de aard (al dan niet wettelijk beschermd) van de opgenomen communicatie.

4.4 De analyse van de inhoud

Het opnemen van vertrouwelijke communicatie levert de autoriteiten niets op als de communicatie niet mag worden bestudeerd. Zoals in paragraaf 3.4 is besproken, bestaat er geen specifieke wettelijke grondslag voor de analyse van de inhoud van de ANOM-*smartphones*: deze bevoegdheid zit ingebakken in artikel 126s Sv. Met het oog op de rechtsbescherming van verdachten is dat mogelijk problematisch. Het analyseren van de inhoud van een *smartphone* levert immers de grootste inbreuk op de privacy op. Of het noodzakelijk is om daarvoor een specifieke wettelijke basis te creëren, is afhankelijk van de ernst van de inbreuk op de persoonlijke levenssfeer van de gebruiker.

In het geval dat de inbreuk beperkt is, is er naar geldend recht geen noodzaak tot een specifieke wettelijke normering voor de bevoegdheid tot het analyseren van de inhoud.[94] Bij het onderzoek aan een in beslag genomen *smartphone* is het samenstel van de artikelen 94, 95 en 96 Sv en het kader uit de *Smartphone*-arresten, zoals aangestipt in paragraaf 3.4, in het kader van artikel 8 lid 2 EVRM voldoende toereikend om de beperkte inbreuk op het recht op privacy te rechtvaardigen.[95] Die bepalingen bevatten echter weinig concrete waarborgen: de inbeslagname is een bevoegdheid die bij heterdaad geen beperking kent. Wel heeft de Hoge Raad in de *Smartphone*-arresten bepaald dat – al naar gelang de te verwachten ernst van de inbreuk op de persoonlijke levenssfeer van de gebruiker van de *smartphone* – alleen een opsporingsambtenaar, de officier van justitie of de rechter-commissaris bevoegd is de inhoud van de in beslag genomen *smartphone* te (laten) analyseren. Toestemming van de rechter-commissaris is dan alleen vereist indien het op voorhand voorzienbaar is dat een onderzoek aan de *smartphone* een zeer ingrijpende inbreuk zal maken op de persoonlijke levenssfeer van de gebruiker van de *smartphone*.[96]

Als de bevoegdheid tot de analyse van de inhoud in onderhavige casus volgt uit de bevoegdheid tot het opnemen van vertrouwelijke communicatie, bestaan duidelijk meer waarborgen dan na de analyse van de inhoud van een in beslag genomen voorwerp. Voor het opnemen van vertrouwelijke communicatie is immers *altijd* een rechterlijke machtiging noodzakelijk (alsook een bevel van de officier van justitie). De rechter-commissaris zal bij het verlenen van de machtiging of het afwijzen van de vordering tot het opnemen van vertrouwelijke communicatie hoogstwaarschijnlijk de consequenties van de uitvoering van de bevoegdheid – d.w.z. de analyse van de opgenomen communicatie – meenemen in zijn afweging of het dringend noodzakelijk is dat de bevoegdheid wordt toegepast in het licht van de rechten van de verdachte. Indien de rechter-commissaris een concrete belangenafweging maakt, wordt bij de toepassing van 126s Sv reeds *voorafgaand* aan de inzet van de bevoegdheid al aandacht besteed aan de inbreuk die zal worden gemaakt op het recht op privacy op het moment dat de opgenomen communicatie in een later stadium wordt geanalyseerd. Daarnaast geldt dat wan-

90. Vgl. EHRM 4 december 2008, appl. nos 30562/04 & 30566/05, par. 103 (*S. and Marper* t. *het Verenigd Koninkrijk)*.
91. www.advocatenorde-middennederland.nl/48389/nieuws/mededeling-inzake-pgp-toestellen, laatst geraadpleegd op 25 augustus 2021.
92. D.R. Doorenbos & M.E. Rosing, 'Recht doen aan het verschoningsrecht', *S&O* 2020/5/6, p. 217.
93. www.advocatenorde-middennederland.nl/48389/nieuws/mededeling-inzake-pgp-toestellen, laatst geraadpleegd op 25 augustus 2021.
94. HR 9 februari 2021, ECLI:NL:HR:2021:202.
95. HR 9 februari 2021, ECLI:NL:HR:2021:202. Zie ook W. Albers, T. Beekhuis & C.M. Taylor Parkins-Ozephius, 'Geef mij toegang tot uw smartphone! Een zoektocht naar de wettelijke grondslag van de gedwongen biometrische ontgrendeling van de smartphone', *TBS&H* 2019/3, p. 7.
96. O.a. HR 4 april 2017, ECLI:NL:HR:2017:588, r.o. 2.8.

doi: 10.5553/TBSenH/229567002021007005003

neer uiteindelijk in de analysefase maar een beperkte inbreuk wordt gemaakt op het recht op privacy – in tegenstelling tot bij de in beslag genomen *smartphone* – de rechter-commissaris betrokken is geweest. Doordat artikel 126s Sv dus altijd voorafgaand aan de inzet van de bevoegdheid een machtiging van de rechter-commissaris verlangt, wordt beter recht gedaan aan het recht op privacy van de gebruiker van de *smartphone* dan wanneer de inhoud van een *smartphone* wordt geanalyseerd op grond van de algemene inbeslagnemingsbevoegdheid .

5 Afronding

Het spel is op de wagen nu de discussie over de rechtmatigheid van de inzet van de opsporingshandelingen tijdens *Operation Trojan Shield* is losgebarsten.[97] In deze bijdrage nemen wij een voorschot op de discussie over de legaliteit van de opsporingshandelingen die in de feitenrechtspraak vermoedelijk los zal gaan barsten. Uit onze analyse blijkt dat geen evidente misstanden bestaan met betrekking tot de toetsing van de uitgevoerde opsporingshandelingen in het licht van het legaliteitsbeginsel.

Wel bestaan twee punten van zorg, te weten (1) de uitbuiting van de ingebouwde kwetsbaarheid; en (2) het gebruik van criminele burgers als distributeurs. Wat betreft de ingebouwde kwetsbaarheid kan discussie ontstaan over de betrouwbaarheid van de communicatie, omdat ook anderen de kwetsbaarheid zouden kunnen hebben gebruikt. Het is daarom van essentieel belang dat de autoriteiten hierover transparant verbaliseren, opdat rechterlijke controle kan plaatsvinden met betrekking tot de kwetsbaarheid en eventueel misbruik daarvan. Wat betreft het gebruik van criminele burgers als distributeurs, is het van belang te wijzen op de inspanningsverplichting die de overheid heeft om die burgers te beschermen. Het feit dat de distributeurs een belangrijke rol hebben gespeeld in het oprollen van criminele organisaties kan voor die laatstgenoemde organisaties voldoende aanleiding vormen om wraak te nemen. Wanneer de overheid hiervan op de hoogte is, ontstaat een positieve verplichting de distributeurs te beschermen tegen aanvallen op hun leven of lichamelijke integriteit.

97. nos.nl/artikel/2384211-politie-trots-advocaten-kritisch-na-ongekende-klap-voor-criminelen, laatst geraadpleegd op 9 juni.

doi: 10.5553/TBSenH/229567002021007005003