Jurisprudentie

Oprichter van cryptotelefoonaanbieder Ennetcom veroordeeld

Annotatie bij Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085

Prof. mr. dr. J.J. Oerlemans*

Inleiding

1. In 2016 heeft het Nederlandse *Team High Tech Crime* in totaal 3,7 miljoen berichten veiliggesteld op een server in Canada. De berichten waren afkomstig van het bedrijf *Ennetcom B.V.*[1] Ennetcom leverde diensten op het gebied van versleutelde communicatie. Klanten konden met *BlackBerry*-telefoons, voorzien van specifieke software, versleutelde tekstberichten versturen.[2] In de onderhavige uitspraak wordt de oprichter van Ennetcom veroordeeld voor (gewoonte)witwassen, deelname aan een criminele organisatie, valsheid in geschrifte en verboden wapenbezit.[3] Deze uitspraak verdient een annotatie, omdat de rechtbank uitgebreid ingaat op (1) de rechtmatigheid van het veiligstellen van de berichten; (2) de vraag of er sprake is van misbruik van bevoegdheden (*détournement de pouvoir*); en (3) de vraag of het aanbieden van de cryptotelefoons een illegale activiteit is.

De feiten

2. In drie Nederlandse strafrechtelijke onderzoeken bestond het ernstige vermoeden dat de personen, die betrokken waren bij onder meer liquidaties, gebruik maakten van PGP-telefoons die werden geleverd door Ennetcom. Dit leidde tot 'de strafrechtelijke hypothese dat de verdachte als bestuurder van de Ennetcom-entiteiten de georganiseerde criminaliteit faciliteerde en in die wetenschap crimineel geld verdiende' (r.o. 17). De belangrijkste producten die de oprichter van Ennetcom verkocht, waren BlackBerry's waarmee versleutelde e-mailberichten konden worden verzonden via PGP- en S/MIME-versleuteling. De meeste functies op deze telefoons – zoals de camera, de microfoon en de bel- en sms-functie – waren uitgeschakeld. De berichten werden na 24 dan wel 48 uur automatisch gewist en daarnaast kon men de helpdesk van het bedrijf verzoeken de inhoud van de telefoon laten wissen (*wipen*). De verzonden e-mailberichten werden – ter versleuteling en ontsleuteling – omgeleid via servers die bij een bedrijf in Toronto (Canada) stonden (r.o. 2).

3. Op 8 april 2016 verstuurden Nederlandse opsporingsautoriteiten een rechtshulpverzoek naar de bevoegde autoriteiten in Canada om forensische kopieën te maken van de data op de *BlackBerry Enterprise Servers* in Toronto. In een vergelijkbare zaak wordt uitgelegd dat

* Prof. mr. dr. J.J. Oerlemans is bijzonder hoogleraar inlichtingen en recht bij het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtsstaat en Rechtspleging van de Universiteit Utrecht

1 T. Kreling, 'Justitie heeft toegang tot 3,6 miljoen versleutelde berichten van criminelen', *De Volkskrant* 9 maart 2017. De Ennetcom-operatie is ook uitvoerig beschreven in B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3.

2 Na de Ennetcom-operatie heeft de Nederlandse politie ook bij andere 'cryptotelefoonaanbieders' operaties uitgevoerd en bewijs verzameld. Zie J.J. Oerlemans, 'Overzicht cryptophone-operaties', jjoerlemans.com, 30 december 2021.

3 Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085 betreft een uitspraak jegens de oprichter en Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086 jegens de rechtspersoon Ennetcom B.V.

doi: 10.5553/TBSenH/229567002022008002008

het met BlackBerry Enterprise mogelijk is een centraal te beheren datacommunicatiearchitectuur op te zetten en te onderhouden en daarmee versleutelde communicatie te faciliteren.[4] De Canadese rechter die oordeelde over het verzoek had als voorwaarde gesteld dat de gegevens uitsluitend mochten worden gebruikt in specifieke, bij naam genoemde, opsporingsonderzoeken. Ook werd als voorwaarde gesteld dat de gegevens beschikbaar gesteld mochten worden voor andere strafrechtelijke onderzoeken dan die in het rechtshulpverzoek waren genoemd met toestemming van een rechter (r.o. 101). Op 16 april 2016 is uitvoering gegeven aan het rechtshulpverzoek en zijn de gegevens van de server door de Canadese politie gekopieerd. Na analyse van de data bleken de kopieën 3,7 miljoen berichten en notities te bevatten. Daarnaast bevatte de server de private sleutels van de gebruikers van de klanten van de verdachte. Daarmee kon de politie de berichten en notities ontsleutelen en kennisnemen van de inhoud daarvan. De politie heeft voor het ontsleutelen en de analyse van de data gebruik gemaakt van het door het Nederlands Forensisch Instituut (NFI) ontwikkelde (technische) hulpmiddel (*tool*) 'Hansken' (r.o. 3).

Rechtmatigheid onderzoek

4. Het maken van een forensische kopie van een server en veiligstellen van een dergelijk grote hoeveelheid gegevens brengt vragen over de wettelijke grondslag in strafvordering met zich mee. In deze zaak paste de officier van justitie de (reguliere) bevoegdheid toe voor het maken van een forensische kopie van een server (buiten een woning), namelijk de doorzoeking voor het vastleggen van gegevens in artikel 125i Sv (r.o. 42). Deze bevoegdheid tot het doorzoeken van een plaats ter vastlegging van gegevens verwijst door naar de reguliere bevoegdheden met betrekking tot een doorzoeking en inbeslagname. De officier van justitie baseert zich vermoedelijk op artikel 96c Sv, kortgezegd de doorzoeking van elke plaats, niet zijnde een woning.

5. De verdediging voert echter aan dat het openbaar ministerie zich had moeten baseren op de bevoegdheid in artikel 125la Sv (r.o. 48-49). Artikel 125i Sv is een bijzondere bepaling die beperkingen stelt aan een doorzoeking bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Als bij die doorzoeking 'gegevens worden aangetroffen die niet voor deze bestemd of van deze afkomstig zijn', heeft de officier van justitie een machtiging van een rechter-commissaris nodig om kennis te nemen van deze gegevens.

6. Het openbaar ministerie stelt dat Ennetcom geen 'aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst' is als bedoeld in artikel 125la Sv, zodat dit artikel toepassing mist. De officier van justitie wijst erop dat voor de uitleg van deze begrippen moet worden aangesloten bij de definities in artikel 1.1 van de Telecommunicatiewet, die op hun beurt implementaties betreffen van de begrippen uit Europese richtlijnen (zoals de e-Privacy Richtlijn). Gelet op de HvJ EU-arresten *SkypeOut* en *Gmail* valt de verdachte niet onder deze definitie, maar betreft het een zogenoemde *Over-The-Top*-dienst (OTT-dienst).[5] Bovendien is de wijze van versleuteling – *Pretty Good Privacy* (PGP) – geen 'openbare' dienst, omdat de gebruikers alleen konden communiceren binnen de gesloten groep van andere PGP-gebruikers. De verdachte heeft zich ook nooit geregistreerd bij de ACM als telecomaanbieder en is nooit aftapbaar geweest, terwijl dit vereisten zijn voor aanbieders van openbare telecommunicatiediensten in de zin van de Telecommunicatiewet (r.o. 50).

7. De rechtbank oordeelt dat het openbaar ministerie bij de verkrijging van de gegevens artikel 125la Sv in acht had moeten nemen. De noodzakelijke machtiging van een rechter-commissaris is daardoor niet verkregen (r.o. 59). De rechtbank past voor het oordeel een teleologische interpretatie van de wet toe. De rechtbank maakt voor de uitleg van de bepaling in artikel 125la Sv een vergelijking met het briefgeheim, waarbij door de toets van de rechter-commissaris extra bescherming wordt gegeven aan de verzenders en ontvangers van berichten, die ervan uit mogen gaan dat hun berichten tijdens het 'transport' niet zomaar mogen worden gelezen (r.o. 51). Ook is voor de vordering van opgeslagen gegevens bij een aanbieder van een communicatiedienst (op grond van art. 126ng lid 2 Sv) een machtiging van de rechter-commissaris vereist. Dit onderstreept volgens de rechtbank de gedachte dat bij gebruikmaking van de doorzoekingsbevoegdheid van artikel 125i Sv geen lichtere voorwaarden of eisen mogen gelden dan bij de bevoegdheid tot vorderen van dezelfde gegevens (r.o. 56). De rechtbank stelt vast dat het ontbreken van de machtiging van de rechter-commissaris is aan te merken als een onherstelbaar vormverzuim in het voorbereidend onderzoek tegen de verdachte als bedoeld in artikel 359a Sv (r.o. 61). Echter, met toepassing van vaste jurisprudentie omtrent vormverzuimen komt de rechtbank slechts tot een constatering van het vormverzuim en acht strafvermindering geen passend rechtsgevolg (r.o. 65-68).

8. Het oorspronkelijke standpunt van de officier van justitie in r.o. 50 – dat Ennetcom geen 'aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst' is als bedoeld in artikel 125la Sv en dit artikel daarom toepassing mist – acht ik persoonlijk overtuigender. In de praktijk wordt bij het maken van een forensische kopie in een datacenter de

4 Rb. Rotterdam 20 januari 2022, ECLI:NL:RBROT:2022:363, r.o. 4. Deze zaak was gericht tegen een leverancier van de 'PGP Safe'-cryptotelefoon (en de achterliggende infrastructuur).

5 Zie HvJ EU 5 juni 2019, nr. C-142/18, ECLI:EU:C:2019:460 (*Skype Communications t. BIPT*), *Computerrecht* 2019/217, m.nt. M.I. Robichon & J. van de Velde.

doi: 10.5553/TBSenH/229567002022008002008

doorzoeking ter vastlegging van gegevens artikel 125i Sv toegepast, in plaats van artikel 125la Sv.[6] De feiten vonden ook plaats voordat het *Smartphone*-arrest van de Hoge Raad is gewezen, maar ook bij toepassing van dit arrest zou een officier van justitie op grond van artikel 125i Sv jo artikel 96c Sv een bevel mogen afgeven.[7] Dat neemt niet weg dat ik sympathie heb voor de overwegingen van de rechtbank en ook liever een machtiging van een rechter-commissaris zou zien bij het veiligstellen van communicatiegegevens van een computer, gezien de ernstige privacy-inbreuk die daarbij plaatsvindt.[8] Met de rechtbank ben ik het eens dat er sprake is van een vérgaande inbreuk op het recht op vertrouwelijke communicatie bij het verzamelen van 3,7 miljoen berichten, inclusief metadata (zie r.o. 60). Zoals ik samen met Bart Schermer elders in dit tijdschrift heb betoogd, acht ik het een goede zaak dat in de meer recente cryptotelefoon-operaties (zoals bij 'EncroChat') alsnog om een machtiging van een rechter-commissaris is verzocht, hoewel de (huidige) wet dat in strikte zin niet vereist.[9] Op die manier worden de fundamentele rechten van de betrokkenen nadrukkelijker worden meegewogen ten opzichte van het opsporingsbelang.

9. In meer recente jurisprudentie met betrekking tot de megazaak *Himalaya* blijkt overigens dat voor het gebruik van de Ennetcom-gegevens alsnog een machtiging van de rechter-commissaris wordt verkregen, (onder andere) door middel van een analoge toepassing van artikel 126ng lid 2 Sv.[10] De rechtbank Noord-Holland verwoordt het ervaren gevoel van rechters denk ik treffend en legt uit dat de rechter-commissaris zich zag 'geconfronteerd met de voorwaarde van een voorafgaande gerechtelijke machtiging die de Nederlandse wet niet kent. Het moet in zekere zin pionieren zijn geweest. Wachten totdat de wetgever (eventueel) in actie zou komen, was daarbij, gelet op de dringende en gerechtvaardigde opsporingsbelangen, geen reële optie (…)'. Met de machtiging wordt (nogmaals) getoetst aan de beginselen van proportionaliteit en subsidiariteit.

Détournement de pouvoir

10. De verdediging stelt dat het openbaar ministerie de gegevens slechts heeft gekopieerd om inzage te verkrijgen in alle inhoudelijke communicatie van gebruikers van de cryptotelefoons. Het doel was het verkrijgen van informatie over vermeende criminelen die gebruikmaakten van de diensten van Ennetcom. Het rechtshulpverzoek aan Canada en de digitale opsporingshandelingen die in Nederland zijn uitgevoerd, waren daarom volgens de verdediging uitsluitend ingegeven door de wens om de data van gebruikers te verkrijgen ten behoeve van andere onderzoeken. Het openbaar ministerie heeft daarmee een aan hem toekomende strafrechtelijke bevoegdheid gebruikt voor een ander doel dan waarvoor deze is gegeven en daarmee het verbod op détournement de pouvoir overtreden (r.o. 21). Het openbaar ministerie heeft daarmee zijn strafrechtelijke bevoegdheden en het rechtshulpverzoek oneigenlijk ingezet. Door de onrechtmatige toepassing van die opsporingsmiddelen zijn miljoenen inhoudelijke berichten en andere persoonsgegevens van niet-verdachten verkregen (r.o. 27). Dit is een belangrijk argument dat ik nog niet vaak voorbij heb zien komen in de talrijke zaken met bewijs uit cryptotelefoons. Daarom is het interessant na te gaan hoe de rechtbank daarmee omgaat.

11. Volgens het openbaar ministerie richtte het opsporingsonderzoek zich op de verdachte rechtspersoon en op de rol van de medeverdachte als (indirect) bestuurder en aandeelhouder van Ennetcom-entiteiten bij het op wereldwijde schaal faciliteren van georganiseerde criminaliteit en het in die wetenschap verdienen van crimineel geld. Voor de verdenking en vervolging van witwassen zou het van belang zijn dat komt vast te staan dat (een groot deel van) de klanten van de verdachte in de criminaliteit actief zijn en dat dus de omzet van de verdachte direct of indirect afkomstig is uit (enig) misdrijf (r.o. 22).

12. De rechtbank is van oordeel dat de stelling dat sprake is van misbruik van recht niet voldoende is onderbouwd. Het openbaar ministerie kon overgaan tot vervolging op basis van een redelijke verdenking van schuld aan enig strafbaar feit. De rechtbank is daarom niet van oordeel dat de dataset door middel van machtsmisbruik of in strijd met fundamentele rechtsbeginselen is verkregen (r.o. 20, 24, 28). Daar komt bij dat de door de verdediging gestelde schending van grondrechten van onbekende derden en het gegeven dat de communicatie van de medeverdachte in andere onderzoeken terecht is gekomen, geen van alle schending opleveren van enig concreet belang van de verdachte rechtspersoon in deze zaak. De *Schutznorm* is met andere woorden niet geschonden (r.o. 29).

13. De stelling van het openbaar ministerie dat het onderzoek zich richtte op de oprichter van Ennetcom (r.o. 22) en het daarom noodzakelijk was miljoenen berichten te analyseren om (met name) het delict witwassen te bewijzen, komt op mij wat gekunsteld over. In het WODC-rapport 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit' staan op pagina 52 twee doelstellingen van de Ennetcom-zaak beschreven, namelijk: 'ten eerste werd onderzocht of de aanbieder van de cryptotelefoons (zowel het bedrijf als de persoon) strafrechtelijk aansprakelijk kon worden gesteld en daarnaast werd gepoogd versleutelde berichten inzichtelijk te maken, die mogelijk ook waardevolle informatie konden opleveren voor andere opsporingsonderzoeken naar

6 Er is geen jurisprudentie beschikbaar op rechtspraak.nl die erop wijst dat in deze situatie art. 125la Sv wordt toegepast.
7 HR 4 april 2017, ECLI:NL:HR:2017:592, *NJ* 2017/230, m.nt. Kooijmans.
8 Zie bijvoorbeeld S. Royer & J.J. Oerlemans, 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017/200, p. 277-284.
9 B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?', *TBS&H* 2022.
10 Rb. Noord-Holland 19 januari 2022, ECLI:NL:RBNHO:2022:264.

doi: 10.5553/TBSenH/229567002022008002008

georganiseerde criminaliteit'.[11] In meer recente jurisprudentie naar aanleiding van cryptotelefoon-operaties worden vaak meervoudige doelen genoemd die geloofwaardiger overkomen. In de Encrochat-machtiging staan bijvoorbeeld de volgende drie doelen beschreven: (1) het identificeren van de gebruikers; (2) onderzoek doen naar de criminele samenwerkingsverbanden waarvan zij deel uitmaken; (3) bewijs verzamelen over door deze criminele samenwerkingsverbanden gepleegde en/of nog te plegen misdrijven.[12] Gezien de praktijk waarbij een deel van de berichten wordt gebruikt en geanalyseerd voor bewijs in nieuwe strafzaken, was het mijns inziens beter geweest ook deze andere doelen van het onderzoek te benoemen.

Is het ontwikkelen en verhandelen van cryptotelefoons een illegale activiteit?

14. De verdachte (de oprichter van Ennetcom) wordt door de rechtbank veroordeeld tot 54 maanden gevangenisstraf vanwege het leidinggeven aan een criminele organisatie (art. 140 Sr), begunstiging (art. 189 Sr), witwassen (art. 240bis e.v. Sr), valsheid in geschrifte (art. 225 Sr) en vuurwapenbezit. De rechtbank stelt expliciet dat het ontwikkelen en verhandelen van cryptotelefoons op zichzelf geen illegale activiteit is. Echter, dit wordt anders als de handelaar bewust geld aanneemt waarvan hij weet dat het uit enig misdrijf afkomstig is en op verzoek de inhoud van telefoons wist (r.o. 246-248).[13] De rechtbank overweegt in r.o. 140-237 uitvoerig waarom sprake is van leidinggeven aan een criminele organisatie met het oogmerk op het plegen van de misdrijven van begunstiging, witwassen en valsheid in geschrifte. Niet alle overwegingen daarbij zijn relevant voor deze annotatie; de feiten spreken deels voor zich. De overwegingen waarom sprake is van witwassen en begunstiging worden in dit onderdeel wel besproken, omdat deze ook relevant kunnen zijn voor toekomstige zaken met betrekking tot leveranciers van cryptotelefoons.

15. De rechtbank concludeert dat sprake is van witwassen, omdat een deel van de omzet van het bedrijf afkomstig is uit 'enig misdrijf'. Om die conclusie te staven neemt de rechtbank verschillende omstandigheden in overweging. In r.o. 159 overweegt de rechtbank bijvoorbeeld dat de telefoons en abonnementen in principe contant werden afgerekend, terwijl het daarbij om aanzienlijke bedragen ging (de telefoon kostte € 1000 à € 1500 inclusief het abonnement voor de komende zes maanden). De verdachte was ervan op de hoogte dat *resellers* zo te werk gingen en faciliteerde dit ook: de contante opbrengst van (een deel van) de resellers werd naar het bedrijf gebracht of opgehaald en vervolgens door medewerkers van het bedrijf afgestort op de bankrekening. Voor het vervoer van deze grote geldbedragen waren voertuigen beschikbaar met daarin aangebrachte verborgen ruimtes. Ook vlogen medewerkers van het bedrijf van de verdachte oprichter naar het buitenland om zo de contante weekopbrengst op te halen of over te laten overmaken op de bankrekening van zijn onderneming. Ook het feit dat de verdachte gegevens op telefoons op verzoek op afstand liet wissen (zie randnummers 17 en 18) draagt bij aan de omstandigheid dat de verdachte moest weten dat de geleverde producten en diensten betaald werden door personen die criminele activiteiten verrichtten en daarmee hun geld verdienden.

16. De rechtbank neemt ook andere omstandigheden in aanmerking om vast te stellen dat een deel van de omzet afkomstig is uit enig misdrijf. Het bewijs waarmee het OM tracht aan te tonen dat de berichten 'veelal crimineel getint' zijn en de telefoons door criminelen worden gebruikt, zijn daarbij opvallend. In r.o. 165 staat bijvoorbeeld beschreven dat uit een 'willekeurige steekproef' zou blijken dat 359 van de 458 beoordeelde gesprekken 'crimineel gerelateerd' waren, oftewel 78,4%. De verwachting van het OM is dat bij herhalingen van de steekproef gemiddeld zo'n 75% crimineel gerelateerd zou zijn. De rechtbank is (terecht, in mijn ogen) niet overtuigd van de analyse dat de berichten vrijwel altijd 'crimineel getint' zouden zijn (r.o. 166), maar de andere overwegingen over de inrichting van de PGP-telefoons en de achterliggende organisatie om anonimiteit te waarborgen, tezamen met de criminele klantenkring, acht de rechtbank wel overtuigend.

17. De rechtbank gaat uitgebreid in op het ten laste gelegde delict begunstiging (art. 189 Sr). Het gaat daarbij om het tegenwerken van een strafrechtelijk onderzoek, bijvoorbeeld door bewijs te vernietigen dat kan bijdragen aan de waarheidsvinding.[14] De verdediging stelt dat het wipen van telefoons niet onder de delictsomschrijving van artikel 189 Sr valt (r.o. 211).

18. Uit het bewijsmateriaal blijkt dat medewerkers van Ennetcom verzoeken honoreerden om de inhoud van

11 C.A.J. van Eeden, J.J. van Berkel, C.C. Lankhaar en C.J. de Poot, 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit', *Cahiers* 2021-23, Den Haag: WODC 2021, p. 43.

12 Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584, r.o. 2.1.

13 Zie in dit kader ook de zaak jegens een leverancier van PGP-Safe cryptotelefoons, waarbij van een vergelijkbare techniek gebruik werd gemaakt: Rb. Rotterdam 20 januari 2022, ECLI:NL:RBROT:2022:363, r.o. 10.2. In deze zaak werd de verdachte van de meeste ten laste gelegde delicten vrijgesproken, maar wel veroordeeld voor begunstiging vanwege het wissen van berichten op verzoek van (opgepakte) personen.

14 In art. 189 lid 1 onderdeel 3 Sr ('begunstiging') is strafbaar gesteld: 'hij die opzettelijk voorwerpen die kunnen dienen om de waarheid aan de dag te brengen of om wederrechtelijk verkregen voordeel als bedoeld in artikel 36e aan te tonen, met het oogmerk om de inbeslagneming daarvan te beletten, te belemmeren of te verijdelen, verbergt, vernietigt, wegmaakt of aan het onderzoek van de ambtenaren van de justitie of politie onttrekt, dan wel door het opzettelijk verstrekken van gegevens of inlichtingen aan derden die inbeslagneming belet, belemmert of verijdelt'.

doi: 10.5553/TBSenH/229567002022008002008

een telefoon te wissen (wipen), omdat klaarblijkelijk het gevaar was dat opsporingsinstanties achter de inhoud van een inbeslaggenomen PGP-telefoon zouden komen. De genoemde berichten in voetnoot 157 van de uitspraak zijn op zich veelzeggend ((‘jongen net aangehouden aub wipen zsm!!’; ‘aub zsm wipen de politie heeft hem’; ‘I need to cancel one phone and erased because the guy was grab by police and they got the phone’; ‘Tu peux wiper eet adresse alerte police’; etc.). Een verzoek tot wipen vond ongeveer bij één op de zeventien verkochte toestellen plaats. De aanhouding van een eigenaar van de telefoon en soortgelijke noodsituaties waren steeds de aanleiding tot een (al dan niet geslaagde) poging de telefoon te wissen (r.o. 225). Daarmee acht de rechtbank het delict begunstiging als bedoeld in artikel 189 lid 1 onderdeel 3 Sr overtuigend bewezen.

19. De rechtbank concludeert dat de verdachte behoorde tot de organisatie rond de verdachte rechtspersoon Ennetcom, deze ook had opgericht en leidde en dat hij handelingen heeft verricht die hebben bijgedragen aan het verwezenlijken van het oogmerk van die organisatie. Hij wist dat deze delicten van begunstiging, witwassen en valsheid in geschrifte door de organisatie werden gepleegd. Daarom is bewezen dat de verdachte heeft deelgenomen aan een organisatie als bedoeld in artikel 140 Sr (r.o. 235-237).

Conclusie

20. De rechtbank Rotterdam heeft een heldere, goed gestructureerde uitspraak geschreven over de oprichter en een leverancier van een destijds populaire cryptotelefoon. De onderhavige zaak valt ook duidelijk binnen de strategie van het Team High Tech Crime om personen die criminele organisaties (digitaal) ondersteunen (*facilitators* genoemd) te vervolgen en hun criminele vermogen af te pakken.[15] De uitspraak steekt uit boven andere uitspraken, vanwege de uitvoerige overwegingen omtrent de rechtmatigheid van de opsporingshandelingen (met aandacht voor de enorme privacy-inbreuk die plaatsvindt bij het kopiëren van 3,7 miljoen berichten). De rechters hebben met een gezonde kritische blik naar de standpunten van zowel de verdediging als het openbaar ministerie gekeken. Ik ben het niet eens met de juridische grondslag die de rechtbank van toepassing acht op het verzamelen van Ennetcom-gegevens, maar wel met de waardering van de zwaarte van de privacy-inbreuk en dat een toets van een rechter-commissaris een wenselijke extra toets vormt op proportionaliteit en subsidiariteit. Het betreft een leerzame uitspraak voor zowel de advocatuur als het openbaar ministerie.

15 Zie ook het persbericht naar aanleiding van de PGP Safe-operatie: ‘Ontsleutelde berichtgeving crypto-gsm’s cruciaal in zaak vergismoord’, OM.nl, 11 december 2017.

doi: 10.5553/TBSenH/229567002022008002008