Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

Artikel

De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?

Prof. mr. dr. B.W. Schermer en prof. mr. dr. J.J. Oerlemans*

1. Inleiding

De *EncroChat*-operatie houdt de juridische gemoederen flink bezig. Zo levert een zoekslag op rechtspraak.nl naar de term 'EncroChat' inmiddels al meer dan honderd resultaten op. Volgens de politie zijn 816 gebruikers geïdentificeerd en liepen er in april 2021 reeds 206 onderzoeken naar aanleiding van de EncroChat-operatie. Tijdens de operatie zijn naar verluidt 25 miljoen berichten van Nederlandse gebruikers van deze 'cryptotelefoons' onderschept.[1]

Een cryptotelefoon is een mobiele telefoon die speciaal is aangepast om anoniem en versleuteld te communiceren. Ze worden naar verluidt vaak door criminelen gebruikt.[2] In tal van spraakmakende zaken spelen de onderschepte EncroChat-berichten een bepalende rol in de bewijsvoering. De politie zit naar eigen zeggen op een 'goudmijn aan bewijs' en de gegevens vormen een *game changer* voor de politie.[3] Strafrechtadvocaten trekken vaak de rechtmatigheid van de operatie in twijfel, maar vooralsnog lijkt de verdediging bot te vangen.

In deze bijdrage geven wij een overzicht van de meest relevante EncroChat-jurisprudentie, die zich met name richt op de onderzoekswensen van de verdediging. Daarbij bespreken wij eerst de details van de EncroChat-operatie. Vervolgens gaan wij in op de bezwaren van de verdediging met betrekking tot de EncroChat-operatie en de onderzoekswensen ten aanzien van de toegang tot de gegevens. Wij sluiten af met een korte beschouwing van de bevindingen.

2. De EncroChat-operatie

De aanleiding van de operatie vormde een onderzoek in 2017 van zowel de Franse autoriteiten als de Nederlandse autoriteiten naar het bedrijf EncroChat.[4] In verschillende strafrechtelijke onderzoeken werden EncroChat-telefoons aangetroffen, waardoor bij de politie de indruk ontstond dat deze telefoons vrijwel uitsluitend in het (georganiseerde) criminele circuit werden gebruikt.[5] Het onderzoek, dat in Nederland '26Lemont' werd genoemd, betrof een strafrechtelijk onderzoek naar de medeplichtigheid van EncroChat zelf aan door de gebruikers van

* Prof. mr. dr. B.W. Schermer is hoogleraar privacy en cybercrime bij het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden (eLaw@Leiden) en partner bij juridisch adviesbureau Considerati. 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 Jaarverantwoording politie 2020, p. 31.

2 Cryptotelefoons maken gebruik van technieken voor de versleuteling van berichten, vaak via zelfontwikkelde 'apps'. Ook de gegevens op de smartphone zelf zijn versleuteld. Het meermalen invoeren van een verkeerd wachtwoord zorgt dat de telefoon automatisch wordt gewist. Ook hebben gebruikers doorgaans een 'paniekmodus' waarmee zij na een handeling direct hun telefoon kunnen wissen. Ten slotte hebben de berichten een door de gebruiker ingestelde 'levensduur' en worden de berichten daarna automatisch gewist. Op de EncroChat-telefoons waren functionaliteiten als de GPS uitgeschakeld uit privacyoverwegingen. Zie o.a. het persbericht, 'Retour sur l'affaire EncroChat', *le Bureau des affaires criminelles*, 31 juli 2020.

3 Stoker, E., 'Politie kon wekenlang meelezen met geheime berichten van duizenden zware criminelen', *De Volkskrant* 2 juli 2020.

4 Zie Europol, 'Ontmanteling van een versleuteld netwerk veroorzaakt schokgolven door georganiseerde misdaadgroepen in heel Europa', 2 juli 2020.

5 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

EncroChat gepleegde misdrijven.[6] In de eerste maanden van 2020 is overleg gevoerd door politie en justitie uit verschillende landen met als doel te komen tot een gecoördineerde aanpak bij de vervolging van EncroChat.[7] Frankrijk en Nederland hebben vervolgens het voortouw genomen en gewerkt in een gemeenschappelijk onderzoeksteam (oftewel een *Joint Investigation Team* (JIT)).[8]

In de eerste fase van de EncroChat-operatie heeft de Franse *Gendarmerie* van 1 april tot 20 juni 2020 vanuit Pontoise (Frankrijk) alle inkomende en uitgaande communicatie vastgelegd van EncroChat-telefoontoestellen.[9] De server van EncroChat bleek bij het bedrijf OVH in Roubaix (Frankrijk) te zijn gevestigd. Het Franse onderzoeksteam verzamelde de EncroChat-telefoondata gedurende de periode van 1 april 2020 17:15 uur tot 20 juni 2020 omstreeks 17:20 uur.[10] Op dat moment waren ongeveer 60.000 toestellen in omloop en zijn in totaal ongeveer 120 miljoen berichten en afbeeldingen vastgelegd.[11]

Voor het vastleggen van de communicatie is een technisch hulpmiddel (een '*hacktool*') ingezet via een update op de telefoontoestellen vanaf de server in Frankrijk. De hacktool legde de volgende gegevens vast en stuurde deze gedurende twee maanden door naar de Franse autoriteiten:

- IMEI-gegevens (een nummer ter identificatie van telefoontoestellen);
- gebruikersnamen;
- wachtwoorden;
- opgeslagen chatberichten;
- afbeeldingen;
- locatiegegevens (ook wel *geodata* genoemd); en
- notities.

In de tweede fase van de operatie heeft de Franse Gendarmerie gegevens gedeeld met de autoriteiten van andere landen voor strafrechtelijke onderzoeken naar de gebruikers van de EncroChat-cryptotelefoons. In het kader van de JIT heeft het Franse onderzoeksteam ook de Nederlandse politie toegang gegeven tot de EncroChat-telefoondata en zijn ongeveer 25 miljoen berichten gedeeld.[12]

3. Extra machtiging van rechter-commissaris

Vanwege de voorzienbare inbreuk die de interceptie van de EncroChat-data op de persoonlijke levenssfeer van de Nederlandse gebruikers van deze communicatiedienst zou hebben, heeft het openbaar ministerie ervoor gekozen om – '*mogelijk ten overvloede*' – in Nederland een rechterlijke toetsing te vorderen.[13] Deze vordering was mogelijk ten overvloede omdat de Franse rechter al had geoordeeld over de gehanteerde onderzoeksmethoden. Via deze weg is de inbreuk nogmaals getoetst aan de vereisten van proportionaliteit en subsidiariteit en op de aanwezigheid van een wettelijke grondslag.[14]

De rechtbank Gelderland geeft in een uitspraak op 8 december 2021 uiteindelijk meer details over de machtiging van de rechter-commissaris.[15] Voor het gebruik van de berichten is een (Nederlandse) rechter-commissaris om een machtiging voor de inzet van de hackbevoegdheid (artikel 126uab Sv) en het opnemen van telecommunicatie (artikel 126t Sv) gevraagd. In het 'proces-verbaal aanvraag' wordt gesteld dat het redelijk vermoeden bestaat dat de EncroChat-gebruikers zich in georganiseerd verband schuldig maken aan (het medeplegen van) één of meer van de volgende misdrijven:

- witwassen;
- deelnemen/leiding geven aan een criminele organisatie;
- Opiumwetdelicten;
- wapenhandel;
- (poging tot) moord/doodslag;
- gijzeling en/of wederrechtelijke vrijheidsberoving; en
- afpersing en/of diefstal met geweld.

Met de aanvraag werden de volgende drie doelen nagestreefd:

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.[16]

De EncroChat-data mocht worden doorzocht met behulp van een lijst met trefwoorden die gerelateerd waren aan te onderzoeken feiten of verdachten. De rechter-commissaris overwoog expliciet dat het onderzoek

6 Dit doel doet ook denken aan het strafrechtelijk onderzoek naar Ennetcom een paar jaar daarvoor. Zie ook Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085 en de annotatie van Oerlemans elders in dit nummer van het *Tijdschrift voor Bijzonder Strafrecht & Handhaving*.

7 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.

8 Zie over de juridische aspecten van de JIT-constructie en in het bijzonder in de context van EncroChat ook het artikel van Verbeek en Beekhuis in dit nummer: L.W. Verbeek & T. Beekhuis, 'Executieve jurisdictie: het (grote) obstakel in grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders?', *TBS&H* 2022 (hierna: Verbeek & Beekhuis 2022).

9 Deze omschrijving van de EncroChat-operatie is met name gebaseerd op Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3. Zie ook J.J. Oerlemans, 'Meer duidelijkheid over EncroChat-operatie', *Computerrecht* 2021/195 en de geüpdatete versie van dit bericht op www.jjoerlemans.com.

10 Rb. Overijssel 29 september 2021, ECLI:NL:RBOVE:2021:3689.

11 Le Bureau des affaires criminelles, 'Retour sur l'affaire EncroChat', *Gend-info.fr*, 31 juli 2020.

12 Jaarverantwoording politie 2020, p. 31.

13 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.

14 Zie ook Rb. Zeeland-West-Brabant 31 maart 2021, ECLI:NL:RBZWB:2021:1556, r.o. 3.3.3.

15 Zie Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584.

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

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

geen *fishing expedition* mocht worden. De rechter-commissaris heeft de vordering vervolgens toegewezen onder de volgende zeven voorwaarden (verkort weergegeven):

1. de wijze waarop is binnengedrongen in het geautomatiseerde werk wordt vastgelegd, als er geen gebruik wordt gemaakt van een reeds goedgekeurd middel;
2. een beschrijving van de gebruikte software die beschikbaar is voor onderzoek, als er geen gebruik wordt gemaakt van een reeds goedgekeurd middel;
3. de integriteit van de opgeslagen informatie wordt gegarandeerd;
4. het onderzoek moet reproduceerbaar zijn, en gebruik moet worden gemaakt van zoeksleutels (woordenlijsten);
5. voorkomen moet worden dat communicatie tussen cliënten en verschoningsgerechtigden wordt opgenomen;
6. de met zoeksleutels vergaarde informatie moet binnen twee weken ter toetsing aan de rechter-commissaris worden aangeboden en pas daarna aan het openbaar ministerie en de politie ter beschikking worden gesteld voor het opsporingsonderzoek;
7. de machtiging wordt voor een beperkte duur van vier weken verleend en kan enkel middels een vordering worden verlengd. De rechter-commissaris kan de machtiging vroegtijdig beëindigen, als de tussentijdse toets daartoe aanleiding zou geven.[17]

Als de EncroChat-gegevens worden gedeeld met andere onderzoeken, moet daarvoor eerst toestemming worden gevraagd aan de rechter-commissaris, waarna de officier(en) in de zaak 26Lemont op grond van artikel 126dd Sv de informatie mag delen met de zaaksofficier van dat betreffende onderzoek.[18]

4. Verweren die zien op de rechtmatigheid van de EncroChat-operatie

Ondanks de rechtmatigheidstoets in Frankrijk en de vordering ten overvloede in Nederland, stelt de verdediging in veel Nederlandse zaken waar de EncroChat-berichten als bewijs worden gebruikt de gang van zaken binnen het voorbereidend onderzoek ter discussie. Een terugkerend punt is dat de verdediging ernstige vormverzuimen in het (Franse) onderzoek vermoed en in staat wil worden gesteld om dat te toetsen. Hiertoe heeft de verdediging onderzoekswensen ingediend die in overwegende mate tot doel hebben om het Franse onderzoek door de Nederlandse rechter te laten toetsen.

Het gaat dan met name om (1) verzoeken die zien op het Franse onderzoek, waaronder de hack zelf en de interceptietool, de JIT-overeenkomst tussen Nederland en Frankrijk en de totstandkoming daarvan, en de wijze waarop Nederland de EncroChat-data heeft verkregen en (2) verzoeken die zien op de processtukken van het onderzoek 26Lemont en de machtiging voor de hackbevoegdheid ex artikel 126uba Sv die door de rechter-commissaris is verleend.[19] Op deze verweren wordt hieronder nader ingegaan.

Ad 1) Verzoeken die zien op het Franse onderzoek

De verdediging is begrijpelijkerwijs geïnteresseerd in de gang van zaken rondom het onderzoek, niet in de laatste plaats omdat delen van de uitvoering tot Frans staatsgeheim zijn verklaard. Meer specifiek wil de verdediging in staat worden gesteld te toetsen of het onderzoek zorgvuldig is uitgevoerd.[20]

De rechtbanken in Nederland zijn vooralsnog echter unaniem in hun oordeel over de onderzoekswensen van de verdediging die zich richten op het toetsen van het Franse onderzoek: een inhoudelijke toetsing van de rechtmatigheid van het Franse onderzoek is niet mogelijk, omdat het (interstatelijke) vertrouwensbeginsel daaraan in de weg staat. De Nederlandse strafrechter moet erop vertrouwen dat de interceptie in Frankrijk op basis van een wettelijke grondslag en in overeenstemming met artikel 8 EVRM heeft plaatsgevonden.[21] De rechtbank Amsterdam overweegt bijvoorbeeld:

> *'Het is met andere woorden niet de taak van de Nederlandse strafrechter om aan de hand van (Franse) stukken te controleren of de machtiging door de Franse rechter op juiste (wettelijke) gronden is verleend, dan wel na te gaan of daar gebreken aan kleven.'*[22]

De rechtbank Rotterdam overweegt in dit kader ook dat het voor de in Frankrijk bij de hack betrokken personen en autoriteiten al van begin af aan duidelijk is geweest dat de werking van de gebruikte interceptietool onder Frans staatsgeheim viel. Het is niet aan de Nederlandse rechter te bepalen of de duiding van die informatie al

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

18 Rb. Midden-Nederland 16 september 2021, ECLI:NL:RBMNE:2021:4480, r.o. 4.1.3.

19 Zie ook Rb. Amsterdam 16 juli 2021, ECLI:NL:RBAMS:2021:3707. De verweren uit 'categorie 3', zoals geïdentificeerd in de uitspraak, worden uitvoerig besproken in paragraaf 5. Uiteraard komen ook nog andere verweren aan bod in de strafzaken waar EncroChat-bewijs wordt gebruikt. In deze bijdrage beperken wij ons tot de genoemde (categorieën van) verweren, omdat deze op basis van onze jurisprudentieanalyse het meest voorkomen en ook door de rechtspraak zelf zijn geïdentificeerd als terugkerende verweren van de verdediging die zien op de rechtmatigheid van het opsporingsonderzoek.

20 Zie voor een overzicht van de onderzoekswensen o.a. Rb. Rotterdam 11 oktober 2021, ECLI:NL:RBROT:2021:9906, r.o. 6.5.8 en Rb. Amsterdam 16 juli 2021, ECLI:NL:RBAMS:2021:3707.

21 Zie voor meer achtergrond over het vertrouwensbeginsel en actuele jurisprudentie S.G.A.M. Adams, 'Vertrouwen is goed, maar controle is beter. De interpretatie van het interstatelijke vertrouwensbeginsel door Nederlandse feitenrechter bij samenwerking tussen EVRM-lidstaten in het kader van internationale digitale rechtshulp in strafzaken en het beginsel van equality of arms', *DD* 2021/74 (hierna: Adams 2021).

22 Rb. Amsterdam 16 juli 2021, ECLI:NL:RBAMS:2021:3707.

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

dan niet juist is.[23] Met een beroep op het vertrouwensbeginsel worden ook de verzoeken tot het horen van Franse of Nederlandse officieren van justitie en rechercheurs over het algemeen afgewezen.[24]

Om gebondenheid aan het vertrouwensbeginsel te onderstrepen wordt in de meeste gevallen verwezen naar het standaardarrest van de Hoge Raad van 15 oktober 2010, waarin de Hoge Raad het volgende overweegt:

> *'Ten aanzien van onderzoekshandelingen waarvan de uitvoering plaatsvindt onder verantwoordelijkheid van de buitenlandse autoriteiten van een andere tot het EVRM toegetreden staat, is de taak van de Nederlandse strafrechter ertoe beperkt te waarborgen dat de wijze waarop van de resultaten van dit onderzoek in de strafzaak tegen de verdachte gebruik wordt gemaakt, geen inbreuk maakt op zijn recht op een eerlijk proces, zoals bedoeld in art. 6, eerste lid, EVRM. Het behoort niet tot de taak van de Nederlandse strafrechter om te toetsen of de wijze waarop dit onderzoek is uitgevoerd, strookt met de dienaangaande in het desbetreffende buitenland geldende rechtsregels (vgl. HR 18 mei 1999, NJ 2000/107).'*[25]

Strafrechtadvocaten betogen echter dat de rechtbanken hiermee miskennen dat de Hoge Raad in hetzelfde arrest stelt dat:

> *'De aard en de omvang van de rechterlijke toetsing van de rechtmatigheid van onderzoekshandelingen die hebben plaatsgevonden in het buitenland, verschillen naar gelang deze onderzoekshandelingen zijn uitgevoerd onder verantwoordelijkheid van de buitenlandse autoriteiten dan wel onder verantwoordelijkheid van de Nederlandse autoriteiten.'*[26]

Het argument is dat de verantwoordelijkheid voor het onderzoek (deels) verschoven is naar Nederland, gezien de nauwe betrokkenheid van de Nederlandse politie bij het Franse onderzoek. Hierdoor zou het vertrouwensbeginsel niet van toepassing zijn. Volgens (onder meer) de rechtbank Midden-Nederland betekent dat echter nog niet dat daarmee sprake is van een dusdanig nauwe samenwerking dat er *de facto* sprake is van een Nederlands onderzoek:

> *'Dat er sprake is geweest van een nauwe samenwerking tussen Frankrijk en Nederland op basis van de JIT-overeenkomst is evident en wordt ook niet door het Openbaar Ministerie ontkend. Dit gegeven maakt echter niet dat er sprake is van het verschuiven van de verantwoordelijkheid van het opsporingsonderzoek. Voorts is gemotiveerd naar voren gebracht dat Nederlandse opsporingsambtenaren, dan wel medewerkers van het NFI, de interceptietool mede hebben ontwikkeld. Dat Nederlandse opsporingsambtenaren de interceptietool (mede) hebben ontwikkeld, wordt door het Openbaar Ministerie in de brief van 24 maart 2021 ontkend. Los daarvan zou Nederlandse (technische) inbreng bij het ontwikkelen van de tool niet direct maken dat de verantwoordelijkheid voor het opsporingsonderzoek in Nederland komt te liggen.'*[27]

Op het tijdstip van het schrijven van dit overzicht is dit oordeel in overige jurisprudentie niet anders.[28] Het aanhouden van het vertrouwensbeginsel in deze zaken, waarbij op grootschalige wijze gegevens worden verzameld, legt volgens Adams wel een probleem bloot met betrekking tot het recht op een eerlijk proces in artikel 6 EVRM:

> *'Het OM heeft verregaande kennis van het internationale digitalebewijsvergaringsproces en de daaruit voortvloeiende resultaten. De verdediging heeft deze kennis niet. (...) Het interstatelijke vertrouwensbeginsel kan daarmee de werking van het equality of arms-beginsel beperken. (...) De rechten van en waarborgen voor de verdediging in het kader van het equality of arms-beginsel raken door een ruimte interpretatie van het interstatelijke vertrouwensbeginsel tussen wal en schip.'*[29]

In de literatuur wordt verder opgemerkt dat wanneer geen sprake is van een Nederlands onderzoek, de Fransen het territorialiteitbeginsel hebben geschonden omdat zij kennis hadden van de geografische locatie van de EncroChat-gebruikers.[30] Zij hadden op het moment dat bekend werd dat er sprake was van een toestel dat zich op Nederlands grondgebied bevond direct het onderzoek moeten staken en de Nederlandse autoriteiten om toestemming moeten vragen, hetgeen niet is gebeurd.[31]

Ook met dit argument lijkt de verdediging vooralsnog bot te vangen. De rechtbank Midden-Nederland overwoog hierover bijvoorbeeld in haar uitspraak van 17 juni 2021 het volgende:

> *'De hack hield niet meer en niet minder in dan dat op individueel niveau door de Franse Gendarmerie software op een toestel werd geïnstalleerd, waardoor de [bedrijfsnaam 1] data, waaronder gegevens over de locatie, konden worden afgevangen. Op het moment van instal-*

23 Rb. Rotterdam 11 oktober 2021, ECLI:NL:RBROT:2021:9906, r.o. 6.5.17.
24 Zie bijvoorbeeld Rb. Midden-Nederland 17 juni 2021, ECLI:NL:RBMNE:2021:2570 en Rb. Oost-Brabant 1 juni 2021, ECLI:NL:RBOBR:2021:2557.
25 HR 15 oktober 2010, ECLI:NL:HR:2010:BL5629, r.o. 4.4.1
26 HR 15 oktober 2010, ECLI:NL:HR:2010:BL5629, r.o. 4.3. Zie voor nuanceringen op het vertrouwensbeginsel ook Adams 2021, p. 967-968.
27 Rb. Midden-Nederland, 17 juni 2021, ECLI:NL:RBMNE:2021:2570. Zie verder ook Verbeek & Beekhuis 2022 over de JIT-constructie.
28 Zie bijvoorbeeld ook Rb. Amsterdam 16 juli 2021, ECLI:NL:RBAMS:2021:3707, Rb. Midden-Nederland 16 september 2021, ECLI:NL:RBMNE:2021:4480 en Rb. Overijssel 29 september 2021, ECLI:NL:RBOVE:2021:3689.
29 Adams 2021, p. 969 en 978. Op de relatie met de *equality of arms* als beginsel dat voortvloeit uit het recht op een eerlijk proces wordt in paragraaf 5 nader ingegaan.
30 R. van Boom & J. Reijsinger, 'Bewijs uit Encrochat in strijd met het recht', *Adv.bl.* 2021-7 (hierna: Van Boom & Reijsinger 2021).
31 Art. 31 van de EOB Richtlijn stelt dat de 'intercepterende lidstaat' de autoriteiten van de lidstaat waar de verdachten zich bevinden in kennis moet stellen voorafgaand aan de interceptie, of wanneer een en ander pas duidelijk wordt tijdens de interceptie, op dat moment. De in kennis gestelde lidstaat heeft dan de mogelijkheid om te bepalen dat de interceptie niet mag worden uitgevoerd, of wanneer de interceptie al heeft plaatsgevonden, voorwaarden te stellen aan het gebruik van het verzamelde materiaal.

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

latie van de hack was de locatie van dat toestel nog niet bekend en ook afhankelijk van de wil van de gebruiker. Deze bepaalt immers op welke locatie het toestel zich bevindt. Pas na het veiligstellen en analyseren van de data in Frankrijk blijkt de locatie van het toestel. Enige, laat staan doorslaggevende bemoeienis van Nederlandse autoriteiten is op individueel gebruikersniveau dan ook niet aanwezig.'[32]

De Nederlandse politie keek niet 'live' mee met het binnenhalen van elk bericht en kon dus ook niet reeds op dat moment beoordelen dat er sprake was van een Nederlandse gebruiker van een cryptotelefoon.

Ad 2) Verzoeken die zien op de processtukken van onderzoek 26Lemont

De tweede categorie onderzoekswensen ziet op de gang van zaken rondom het onderzoek 26Lemont. Het argument van de verdediging is dat er in deze zaak mogelijk onherstelbare vormverzuimen zijn begaan, waardoor de EncroChat-berichten uit 26Lemont niet in andere zaken gebruikt hadden mogen worden.

Normaliter staat de *Schutznorm* aan een dergelijke conclusie in de weg: wanneer de vormverzuimen zijn begaan buiten het kader van het voorbereidend onderzoek in de tegen hem aanhangige zaak (bijvoorbeeld in het kader van een andere zaak), dan heeft dat geen gevolgen voor de beoordeling in de zaak tegen de verdachte. Echter, wanneer het betreffende vormverzuim van bepalende invloed is geweest op het verloop van het opsporingsonderzoek naar en/of de (verdere) vervolging van de verdachte ter zake van het ten laste gelegde feit, dan kunnen daaraan toch rechtsgevolgen worden verbonden.[33]

Het openbaar ministerie stelt zich steeds op het standpunt dat de EncroChat-operatie en het veiligstellen van de berichten gericht was op het bedrijf EncroChat en niet op de cryptotelefoongebruikers, zodat de Schutznorm van toepassing is en aan eventuele vormverzuimen geen gevolg moet worden verbonden in de strafzaak tegen de verdachte.[34] Niet iedere rechtbank is hiervan overtuigd. De rechtbank Amsterdam overweegt bijvoorbeeld:

'(...) dat door het Openbaar Ministerie in 26Lemont aan de rechter-commissaris een lijst werd overgelegd met Nederlandse strafrechtelijke onderzoeken naar georganiseerde verbanden, waarvan bekend was dat gebruik werd gemaakt van EncroChat-toestellen in Nederland. Daarmee kan niet worden volgehouden dat het onderzoek 26Lemont uitsluitend ziet op het bedrijf EncroChat zelf. De rechtbank gaat er daarom van uit dat het onderzoek ook tot doel had om strafbare feiten van de gebruikers op te kunnen sporen, waarna nieuwe opsporingsonderzoeken zouden worden gestart teneinde daarnaar verder onderzoek te doen. Daarmee is de machtiging van de rechter-commissaris ook van belang in de onderhavige zaak.'[35]

Een ander argument voor het toetsen van de machtiging ex artikel 126uba Sv die wordt gebezigd, is dat het deel van het opsporingsonderzoek dat in Nederland heeft plaatsgevonden wél door de rechter op rechtmatigheid moet worden getoetst. De rechtbank Midden-Nederland overweegt bijvoorbeeld dat de analyse van de EncroChat-gegevens (na de verstrekking ervan door de Fransen) heeft plaatsgevonden in het kader van het voorbereidend onderzoek ten aanzien van de verdachte door Nederlandse opsporingsambtenaren in een Nederlands strafrechtelijk onderzoek. Dat betekent dat een rechtsgevolg op zijn plaats kan zijn, indien er een vormverzuim heeft plaatsgevonden in de *verwerkingsfase* van de EncroChat-gegevens. De rechtbank Midden-Nederland overweegt daarom dat de rechtmatigheid en naleving van de machtiging op grond van artikel 126uba Sv moet worden getoetst.[36]

In de loop van tijd is aldus meer over de machtiging ex artikel 12uba Sv en de processtukken bekend geworden. De openbaarmaking van de machtiging en de onderliggende stukken kan als een kleine overwinning voor de verdediging worden gezien. Nog steeds worden daarbij delen in de machtiging of onderliggende processtukken weggelakt, omdat openbaarmaking van bepaalde details toekomstige onderzoeken zou kunnen schaden. In een beschikking van de rechtbank Rotterdam geeft een rechter-commissaris bijvoorbeeld aan dat bepaalde passages over 'de aard en werking van het ingezette interceptiemiddel' en 'identificerende gegevens van medewerkers' mogen worden weggelakt. Dit wordt als volgt gemotiveerd:

'Naar het oordeel van de rechters-commissarissen kan de onthulling daarvan verstrekkende gevolgen hebben voor lopende en toekomstige onderzoeken die afhankelijk zijn van een succesvolle inzet van (een) soortgelijk(e) interceptiemiddel(en). Kennisneming van deze werkwijze(n) door de verdachte(n) of door derden maakt immers dat zij daarop kunnen anticiperen en dat de informatiegaring, onderzoeksvoorbereiding en opsporingsmogelijkheden aan effectiviteit zullen inboeten of niet langer mogelijk zullen zijn. Gelet daarop wordt het onthouden van die passages aan de processtukken noodzakelijk geacht op grond van art. 187d lid 1 sub b Sv. Dat kan niet nader worden gemotiveerd zonder de informatie te verstrekken die nu juist afgeschermd moet blijven.'[37]

32 Rb. Midden-Nederland, 17 juni 2021, ECLI:NL:RBMNE:2021:2570.
33 Zie HR 1 december 2020, ECLI:NL:HR:2020:1889.
34 Zie bijvoorbeeld Rb. Midden-Nederland 16 september 2021, ECLI:NL:RBMNE:2021:4480, r.o. 4.1.3.
35 Rb. Amsterdam 16 juli 2021, ECLI:NL:RBAMS:3707.
36 Rb. Midden-Nederland 16 september 2021, ECLI:NL:RBMNE:2021:4480, r.o. 4.1.3.
37 Rb. Rotterdam 11 oktober 2021, ECLI:NL:RBROT:2021:10412. Een saillant detail is dat rechters in het onderzoek Sartell wél de ongelakte machtiging hebben kunnen inzien. Deze rechters hebben zich echter onmiddellijk verschoond. De argumenten van de verdediging dat de ongelakte machtiging daarmee een processtuk is geworden en gevoegd moet wor-

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

Een bezwaar dat in de literatuur wordt opgeworpen, maar nog niet als zodanig is voorgelegd aan de rechter, is dat de verstrekkingen uit het onderzoek 26Lemont op grond van artikel 126dd Sv onrechtmatig zijn.[38] Van Boom en Reijsinger stellen in een opiniestuk voor het Advocatenblad dat artikel 126dd Sv niet kan dienen als een grondslag voor verstrekking aan andere onderzoeken nu in dit artikel de hackbevoegdheid van artikel 126uba Sv niet wordt genoemd.

Het argument van Van Boom en Reijsinger dat gegevens die zijn verkregen op grond van artikel 126uba Sv niet gedeeld kunnen worden tussen onderzoeken nu deze bevoegdheid niet genoemd is in de opsomming van artikel 126dd Sv, is volgens ons onjuist.[39] In de memorie van toelichting bij de Wet computercriminaliteit III (waarin de hackbevoegdheid is geregeld) heeft de wetgever namelijk expliciet kenbaar gemaakt dat de regeling van artikel 126dd Sv van overeenkomstige toepassing is op gegevens die zijn verkregen op basis van onderzoek in een geautomatiseerd werk:

> *'Op grond van de regeling van artikel 126dd Sv kan de officier van justitie bepalen dat de gegevens, die zijn verkregen in het kader van het aftappen van communicatie, het direct afluisteren en de stelselmatige observatie met een technisch hulpmiddel worden gebruikt voor een ander strafrechtelijk onderzoek of voor de verwerking van gegevens met het oog op de verkrijging van inzicht in de betrokkenheid van personen bij ernstige strafbare feiten. Deze regeling is eveneens van toepassing als deze bevoegdheden worden uitgeoefend in het kader van een onderzoek in een geautomatiseerd werk.'*[40]

Zelfs al zou dit niet het geval zijn, dan is niet uitgesloten dat onderzoeksgegevens die afkomstig zijn vanuit een buitenlandse hack gedeeld kunnen worden. De artikelen 126cc Sv en 126dd Sv die in samenhang dienen te worden gelezen, hebben volgens Blom een beperkte strekking.[41] Alleen voor de gegevens genoemd in artikel 126cc lid 1 Sv geldt een vernietigingsplicht. Voor gegevens afkomstig uit de toepassing van andere opsporingsbevoegdheden, bestaat niet altijd een plicht tot vernietigen. Die kunnen ingevolge het uitgangspunt van de Wet politiegegevens voor andere politietaken worden gebruikt, voor zover die rechtmatig zijn verkregen. Dat artikel 126uba Sv-gegevens niét genoemd zijn in artikel 126cc Sv betekent dus niet aanstonds dat deze gegevens niet mogen worden gedeeld.[42]

5. Toegang tot de gegevens

Begin 2020 schreven wij een artikel over de toegang tot gegevens door de verdediging die als bewijs worden gebruikt van cryptotelefoonaanbieder Ennetcom.[43] In dat artikel wezen wij onder andere op de noodzaak de verdediging toegang te geven tot gegevens van de cryptotelefoon die zowel belastend als ontlastend kunnen zijn voor de verdachte. Dit recht moet worden afgeleid uit het beginsel van de *equality of arms*, dat wordt afgeleid uit artikel 6 EVRM. De discussie over de toegang én de wijze waarop de toegang wordt verleend tot de veiliggestelde gegevens uit cryptotelefoons heeft zich sindsdien verder ontwikkeld.

Rond 2017 werden gegevens op verzoek van de verdediging verstrekt op een cd-rom en kreeg de verdediging een demonstratie van het Hansken-systeem bij het Nederlands Forensisch Instituut (NFI) waar de gegevens verder worden verwerkt. De verdediging kon het systeem uitproberen en vragen stellen over de werking van het systeem. De verdediging voelde zich destijds niet voldoende in de gelegenheid gesteld de gegevens die tegen de verdachte worden gebruikt te onderzoeken, onder andere om een 'alternatief scenario' van gebeurtenissen te onderbouwen. Ook speelde de vraag in hoeverre de verdediging toegang kreeg tot *alle* gegevens die in het onderzoek Ennetcom waren veiliggesteld. De verdediging beschikte met andere woorden niet of niet volledig over dezelfde kennis en hulpmiddelen als het OM. Zij ervaarde (en ervaart volgens sommigen nog steeds) weinig tot geen mogelijkheden om het bewijsvergaringsproces te controleren en ontlastend bewijs te vergaren.[44]

De toegang tot gegevens die van belang kunnen zijn voor de verdachte is niet absoluut (dat wil zeggen, de toegang tot *alle* verzamelde gegevens), maar wij stelden destijds dat het openbaar ministerie wel meer stappen kon ondernemen om toegang tot datasets te faciliteren als uitvloeisel van het beginsel van de equality of arms.[45] Meer concreet was onze aanbeveling een *dataroom* in te richten, van waaruit de verdediging op een veilige en digitaal-forensisch verantwoorde manier de gegevens kon onderzoeken. Galič (2021) en Adams (2021) gaan nog een stap verder en wijzen op recente jurisprudentie waaruit zou blijken dat het openbaar ministerie de ver-

den in het procesdossier heeft de rechter echter aan de kant geschoven. Zie Rb. Rotterdam 11 oktober 2021, ECLI:NL:RBROT:2021:9906.

38 Van Boom & Reijsinger 2021, p. 62.

39 Van Boom & Reijsinger 2021, p. 63.

40 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 109.

41 T. Blom, Commentaar op artikel 126dd Sv, *Tekst & Commentaar Strafvordering* (online versie) (laatst geraadpleegd op 17 december 2021).

42 Overigens zou het wel logisch zijn dat de bevoegdheden ex art. 126nba en 126uba Sv zouden worden toegevoegd aan de opsomming in art. 126cc lid 1 Sv.

43 B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3.

44 Adams 2021, p. 965. Zie in gelijke strekking D.N. de Jonge, 'Verdedigen in tijden van digitale bewijsvoering. Een onderzoek naar de mogelijkheden van toegang tot niet van het procesdossier uitmakende, maar mogelijk wel relevante, (digitale/technische) gegevens' in: P.P.J. van der Meij e.a. (red.), Aan de slag: Liber amicorum Gerard Hamer, Den Haag: Sdu Uitgevers 2018.

45 Zie ook F.P. Ölçer, *Recht op een eerlijk proces en bijzondere opsporing* (diss. Leiden), Nijmegen: Wolf Legal Publishers 2006, p. 151-152; M.J. Vetzo, J.H. Gerards & R. Nehmelman, *Algoritmes en grondrechten*, Den Haag: Boom juridisch 2018, p. 120; M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2 (hierna: Galič 2021), p. 43-45 en Adams 2021, p. 369-374.

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

dediging zou moeten betrekken bij het selecteren van de secundaire dataset aan de hand van zoekwoorden of filters.[46]

In de afgelopen paar jaar heeft het openbaar ministerie (samen met het NFI) aanzienlijke stappen gezet in de beschikbaarstelling van de gegevens uit cryptotelefoons die tegen een verdachte in een strafzaak kunnen worden gebruikt. In een recent artikel van Janssen en De Jong (2021) is de huidige stand van zaken te lezen over de toegang tot de gegevens voor de verdediging.[47] Daarin staat dat gegevens die relevant kunnen zijn voor de verdachte op verzoek in een Excelbestand beschikbaar kunnen worden gesteld. Belangrijker nog, de verdediging krijgt de mogelijkheid om in een dataroom met behulp van Hansken (hetzelfde systeem dat de rechercheurs gebruiken) de datasets te doorzoeken op gegevens die van belang kunnen zijn voor de verdachte, onder andere om een alternatief scenario te kunnen onderbouwen.[48]

Janssen en De Jong schetsen dat in de huidige praktijk nog steeds knelpunten bestaan omtrent de toegang tot de gegevens en uitoefening van de rechten van de verdediging. Zo is de verdediging gebonden aan de locatie en de openingstijden van het NFI. Misschien wel belangrijker nog is dat de verdachte er tijdens het onderzoek meestal niet bij kan zijn, bijvoorbeeld omdat hij of zij in de penitentiaire inrichting zit. Het is daardoor lastig te bepalen naar welk bewijs de advocaat, in vertegenwoordiging van de verdachte, op zoek moet gaan.[49]

Het verder faciliteren van de toegang tot de gegevens met dezelfde tools waar de politie gebruik van maakt – door middel van *remote access* en een beveiligde verbinding – zou wat ons betreft een aanzienlijke stap in de goede richting zijn.[50] Daarbij waarschuwen experts wel meteen dat het analyseren van de gegevens complex is en bijzondere vaardigheden vergt, waarvoor mogelijk eerst een training is vereist.[51]

Wij zijn van mening dat – bezien vanuit het beginsel van de equality of arms zoals dat voortvloeit uit artikel 6 EVRM – de aanvankelijke frustratie bij advocaten over de gebrekkige toegang tot de gegevens die tegen hun cliënten worden gebruikt begrijpelijk en terecht is. De huidige praktijk, waarbij het ook voor de verdediging mogelijk is om de data te bevragen via het Hanskensysteem en deze in een toegankelijk en leesbaar format te ontvangen, is echter al een flinke stap vooruit. Het stelt de verdediging in ieder geval beter in staat om effectief en efficiënt onderzoek uit te voeren.[52]

6. Afsluitende beschouwing

Uit de EncroChat-jurisprudentie komt vooralsnog niet het beeld naar voren dat er sprake is geweest van (ernstige) schendingen van de beginselen van een goede procesorde. Gesteld kan worden dat sommige rechtbanken wel heel snel naar het vertrouwensbeginsel of de Schutznorm wijzen om bezwaren of onderzoekswensen van de verdediging af te doen en het heeft lang geduurd voordat de feiten over de operatie en de verleende Nederlandse machtiging voor de hackbevoegdheid boven tafel kwamen, maar dit alles doet niet af aan de conclusie dat justitie tot op heden als winnaar uit de bus komt in de EncroChat-jurisprudentie.

In de kern dient het handelen van de politie onder leiding van het openbaar ministerie op rechtmatigheid getoetst te kunnen worden. Toegang tot informatie over de wijze waarop bewijs is verzameld en tegen de verdachte wordt gebruikt, is een vereiste dat voortvloeit uit het strafvorderlijk legaliteitsbeginsel en het recht op een eerlijk proces. In de EncroChat-zaken blijkt de verleende machtiging van de rechter-commissaris een dankbaar ankerpunt te zijn om deze toets (alsnog) uit te voeren, met enige beperkingen die naar onze mening te billijken zijn. Deze machtiging was strikt strafvorderlijk gezien niet vereist, maar wordt door de rechtspraktijk wel als 'gepast' gezien. Wij juichen een dergelijke extra tussenstap ook toe, omdat hiermee de fundamentele rechten van de betrokkenen nadrukkelijker worden meegewogen ten opzichte van het opsporingsbelang. Als gevolg van de machtiging richt de rechtmatigheidstoets in de Nederlandse strafzaken zich meer op de verwerking van de gegevens onder de voorwaarden die in de machtiging door de Nederlandse rechter-commissaris zijn gesteld, in plaats van op de initiële verzameling van de gegevens in het buitenland.

Bovenstaande bevindingen nemen niet weg dat er nog andere juridische vragen liggen (onder andere met betrekking tot geheimhouderscommunicatie) waar wij in deze bijdrage niet op zijn ingegaan. Ook geeft het jurisprudentieoverzicht in dit artikel geen antwoord op de vraag of het juridisch kader voor grootschalige gegevensverzameling en analyse moet worden verbeterd. De gevraagde machtiging is naar onze mening een welkome extra waarborg in deze zaak, maar strikt genomen niet een vereiste binnen het huidige kader van het Wetboek van Strafvordering en de Wet politiegegevens. Galič gaat elders in dit nummer na wat wij kunnen leren van de jurisprudentie van het Europees Hof voor de Rechten

46 Zie ook Adams 2021, p. 973 en Galič 2021, p. 46-47 met verwijzing naar EHRM 4 juni 2019, nr. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715, par. 90 (*Sigurður Einarsson e.a. t. IJsland*) en EHRM 25 juli 2019, nr. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615, par. 58 (*Rook t. Duitsland*).

47 D.N. de Jonge & S.L.J. Janssen, 'Eindelijk toegang tot datasets. (Erg) langzaam maar zeker naar een nieuw normaal', *NJB* 2021/2532, p. 2793-2799 (hierna: De Jonge & Janssen 2021). Zie ook in reactie op het artikel: J.C. van der Pijll, 'De dataset langs de meetlat van artikel 6 EVRM', *NJB* 2022/291, p. 346-351 (hierna: van der Pijll 2022).

48 Zie ook Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504, Rb. Amsterdam 1 april 2021, ECLI:NL:RBAMS:2021:1507 en Rb. Amsterdam 21 mei 2021, ECLI:NL:RBAMS:2021:2585.

49 De Jonge & Janssen 2021, p. 2796-2797.

50 Zie voor een discussie hieromtrent: Rb. Amsterdam 21 mei 2021, ECLI:NL:RBAMS:2021:2585, r.o. 34-38.

51 Zie ook H. Henseler, 'Het inzagerecht en de groeiende omvang van digitaal bewijs', *Expertise en Recht* 2020-6, p. 215-217.

52 Zie ook van der Pijll 2022.

doi: 10.5553/TBSenH/229567002022008002002

Dit artikel uit Tijdschrift voor Bijzonder Strafrecht & Handhaving is gepubliceerd door Boom juridisch en is bestemd voor Universiteitsbibliotheek Utrecht (202441)

van de Mens met betrekking tot bulkbevoegdheden ten aanzien van grootschalige data-analyse in strafrechtelijk onderzoek.[53] De privacy-inbreuk zit namelijk niet alleen in de verzameling en selectie van gegevens voor toekomstige strafzaken, maar juist ook in de kennisname/analyse van de gegevens.

In het huidige systeem krijgen vormverzuimen ten aanzien van de naleving van de Wet politiegegevens of regelgeving omtrent gegevensbescherming uit verdragen geen aandacht van de strafrechter en in de praktijk nauwelijks aandacht van de toezichthouder (de Autoriteit Persoonsgegevens).[54] Het is echter niet bepaald een vanzelfsprekendheid dat bij het verzamelen van dergelijke grote hoeveelheden gegevens van de achterliggende gebruikers van een communicatiedienst waar het opsporingsonderzoek op is gericht, ál deze gegevens voor *toekomstige* opsporingsonderzoeken mogen worden gebruikt. Dit is naar de letter van de huidige wet met toestemming van een officier van justitie juridisch wel mogelijk, maar het valt te betwijfelen of deze constructie de fundamentele rechten van de betrokkenen voldoende beschermt. De wetgever heeft zich over deze nieuwe opsporingspraktijk nog niet kunnen uitlaten. Nader onderzoek of een aanpassing van de wet wenselijk is, is daarom volgens ons op zijn plek.

53 M. Galič, 'Bulkbevoegdheden en strafrechtelijk onderzoek: lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse', *TBS&H* 2022.

54 Zie bijvoorbeeld Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584, r.o. 2.1: *'De rechtbank heeft op 28 april 2021 al besloten dat de Wpg geen belangrijk strafvorderlijk voorschrift is. De verdediging heeft dan ook geen belang bij een toetsing aan de voorschriften van de Wpg. Deze toetsing is immers niet van belang voor de vragen die de rechtbank in het kader van de artikelen* 348 *en* 350 *Sv dient te beantwoorden, noch een vraag die beantwoord moet worden bij de toetsing of sprake is van een eerlijk proces als bedoeld in artikel 6 EVRM.'*

doi: 10.5553/TBSenH/229567002022008002002