Antwoorden op prejudiciële vragen in de EncroChat- en SkyECC-zaken

Jan-Jaap Oerlemans & Bart Schermer[1]

In talloze zaken vormen door de Franse opsporingsautoriteiten buitgemaakte berichten van Encrochat en SkyECC cryptotelefoons het sleutelbewijs voor een veroordeling. In veel zaken waarin deze gegevens als bewijs zijn gebezigd heeft de verdediging uitgebreid verweer gevoerd inzake de rechtmatigheid van deze bewijsgaring. Gegeven de onduidelijkheid over de reikwijdte van het interstatelijke vertrouwensbeginsel in dezen besloten zowel Rechtbank Overijssel als Rechtbank Noord-Nederland prejudiciële vragen te stellen aan de Hoge Raad. In een arrest van juni 2023 zijn deze beantwoord. Nu dit type 'datagedreven' onderzoek de toekomst lijkt van de opsporing van georganiseerde criminaliteit is het zaak deze antwoorden nauwkeurig te bestuderen.

1. Inleiding

EncroChat en SkyECC hebben de laatste jaren een groot stempel gedrukt op strafzaken in Nederland. De verzamelde gegevens uit deze operaties hebben bijgedragen aan honderden veroordelingen voor ernstige delicten.[2]

De wijze waarop het bewijsmateriaal is verkregen is echter omstreden en de verdediging heeft dan ook de legitimiteit van de hele operatie in twijfel getrokken. Dit heeft uiteindelijk geleid tot het stellen van prejudiciële vragen aan de Hoge Raad. Sinds 1 oktober 2022 bestaat voor rechtbanken en gerechtshoven de mogelijkheid om prejudiciële vragen aan de strafkamer van de Hoge Raad te stellen. Dit is het eerste arrest waarin de Hoge Raad prejudiciële vragen in strafzaken beantwoordde.[3]

In dit artikel bespreken wij de antwoorden van de Hoge Raad op de prejudiciële vragen in de EncroChat- en SkyECC-zaken. Kennisname van deze antwoorden en een kritische reflectie daarop zijn relevant gezien het belang van deze 'crypto-telefoonzaken' voor het strafrecht. De zaken hebben niet alleen tot veel veroordelingen geleid; de manier van werken waarbij vanuit grootschalige gegevenssets nieuwe opsporingsonderzoeken worden gestart ('datagedreven opsporing')[4] staat ook indirect ter discussie.

Allereerst schetsen wij de achtergrond van de EncroChat- en SkyECC-zaken die aanleiding hebben gegeven tot het stellen van de prejudiciële vragen. Vervolgens bespreken wij de antwoorden van de Hoge Raad en reflecteren we op de vraag wat deze antwoorden nu betekenen voor strafzaken waarin EncroChat- of SkyECC-berichten tot het bewijs worden gebezigd. Ten slotte identificeren wij nog enkele openstaande vraagstukken.

2. Aanleiding

EncroChat en SkyECC waren aanbieders van zogenaamde 'cryptotelefoons'. Deze telefoons maakten het mogelijk om berichten te versleutelen waardoor ze onleesbaar waren voor derden zoals de politie. Het is niet mogelijk met cryptotelefoons via het reguliere telefoonnetwerk te bellen. Gebruikers kochten een telefoontoestel in combinatie met een abonnement waarop de EncroChat- en SkyECC-applicaties vooraf waren geïnstalleerd om de service te kunnen gebruiken.[5]

De Nederlandse politie startte een onderzoek naar cryptotelefoons, omdat uit meerdere opsporingsonderzoeken bleek dat personen die zich bezighielden met het beramen en plegen van zware criminaliteit, in de periode vanaf augustus 2015 gebruik maakten van cryptotelefoons om versleuteld te communiceren. Uiteindelijk startten de politie en het Openbaar Ministerie in 2020 verschillende opsporingsonderzoeken naar de bedrijven EncroChat en SkyECC, alsmede de 'NN-gebruikers' (onbekende gebruikers) die zich bezighielden met diverse vormen van georganiseerde criminaliteit.

Ondertussen begon de Franse Gendarmerie haar onderzoek naar EncroChat in 2017. Tijdens het Franse onderzoek kwamen de autoriteiten erachter dat de EncroChat-servers gehost werden bij hosting provider 'OVH' in Roubaix, Frankrijk. Voor het onderzoek naar zowel Encro-

Chat als SkyECC werd samen met de Franse politie een Joint Investigation Team (JIT) opgericht.[6]

Door middel van een hack slaagde de Franse politie erin om in april 2020 – vanaf de servers van EncroChat in Frankrijk – toegang te krijgen tot tienduizenden EncroChat-toestellen wereldwijd. De software die de politie gebruikte legde gegevens van de telefoons vast, waaronder gebruikersnamen, adresboeken en opgeslagen chatberichten. Daarna werden gedurende een aantal maanden naar schatting 115 miljoen berichten door middel van interceptie onderschept.[7] Het Franse onderzoeksteam heeft daarna de Nederlandse politie en Europol toegang gegeven tot deze gegevens.

Ten behoeve van de bewijsverzameling in het SkyECC-onderzoek ontwikkelden Nederlandse onderzoekers een techniek om (heimelijk) SkyECC-berichten van circa 70.000 SkyECC telefoons af te tappen en de berichten – met de verkregen sleutels – later te ontsleutelen. Vanaf 17 december 2020 tot en met maart 2021 zijn door Franse autoriteiten in Roubaix, Frankrijk, naar schatting 1 miljard berichten onderschept, waarvan in ieder geval honderden miljoenen berichten zijn ontsleuteld.[8]

De EncroChat- en SkyECC-gegevens zijn vervolgens door de Nederlandse politie met behulp van algoritmes en zoektermen geanalyseerd en onderzocht. Na goedkeuring door de rechter-commissaris, worden de gegevens ook gebruikt voor andere opsporingsonderzoeken dan de onderzoeken naar EncroChat en SkyECC. Volgens Franse en Nederlandse autoriteiten heeft alleen al de EncroChat-operatie geleid tot 6500 arrestaties en de inbeslagname van € 900 miljoen aan illegaal verkregen bezittingen.[9]

In veel zaken waarin de gegevens tot het bewijs zijn gebezigd heeft de verdediging uitgebreid verweer gevoerd. Kortgezegd twijfelt de verdediging aan de rechtmatigheid van de bewijsgaring in de EncroChat- en SkyECC-operaties en wil om die reden een toetsing van de opsporingshandelingen door de Nederlandse rechter.[10] Het interstatelijke vertrouwensbeginsel staat een dergelijke toetsing echter in de weg. In diverse zaken hebben advocaten getracht meer te weten te komen over de operatie en de rol die de Nederlandse politie en het OM daarin hebben gespeeld. De verweren met betrekking tot interstatelijke vertrouwensbeginsel en de betrouwbaarheid van gegevens hebben tot dusver echter weinig succes gehad.[11]

3. De vragen

Gegeven de onduidelijkheid over de reikwijdte van het interstatelijke vertrouwensbeginsel besloten zowel de Rechtbank Overijssel als de Rechtbank Noord-Nederland om prejudiciële vragen te stellen aan de Hoge Raad.[12] De Rechtbank Overijssel heeft de volgende prejudiciële vraag gesteld:

> *'Mag de Nederlandse rechter, gelet op het interstatelijke vertrouwensbeginsel, ervan uitgaan dat in het buitenland een opsporingsbevoegdheid rechtmatig*

Volgens Franse en Nederlandse autoriteiten heeft alleen al de EncroChat-operatie geleid tot 6500 arrestaties en de inbeslagname van € 900 miljoen aan illegaal verkregen bezittingen

Auteurs

1. Prof. mr. dr. J.J. Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht en senioronderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). 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.

Noten

2. Een zoekslag op rechtspraak.nl op de woorden 'EncroChat + gevangenisstraf', gefilterd op strafzaken en uitspraken van rechtbanken, levert meer dan 300 resultaten op. Een zoekslag op rechtspraak.nl op het woord 'SkyECC + gevangenisstraf', gefilterd op strafzaken en uitspraken van rechtbanken, levert meer dan 150 resultaten op.

3. HR 13 juni 2023, ECLI:NL:HR:2023:913.

4. Het fenomeen van datagedreven opsporing is al uitgebreid in de literatuur beschreven naar aanleiding van deze 'cryptotelefoon operaties'. Zie J.S. Boeser, 'Cybersecurity en "datagedreven" opsporing: stand van zaken met betrekking tot de interceptie van versleutelde cryptocommunicatie', *TBS&H* 2021, afl. 5, p. 351-356, M. Galič, 'Bulkbevoegdheden en strafrechtelijk onderzoek', *TBS&H* 2022, afl. 2, p. 130-137 (hierna: Galič 2022), J.C. van der Pijl, 'De dataset langs de meetlat van artikel 6 EVRM', *NJB* 2022/291 p. 346-351 met nawoord van D.N. de Jonge en S.L.J. Janssen in *NJB* 2022/462. Zie verder B.W. Schermer, *De gespannen relatie tussen privacy en cybercrime* (oratie Leiden), 2022 (hierna: Schermer 2022), M.F.H. Hirsch Ballin & J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden', *DD* 2023/2, p. 18-38 (hierna: Hirsch Ballin & Oerlemans 2023) en R.M. te Molder, M.J. Dubelaar, M.I. Fedorova, S.M.A. Lestrade & T.F. Walree, 'Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing', *Computerrecht* 2023/64, p. 110-117 (hierna: te Molder e.a. 2023).

5. Zie voor een uitgebreidere beschrijving van de feiten met betrekking tot EncroChat: B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?', *TBS&H* 2022/2.2 (hierna: Schermer & Oerlemans 2022) en J.J. Oerlemans, 'Meer duidelijkheid over EncroChat-operatie', *Computerrecht* 2021/195. Zie voor een beschrijving met betrekking tot SkyECC: J.J. Oerlemans, 'Nieuwe details bekend over verloop bewijsverzameling SkyECC', *Computerrecht* 2023/46.

6. In het onderzoek naar SkyECC was ook de Belgische politie onderdeel van het JIT.

7. Zie, naar aanleiding van een persconferentie van Franse en Nederlandse instanties, het verslag van Bill Goodin, 'Three years on, EncroChat cryptophone hack nets 6,500 arrests and seizures of €900m', *Computerweekly.*com, 27 juni 2023. De politie sprak in 2021 over 25 miljoen berichten (Jaarverantwoording Politie 2020, 23 april 2021, p. 39.

8. In Belgische media wordt gesproken over 1 miljard berichten, waarvan er minstens 500 miljoen zijn ontsleuteld. Zie, o.a., 'D. Hiroux, 'Na advocatuur, parket en politie nu ook arrestaties bij fiscus en stad Antwerpen na operatie Sky": wat weten we nu al?', *vrt nws* 6 april 2021.

9. Zie Bill Goodin, 'Three years on, EncroChat cryptophone hack nets 6,500 arrests and seizures of € 900m', *Computerweekly.*com, 27 juni 2023.

10. Zie bijvoorbeeld het bericht 'Brandbrief over gekraakte chatberichten', *Advocatenblad* 24 oktober 2022. De brandbrief werd ondertekend door 133 advocaten.

11. Schermer & Oerlemans 2022.

12. Rb. Overijssel 30 december 2022, ECLI:NL:RBOVE:2022:4015 en Rb. Noord-Holland 19 december 2022, ECLI:NL:RBNNE:2022:4797.

> *is ingezet en de betrouwbaarheid van de resultaten ervan gegeven is, zolang de (on)rechtmatigheid van dat opsporingsmiddel en de (on)betrouwbaarheid van die resultaten niet onherroepelijk in rechte zijn komen vast te staan in dat land?'*[13]

De Rechtbank Noord-Nederland heeft zeven prejudiciële vragen (inclusief sub-vragen) gesteld.[14] Omwille van de omvang geven wij hier onze eigen verkorte weergave van de vragen:

1. Is het interstatelijke vertrouwensbeginsel zonder meer van toepassing wanneer bewijs is verzameld in het buitenland?
2. Geldt het interstatelijke vertrouwensbeginsel onverkort wanneer telecommunicatiegegevens van Nederlandse gebruikers worden verzameld vanuit een andere EU-lidstaat?
3. Is voor de verzameling van gegevens in/vanuit het buitenland waarvan duidelijk is dat de gebruikers zich (ook) op Nederlands grondgebied bevinden een machtiging van een Nederlandse rechter vereist?
4. Hoe verhoudt het internationale vertrouwensbeginsel zich tot het *equality of arms*-beginsel?
5. Zijn, indien het interstatelijke vertrouwensbeginsel niet onverkort geldt, gebreken bij het bewijsgaringsproces vanuit het buitenland 'afgedekt' door de machtigingen van Nederlandse rechters-commissarissen?
6. Als er sterke aanwijzingen zijn dat gebreken kleven aan het buitenlandse opsporingsonderzoek wat zijn dan de consequenties voor de toepassing van het interstatelijke vertrouwensbeginsel?
7. Is een wettelijke grondslag vereist voor het bewaren en gebruiken van de metadata en communicatie van gebruikers van een elektronische communicatiedienst door de Nederlandse autoriteiten, ten behoeve van de opsporing en vervolging van strafbare feiten, als deze is verkregen van een andere lidstaat, nadat die andere lidstaat deze data heeft geïntercepteerd?

We kunnen stellen dat de vragen van de beide rechtbanken qua inhoud min of meer gelijk zijn. De Rechtbank Overijssel stelt een overkoepelende vraag, de Rechtbank Noord-Nederland verdeelt de rechtsvraag netjes in meer specifieke vragen met subvragen.

4. De antwoorden

Omdat dit de eerste keer is dat er prejudiciële vragen zijn gesteld, start de Hoge Raad haar uitspraak met een uitgebreide bespreking van artikel 553 Sv en de te volgen procedure voor het stellen van prejudiciële vragen.[15] Deze inleidende opmerkingen komen erop neer dat een rechter die overweegt om een prejudiciële vraag te stellen, betrokken procespartijen in de gelegenheid moet stellen om zich uit te laten over dat voornemen en over de beoogde inhoud van de vraag.[16] Wij zullen in deze bijdragen niet nader stil staan bij deze 'mededelingen van huishoudelijke aard', maar ons enkel richten op de prejudiciële vragen zelf.

De Hoge Raad bespreekt in hoofdstuk 6 van haar dictum de vraag van de Rechtbank Overijssel. Vervolgens bundelt de Hoge Raad de verschillende vragen van de Rechtbank Noord-Nederland tot een vijftal thema's waarbij in de beantwoording vaak wordt verwezen naar de beantwoording van de vraag van de Rechtbank Overijssel. Wij nemen in deze bijdrage voor de leesbaarheid de vijf thema's van de Hoge Raad als uitgangspunt voor onze bespreking. Het gaat om: (1) de reikwijdte van het interstatelijke vertrouwensbeginsel, (2) onderzoek naar Nederlandse gebruikers, (3) de geldigheid van de machtigingen van Nederlandse rechter-commissarissen, (4) het beginsel van de *equality of arms*, en (5) het bewaren en gebruiken van de gegevens.

4.1. Reikwijdte van het interstatelijke vertrouwensbeginsel

De eerste en de zesde prejudiciële vraag van de Rechtbank Noord-Nederland hebben betrekking op de toepassing van het interstatelijke vertrouwensbeginsel bij de verzameling van het bewijsmateriaal, in het bijzonder wanneer dat materiaal is verkregen in het kader van het optreden van een gemeenschappelijk onderzoeksteam.

De Hoge Raad maakt in de beantwoording van de vragen een onderscheid tussen de toetsing van de *rechtmatigheid* van het verkrijgen van het bewijsmateriaal en de toetsing van de *betrouwbaarheid* van het materiaal.

Rechtmatigheid

Of, en zo ja, in welke mate de *rechtmatigheid* van onderzoekshandelingen die hebben plaatsgevonden in het buitenland, kunnen worden getoetst door de Nederlandse rechter hangt volgens de Hoge Raad samen met de vraag of de onderzoekshandelingen zijn uitgevoerd onder

De Hoge Raad maakt een onderscheid tussen de toetsing van de *rechtmatigheid* van het verkrijgen van het bewijsmateriaal en de toetsing van de *betrouwbaarheid* van het materiaal

verantwoordelijkheid van de buitenlandse autoriteiten, of onder verantwoordelijkheid van de Nederlandse autoriteiten.[17]

Voor wat betreft de situatie waarin de onderzoekshandelingen zijn uitgevoerd onder verantwoordelijkheid van de buitenlandse autoriteiten is de Hoge Raad helder: het behoort niet tot de taak van de Nederlandse strafrechter om de rechtmatigheid van de uitvoer van het buitenlandse onderzoek te toetsen.[18] Zou de rechter dit wel doen, dan levert dat een aantasting op van de soevereiniteit van het betreffende land.[19] Met andere woorden, het interstatelijke vertrouwensbeginsel staat toetsing door de Nederlandse rechter in de weg. Wij moeten erop vertrouwen dat, net als in Nederland, het recht op een eerlijk proces in Frankrijk wordt gewaarborgd door een zorgvuldige toepassing van het strafprocesrecht. De Hoge Raad merkt verder op dat wanneer enig recht van de verdachte geschonden is, daar een daadwerkelijk rechtsmiddel als bedoeld in artikel 13 EVRM tegenover staat in het betreffende land (in casu Frankrijk).[20]

In Frankrijk wordt momenteel ook de rechtmatigheid van de EncroChat- en SkyECC-operaties door Franse advocaten ter discussie gesteld. Het Franse Hof van Cassatie heeft op 11 oktober 2022 een zaak waarin EncroChat-berichten als bewijs werden gebezigd teruggewezen op grond van een motiveringsgebrek. Dat gebrek betrof het ontbreken van een door het hoofd van de technische instantie afgegeven certificaat waarin de oprechtheid van de verstrekte resultaten wordt bevestigd.[21] Het Hof Arnhem-Leeuwarden vond dat oordeel onvoldoende om te concluderen dat in het Franse onderzoek sprake is geweest van zodanige onrechtmatigheden dat die rechtsgevolgen zouden moeten hebben voor het gebruik van EncroChat-data in Nederlandse zaken.[22] Het Hof Den Haag wijst er ook op dat de Franse 'Conseil Constitutionnel' (Grondwettelijke Raad) in haar arrest van 8 april 2022 de interceptie bij EncroChat niet strijdig acht met de Franse grondwet.[23]

13. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 4.1.
14. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 4.2.
15. Zie hoofdstuk 3 van het dictum.
16. Ontleend aan de inhoudsindicatie bij HR 13 juni 2023, ECLI:NL:HR:2023:913.
17. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 6.5.1. Zie ook HR 5 oktober 2010, ECLI:NL:HR:2010:BL5629.
18. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 6.5.2.
19. Idem.
20. R.o. 6.5.1.
21. Zie Cour de cassation 11 oktober 2022, ECLI:FR:CCASS:2022:CR01226 en ECLI:FR:CCASS:2022:CR01216. Ook heeft het Landsgericht Berlin aan het Hof van Justitie van de Europese Unie om antwoorden op prejudiciële vragen verzocht met betrekking tot het Europese Onderzoeksbevel dat in deze operatie is afgegeven. Zie C-670/22, Verzoek om een prejudiciële beslissing ingediend door het Landgericht Berlin (Duitsland) op 24 oktober 2022 – Strafzaak tegen M.N.
22. Hof Arnhem-Leeuwarden 16 november 2022, ECLI:NL:GHARL:2022:9878.
23. Conseil Constitutionnel 8 april 2022, Besluit nr. 2022-987. Hof Den Haag 5 januari 2022, ECLI:NL:GHDHA:2023:6. Zie ook J.J. Oerlemans, 'Jurisprudentie na de prejudiciële vragen over EncroChat en SkyECC', *Computerrecht* 2023/48.

Wanneer in Frankrijk onherroepelijk vast komt te staan dat het onderzoek niet in overeenstemming met de daarvoor geldende rechtsregels is verricht, dan kan de Nederlandse rechter daar op grond van het Nederlandse strafprocesrecht consequenties aan verbinden. Gezien het bovenstaande ligt dat niet voor de hand. Bovendien betekent dat niet dat het bewijs uit de EncroChat of SkyECC automatisch wordt uitgesloten. Het is ook mogelijk dat een vormverzuim slechts wordt geconstateerd en er verder geen consequenties aan worden verbonden.[24]

Wanneer het onderzoek onder de verantwoordelijkheid van de Nederlandse autoriteiten is uitgevoerd, dan blijft het interstatelijke vertrouwensbeginsel buiten beschouwing. Wanneer dit het geval is, wordt besproken in het antwoord op de tweede prejudiciële vraag hieronder.

Wanneer het onderzoek onder de verantwoordelijkheid van de Nederlandse autoriteiten is uitgevoerd blijft het interstatelijke vertrouwensbeginsel buiten beschouwing

Betrouwbaarheid

Met betrekking tot de *betrouwbaarheid* van het bewijs overweegt de Hoge Raad dat de rechter voor de bewezenverklaring alleen dat bewijsmateriaal gebruikt dat hij betrouwbaar en bruikbaar acht.[25] Hierbij maakt het in beginsel geen verschil of die onderzoeksresultaten zijn verkregen onder verantwoordelijkheid van buitenlandse of Nederlandse autoriteiten.

Het uitgangspunt is wel dat het door de buitenlandse autoriteiten verkregen materiaal betrouwbaar mag worden geacht, omdat het immers in overeenstemming met het buitenlandse strafprocesrecht is verkregen. Als er echter concrete aanwijzingen voor het tegendeel bestaan, dan is de rechter gehouden de betrouwbaarheid van die resultaten te onderzoeken.[26] Die aanwijzingen kunnen voortkomen uit een specifiek verweer. De rechter kan vervolgens nadere informatie inwinnen over de wijze waarop het onderzoek onder de verantwoordelijkheid van de buitenlandse autoriteiten heeft plaatsgevonden.[27]

4.2. Onderzoek naar Nederlandse gebruikers

Een van de bezwaren die de advocatuur heeft opgeworpen tegen de onderzoeken naar EncroChat en SkyECC is dat er willens en wetens onderzoek is gedaan vanuit Frankrijk naar gebruikers op Nederlands grondgebied en dat dit (waarschijnlijk) plaats heeft gehad onder aansturing van de Nederlandse autoriteiten.[28]

De tweede prejudiciële vraag ziet op de interceptie van gegevens door de Franse autoriteiten van personen die zich op Nederlandse grondgebied bevinden. De vraag is of dit aanleiding geeft tot een ander of gewijzigd beoordelingskader. De Hoge Raad beantwoordt die vraag ontkennend.[29]

De Hoge Raad stelt dat wanneer onderzoek wordt gedaan naar Nederlandse gebruikers vanuit het buitenland, de verantwoordelijkheid daarvoor ligt bij de Nederlandse autoriteiten:

(i) als onder gezag van de (Nederlandse) officier van justitie in het buitenland overeenkomstig artikel 539a Sv door Nederlandse opsporingsambtenaren toepassing wordt gegeven aan de hun bij de Nederlandse wet toegekende opsporingsbevoegdheden; of
(ii) als een zodanig nauwe samenwerking bestaat tussen Nederlandse en buitenlandse autoriteiten bij de opsporing dat het gezag daarover feitelijk volledig of in overwegende mate toekomt aan de (Nederlandse) officier van justitie.[30]

Wanneer een van deze situaties zich voordoet, dan blijft het interstatelijke vertrouwensbeginsel buiten beschouwing. Dit is relevant voor de verdediging, omdat daarmee de weg tot een toetsing door de Nederlandse rechter openstaat.

De onder (i) bedoelde situatie doet zich volgens de Hoge Raad nog niet voor wanneer een Nederlandse opsporingsambtenaar betrokken is bij de uitvoering van een opsporingsbevoegdheid die wordt aangestuurd door de buitenlandse autoriteiten. Van de onder (ii) bedoelde situatie is nog geen sprake wanneer een Nederlandse opsporingsambtenaar aanwezig is bij de uitvoering van een onderzoekshandeling door een buitenlandse autoriteit, of wanneer Nederlandse opsporingsambtenaren technische assistentie verlenen.[31]

Op grond van hetgeen bekend is over de EncroChat- en SkyECC-operaties, zijn er tot op heden volgens de lagere rechters onvoldoende concrete aanwijzingen dat er sprake is van een situatie zoals beschreven onder i of ii.[32] Aldus is er tot op heden geen reden om het interstatelijke vertrouwensbeginsel buiten werking te stellen.

4.3. Machtiging van de rechter-commissaris

De derde en de vijfde prejudiciële vraag gaan over de vraag of en, zo ja, onder welke omstandigheden een machtiging van de Nederlandse rechter-commissaris is vereist voor de uitoefening van opsporingsbevoegdheden die worden uitgevoerd onder de verantwoordelijkheid van een buitenlandse autoriteit.[33]

In de EncroChat- en SkyECC-zaken is door de officier van justitie een machtiging voor het gebruik van de gegevens uit het Franse onderzoek aan de Nederlandse rechter-commissaris gevraagd. Strikt genomen was een dergelijke machtiging niet noodzakelijk, omdat het binnentreden werd gedaan door de Franse politie, onder aansturing van de Franse autoriteiten. In de machtiging heeft de rechter-commissaris aanvullende voorwaarden gesteld aan het gebruik van de buitgemaakte gegevens.[34]

De Hoge Raad overweegt dat een machtiging van de Nederlandse rechter-commissaris niet noodzakelijk is, wanneer een onderzoek wordt uitgevoerd onder de verantwoordelijkheid van een buitenlandse autoriteit. Dit is

Een machtiging van de Nederlandse rechter-commissaris is niet noodzakelijk wanneer een onderzoek wordt uitgevoerd onder de verantwoordelijkheid van een buitenlandse autoriteit

slechts anders wanneer de bevoegdheden worden uitgeoefend op initiatief van de Nederlandse autoriteiten.[35]

De Hoge Raad is verder van mening dat het Nederlandse strafprocesrecht zich niet verzet tegen het onverplicht vorderen van een machtiging van de rechter-commissaris. Het kan bijvoorbeeld een goede manier zijn om meer duidelijkheid te krijgen over een situatie waarin de wet nog niet, of onvoldoende, heeft voorzien:

> *'Van de ruimte die het wettelijk stelsel hier biedt, kan bijvoorbeeld gebruik worden gemaakt als zich technologische ontwikkelingen voordoen die, ook in grensoverschrijdend verband, voor de opsporing relevant zijn, terwijl de bestaande (wettelijke) regelingen – en daarmee de normering van de betreffende vormen van opsporing – nog slechts in beperkte mate op die ontwikkelingen zijn toegesneden.'*[36]

Een aanvullende toets van de rechter-commissaris biedt naast duidelijkheid ook een extra waarborg voor de bescherming van de persoonlijke levenssfeer, aldus de Hoge Raad.

Wat opvalt is dat de Hoge Raad niet expliciet vraag 5 van de Rechtbank Noord-Nederland beantwoordt. De Hoge Raad volstaat in haar beantwoording met het verwijzen naar de overwegingen 6.20 tot en met 6.24. Maar in deze overwegingen wordt niet met zoveel woorden gesproken over de situatie omschreven in vraag 5.

Dit zou kunnen zijn omdat de Hoge Raad in het antwoord op vraag 2 al heeft vastgesteld dat het interstatelijke vertrouwensbeginsel wél van toepassing is wanneer vanuit het buitenland onderzoek wordt gedaan naar Nederlandse gebruikers onder aansturing van de Franse autoriteiten. Maar het vertrouwensbeginsel zou wel buiten beschouwing kunnen blijven wanneer een van de hierboven genoemde situaties genoemd onder i en ii zich voordoet. Wanneer uit de feiten blijkt dat dit toch het geval is, dan wordt de beantwoording van vraag 5 ineens wél relevant. Het is jammer dat de Hoge Raad niet expliciet ingaat op dit scenario.

We zouden de vraag van de Rechtbank Noord-Nederland ook als volgt kunnen begrijpen:

> *Wanneer in het Franse onderzoek onherroepelijk vast is komen te staan dat er onherstelbare vormverzuimen zijn begaan, kan de situatie dan alsnog 'gered' worden door de Nederlandse machtiging?*

Wanneer deze situatie zich voordoet, dan moet de Nederlandse rechter op grond van artikel 359a Sv bepalen wat de strafvorderlijke consequenties van deze vormverzuimen zijn. Het komt ons voor dat de machtiging van de Nederlandse rechter-commissaris niet de Franse vormverzuimen kan herstellen, maar in ieder geval de ernst van deze vormverzuimen wel afzwakt, omdat de rechterlijke toetsing en de waarborgen uit deze machtiging het recht op een eerlijk proces van de verdachten en toekomstige verdachten aanvullend beschermen. Zelfs als blijkt dat in het Franse onderzoek onherstelbare vormverzuimen zijn begaan, hoeft dat dus nog niet te leiden tot bewijsuitsluiting of niet-ontvankelijkheid van het Nederlandse Openbaar Ministerie, omdat de verdachte niet noodzakelijkerwijs in zijn recht op een eerlijk proces is aangetast.

4.4. Het beginsel van the equality of arms

De *vierde* prejudiciële vraag betreft, kort gezegd, de mogelijkheden voor de verdediging om de rechtmatigheid van de bewijsverkrijging te onderzoeken, gelet op het beginsel van de *equality of arms*. Het gaat hier dan met name om onderzoekswensen gericht op het voegen van processtukken die betrekking hebben op de uitvoering van de onderzoekshandelingen in Frankrijk.

Met betrekking tot het voegen van processtukken overweegt de Hoge Raad dat het doel van de onderzoekswensen van doorslaggevende betekenis is voor de vraag of de stukken moeten worden bijgevoegd. Voor zover dergelijke verzoeken verband houden met de wijze waarop het onderzoek is verlopen dat is uitgevoerd door en onder verantwoordelijkheid van buitenlandse autoriteiten, wijst de Hoge Raad nogmaals op het interstatelijke vertrouwensbe-

24. Zie art. 359a Sv.

25. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 6.6.

26. Idem.

27. Idem.

28. Zie ook R. van Boom & J. Reijsinger, 'Bewijs uit Encrochat in strijd met het recht', *Advocatenblad* 2021, afl. 7.

29. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 7.4. De Hoge Raad gaat niet met zoveel woorden in op de vraag of het feit dat Nederlandse gebruikers (al dan niet bewust) doelwit zijn van de operatie betekent dat het vertrouwensbeginsel niet van toepassing is. Het Hof Arnhem-Leeuwarden gaat wel uitgebreid in op deze vraag en komt tot de conclusie dat het feit dat Nederlandse gebruikers geraakt worden door de Franse operatie niets verandert aan het feit dat de opsporingshandeling onder aansturing van de Franse autoriteiten heeft plaatsgehad. In zoverre de Fransen hiermee de territoriale soevereiniteit van Nederland hebben geschonden, is dat geen rechtens te respecteren belang van de verdachte. Zie Hof Arnhem-Leeuwarden 16 november 2022, ECLI:NL:GHARL:2022:9878.

30. R.o. 6.18.

31. R.o. 6.18.

32. Zie in dit kader bijvoorbeeld Hof Arnhem-Leeuwarden 16 november 2022, ECLI:NL:GHARL:2022:9878.

33. R.o. 7.5.

34. Meer specifiek ging het om een machtiging voor het digitaal binnentreden en onderzoeken van een geautomatiseerd werk in opsporingsonderzoeken naar misdrijven die in georganiseerd verband worden beraamd of gepleegd (de hackbevoegdheid in 126uba Sv) en het aftappen van (tele)communicatiegegevens (126t Sv). In Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584 zijn de voorwaarden te lezen.

35. R.o. 6.21.1.

36. R.o. 6.24.1.

ginsel.[37] Als het gaat om de productie van stukken gericht op het zicht krijgen op de rechtmatigheid van het Franse onderzoek, dan moet de rechter deze naast zich neerleggen, omdat op grond van het interstatelijke vertrouwensbeginsel de rechter geen oordeel toekomt op deze punten.

De onderzoekswensen moeten worden onderbouwd, waarbij die onderbouwing moet zien op het belang van de voeging dan wel de inzage in het licht van de beslissingen die in de strafzaak kunnen en moeten worden genomen.[38] Dit creëert een soort 'Catch 22' voor de verdediging: onderzoekswensen die erop gericht zijn om de betrouwbaarheid van het bewijsmateriaal te kunnen toetsen worden afgewezen, omdat daarmee in de beoordeling van de rechtmatigheid van het Franse onderzoek wordt getreden. In enkele strafzaken wordt overigens wel verwezen naar rapportages van het Nederlands Forensisch Instituut (NFI) over de betrouwbaarheid van bewijs. Eventuele gebreken in de betrouwbaarheid of volledigheid van het bewijs hebben vooralsnog niet tot vaststelling van een vormverzuim of een succesvol verweer geleid.[39]

Als het gaat om de productie van stukken gericht op het zicht krijgen op de rechtmatigheid van het Franse onderzoek, dan moet de rechter deze verzoeken naast zich neerleggen

Wij begrijpen de frustratie van advocaten over deze situatie. Omdat de operatie in JIT-verband is uitgevoerd en er daarbij sprake is geweest van een (nauwe) samenwerking tussen de Nederlandse en Franse autoriteiten, voelt het wat gekunsteld aan om te stellen dat het hier om een Frans onderzoek gaat waarover de Nederlandse rechter zich niet kan en mag uitspreken. Ook valt het te betwijfelen of in alle vervolgzaken waarin EncroChat/SkyECC-bewijs is gebruikt en gebruikt gaat worden, voor de verdachten wel een effectief rechtsmiddel in Frankrijk openstaat.

Dit geconstateerd hebbende menen wij echter niet dat de verdediging nu volledig met lege handen staat. Wij wijzen erop dat deze overwegingen omtrent het interstatelijke vertrouwensbeginsel betrekking hebben op de *verzameling* van de gegevens door en onder verantwoordelijkheid van buitenlandse autoriteiten. In de EncroChat- en SkyECC-zaken hebben de Franse autoriteiten tientallen tot honderden miljoenen gegevens doorgestuurd naar de Nederlandse autoriteiten. Na de ontvangst zijn de gegevens door de Nederlandse autoriteiten verder *gebruikt*. Vanaf dat moment is het interstatelijke vertrouwensbeginsel niet meer van toepassing. Het beginsel houdt met andere woorden op bij de Nederlandse grens. De Hoge Raad gaat hier verder niet op in, maar dit is onzes inziens een belangrijk gegeven, omdat advocaten op deze verdere verwerking van gegevens verweer kunnen voeren en de betrouwbaarheid van de ruwe data zelf en de daarop verrichte analyses ter discussie kunnen stellen. Met andere woorden: hoewel de verzameling van het bewijs niet te controleren valt, valt het verdere gebruik van het bewijs dat wél.

Daarbij is het van belang op te merken dat voor de analyse van grote hoeveelheden gegevens ook gebruikt wordt gemaakt van algoritmen en kunstmatige intelligentie (AI). Voor de analyse van deze gegevens in Nederland wordt het platform 'Hansken' gebruikt. Met dit systeem is het mogelijk berichten te clusteren met behulp van zoektermen en zoekfilters en daarna te onderzoeken. Algoritmen en AI worden volgens het NFI bijvoorbeeld gebruikt voor het herkennen van objecten in foto's zoals zeecontainers, bankpassen, vuurwapens en drugs.[40] Het voert te ver om in dit artikel te bespreken hoe zich dat verhoudt tot de jurisprudentie met betrekking tot het recht op een eerlijk proces, zoals bedoeld in artikel 6 EVRM.[41] Feit is wel dat digitaal bewijs – net als elk ander bewijs – niet 100% betrouwbaar is en ook software fouten kan maken.[42] Het is bijvoorbeeld denkbaar dat de software een keer een 'false positive' teruggeeft in een automatische selectie van berichten of foto's waarbij dat resultaat wordt gerelateerd aan de verdachte, of dat er bijvoorbeeld iets misgaat in de koppeling van gegevens aan de identiteit van een verdachte.

Voor zover daartoe aanleiding is, bijvoorbeeld omdat de verdediging ontkent dat het digitale bewijs betrekking heeft op de cliënt, moet de verdediging hierop effectief verweer kunnen voeren. Wij hebben als buitenstaanders geen zicht op welke documentatie of gegevens de verdediging van de politie en het Openbaar Ministerie ontvangt. Maar in beginsel zou toch op hoofdlijnen duidelijk moeten zijn hoe resultaat van het digitale bewijs uit de miljoenen verzamelde gegevens tot stand is gekomen. De gekozen toepassingen zouden transparant, uitlegbaar en controleerbaar moeten zijn.[43] De verdediging moet effectief verdediging kunnen voeren door in de gelegenheid te zijn schriftelijke vragen aan de politie of het NFI te stellen en te kunnen verzoeken tot het horen van getuigen of het uitvoeren van een deskundigenonderzoek. Jurisprudentie laat zien dat de mogelijkheid van deze verzoeken in de praktijk er ook is, maar dat deze verzoeken vaak worden afgewezen, vanwege onvoldoende aanleiding of een gebrekkige onderbouwing van de noodzaak.[44]

4.5. Het gebruiken en bewaren van de resultaten

De *zevende* prejudiciële vraag heeft betrekking op de wettelijke grondslag voor het bewaren en gebruiken van de verkregen onderzoeksresultaten. De Hoge Raad volstaat hier met het uiteenzetten van het wettelijk kader voor het delen van gegevens tussen opsporingsonderzoeken. Allereerst overweegt de Hoge Raad dat de verkregen onderzoeksresultaten uiteraard gebruikt mogen worden in het onderzoek waartoe de gegevens zijn verkregen. Daarnaast kunnen de gegevens op grond van artikel 126dd Sv en de regels uit de Wet Politiegegevens ook gedeeld worden ten behoeve van andere opsporingsonderzoeken.[45]

Het was interessant geweest als de Hoge Raad meer had gezegd over het gebruik van de gegevens in de praktijk en het toezicht daarop. Maar door de formulering van de prejudiciële vraag heeft de Hoge Raad zich die moeite kunnen besparen.

De Autoriteit Persoonsgegevens (AP) is verantwoordelijk voor de toetsing van de verwerking van persoonsgegevens bij de politie (en het NFI). De AP is naar aanleiding van de operaties klaarblijkelijk nog geen onderzoek gestart. Een mogelijke verklaring is dat veel vragen naar aanleiding van de operaties ook betrekking op de bescherming van andere waarden dan de bescherming van persoonsgegevens.

Wij wijzen er op dat verschillende auteurs in dit kader reeds hebben gepleit voor (aanvullend) onafhankelijk effectief toezicht op de verwerking van gegevens ten behoeve van de opsporing. Een belangrijke reden is dat zittingsrechters zich niet uitlaten over de naleving van de Wet politiegegevens en niet alle zaken waarin de gegevens worden verwerkt bij strafrechters verschijnen. Ook pleitten de auteurs voor een mogelijke koppeling tussen het wettelijk kader voor de verwerking van gegevens (de Wet politiegegevens) met de verzameling van gegevens (het Wetboek van Strafvordering), zodat de zittingsrechter ook aan die regelgeving kan toetsen.[46]

5. Slotbeschouwing

Wat betekenen de antwoorden op deze prejudiciële vragen nu voor de voortgang van al die zaken waarin EncroChat- en/of SkyECC-berichten tot het bewijs worden gebezigd? Want: 'Er staat nogal wat op het spel.'[47] In talloze zaken vormen de berichten het sleutelbewijs voor een veroordeling en daarmee is dit type 'datagedreven' onderzoek voorlopig de toekomst van de opsporing van de georganiseerde criminaliteit.

De antwoorden van de Hoge Raad met betrekking tot het interstatelijke vertrouwensbeginsel zijn over het geheel genomen niet verassend. De meeste auteurs waren het er al over eens dat het bewijs dat in Frankrijk binnen een JIT is verzameld, gedeeld mag worden in Nederland en dat wij moeten vertrouwen op de rechtmatigheid van het Franse systeem.[48] Wij zien in de antwoorden van de Hoge Raad dan ook vooral een indirecte legitimatie van de manier van werken van de politie en het OM in de EncroChat- en SkyECC-zaken. De nauwe samenwerking in de vorm van een JIT en (bulk)verzameling van gegevens op buitenlands grondgebied is, behoudens tegenbewijs, legitiem.

Uiteindelijk zijn – dankzij de verweren van ogenschijnlijk onvermoeibare advocaten – toch nog veel details over de verzameling van de gegevens naar boven gekomen. Enkele rechtbanken merken op dat het verstrekken van deze stukken relatief lang heeft geduurd,[49] maar uiteindelijk is er veel informatie voorhanden over de bewijsverzameling. Dat is noodzakelijk teneinde de bewijsverzameling van opsporingsinstanties te kunnen nagaan en controleren. Wij spreken de hoop uit dat het Openbaar Ministerie in toekomstige zaken van meet af aan de nodige duidelijkheid over het verloop van dit soort complexe operaties geeft, zodat advocaten zich beter op een verweer kunnen voorbereiden. De reeds verschafte transparantie over de beide operaties rechtvaardigt het huidige wantrouwen bij sommige advocaten volgens ons in ieder geval niet (meer).

Wij zien in de antwoorden van de Hoge Raad vooral een indirecte legitimatie van de manier van werken van de politie en het OM in de EncroChat- en SkyECC-zaken

De 'Catch 22' die de verdediging ervaart wordt helaas voor hen niet opgelost door de Hoge Raad. De situatie blijft bestaan waarbij er maar beperkt wordt ingegaan op onderzoekswensen ter toetsing van de betrouwbaarheid van het bewijsmateriaal, omdat deze (indirect) ook betrek-

37. R.o. 7.7.4.

38. R.o. 7.7.4.

39. Zie bijvoorbeeld Rb. Amsterdam 21 november 2022, ECLI:NL:RBAMS:2022:6800, r.o. 5.1.8; Rb. Oost-Brabant 23 maart 2023, ECLI:NL:RBOBR:2023:1853; Rb. Rotterdam 17 mei 2023, ECLI:NL:RBROT:2023:4136; en Rb. Limburg 16 augustus 2023, ECLI:NL:RBLIM:2023:4811.

40. Ch. van der Meer & M. Willebrands, 'Duizenden foto's sneller doorzoeken dankzij slim algoritme', *Magazines Forensisch Instituut* 27 januari 2021. Nieuwsbericht forensischinstituut.nl, 'NFI leert computers om berichten met doodsbedreiging uit grote hoeveelheden data te filteren', 5 mei 2021. Zie ook Hansken.nl en de video 'demo Hansken' van 16 februari 2023.

41. Voor een begin van die bespreking wijzen wij op het werk van R.M. te Molder, 'Digitaal forensische zoekmachines, effectieve verdedigingsrechten en de modernisering van het Wetboek van Strafvordering: is aanpassing van het conceptwetsvoorstel gewenst?', *Boom Strafblad* 2022/5.3; R. Stoykova, 'The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations', *Computer Law & Security Review* 2023, *49*, p. 1-26; en R. Stoykova, 'Encrochat: The hacker with a warrant and fair trials?', *Forensic Science International: Digital Investigation*, vol. 46, p. 1-14.

42. Zie ook het eerdergenoemde nieuwsbericht van het NFI van 5 mei 2021: '*Het model geeft nooit 100 procent garantie dat het klopt. De computer helpt de mens bij het zoeken. Een algoritme kan dingen missen, zogenoemde 'blind spots'. Het is belangrijk dat de gebruikers van het model zich daarvan bewust zijn'*.

43. B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3, afl. 1, p. 21.

44. Zie bijvoorbeeld Rb. Limburg 16 augustus 2023, ECLI:NL:RBLIM:2023:4811; Rb. Den Haag 15 augustus 2023, ECLI:NL:RBLIM:2023:4811; Rb. Amsterdam 28 juli 2023, ECLI:NL:RBAMS:2023:4919 en Hof Amsterdam 27 januari 2023, ECLI:NL:GHAMS:2023:777.

45. HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 6.25.

46. Zie B.W. Schermer & M. Galič, 'Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?', *NTS* 2022, afl. 3, p. 167-177, Galič 2022, Schermer 2022, Hirsch Ballin & Oerlemans 2023 en te Molder e.a. 2023.

47. T.N.B.M. Spronken, 'De eerste prejudiciele vragen in strafzaken gaan over EncroChat', *NJB* 2023/1.

48. Zie S.G.A.M. Adams, 'Vertrouwen is goed, maar controle is beter', *DD* 2021/74, p. 959-981, J.C. van der Pijll, 'Niet tornen aan het vertrouwensbeginsel!', *DD* 2022/22 (reactie), Schermer & Oerlemans 2022, p. 84-85, L.W. Verbeek & T. Beekhuis, 'Executieve jurisdictie: het (grote) obstakel in grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders?', *TBS&H* 2022, afl. 2, p. 106-118. Anders: Z.L. Moezel, 'Het vertrouwensbeginsel: een heet hangijzer', *TBS&H* 2023, afl., 3, p. 127-131.

49. Zie bijvoorbeeld uitspraak Rb. Gelderland 20 december 2022, ECLI:NL:RBGEL:2022:7105 en Hof Den Haag 5 januari 2022, ECLI:NL:GHDHA:2023:6.

king hebben op de toetsing van de rechtmatigheid van het Franse onderzoek waar het interstatelijke vertrouwensbeginsel aan in de weg staat. De verweren zijn daarmee lastig te onderbouwen. Wij vragen ons af of de bal hier niet te veel bij de verdediging wordt gelegd en pleiten voor een meer proactieve informatieverstrekking over de verzameling van gegevens in dit soort operaties in de toekomst. Positief op het gebied van de *equality of arms* is wel dat de politie, het NFI en het OM stappen hebben gezet met betrekking tot het verlenen van inzage in de EncroChat- en SkyECC-dataset. Het is nu zelfs mogelijk dat advocaten op afstand vanaf hun werkplek de gegevens kunnen analyseren met dezelfde technische mogelijkheden als rechercheurs.[50]

Wij wijzen er in het artikel op dat het interstatelijke vertrouwensbeginsel alleen betrekking heeft op de verzamelfase van de gegevens. De analyse van de gegevens in Nederland, waarbij gebruik wordt gemaakt van algoritmen en AI, staat volledig open ter toetsing aan het recht op een eerlijk proces. Als daartoe aanleiding is, moet de verdediging uitleg krijgen hoe het resultaat van die verdere gegevenswerking – het bewijs – tot stand is gekomen en daar verweer op kunnen voeren. Onzes inziens ligt op dit punt nog ruimte voor verweren en jurisprudentievorming.

De aanvullende machtiging van de rechter-commissaris acht de Hoge Raad mogelijk en zelfs wenselijk. Het vormt een extra toets op proportionaliteit en de rechter-commissaris heeft de mogelijkheid extra voorwaarden te stellen. Of deze voorwaarden daadwerkelijk zijn en worden nageleefd blijft onduidelijk. In de jurisprudentie zien wij vooralsnog geen aanwijzingen dat de voorwaarden niet zijn nageleefd en de Autoriteit Persoonsgegevens heeft (nog) geen onderzoek gedaan naar het gebruik van de bulkgegevens. Hoe het ook zij, onafhankelijk en effectief toezicht bij dit soort politieoperaties blijft een punt van aandacht. •

50. Nieuwsbericht, 'Digitaal bewijsmateriaal via Hansken nu raadpleegbaar voor advocaten vanaf werkplek', *OM.nl*, 20 maart 2023.