

NJFS 2021/305

## Tussenbeslissing met betrekking tot encrochat-gegevens.

Rb. Midden-Nederland 17-06-2021, ECLI:NL:RBMNE:2021:2570

Instantie	Rechtbank Midden-Nederland
Datum	17 juni 2021
Magistraten	Mrs. J.A. Spee, J.G. van Ommeren, P.M. Leijten
Zaaknummer	16/169895-20 16/169860-20 16/169884-20 16/169879-20 16/194307-20 16/194315-20 16/169888-20 16/194332-20 16/169890-20 16/169881-20 16/169877-20 16/169678-20 16/169429-20 16/303624-20
Vakgebied(en)	Strafprocesrecht / Voorfase
Brondocumenten	ECLI:NL:RBMNE:2021:2570, Uitspraak, Rechtbank Midden-Nederland, 17-06-2021
Wetgeving	Art. 126uba, 328, 359a Sv

### Essentie

Onderzoekswensen. Gelet op het vertrouwensbeginsel wordt er vanuit gegaan dat het verkrijgen van de Encrochat-data en het verstrekken daarvan door de Franse autoriteiten aan de Nederlandse autoriteiten niet onrechtmatig is geweest. Niet kan worden volgehouden dat het onderzoek Lemont, waarbinnen die data zijn verkregen, uitsluitend ziet op het bedrijf Encrochat zelf en daarom wordt er vanuit gegaan dat dit onderzoek ook tot doel had het opsporen van strafbare feiten van de gebruikers in gekoppelde onderzoeken. Het vermoeden bestaat dat de rechter-commissaris de privacybelangen van de Encrochat gebruikers heeft afgewogen tegen de relevante opsporingsbelangen en daarbij aan de vereisten van subsidiariteit en proportionaliteit heeft getoetst. Zowel de verdediging als de rechtbank beschikt slechts over het dictum van de 126uba-machtiging en niet over de inhoudelijke afwegingen van de rechter-commissaris om tot verlening van de machtiging over te gaan. De rechtbank wil op dit punt nader worden geïnformeerd. Indien het niet mogelijk is om de machtiging aan het dossier toe te voegen, dient de verdediging en de rechtbank op zijn minst te beschikken over een proces-verbaal van de rechter-commissaris met daarin zijn inhoudelijke afwegingen om tot verlening van de machtiging over te gaan en de achtergrond van het stellen van de voorwaarden voor het gebruik van de dataset Lemont voor andere strafrechtelijke onderzoeken. Dit proces-verbaal moet zien op de verwerking van de data in andere onderzoeken in Nederland en de overwegingen die aan die toestemming ten grondslag hebben gelegen.

### Partij(en)

*Beslissingen* van de rechtbank op de onderzoekswensen inzake 03Appel20, zoals ingediend voorafgaand aan en tijdens de regiezittingen van 1 en 3 juni 2021, in de zaken van de verdachten:

(16/169895-20)

[Verdachte 1], bijgestaan door mr. C.W. Flokstra,

(16/169860-20)

[Verdachte 2], bijgestaan door mr. M.M.J. Nuijten,

(16/169884-20)

[Verdachte 3], bijgestaan door mr. L. van Poucke,

(16/169879-20)

[Verdachte 4], bijgestaan door mr. D.M. Penn,

(16/194307-20)

[Verdachte 5], bijgestaan door mr. S.R. Bordewijk,

(16/194315-20)

[Verdachte 6], bijgestaan door mr. F.A.G.M. Landerloo,

(16/169888-20)

[Verdachte 7], bijgestaan door mr. O. Saki,

(16/194332-20)

[Verdachte 8], bijgestaan door mr. G.J.M. Kruizinga,

(16/169890-20)

[Verdachte 9], bijgestaan door mr. B.H.J. van Rhijn,

(16/169881-20)

[Verdachte 10], bijgestaan door mr. H. Raza,

(16/169877-20)

[Verdachte 11], bijgestaan door mr. R. van Veen,

(16/169678-20)

[Verdachte 12], bijgestaan door mr. M. Hoevers,

(16/169429-20)

[Verdachte 13], bijgestaan door mr. S.R. Bordewijk,

(16/303624-20)

[Verdachte 14], bijgestaan door mr. M.J. Lamers.

### 1. Inleiding

#### 1.1. Wat is [bedrijfsnaam 1]?

In het dossier (p. 2743 en 2744) beschrijft de politie de werking van [bedrijfsnaam 1] telefoons als volgt:

[bedrijfsnaam 1] was een communicatieaanbieder van telefoons, waarmee middels de [bedrijfsnaam 1] applicatie versleutelde chats, bestaande uit tekstberichten en afbeeldingen, konden worden verzonden en ontvangen en waarmee onderling gebeld kon worden. Ook was het mogelijk om notities te bewaren op de telefoontoestellen. De gebruiker had niet de mogelijkheid om zelf applicaties te installeren op het toestel en was dus beperkt in het gebruik van de communicatie applicaties die er door de leveranciers op gezet werden. Gebruikers kochten een telefoontoestel waarop de [bedrijfsnaam 1] applicaties vooraf geïnstalleerd waren in combinatie met een abonnement om de service te kunnen gebruiken. De duur van het abonnement was vaak 1, 3 of 6 maanden en kon verlengd worden.

Een [bedrijfsnaam 1] telefoon werd geleverd met een simkaart waarmee alleen dataverkeer verzonden en ontvangen kon worden. Deze simkaart had een wereldwijde dekking.

De inhoud van een [bedrijfsnaam 1] telefoon kon door de gebruiker volledig worden gewist. Dit werd ook wel 'panic-wipe' genoemd.

Door [bedrijfsnaam 1] zijn diverse typen telefoontoestellen geleverd voor het gebruik van de [bedrijfsnaam 1] applicatie. In de periode dat er data van de telefoons is verkregen, in de maanden april, mei en juni 2020, betroffen dit de typen BQ Aquaris X2 en de BQ Aquaris X3/Carbon.

Middels de [bedrijfsnaam 1] applicatie konden de [bedrijfsnaam 1] gebruikers alleen onderling en één-op-één communicatie voeren. Er konden dus geen groepsgesprekken worden gevoerd. Deze communicatie kon tot stand komen nadat een gebruiker zijn 'username' stuurde naar een andere gebruiker, met het verzoek om toegevoegd te worden aan diens contactenlijst. Gebruikers konden elkaars username opslaan in hun contactenlijst onder een zelfgekozen omschrijving ('nickname'). Er kon dus slechts gecommuniceerd worden met contacten in de contactenlijst en niet met elke [bedrijfsnaam 1] gebruiker waarvan de [bedrijfsnaam 1] gebruikersnaam bekend was.

Een chat kon bestaan uit tekstberichten en foto's. Ieder bericht verliep na een vooraf ingestelde tijd, ook wel burn-time of beveiligde verwijdertijd genoemd. Deze tijd was door de gebruiker aan te passen, standaard stond hij ingesteld op zeven dagen.

Tevens kon er vanuit de chat een 'VoIP' spraakgesprek gevoerd worden.

De kosten voor een [bedrijfsnaam 1] telefoon bedroegen ongeveer € 1.500,- voor een abonnement van zes maanden.

#### 1.2. Wat houdt de [bedrijfsnaam 1] hack in?

Al vanaf 2017 vinden er in onder meer Frankrijk en Nederland onderzoeken plaats naar [bedrijfsnaam 1]. Telefoons van [bedrijfsnaam 1] zijn in meerdere strafrechtelijke onderzoeken aangetroffen en in beslag genomen bij personen die van ernstige strafbare feiten werden verdacht. De indruk ontstond bij de politie dat deze telefoons vrijwel uitsluitend in het (georganiseerde) criminele circuit werden gebruikt. De gebruikers van deze [bedrijfsnaam 1] telefoons waren onbekend. De onmogelijkheid om de telefoons te herleiden tot de persoon die de telefoon gebruikte, zou maken dat deze dienst populair was binnen de georganiseerde

criminaliteit. De mogelijkheden van 'burn time' en 'panic wipe' maakte dat ook op het moment dat een dergelijke telefoon in beslag was genomen én forensisch kon worden ontsleuteld er zeer beperkt berichtenverkeer kon worden uitgelezen.

Uit in het dossier gevoegde stukken en met name uit door de verdediging vanuit Engeland in het geding gebrachte stukken, volgt dat er in de eerste maanden van 2020 overleg is gevoerd door politie en justitie uit verschillende landen met als doel te komen tot een gecoördineerde aanpak bij de vervolging van [bedrijfsnaam 1].

De server van [bedrijfsnaam 1] bleek te zijn gevestigd in [plaatsnaam 1], Frankrijk, bij het bedrijf [bedrijfsnaam 2]. Bij het verzenden van een [bedrijfsnaam 1] bericht van het ene naar het andere toestel, verloopt de communicatie via deze server. De communicatie is versleuteld (encrypted). Deze versleutelde communicatie bleek niet of nauwelijks inzichtelijk te zijn voor opsporingsdiensten.

Uit het dossier (p. 2737 en 2738) volgt dat de Franse Gendarmerie op 1 april 2020 vanuit [plaatsnaam 2], Frankrijk, rond 17:15 uur een door een Franse technische politiedienst ontwikkeld opnamemiddel heeft geïnstalleerd. Het doel van dit middel is geweest het vastleggen van de inkomende en uitgaande communicatie middels de [bedrijfsnaam 1] telefoontoestellen.

Door de verdediging, meer specifiek mr. Landerloo, zijn documenten in het geding gebracht uit Engelse procedures. In een "Warrant Application" die ziet op "Targeted Equipment Interference" van de National Crime Agency, staat onder meer - in het Engels - het volgende:

De [bedrijfsnaam 1] servers staan in Frankrijk. De NCA heeft daarom vanaf 2018 samengewerkt met de Franse Gendarmerie. De samenwerking had tot doel het gebruikmaken van kwetsbaarheden in de servers om zo gegevens te verzamelen.

De Franse Gendarmerie heeft in januari 2020 te kennen gegeven aan de NCA dat zij [bedrijfsnaam 1] konden hacken.

In een "Schedule of Conduct" staat vermeld dat in de eerste fase (stage 1) een 'implant' (oftewel een hacktool, toevoeging rechtbank) zal worden ingezet op alle [bedrijfsnaam 1] toestellen wereldwijd. Dit middel zal op de toestellen worden gezet via een update vanaf de server in Frankrijk. Dit middel zal de op de toestellen vastgelegde data verzamelen en deze verzenden naar de Franse autoriteiten. Het gaat dan om alle data, waaronder IMEI-gegevens, gebruikersnamen, wachtwoorden, opgeslagen chatberichten, afbeeldingen, locatiegegevens ('geodata') en notities.

Gedurende de tweede fase (stage 2) zal communicatie, zoals chatberichten, opgeslagen op de [bedrijfsnaam 1] toestellen, worden verzameld. Deze berichten worden verzameld, zodra deze in het toestel worden opgeslagen. De geplande duur van de interceptie is naar verwachting twee maanden.

De vanuit Engeland verkregen informatie sluit aan bij de informatie die de Nederlandse politie in het dossier heeft opgenomen. Op pagina 2753 verantwoordt de politie het veiligstellen van de dataset Lemont. In dit proces-verbaal staat onder meer:

"Het Franse onderzoeksteam heeft uitgaande en inkomende communicatie verzameld van [bedrijfsnaam 1] telefoontoestellen. (...) Ik verwijs naar de door het Franse onderzoeksteam verzamelde data afkomstig van [bedrijfsnaam 1]-telefoontoestellen met de [bedrijfsnaam 1]-telefoondata.

Het Franse onderzoeksteam verzamelde de [bedrijfsnaam 1]-telefoondata gedurende de periode van 1 april 2020 17.15 uur tot 20 juni 2020 omstreeks 17.20. Het Franse politieteam sloeg deze data gedurende deze periode op op computersystemen in Frankrijk. Het Franse onderzoeksteam heeft de Nederlandse politie toegang gegevens tot de [bedrijfsnaam 1]-telefoondata over een beveiligde verbinding met die computersystemen in Frankrijk.

(..) Ik kopieerde de [bedrijfsnaam 1]-telefoondata gedurende deze periode naar het onderzoeksnetwerk van de Nederlandse politie. Om een zo actueel mogelijke kopie van de [bedrijfsnaam 1]-telefoondata van de Franse computersystemen te krijgen, gebruikte ik een wijze van kopiëren, waarbij, gedurende deze periode, met een

zo klein mogelijke vertraging de nieuwe [bedrijfsnaam 1]-telefoondata werd gekopieerd naar het onderzoeksnetwerk van de Nederlandse politie.”

De aldus verkregen data vanuit Frankrijk, veelal bestaand uit [bedrijfsnaam 1] berichten, is de dataset die de politie in Nederland heeft verkregen binnen het onderzoek 26Lemont (hierna: onderzoek Lemont), het strafrechtelijke onderzoek naar de medeplichtigheid van [bedrijfsnaam 1] zelf aan door gebruikers van [bedrijfsnaam 1] gepleegde misdrijven.

### 1.3. Start onderzoek Appel

Uit het proces-verbaal ‘Kaders gebruik dataset 26Lemont’ volgt dat voorafgaand aan de interceptie reeds bekend was dat in Nederland binnen de georganiseerde criminaliteit op grote schaal gebruik werd gemaakt van cryptotelefoons van deze aanbieder. Er waren ook al vele cryptotelefoons van deze aanbieder in beslag genomen bij personen die van ernstige strafbare feiten werden verdacht. Vanwege de voorzienbare inbreuk die de interceptie van de [bedrijfsnaam 1] data op de persoonlijke levenssfeer van de Nederlandse gebruikers van deze dienst zou hebben, heeft het Openbaar Ministerie ervoor gekozen om - mogelijk ten overvloede - in Nederland een rechterlijke toetsing te vorderen.

De rechter-commissaris, mr. Schols, is gevorderd om een machtiging te geven teneinde de informatie betreffende de Nederlandse gebruikers te mogen analyseren en gebruiken (vgl. proces-verbaal ‘Kaders gebruik dataset 26Lemont, p. 2700). Aan de rechter-commissaris is een lijst verstrekt van opsporingsonderzoeken waarin georganiseerde verbanden, gebruikmakend van toestellen van deze aanbieder, nader werden omschreven.

Ter zitting hebben de officieren van justitie verduidelijkt dat één van die onderzoeken die aan de rechter-commissaris zijn voorgelegd het onderzoek Primero betrof. In dit onderzoek was onder een verdachte - van georganiseerde harddrugshandel te Utrecht - een [bedrijfsnaam 1] telefoon aangetroffen. Deze verdachte en zijn vijf in Utrecht gelokaliseerde tegencontacten zijn onderdeel gaan uitmaken van het onderzoek Fruit. De berichten van deze zes gebruikers zijn na instemming van de rechter-commissaris op 27 april 2020 (p. 2761) vanuit de dataset Lemont aan het onderzoeksteam Fruit ter beschikking gesteld. Eén van die gebruikers betrof verdachte [verdachte 9]. De berichten die door het aan [verdachte 9] toegeschreven account werden verzonden en ontvangen houden - zo leidt de rechtbank af uit het dossier - onder meer in berichten over afvalverwerking van twee productielocaties van synthetische drugs. Het onderzoek hiernaar is onderzoek 09APPEL (hierna: Appel), een onderzoek waarbij met instemming van de rechter-commissaris op 29 mei 2020 gebruik is gemaakt van de dataset van het onderzoek Lemont. Na de instemming van de rechter-commissaris is middels toestemming ex artikel 126dd van het Wetboek van Strafvordering (hierna: Sv) op 29 mei 2020 door de officieren van justitie van Lemont informatie uit dat onderzoek gedeeld met de officier van justitie in Appel (p. 2706).

Aldus blijkt dat de verdenking in het onderzoek Appel tegen de verdachten is voortgekomen op basis van ‘tegencontact-onderzoek’. Deze verdenking is - zoals door een aantal raadslieden werd verondersteld - niet ontstaan op basis van zoektermen binnen de dataset Lemont. Wat voorts voor verwarring heeft geleid, is dat bij de persconferentie van 2 juli 2020 is benoemd dat politie en justitie “live” konden meekijken met de door [bedrijfsnaam 1] gebruikers uitgewisselde berichten. Dit is echter niet, althans niet van begin af aan, in het onderzoek Appel het geval geweest. Ook de veronderstelling bij een aantal raadslieden dat de afgevangen [bedrijfsnaam 1] data eerst ontsleuteld moest worden, voordat deze konden worden gelezen, blijkt op basis van het dossier alsmede de door de verdediging overgelegde stukken uit Engeland niet juist.

## 2. De onderzoekswensen

Gelet op hetgeen in de inleiding uiteen is gezet, wijst de rechtbank een aantal onderzoekswensen - gelet op de hiervoor beschreven feitelijke gang van zaken - af:

- het toevoegen van stukken die zien op vragen over de (betrouwbaarheid van de) versleuteling van de [bedrijfsnaam 1] berichten;
- een aanvullend proces-verbaal waarin zijn opgenomen de woordenlijsten/zoektermen op basis waarvan

in onderzoek Appel de datasets zijn samengesteld;

- een aanvullend proces-verbaal waarin wordt uitgelegd hoe onderzoek Appel is voortgekomen uit de dataset van Lemont;
- een aanvullend proces-verbaal over de werking van [bedrijfsnaam 1] en de wijze waarop de gegevens in onderzoek Appel zijn vergaard en de wijze waarop het uit bronmateriaal (26Lemont) de in het dossier Appel weergegeven [bedrijfsnaam 1] gesprekken zijn samengesteld.

#### **A. Verzoeken met betrekking tot de rechterlijke machtiging in Frankrijk en samenwerking met Frankrijk**

Door de verdediging is verzocht om het toevoegen van diverse stukken omtrent - kort gezegd - het verlenen van de machtiging van de Franse rechter voor de interceptie van de [bedrijfsnaam 1] data, dan wel het horen van diverse (Franse) getuigen die bij het proces rondom het verlenen van de machtiging betrokken zijn geweest. Zonder het verkrijgen van de Franse stukken en/of het doen horen van de (Franse) getuigen kan er geen onderbouwd verweer worden gevoerd dat het verlenen van de machtiging in Frankrijk onrechtmatig is geweest. De verdediging noemt in dit kader verder dat nu deze stukken niet inzichtelijk zijn, niet controleerbaar is of de machtiging voldoet aan de vereisten van artikel 8, tweede lid, van het EVRM. Daarnaast wordt verzocht om stukken die betrekking hebben op (de totstandkoming van) de JIT-overeenkomst en/of het horen van getuigen die betrokken waren bij de totstandkoming van deze overeenkomst alsook het horen van (Engelse) getuigen die aanwezig zijn geweest bij vergaderingen over het doel van deze samenwerking tussen Frankrijk en Nederland in het kader van het JIT.

De rechtbank stelt voorop dat zij uitgaat van de gang van zaken zoals die uiteen is gezet in de inleiding. Daarbij is in het kader van deze verzoeken relevant dat in Frankrijk de inzet van de interceptietool en de daarvoor benodigde aanvragen en toetsing heeft plaatsgevonden. Daarbij heeft het Openbaar Ministerie vanaf het begin benadrukt, en laatstelijk in de brief van 24 maart 2021 bevestigd, dat sprake is geweest van een Frans strafrechtelijk opsporingsonderzoek naar het bedrijf [bedrijfsnaam 1]. Frankrijk heeft de aanvraag tot machtiging en inzet op basis van eigen feiten en omstandigheden onderbouwd, waarbij Nederland geen feiten en omstandigheden betreffende lopende Nederlandse strafrechtelijke onderzoeken heeft aangedragen om de aanvraag van de machtiging te onderbouwen.

Bij die stand van zaken, die vooralsnog op basis van de stukken die vanuit de Engelse procedure over [bedrijfsnaam 1] door de verdediging zijn overgelegd ook niet anders blijkt, is sprake van een opsporingsonderzoek dat onder verantwoordelijkheid van de Franse autoriteiten heeft plaatsgevonden. Gelet op het vertrouwensbeginsel zoals de Hoge Raad dat heeft uitgelegd in het arrest van 5 oktober 2010<sup>[1]</sup> staat niet ten toets van de Nederlandse strafrechter of in het recht van het desbetreffende land al dan niet een toereikende wettelijke grondslag bestond voor de door de buitenlandse autoriteiten verrichte onderzoekshandelingen. 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. De taak van de Nederlandse strafrechter is ertoe beperkt te waarborgen dat de wijze waarop van de resultaten van dit buitenlandse onderzoek in de strafzaak gebruik wordt gemaakt, geen inbreuk maakt op zijn recht op een eerlijk proces, als bedoeld in artikel 6, eerste lid, van het EVRM.

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.

Vanuit de verdediging is voorts aangevoerd dat geen sprake is van een onder Franse verantwoordelijkheid uitgevoerde opsporingsoperatie. Nu de Nederlandse autoriteiten wisten dat er in Nederland [bedrijfsnaam 1]

telefoons in omloop waren, wisten zij ook dat door de hackoperatie in Frankrijk de Nederlandse autoriteiten de beschikking zouden krijgen over de communicatie die vanuit [bedrijfsnaam 1] telefoons in Nederland werd gevoerd.

De rechtbank overweegt als volgt. Zoals in de inleiding beschreven, heeft de Franse hackoperatie tot gevolg gehad dat van alle [bedrijfsnaam 1] telefoontoestellen de opgeslagen data, waaronder “geodata” oftewel locatiegegevens, werden veiliggesteld. De verkregen data zijn op basis van deze locatiegegevens vervolgens gedeeld met het land van herkomst en daar verder geanalyseerd en verwerkt voor strafrechtelijke onderzoeken naar de gebruikers.

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 installatie 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.

Gezien de hoeveelheid [bedrijfsnaam 1] telefoons in omloop (ongeveer 55.000) en lopende onderzoeken was bekend dat deze zich ook in Nederland en Engeland bevonden. Uit de Engelse stukken is af te leiden dat de autoriteiten aldaar meenden dat naar Engels nationaal recht voor het afvangen van data van zich in Engeland bevindende telefoons een machtiging (“Warrant”) nodig was. De Nederlandse wetgeving kent een dergelijke verplichting niet.

Van een onder Nederlandse verantwoordelijkheid uitgevoerd onderzoek zou sprake zijn indien *op basis van rechtshulpverzoeken* uit Nederland de Gendarmerie in Frankrijk een hack uitvoert ter verkrijging van data van specifieke in Nederland geïdentificeerde toestellen. De rechtbank heeft geen reden te twifelen aan de mededeling vanuit het Openbaar Ministerie dat deze rechtshulpverzoeken, gelet op de aard van het onderzoek, er niet zijn geweest.

#### **Inbreuk artikel 6 EVRM**

Mede naar aanleiding van de uitspraken van andere rechtbanken die reeds over dit punt zijn verschenen, merkt de verdediging op dat een schending van artikel 8 EVRM bij het verlenen van de machtiging voor de interceptie relevant is voor de beoordeling of sprake is van schending van artikel 6 EVRM, dat volgens de jurisprudentie van de Hoge Raad over het internationaal vertrouwensbeginsel wél ter toetsing van de Nederlandse strafrechter voorligt. Bovendien volgt uit de jurisprudentie van het EHRM dat een beperking van het recht op kennisname van deze stukken in strijd is met het beginsel van *equality of arms* en het recht op een eerlijk proces zoals neergelegd in artikel 6 EVRM.

De rechtbank stelt voorop dat op basis van het vertrouwensbeginsel zoals hiervoor uiteen is gezet, uitgangspunt is dat de Nederlandse strafrechter er op moet vertrouwen dat de interceptie in Frankrijk op basis van een toereikende wettelijke grondslag en in overeenstemming met artikel 8 EVRM heeft plaatsgevonden.

Het beginsel van *equality of arms* brengt met zich dat de verdediging toegang moet krijgen tot het bewijs (in deze zaak: de [bedrijfsnaam 1] data van het aan de verdachten toegeschreven accounts) en in beginsel ook tot stukken die kunnen zien op onrechtmatigheden in het onderzoek. Dat er vanwege het beginsel van *equality of arms*, een recht op kennisname door de verdediging van deze stukken zou bestaan, zou echter betekenen dat de Nederlandse strafrechter alsnog via een omweg van artikel 6 EVRM de rechtmatigheid van het Franse strafrechtelijke optreden zou (kunnen/moeten) toetsen. Dit is naar het oordeel van de rechtbank in strijd met de bedoeling van het internationale vertrouwensbeginsel. Aldus ziet zij eveneens op basis van deze beginselen geen grond voor toewijzing van de verzoeken van de verdediging.

Gelet hierop wijst de rechtbank de verzoeken ter inzage en/of voeging van de volgende stukken af en/of het horen van de volgende getuigen af:

- de JIT-overeenkomst tussen Frankrijk en Nederland met betrekking tot het onderzoek naar het bedrijf

[bedrijfsnaam 1] en de aan het JIT ten grondslag liggende documenten, waaronder alle gespreksverslagen en notities;

- alle processen-verbaal aangaande informatie die vóór de vorming van het JIT door de Franse autoriteiten is verzameld en later is gevoegd in het JIT;
- alle documenten waaruit blijkt dat beide JIT-partners bij het verzamelen van informatie over de gebruikers van [bedrijfsnaam 1] hebben gehandeld op basis van de geldende rechtsregels van het desbetreffende land;
- de rechtshulpverzoeken die sinds 2019 zijn gedaan met betrekking tot [bedrijfsnaam 1];
- persberichten inzake het onderzoek naar [bedrijfsnaam 1];
- verslagen van overlegstructuren binnen politie en justitie die hebben geleid tot gebruik/delen van [bedrijfsnaam 1] data;
- het laten opmaken van aanvullende processen-verbaal die betrekking hebben op de gang van zaken van het [bedrijfsnaam 1] onderzoek;
- het horen van de getuige [getuige 12];
- het horen van de getuige [getuige 13];
- het horen van de officieren van justitie van het Landelijk Parket [aanduiding 1], [aanduiding 2] en [aanduiding 3];
- het horen van alle Franse opsporingsambtenaren;
- het horen van alle Engelse medewerkers van de National Crime Agency;
- het horen van de getuigen [getuige 14], [getuige 15], [getuige 16], [getuige 17], [getuige 18];
- het horen van Engelse officieren van justitie;
- het toevoegen van alle processen-verbaal, bevelen, machtigingen en vorderingen die in Frankrijk voor de inzet van de interceptietool zijn ingediend/verleend (in een Nederlandse vertaling);
- het toevoegen van alle officiële overheidsstukken uit het Verenigd Koninkrijk en Frankrijk die aldaar in de lopende procedures door de vervolgende instantie wordt ingebracht in het kader van [bedrijfsnaam 1];
- het horen van Franse onderzoeksrechters;
- het horen van getuigen bij project [naam project] betrokken medewerkers van het NFI;
- het horen van alle verantwoordelijken die betrokken waren bij de uitvoering van de Franse operatie ter verkrijging van de berichten, waaronder ook uitdrukkelijk worden verstaan de betrokken medewerkers van [.....] die de interceptietool zouden hebben ontwikkeld.

#### **Verzoeken met betrekking tot machtiging 26Lemont**

#### **Verzoeken met betrekking tot onderzoek Lemont**

De verdediging heeft aangevoerd dat mogelijke vormverzuimen in het voorbereidend onderzoek van Lemont



vallen binnen het toetsingsbereik van artikel 359a Sv, gelet op de recente jurisprudentie van de Hoge Raad over het toepassingsbereik van artikel 359a Sv. De verdediging moet om die reden kunnen beschikken over een aantal stukken uit onderzoek Lemont, om op die manier te toetsen of het onderzoek naar de verdachten in Appel - dat voortkomt uit de data van Lemont - een rechtmatige aanvang heeft gehad en mogelijk een 359a-verweer te kunnen voeren.

De officier van justitie stelt dat deze verzoeken geen informatie kunnen opleveren die relevant zijn voor de beantwoording van de vragen van de artikelen 348 en 350 Sv. Allereerst is de gevraagde machtiging aan de Nederlandse rechter-commissaris - gelet op de verkregen toestemming van de Franse rechter - ten overvloede geweest. Daarnaast kunnen eventuele onrechtmatigheden in het onderzoek Lemont niet leiden tot onrechtmatigheden in de zin van 359a Sv (in het voorbereidend onderzoek) jegens de verdachten in onderzoek Appel (Schutznorm). Daarbij wordt benadrukt dat Lemont een ander voorbereidend onderzoek betreft dan de strafrechtelijke onderzoeken naar de specifieke gebruikers van de telefoons en de strafbare feiten waaraan die verdachten zich mogelijk schuldig maken. Verwezen wordt naar de recente beslissingen van andere rechtbanken op dit punt. Tot slot heeft de officier van justitie een praktisch bezwaar aangevoerd tegen het verstrekken van de gevraagde stukken uit onderzoek Lemont: in deze stukken is gevoelige informatie weergegeven over andere (lopende) opsporingsonderzoeken en over de werking van de (als staatsgeheim aangemerkte) Franse hacktool.

### **Vertrouwensbeginsel: verkrijgen, verstrekken en verwerken van [bedrijfsnaam 1] data**

Gelet op hetgeen hiervoor is overwogen, is naar het oordeel van de rechtbank thans onvoldoende onderbouwd waarom ten aanzien van het *verkrijgen* van de [bedrijfsnaam 1] data door de Franse autoriteiten en het *verstrekken* van die data aan de Nederlandse autoriteiten aan het vertrouwensbeginsel voorbij moet worden gegaan.

Dat de toetsing van de rechter-commissaris eveneens ten aanzien van het vervolgens *verwerken* van die gegevens ten behoeve van Nederlandse strafrechtelijke onderzoeken naar de individuele gebruikers van [bedrijfsnaam 1] als een toets 'ten overvloede' moet worden gezien, en daarmee niet relevant kan zijn voor de beantwoording van de vragen van 348 en 350 volgt de rechtbank vooralsnog niet. Mede gelet op de door de verdediging aangehaalde verdragsrechtelijke verplichtingen bij het verwerken van persoonsgegevens, kan de rechtbank niet op voorhand uitsluiten dat de machtiging van de rechter-commissaris niet relevant kan zijn voor de inhoudelijke beoordeling van de strafzaak. Daar komt bij dat - zoals het Openbaar Ministerie ook onderkent - duidelijk was dat met de fase van het analyseren van de data bewijs voor strafrechtelijke onderzoeken van individuele gebruikers van [bedrijfsnaam 1] zou worden verkregen en een inbreuk zou plaatsvinden op de persoonlijke levenssfeer van de individuele [bedrijfsnaam 1] gebruiker. De toets die door de rechter-commissaris heeft plaatsgevonden en waarbij voorwaarden zijn gesteld aan het *gebruik* van de dataset Lemont voor andere strafrechtelijke onderzoeken kan daarmee in het kader van de door de verdediging benoemde verweren bij de inhoudelijke behandeling van de strafzaak relevant zijn.

### **Schutznorm**

De rechtbank stelt vast dat uit jurisprudentie van de Hoge Raad (ECLI:NL:HR:2020:1889) volgt dat onder omstandigheden een rechtsgevolg kan worden verbonden aan een vormverzuim door een ambtenaar die met opsporing en vervolging is belast, maar dat niet is begaan bij het voorbereidend onderzoek tegen de verdachte. In de rechtspraak ligt als algemene overkoepelende maatstaf besloten dat een rechtsgevolg op zijn plaats kan zijn indien het betreffende vormverzuim of de betreffende onrechtmatige handeling van bepalende invloed is geweest op het verloop van het opsporingsonderzoek naar en/of de (verdere) vervolging van verdachte ter zake van het tenlastegelegde feit.

De rechtbank is met de verdediging van oordeel dat de verkregen [bedrijfsnaam 1] data uit onderzoek Lemont van bepalende invloed lijkt te zijn geweest op het opsporingsonderzoek naar en de vervolging van alle verdachten in het onderzoek Appel. Immers, het laat zich moeilijk inzien hoe *zonder* de inhoud van de [bedrijfsnaam 1] data verkregen binnen het onderzoek Lemont er een concrete verdenking van het criminele samenwerkingsverband in het onderzoek Fruit en vervolgens Appel kon worden geformuleerd. De [bedrijfsnaam 1] data uit Lemont lijkt daarmee van bepalende invloed te zijn geweest op het ontstaan van de

verdenking jegens de verdachten in onderzoek Appel. Dat de data in Lemont is verkregen in een *ander* strafrechtelijk onderzoek, namelijk een onderzoek gericht - kort gezegd - tegen het bedrijf [bedrijfsnaam 1] zelf en niet de gebruikers ervan, vindt de rechtbank een moeizaam te volgen redenering. Immers, door het Openbaar Ministerie werd een lijst met concrete opsporingsonderzoeken overgelegd aan de rechter-commissaris waarin een [bedrijfsnaam 1] telefoon werd gevonden. De chatberichten uit de telefoons van die gebruikers (en ook de tegencontacten) mochten op basis van deze toestemming worden geanalyseerd. Die analyse is noodzakelijk om überhaupt tot vervolging van [bedrijfsnaam 1] over te kunnen gaan. Daarmee kan niet worden volgehouden dat het onderzoek Lemont uitsluitend ziet op [bedrijfsnaam 1] zelf en gaat de rechtbank ervan uit dat dit onderzoek ook tot doel had het opsporen van strafbare feiten van de gebruikers in gekoppelde onderzoeken.

Het feit dat de rechter-commissaris diverse voorwaarden heeft gesteld aan het gebruik van de dataset Lemont voor andere opsporingsonderzoeken doet vermoeden dat hij de privacybelangen van de [bedrijfsnaam 1] gebruikers heeft afgewogen tegen de relevante opsporingsbelangen en daarbij aan de vereisten van subsidiariteit en proportionaliteit heeft getoetst. Zowel de verdediging als de rechtbank beschikt echter slechts over het dictum van de 126uba-machtiging en niet over de inhoudelijke afwegingen van de rechter-commissaris om tot verlening van de machtiging over te gaan. De rechtbank wil op dit punt nader worden geïnformeerd. De rechtbank ziet echter ook het door het Openbaar Ministerie genoemde bezwaar tegen openbaarmaking van de 126uba-machtiging. Zoals het Openbaar Ministerie heeft toegelicht, spelen naast onderzoeksbelangen ook geheimhoudingsverplichtingen. Indien het - gelet op deze belangen - niet mogelijk is om (een gedeelte van) de machtiging aan het dossier toe te voegen, dient de verdediging en de rechtbank op zijn minst te beschikken over een proces-verbaal van de rechter-commissaris J.J.J. Schols met daarin zijn inhoudelijke afwegingen (o.a. over proportionaliteit en subsidiariteit) om tot verlening van de 126uba-machtiging (a t/m d) over te gaan en de achtergrond van het stellen van de voorwaarden voor het gebruik van de dataset Lemont voor andere strafrechtelijke onderzoeken. Gelet op de overwegingen hiervoor over het vertrouwensbeginsel in relatie tot het verkrijgen van de data in Frankrijk en het verstrekken van die data aan Nederland, zal dit proces-verbaal moeten zien op de *verwerking* van de data (dataset Lemont) in andere onderzoeken in Nederland en de overwegingen die aan die toestemming - onder voorwaarden - ten grondslag hebben gelegen.

De rechtbank draagt het Openbaar Ministerie op om de machtiging van 27 maart 2020 in het onderzoek Lemont dan wel een proces-verbaal van de rechter-commissaris aan het dossier Appel toe te voegen.

De rechtbank verwacht met deze informatie voldoende geïnformeerd en in staat te zijn verweren over de rechtmatigheid van het opsporingsonderzoek naar de verdachten in onderzoek Appel te kunnen beoordelen. De rechtbank wijst daarom vooralsnog af de verzoeken tot:

- het toevoegen van alle vorderingen, afwijzingen en aan de machtigingen/bevelen ex artikel 126uba ten grondslag liggende processen-verbaal welke in het kader van onderzoek Lemont of daaruit voortvloeiende onderzoeken voorhanden zijn bij het Openbaar Ministerie;
- het laten opmaken van nadere processen-verbaal met betrekking tot de wijze waarop informatie is vergaard over de [bedrijfsnaam 1] accounts die aan de betreffende verdachten worden toegedicht;
- een aanvullend proces-verbaal van de officieren van 26Lemont waarin wordt ingegaan op de nog te stellen vragen van de verdediging;
- het horen van verbalisant [aanduiding 4] en de officieren van het LP betrokken bij 26Lemont.

### **Overige verzoeken over onderzoek Lemont**

Diverse raadslieden hebben gevraagd om toevoeging van 'stukken uit onderzoek Lemont' en/of inzage in de (dataset van en/of het procesdossier van) onderzoek Lemont.

De rechtbank overweegt dat de dataset Lemont bestaat uit berichten van duizenden [bedrijfsnaam 1] gebruikers. Niet valt in te zien waarom toevoeging van andere stukken uit onderzoek Lemont kunnen bijdragen aan de beantwoording van de vragen van artikel 348 en 350 Sv in onderzoek Appel. Iedere verdachte heeft

immers toegang tot de data die beschikbaar is met betrekking tot het [bedrijfsnaam 1] account dat aan de betreffende verdachte wordt toegeschreven. Deze verzoeken zijn dan ook onvoldoende onderbouwd. De rechtbank wijst deze verzoeken dus af.

De raadsman mr. Raza heeft verder gevraagd om informatie te laten toevoegen over de wijze waarop gebruik gemaakt is van geheimhouderscommunicatie. De rechtbank wijst ook dit verzoek af. Het Openbaar Ministerie heeft immers geantwoord dat in onderzoek Appel geen geheimhouderscommunicatie is verwerkt en de rechtbank ziet geen aanleiding om anders te vermoeden. Ook ziet de rechtbank niet in hoe deze informatie kan bijdragen bij de beantwoording van de vragen van artikel 348 en 350 Sv in de zaak tegen verdachte [verdachte 10].

### **Prejudiciële vragen**

#### **[verdachte 10], [verdachte 3], [verdachte 12] en [verdachte 4]**

De verdediging heeft aangevoerd dat het verkrijgen, bewaren en gebruiken van alle [bedrijfsnaam 1] data in dit onderzoek valt binnen de werkingssfeer van het unierecht, in het bijzonder worden genoemd Richtlijn 2002/58<sup>[2.]</sup> en Richtlijn 2016/680. Daarom moeten deze activiteiten worden getoetst aan de bepalingen van de richtlijnen in het licht van de rechten zoals opgenomen in het Handvest. Gelet hierop is het noodzakelijk dat er prejudiciële vragen worden gesteld aan het Hof van Justitie van de Europese Unie (hierna: het Hof), omdat de beantwoording van de vragen van doorslaggevend belang is voor de beoordeling van de onderhavige strafzaak. Daarnaast is er in de Nederlandse jurisprudentie niet eerder inhoudelijk beslist over deze vragen en is er een zaak overstijgend belang, gelet op het feit dat er veel strafzaken bestaan die worden beheerst door [bedrijfsnaam 1] data.

De officier van justitie stelt zich primair op het standpunt dat de rechtbank zelf de door de verdediging geformuleerde vragen kan beantwoorden en het stellen van prejudiciële vragen aan het Hof niet noodzakelijk is. Daarnaast stelt de officier van justitie dat het verzoek tot het stellen van prejudiciële vragen op dit moment prematuur is, omdat de zaak bij de nationale rechter feitelijk en juridisch moet zijn besproken en uitgekristalliseerd moet zijn. Verder voert de officier van justitie aan dat Richtlijn 2002/58 niet van toepassing is op de interceptie van [bedrijfsnaam 1] data zoals dat in deze zaak heeft plaatsgevonden en dat Richtlijn 2016/680 reeds is geïmplementeerd in de nationale wetgeving en dat er geen aanleiding is om aan te nemen dat deze richtlijn onjuist of niet in overeenstemming met het Handvest is geïmplementeerd.

De rechtbank stelt voorop dat - zoals hiervoor is overwogen - zij ervan uitgaat dat de interceptie van de [bedrijfsnaam 1] gegevens heeft plaatsgevonden onder verantwoordelijkheid van de buitenlandse autoriteiten, namelijk die van Frankrijk. Het vertrouwensbeginsel brengt met zich dat de rechtbank ervan uitgaat dat de Franse interceptie heeft plaatsgevonden in overeenstemming met - voor zover het van toepassing is - het unierecht. Frankrijk is immers een lidstaat van de Europese Unie. Voor zover de verdediging betoogt dat bij de *verwerking* van de uit Frankrijk verkregen gegevens door de Nederlandse autoriteiten eveneens het unierecht van toepassing is, overweegt de rechtbank het volgende.

#### **Richtlijn 2002/58**

Artikel 1, derde lid, van de Richtlijn 2002/58 bepaalt dat de richtlijn niet van toepassing is op de activiteiten van de staat op strafrechtelijk gebied. Uit het arrest van het Hof van 6 oktober 2020 (*La Quadrature du net*)<sup>[3.]</sup> volgt dat er bij de uitleg van deze richtlijnbevestiging een onderscheid moet worden gemaakt naar de persoon die de gegevensverwerking uitvoerde. Het Hof legt uit dat

“elke verwerking van persoonsgegevens door aanbieders van elektronische communicatie binnen de werkingssfeer van de richtlijn valt, inclusief de verwerking die het gevolg is van door de overheid aan die aanbieders opgelegde verplichtingen.” <sup>[4.]</sup> Het Hof vervolgt in dat arrest “Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronische communicatiediensten, wordt de bescherming van de gegevens van de betrokken personen niet

beheerst door Richtlijn 2002/58, maar uitsluitend door nationaal recht, behoudens de toepassing van richtlijn 2016/680 (..), wat betekent dat de betrokken maatregelen met name in overeenstemming moeten zijn met het nationale constitutionele recht en met de vereisten van het EVRM.”

Nu bij de interceptie van de [bedrijfsnaam 1] data geenszins sprake is geweest van een verwerking van persoonsgegevens door een elektronische communicatiedienst (het ‘bedrijf [bedrijfsnaam 1]’ heeft immers geen data van [bedrijfsnaam 1] gebruikers aan de Franse of Nederlandse autoriteiten verstrekt), maar van rechtstreekse interceptie van [bedrijfsnaam 1] data door de Franse staat (buiten medeweten van het ‘bedrijf [bedrijfsnaam 1]’ om) en verwerking van die gegevens door de Nederlandse autoriteiten, is de rechtbank van oordeel dat deze activiteiten niet vallen onder de werkingssfeer van de richtlijn 2002/58.

### **Richtlijn 2016/680**

De rechtbank herhaalt dat zij ervan uitgaat dat de Franse rechter bij het verstrekken van de machtiging tot de interceptie heeft getoetst of de inzet van de tool (met het gevolg dat berichten werden onderschept) voldoet aan de Richtlijn 2016/680, althans de implementatie daarvan in Frans recht. Daar komt bij dat een rechtstreeks beroep op de richtlijn niet mogelijk is nu deze in nationale wetgeving is geïmplementeerd. Ten overvloede merkt de rechtbank op dat Richtlijn 2016/680 op zich de verwerking van persoonsgegevens ter opsporing van strafbare feiten niet verbiedt, maar reguleert. Het onderzoek naar strafbare feiten gepleegd door [bedrijfsnaam 1] (als medeplichtige) impliceert dat tevens onderzoek wordt verricht naar misdrijven gepleegd door gebruikers van [bedrijfsnaam 1] (waaraan [bedrijfsnaam 1] medeplichtig zou zijn). Het verzamelen van gegevens van [bedrijfsnaam 1] gebruikers is naar het voorshands oordeel van de rechtbank niet in strijd met de Richtlijn. De [bedrijfsnaam 1] berichten zijn immers slechts aan Nederland ter beschikking gesteld voor zover het in Nederland verzonden berichten betreft en de Nederlandse opgeslagen dataset is slechts beperkt toegankelijk, namelijk uitsluitend door bevoegde opsporingsambtenaren in onderzoeken waarvoor vooraf door de rechter-commissaris toestemming is verleend.

Gelet hierop ziet de rechtbank geen aanleiding tot het stellen van prejudiciële vragen.

### **Verzoeken tot het benoemen van deskundigen**

#### **[verdachte 10]**

De raadsman heeft aangevoerd dat in het kader van de identificatie van gebruikers van [bedrijfsnaam 1] accounts voornamelijk gebruik is gemaakt van zendmastgegevens en dat dit soort gegevens vaak tot onjuiste vaststellingen door de politie kan leiden. De raadsman wenst daarom een deskundige van het [bedrijfsnaam 3] te laten benoemen, waarbij het nodig is dat de broninformatie aan de hand waarvan de metingen zijn verricht aan de deskundige wordt verstrekt.

#### **[verdachte 3]**

De raadvrouw heeft aangevoerd dat het van belang is om te weten hoe [bedrijfsnaam 1] werkt en op welke wijze meegelezen kon worden met de gesprekken, om op die manier een goed beeld te krijgen van hoe de hack (of installatie van de malware) heeft plaatsgevonden. Hiervoor zouden een aantal vragen gesteld kunnen worden aan deskundigen op het gebied van cybercrime, bijvoorbeeld [A] en [B].

#### **[verdachte 5] en [verdachte 13]**

De raadsman heeft verzocht een deskundige te benoemen die vragen kan beantwoorden met betrekking tot de betrouwbaarheid van [bedrijfsnaam 1] zendmastgegevens die onder andere zien op de precieze locatie van het toestel, welke factoren van invloed zijn op die gegevens, wat de dekkingsgebieden zijn van de zendmasten waaraan de accounts [account 1], [account 2] en [account 3] werden gekoppeld en of een derde berichten kon verwijderen, toevoegen of wijzigen.

De officier van justitie stelt zich op het standpunt dat voor de identificatie van de gebruikers niet voornamelijk gebruik is gemaakt van zendmastgegevens en dat er geen reden is om te twifelen aan de betrouwbaarheid van de data. De officier van justitie verzet zich dan ook tegen de verzoeken tot het benoemen van getuigen-

deskundigen.

De rechtbank overweegt met betrekking tot de verzoeken van de raadslieden van verdachten [verdachte 10], [verdachte 5] en [verdachte 13] ten aanzien van de (betrouwbaarheid van de) zendmastgegevens dat uit de processen-verbaal ter identificatie van voornoemde verdachten volgt dat de door de politie vastgestelde identificatie van de verdachten als de gebruikers van de [bedrijfsnaam 1] accounts, niet louter gebaseerd is op zendmastgegevens. Bij verdachte [verdachte 10] lijken deze gegevens zelfs op geen enkele manier te hebben bijgedragen aan zijn identificatie. Om die reden overweegt de rechtbank dat de zendmastgegevens en een al dan niet aanwezige onzekerheidsmarge met betrekking tot de betrouwbaarheid daarvan, niet van doorslaggevend belang zullen zijn voor een in het kader van de artikelen 348 en 350 Sv te nemen beslissing. Het belang van deze onderzoekswens is voor het overige onvoldoende onderbouwd.

Met betrekking tot het verzoek van de raadsman van [verdachte 13] en [verdachte 5] om de mogelijkheid dat een derde berichten zou kunnen verwijderen, toevoegen of wijzigen op een [bedrijfsnaam 1] telefoon te laten onderzoeken, overweegt de rechtbank dat het zeer complexe encryptie-/beveiligingsmechanisme van [bedrijfsnaam 1] meebrengt dat op geen enkele manier aannemelijk is geworden - hetgeen ook niet uit het procesdossier is gebleken - dat een willekeurige derde, met een onbekend gebleven belang, zonder wetenschap of vermoeden van de gebruiker zich toegang heeft verschaft tot de [bedrijfsnaam 1] accounts van [account 1], [account 2] of [account 3] om via die telefoons berichten te verzenden, wijzigen of verwijderen.

De rechtbank wijst de verzoeken van de raadslieden tot het benoemen van getuigen-deskundigen af.

De rechtbank overweegt met betrekking tot het verzoek van de raadsvrouw van verdachte [verdachte 3] dat uit de hiervoor weergegeven inleiding met betrekking tot [bedrijfsnaam 1] - die deels gebaseerd is op de stukken van de Britse National Crime Agency - volgt dat zij op dit moment voldoende geïnformeerd is over de werking van [bedrijfsnaam 1] teneinde de vragen van artikelen 348 en 350 Sv te kunnen beantwoorden. De rechtbank wijst het verzoek van de raadsvrouw tot het benoemen van een getuige-deskundige af.

### **Verzoeken tot het horen van getuigen**

De verdediging heeft verzocht een groot aantal getuigen te laten horen. De officieren van justitie hebben op 10 mei 2021 in een schriftelijke reactie aangegeven of zij zich verzetten tegen het horen van bepaalde getuigen en dit gemotiveerd.

### **Medeverdachten Appel**

De rechtbank stelt ten eerste voorop dat er sprake is van een verdedigingsbelang bij het horen van getuigen die tevens medeverdachten zijn in onderzoek Appel, voor zover zij door het Openbaar Ministerie verdacht worden van deelname aan hetzelfde criminele samenwerkingsverband (CSV), door het Openbaar Ministerie omschreven als CSV A ([verdachte 1], [verdachte 2], [verdachte 3], [verdachte 4], [verdachte 5], [verdachte 6], [verdachte 7], [verdachte 9], [verdachte 10], [verdachte 13] en [verdachte 14]) en CSV B ([verdachte 1], [verdachte 11] en [verdachte 12]).

Ten tweede is er sprake van een verdedigingsbelang indien uit het procesdossier is gebleken dat er rechtstreeks contact heeft plaatsgevonden tussen de [bedrijfsnaam 1] accounts die door het Openbaar Ministerie worden toegeschreven aan een verdachte en een verzochte getuige. Wanneer een verzochte getuige ofwel wordt verdacht in hetzelfde CSV dan wel er contact is geweest tussen de accounts, wijst de rechtbank de verzoeken tot het horen van deze getuigen toe in de zaken van de voornoemde verdachten, mits hiertoe is verzocht door de verdediging. Indien niet is gebleken dat (één of meer van) deze getuigen contact heeft gehad met de verdachte die het verzoek tot horen doet en/of geen onderdeel uitmaakt van hetzelfde CSV, ziet de rechtbank geen verdedigingsbelang en wijst zij het verzoek af.

### **[getuige 1]**

Gelet op de rol die de getuige in het procesdossier wordt toegeschreven en hetgeen de rechtbank hiervoor heeft overwogen, ziet de rechtbank in de zaak van verdachten [verdachte 7] en [verdachte 10] een verdedigingsbelang om haar te horen. Het verzoek om de getuige te horen in deze zaken wordt toegewezen.

Nu er vooralsnog geen reden is om aan te nemen dat de getuige contact heeft gehad met verdachte [verdachte 12] en/of onderdeel is van CSV B, wordt het verzoek van de raadsman in zijn zaak afgewezen.

### **Getuigen locatie [locatie 1]**

#### **[getuige 19], [getuige 20] en [getuige 21]**

Deze personen worden in het procesdossier gekoppeld aan twee aangetroffen drugslaboratoria in [locatie 1]. [locatie 1] wordt echter niet aan één of meer verdachten in onderzoek Appel ten laste gelegd als pleegplaats. De rechtbank zal het verzoek tot het horen van deze getuigen afwijzen, nu dit niet van belang is voor enig te nemen beslissing ex artikelen 348 en 350 Sv.

### **Getuigen locatie [locatie 2] (onderzoek Hopper)**

#### **[getuige 2], [getuige 3], [getuige 4], [getuige 5], [getuige 6], [getuige 9], [getuige 8] en [getuige 7]**

Gelet op de rollen die de getuigen in het procesdossier worden toegeschreven met betrekking tot de aangetroffen productielocatie in [locatie 2], ziet de rechtbank in de zaken van verdachten [verdachte 7], [verdachte 2] en [verdachte 10] een verdedigingsbelang om deze getuigen te horen en de verzoeken in deze zaken worden toegewezen. De rechtbank ziet in de zaak van [verdachte 3] eveneens een verdedigingsbelang om de verzochte getuige [getuige 3] te horen en wijst dat verzoek dan ook toe. De rechtbank merkt op dat deze getuigen verdachten zijn in het onderzoek Hopper. De gegevens van deze verdachten zijn derhalve bekend bij het Openbaar Ministerie.

Ten aanzien van de verzoeken van de raadsman van verdachte [verdachte 12] om één of meer van deze getuigen te horen, is de rechtbank van oordeel dat niet is gebleken dat (één of meer van) deze getuigen contact heeft/hebben gehad met verdachte [verdachte 12] of het aan hem toegeschreven [bedrijfsnaam 1] account, noch dat zij enige betrokkenheid hebben gehad bij de aan hem tenlastegelegde feiten. De rechtbank zal in de zaak van verdachte [verdachte 12] het verzoek tot het horen van deze getuigen afwijzen.

### **Getuigen locatie [locatie 3]**

#### **[account 4], [account 5], [account 15], [account 6], [account 16], [account 7], '[account 8]', [account 9], [account 10], [account 11], [account 12], [account 13]**

De personen achter de voornoemde [bedrijfsnaam 1] accounts lijken in het procesdossier betrokken te zijn geweest bij de aangetroffen productielocatie in [locatie 3]. Verder is er contact geweest tussen [bedrijfsnaam 1] accounts die aan verdachten in het onderhavige onderzoek worden toegeschreven en de voornoemde accounts. Het Openbaar Ministerie heeft echter aangegeven dat van geen van de voornoemde accounts - met uitzondering van [account 15] - bekend is wie de gebruiker van het betreffende [bedrijfsnaam 1] account was ten tijde van de ten laste gelegde pleegperiode. De rechtbank is daarom van oordeel dat het horen van deze personen op dit moment praktisch onuitvoerbaar is en wijst het verzoek van de raadsman van verdachte [verdachte 10] om deze personen als getuige te horen af.

Met betrekking tot [account 15] wijst de rechtbank het verzoek van verdachte [verdachte 10] tot het horen van de persoon achter dit [bedrijfsnaam 1] account toe. De rechtbank ziet een verdedigingsbelang bij verdachte [verdachte 10] om deze getuige te horen nu er berichtenverkeer bestaat tussen [account 15] en het account [account 14] (waar verdachte [verdachte 10] aan wordt gekoppeld). Het Openbaar Ministerie heeft aangegeven dat de politie weet wie gebruik heeft gemaakt van dit account. De rechtbank ziet ook het verdedigingsbelang bij verdachte [verdachte 3] om de persoon achter alias [account 15] te horen als getuige en wijst dit verzoek toe.

Met betrekking tot [account 9] en [account 10] stelt de rechtbank vast dat niet is gebleken dat er berichtenverkeer bestaat tussen deze accounts en het [bedrijfsnaam 1] account dat aan verdachte [verdachte 10] wordt gekoppeld. De rechtbank wijst het verzoek tot het horen van deze getuigen om die reden af.

### **Locatie getuigen [locatie 4] (26Rockdale)**

#### **[getuige 11]**

Gelet op de rol die de getuige in het procesdossier wordt toegeschreven met betrekking tot de locaties in [locatie 2] en [locatie 4], ziet de rechtbank in de zaken van verdachten [verdachte 7], [verdachte 2] en [verdachte 10] een verdedigingsbelang om deze getuigen te horen. De rechtbank wijst de verzoeken in deze zaken toe. Nu er geen officieel adres van deze getuige bekend is, zal het de vraag zijn of het mogelijk is deze getuige binnen een aanvaardbare termijn te horen.

**[getuige 22], [getuige 23], [getuige 24], [getuige 25], [getuige 26], [getuige 27], [getuige 28], [getuige 29], [getuige 30], [getuige 31], [getuige 33], [getuige 34], [getuige 10], [getuige 35], [getuige 36], [getuige 37], [getuige 38], [getuige 39], [getuige 40], [getuige 41], [getuige 42], [getuige 43], [getuige 44], [getuige 45], [getuige 46], [getuige 47], [getuige 48], [getuige 49], [getuige 32]**

De raadsman van verdachte [verdachte 10] en de raadsvrouw van verdachte [verdachte 7] hebben verzocht om (een deel van) deze getuigen te horen. Hoewel de officieren van justitie zich niet hebben verzet tegen het horen van [getuige 23], [getuige 29] en [getuige 47], is de rechtbank van oordeel dat het belang om (één of meer van) deze personen te horen als getuige onvoldoende is onderbouwd. Uit het procesdossier blijkt dat voor alle verzochte getuigen geldt dat er geen reden is om aan te nemen dat zij op enig moment contact hebben gehad met verdachten [verdachte 10] en/of [verdachte 7], noch met de aan hen gekoppelde [bedrijfsnaam 1] accounts. Anders dan bij de locaties [locatie 2] en [locatie 3], wordt de locatie [locatie 4] in het einddossier niet direct gekoppeld als een locatie van het CSV waarvan verdachten onderdeel zouden uitmaken, maar als locatie waarover een andere groepering de leiding heeft. Daarnaast komen sommige namen van verzochte getuigen geheel niet voor in het procesdossier. De rechtbank wijst de verzoeken tot het horen van deze getuigen af.

### **Alle [bedrijfsnaam 1] namen met wie verdachte heeft gechat**

Voor zover de raadsman van verdachte [verdachte 10] dit verzoek thans handhaaft, wijst de rechtbank dit verzoek af nu dit onvoldoende is onderbouwd.

De rechtbank stelt de stukken in handen van de rechter-commissaris, belast met de behandeling van strafzaken in deze rechtbank, om de volgende getuigen te horen.

[verdachte 1],

geboren op [1984] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 3], [verdachte 6], [verdachte 7], [verdachte 10], [verdachte 14] en [verdachte 12].

[verdachte 2],

geboren op [1987] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 1], [verdachte 3], [verdachte 6], [verdachte 7], [verdachte 10] en [verdachte 14].

[verdachte 3],

geboren op [1981] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 6], [verdachte 7], [verdachte 10] en [verdachte 14].

[verdachte 4],

geboren op [1987] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 3], [verdachte 6], [verdachte 7], [verdachte 10] en [verdachte 14].

[verdachte 5],

geboren op [1969] te [geboorteplaats], thans gedetineerd in de [verblijfplaats], in de zaken van verdachten [verdachte 3], [verdachte 6], [verdachte 7], [verdachte 10], [verdachte 13] en [verdachte 14].

[verdachte 6],

geboren op [1980] te [geboorteplaats], thans gedetineerd in de [verblijfplaats], in de zaken van verdachten [verdachte 2], [verdachte 3], [verdachte 5], [verdachte 7], [verdachte 10], [verdachte 13] en [verdachte 14].

[verdachte 7],

geboren op [1981] te [geboorteplaats], thans gedetineerd in de [verblijfplaats], in de zaken van verdachten [verdachte 1], [verdachte 2], [verdachte 3], [verdachte 5], [verdachte 6], [verdachte 10], [verdachte 13] en [verdachte 14].

[verdachte 8],

geboren op [1984] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaak van verdachte [verdachte 3].

[verdachte 9],

geboren op [1983] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 3], [verdachte 6], [verdachte 7], [verdachte 10] en [verdachte 14].

[verdachte 10],

geboren op [1982] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 3], [verdachte 6], [verdachte 7] en [verdachte 14].

[verdachte 11],

geboren op [1989] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 1], [verdachte 3] en [verdachte 12].

[verdachte 12],

geboren op [1985] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaak van verdachte [verdachte 1].

[verdachte 13],

geboren op [1959] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 3], [verdachte 5], [verdachte 6], [verdachte 7], [verdachte 10] en [verdachte 14].

[verdachte 14],

geboren op [1986] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 3], [verdachte 5], [verdachte 6], [verdachte 7], [verdachte 10] en [verdachte 13].

[getuige 1],

geboren op [1961] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 7] en [verdachte 10].



[getuige 2], geboren op [1985] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 7] en [verdachte 10].

[getuige 3],

geboren op [1982] te [geboorteplaats], verblijfplaats onbekend, in de zaken van verdachten [verdachte 3], [verdachte 7] en [verdachte 10].

[getuige 4],

geboortedatum onbekend, verblijfplaats onbekend, in de zaken van verdachten [verdachte 2], [verdachte 7] en [verdachte 10].

[getuige 5],

geboren op [1987] te [geboorteplaats] (Dominicaanse Republiek), verblijfplaats onbekend, in de zaken van verdachten [verdachte 7] en [verdachte 10].

[getuige 6],

geboren op [1975] te [geboorteplaats] (Mexico), verblijfplaats onbekend, in de zaken van verdachten [verdachte 2], [verdachte 7] en [verdachte 10].

[getuige 9],

geboren op [1994] te [geboorteplaats] (Mexico), verblijfplaats onbekend, in de zaken van verdachten [verdachte 2], [verdachte 7] en [verdachte 10].

[getuige 8],

geboren op [1956] te [geboorteplaats], wonende te [adres], [postcode] [woonplaats], in de zaken van verdachten [verdachte 2], [verdachte 7] en [verdachte 10].

[getuige 7],

geboren op [1955] te [geboorteplaats] (Joegoslavië), verblijfplaats onbekend, in de zaak van verdachte [verdachte 2].

[account 15]

personalia bekend bij het Openbaar Ministerie, in de zaken van verdachten [verdachte 3] en [verdachte 10].

[getuige 11],

geboren op [1977] te [geboorteplaats] (België), verblijfplaats onbekend, in de zaak van verdachten [verdachte 2], [verdachte 7] en [verdachte 10].

De rechtbank draagt de rechter-commissaris daarnaast op om datgene te doen wat hij ambtshalve noodzakelijk vindt.

## **Verzoeken met betrekking tot individuele verdachten**

### **Inzage in de datasets van medeverdachten**

Het Openbaar Ministerie heeft toegezegd een downloadlink te verstrekken aan alle raadslieden waarmee zij inzage verkrijgen in een forensische kopie van alle chatgesprekken (dus verzonden en ontvangen berichten)

van de accounts die aan de individuele verdachten worden toegeschreven. Daarnaast hebben de officieren van justitie reeds alle chatberichten die zij koppelen aan de productielocaties [locatie 2], [locatie 3] en [locatie 4] verstrekt bij het einddossier. De raadslieden van verdachten [verdachte 10] en [verdachte 7] hebben op de regiezitting hun verzoek gehandhaafd om inzage te verkrijgen in alle chatberichten die zij relevant achten. De officieren van justitie verzetten zich hiertegen, omdat zij - gelet op de verstrekking van de downloadlink in combinatie met de reeds opgenomen chatberichten van het CSV in het einddossier - de chatberichten van anderen niet relevant achten voor de verdenking tegen de voornoemde verdachten. Bovendien staan er privacybelangen van derden aan een toewijzing van het verzoek in de weg. Indien de rechtbank het verzoek wel zou toewijzen, dan zou inzage slechts mogelijk zijn op locatie van het NFI door gebruik te maken van het programma [...].

De rechtbank stelt voorop dat de verdediging de mogelijkheid moet krijgen om de inhoud van het tegen de verdachten aangebrachte bewijs te onderzoeken. Voor de beoordeling van het ingediende verzoek is van belang dat verdachten [verdachte 10] en [verdachte 7] worden verdacht van deelname respectievelijk het leidinggeven aan een criminele organisatie in het kader van de Opiumwet met 10 medeverdachten, waardoor allerm minst kan worden uitgesloten dat er in de chatberichten die aan medeverdachten worden gekoppeld belastende en/of ontlastende feiten voor verdachten [verdachte 10] en [verdachte 7] gevonden kunnen worden. De rechtbank is daarom van oordeel dat de verdediging in de gelegenheid moet worden gesteld om de datasets die worden gekoppeld aan de medeverdachten te onderzoeken. De rechtbank weegt daarbij tevens de privacybelangen van derden mee. Gelet hierop wijst de rechtbank de verzoeken van de raadsman van verdachte [verdachte 10] en de raadvrouw van verdachte [verdachte 7] tot inzage in de datasets die aan de medeverdachten worden gekoppeld toe, met daaraan de voorwaarden gebonden dat alleen de raadsman en raadvrouw van de verdachten [verdachte 10] en [verdachte 7] inzage in de datasets bij het NFI kunnen krijgen en dat zij slechts inzage krijgen in de datasets zoals deze ter beschikking zijn gesteld aan de verdediging van medeverdachten [verdachte 1], [verdachte 2], [verdachte 3], [verdachte 4], [verdachte 5], [verdachte 6], [verdachte 7], [verdachte 9], [verdachte 10], [verdachte 13] en [verdachte 14] (die worden verdachte van deelname aan hetzelfde CSV).

#### **Onderzoek naar de in de woning van verdachte [verdachte 11] aangetroffen substanties wit poeder**

De raadsman van verdachte [verdachte 11] heeft verzocht dat er aanvullend onderzoek wordt verricht naar de samenstelling van de in de woning van verdachte aangetroffen hoeveelheden wit poeder (met SIN-nummers: AAHP0674NL, AAHP0675NL en AAHP0676NL) nu verdachte betwist dat het hier om voor consumptie geschikte drugs betreft en dat het percentage cocaïne dusdanig klein is dat het niet voor consumptie is geschikt.

De rechtbank stelt voorop dat uit het reeds verrichte onderzoek door het RIVM en het NFI naar de in de woning van verdachte aangetroffen substanties wit poeder een uitslag naar voren is gekomen en dat deze uitslag inhoudt dat het materialen zijn die cocaïne bevatten. De rechtbank ziet niet in dat nader onderzoek naar de kwaliteit van de cocaïne (de mate waarin de cocaïne versneden is) relevant is voor de beantwoording van de vragen van artikel 348 en 350 Sv. De rechtbank ziet dan ook niet het verdedigingsbelang bij een aanvullend onderzoek waarin, voor zover mogelijk, wordt vastgesteld welk percentage van het materiaal uit cocaïne zou bestaan. De rechtbank wijst het verzoek van de raadsman tot aanvullend onderzoek af.

De rechtbank merkt hierbij op dat het door het Openbaar Ministerie toegezegde onderzoek naar de bij medeverdachte [verdachte 1] aangetroffen substanties gelegen is in de grotere hoeveelheid en de van cocaïne afwijkende kleur die bij de substanties is waargenomen.

(enz.)

---

#### **Voetnoten**

[1.] HR 5 oktober 2010, ECLI:NL:HR:2010:BL5629, rov. 4.4.1.

[2.] Richtlijn 2002/58/EG van het Europees parlement en de Raad van 12 juli 2002 betreffende de verwerking

van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en de elektronische communicatie), L201/37.

[3.] Rov 101.

[4.] Rov. 103.