ANNOTATIE

M.N. (EncroChat) (HvJ EU C-670/22) – Grensoverschrijdende aspecten van de EncroChat-operatie

D.A.G. van Toor en C.M. Taylor Parkins-Ozephius

Annotatie bij Hof van Justitie van de Europese Unie, 30-04-2024, ECLI:EU:C:2024:372 (EHRC-2024-0128)

1. De EncroChat-operatie heeft tot een aardverschuiving in het strafprocesrechtelijke landschap geleid: eind 2022 stond de teller op meer dan tweehonderd rechterlijke uitspraken waarin EncroChat-berichten als bewijs werden gebruikt.[1] Een simpele zoekslag in strafrechtelijke uitspraken van feitenrechters op rechtspraak.nl levert medio 2024 657 hits op (deze hits zijn, gezien het omvangrijke aantal, niet nader onderzocht). Het onderhavige arrest is evenwel het eerste internationaalrechtelijke arrest over de EncroChat-operatie. De operatie wordt in deze noot niet nader toegelicht;[2] het is voldoende om te weten dat de door de Nederlandse autoriteiten ontwikkelde spyware op een totaal van 66.134 geregistreerde toestellen werd geïnstalleerd – de spyware werd als update op de toestellen gepusht, maar niet automatisch geïnstalleerd – bij 32.477 gebruikers in 122 verschillende landen. Een, gezien deze omvang, ongelooflijk succesvolle operatie waarmee ongekende inzichten in de wereldwijde criminaliteit is verkregen. Ongeveer 4.600 van de 66.134 toestellen bevonden zich, tijdens de installatie van de spyware, op het Duitse grondgebied. De Duitse autoriteiten haken, middels een op 2 juni 2020 uitgevaardigd Europees onderzoeksbevel (hierna: EOB), aan bij de operatie die op 1 april 2020 officieel van start is gegaan met de installatie van de spyware (maar waar meerdere besprekingen tussen verschillende lidstaten aan vooraf zijn gegaan). Vanaf het moment van de uitvaardiging van het EOB (2 juni 2020), en na aanvullende verzoeken in september 2020 en juli 2021, hebben de Duitse autoriteiten onbegrensde toegang tot de via Europol uitgewisselde Encrochat-berichten. M.N. – de naamgever aan het onderhavige arrest

– is een van de personen die naar aanleiding van de analyse van de EncroChat-berichten in beeld komt als verdachte van overtreding van de Duitse Opiumwet.

2. De verdenking en strafzaak tegen M.N. (en de EncroChat-operatie in het algemeen) hebben de pennen losgemaakt in Duitsland, met een veel fundamentelere discussie binnen de rechtspraak zelf in vergelijking met de Nederlandse praktijk.[3] De onderhavige prejudiciële vragen zijn de volgende stap in die discussie. Het is het *Landgericht*[4] Berlijn dat de grote roerganger in deze discussie is en ook de onderhavige prejudiciële vragen heeft gesteld. In punt 30 van het arrest staat deze achtergrond kort, maar krachtig, aangeduid: het *Landgericht* deelt de uitleg die het *Bundesgerichtshof* (hierna: BGH; Duitse cassatierechter) aan artikel 6 en 31 van richtlijn 2014/41/EU betreffende het Europees onderzoeksbevel in strafzaken (hierna: EOB-Richtlijn) geeft niet (en neemt daarmee geen genoegen nadat het BGH de zaak M.N. terugwees, omdat het *Landgericht* de verkrijging van de EncroChat-berichten middels het EOB als onrechtmatig had bestempeld).

3. Het is namelijk een onderdeel van het openbaar ministerie (het *Generalstaatsanwaltschaft* in Frankfurt, vergelijkbaar met het ressortsparket in Nederland) die het EOB tot het verkrijgen van onbeperkte toegang tot de EncroChat-gegevens heeft uitgevaardigd. Het *Landgericht*, daarbij verwijzend naar *Prokuratuur*,[5] neemt de stelling in dat deze instantie een onvoldoende onafhankelijke autoriteit is (punt 30). De in Duitsland geldende bevoegdheid voor vergelijkbare handeling is (volgens de meerderheid van de Duitse gerechten, incl. het BGH) paragraaf 100b *Strafprozessordnung* (het Duitse wetboek van strafvordering, hierna: *StPO)*, waarin duidelijk staat dat de rechter bevoegd is toestemming te verlenen voor onlinedoorzoeking.[6] Op basis van artikel 6 EOB-Richtlijn had de situatie volgens het *Landgericht* in Duitsland dus niet rechtmatig op deze wijze kunnen plaatsvinden; het verzoek is namelijk door vertegenwoordigers van de staande magistratuur uitgevaardigd, zonder voorafgaande onafhankelijke controle (hieronder rns. 4-5). Ook op andere punten neemt het *Landgericht* een ander standpunt in dan het BGH: (i) volgens het *Landgericht* voldoet het EOB niet aan het evenredigheidsbeginsel, omdat niet tegen elke individuele gebruiker van EncroChat een *verdenking* bestond, maar wel tegen elke gebruiker opsporingshandelingen zijn verricht (punten 35-36); (ii) het EOB moet wél aan het geldende nationale recht, via artikel 6 EOB-Richtlijn, worden getoetst, omdat deze bepaling ook op de *overdracht* van bewijs ziet en niet alleen op de *vergaring* van bewijs (punten 39-40; deze en de vorige vraag worden gezamenlijk beantwoord door het HvJ EU; rns. 6-8); en (iii) dat artikel 31 EOB-Richtlijn vereist dat de kennisgeving van een operatie als EncroChat (welke volgens het *Landgericht* onder de interceptie van *telecommunicatie* valt) indien de interceptie wordt uitgevoerd op het grondgebied van een andere lidstaat moet worden gericht aan een bij het onderzoek onafhankelijke autoriteit (en dus niet aan het openbaar ministerie); (iv) tevens worden

vraagtekens geplaatst bij de beoogde beschermde belangen door dit artikel (punten 43-46; hieronder rns. 9-14). Deze punten worden hieronder nader besproken, waarna wij tot een afronding komen in rn. 15.

4. De eerste prejudiciële vraag betreft de uitleg die aan het begrip *rechterlijke autoriteit* wordt gegeven. Uit artikel 1 EOB-Richtlijn volgt dat een EOB kan worden uitgevaardigd door een rechterlijke autoriteit, maar dat begrip wordt in de Richtlijn niet nader uitgewerkt. Het is, gezien onder andere het *Prokuratuur*-arrest (eerder aangehaald), niet verwonderlijk dat deze EOB-bepaling vragen oproept. In *Prokuratuur* heeft het HvJ EU namelijk geoordeeld dat een officier van justitie die betrokken is bij de opsporing en vervolging van strafbare feiten een onvoldoende onafhankelijke autoriteit is om te oordelen over de toegang tot gegevens opgeslagen door telecommunicatieaanbieders. In de meeste strafvorderlijke systemen is de officier van justitie zowel de leidinggevende over de opsporing als de persoon die tot vervolging overgaat. Het is dan natuurlijk al snel dat het verkrijgen van (veel) data in de ogen van de officier van justitie van belang is voor zijn zaak, en dat een wat meer magistratelijke toets mogelijk niet van hem kan worden verwacht. Specifiek in *Prokuratuur* acht het HvJ EU de officier van justitie in de procedure in Estland onvoldoende onafhankelijk, ongeacht het feit dat de officier van justitie wettelijk gezien aan waarheidsvinding doet en dus zowel belastend als ontlastend bewijs dient te verzamelen (punten 55-56; *Prokuratuur*). De toetsende instantie bij het vorderen van gegevens moet een derde zijn, die geen verband heeft met de autoriteit die de vordering indient (punt 54; *Prokuratuur*).

5. Met betrekking tot het EOB wordt de soep echter niet zo heet gegeten: de betekenis van rechterlijke autoriteit in die Richtlijn wordt bepaald door het in artikel 2 onder c genoemde begrip 'uitvaardigende autoriteit'.[7] In de zin van de EOB-Richtlijn is de uitvaardigende autoriteit de autoriteit die naar nationaal recht bevoegd is in een zaak.[8] Dat betekent dat de officier van justitie, die volgens het recht van de uitvaardigende staat in de nationale procedure bevoegd is om (zoals in het onderhavige geval) te beslissen over de *overdracht* van bewijs, onder het begrip uitvaardigende autoriteit valt in de zin van het EOB (punt 74). De Duitse regering beargumenteert dat, op grond van artikel 100e lid 6 StPO, de overdracht van het bewijs (anders de *vergaring* van het bewijs) niet met rechterlijke toestemming hoeft plaats te vinden. Het HvJ EU kaatst, op basis van dit standpunt van de Duitse regering, de bal terug: het is het *Landgericht* dat moet oordelen of dit de juiste uitleg van het nationale recht is. Het is evenwel, op basis van de eerder aangehaalde jurisprudentie, niet zo dat in het kader van het EOB het begrip rechterlijke autoriteit dezelfde betekenis toekomt als in *Prokuratuur*. Als het nationale recht de officier van justitie (die ook de vervolgende autoriteit kan zijn) als bevoegd bestempelt voor een bepaalde handeling, dan is hij de competente uitvaardigende autoriteit. Voor de Nederlandse EncroChat-zaken is deze discussie niet van belang: Nederland was

betrokken bij de *vergaring* van het bewijs, en daarvoor heeft een Nederlandse rechter-commissaris te Rotterdam op 27 maart 2020 toestemming verleend. Voor de overdracht van de gegevens naar andere strafdossiers heeft dezelfde rechter-commissaris per 6 augustus 2020 toestemming verleend.

6. Na de beantwoording van de hierboven besproken eerste prejudiciële vraag beantwoordt het HvJ EU de tweede en derde vraag gezamenlijk (punt 85). De tweede vraag betreft de zienswijze van het *Landgericht* over de afwezigheid van een verdenking tegen alle individuele gebruikers, terwijl tegen hen wel (ingrijpende) opsporingshandelingen zijn verricht. Het Hof behandelt die vraag tezamen met de vraag naar de wijze waarop de verdediging doeltreffend commentaar op de *vergaring* van het bewijs kan leveren en in hoeverre voor de rechtmatigheid van de *vergaring* aan het nationale recht moet worden getoetst. Het HvJ EU herformuleert deze vragen naar de vaststelling van de noodzakelijkheid en evenredigheid van de onderzoeksmaatregelen (punt 88). Dit moet volgens artikel 6 EOB-Richtlijn worden vastgesteld aan de hand van het recht van de *uitvaardigende* staat – in dit geval dus Duitsland – (punt 87-88). Aan de hand van het Duitse recht moet derhalve worden bepaald of voor de *overdracht* van bewijs een individuele, specifieke verdenking noodzakelijk is. Hetzelfde geldt voor alle andere voorwaarden; aan de hand van het nationale recht moet worden bepaald of in dezelfde omstandigheden in een vergelijkbare binnenlandse zaak de overdracht van bewijs mogelijk zou zijn (punt 92).

7. Dat geldt niet voor de *vergaring* van het bewijs; als het bewijs al in bezit is van de uitvoerende staat – in dit geval Frankrijk – hoeft in de uitvaardigende staat niet te zijn voldaan aan de materiële voorwaarden met betrekking tot de vergaring van het bewijs (punt 96). Het HvJ EU roept vervolgens, als een soort nabrander, nog ter herinnering dat het beginsel van wederzijdse erkenning berust op wederzijds vertrouwen dat andere lidstaten de geldende normen handhaven. Deze formulering zal de Nederlandse lezer en EncroChat-ingewijde niet vreemd voorkomen: alle verzoeken tot (vergaande) controle op de rechtmatigheid van de vergaring van het bewijs zijn door Nederlandse rechters op dezelfde wijze afgewezen.[9]

8. Ten slotte verbindt het HvJ EU aan de beantwoording van vragen twee en drie een vaag geformuleerde verplichting om de verdedigingsrechten te waarborgen wanneer de rechter de door de uitvoering van het EOB verkregen bewijs *gebruikt* (punt 104 e.v.). De verdediging moet in de gelegenheid worden gesteld om *doeltreffend* commentaar te leveren op het bewijsmateriaal. Het is volstrekt onduidelijk op welke wijze de nationale rechter hieraan kan bijdragen, zeker in het licht van de eerdere opmerking dat de nationale rechter niet in de rechtmatigheidstoets van de vergaring van het bewijs mag treden. Bij het rechtmatig vergaren van digitaal bewijs horen namelijk ook voorwaarden met betrekking tot het verkrijgen, opslaan en ter beschikking stellen van het materiaal waarbij de authenticiteit van de gegevens

niet (onbewust) wordt geschonden. Moeten dergelijke aspecten – die betrouwbaarheidsvereisten in een rechtmatigheidsjasje zijn – als pure betrouwbaarheidsvereisten worden behandeld en dient de rechter dan op basis van het feit dat hij de authenticiteit van het bewijs in onvoldoende mate kan vaststellen het bewijs op die grond buiten beschouwing te laten? Welke verantwoordelijkheden hebben de autoriteiten dan om informatie te verstrekken zodat de authenticiteit van de gegevens kan worden beoordeeld om van een voldoende doeltreffend commentaar te spreken? Of bedoelt het HvJ EU hier, simpelweg en kort gezegd, alleen dat de verdediging de mogelijkheid moet worden geboden de authenticiteit te betwisten?[10] Omdat onduidelijk is wanneer sprake is van een doeltreffend commentaar, en in hoeverre de autoriteiten de verdediging daarvoor (technische) informatie ter beschikking moet stellen, is de invloed van deze passage op het Nederlandse strafproces onzeker. Hoogstwaarschijnlijk zal, met betrekking tot de waarheidsgetrouwheid van de EncroChat-berichten, weinig veranderen: die berichten vinden vaak ondersteuning in ander bewijs, zoals de in beslag genomen verboden middelen en wapens, een kroongetuigeverklaring en/of de verklaringen van of de onderzoeken aan de slachtoffers van het toegepaste geweld. Hierdoor zal een veroordeling niet enkel en mogelijk ook niet doorslaggevend op digitaal bewijs berusten.[11]

9. Het HvJ EU gaat vervolgens over tot de beantwoording van de vierde prejudiciële vraag, die feitelijk uit drie onderdelen bestaat die zich richten op de interpretatie van artikel 31 EOB-Richtlijn. Uit dit artikel vloeit een notificatieplicht voort voor de intercepterende lidstaat (in dit geval Frankrijk) in het geval de interceptie van *telecommunicatie* betrekking heeft op een persoon wiens communicatieadres in gebruik is op het grondgebied van een andere lidstaat en de interceptie kan worden uitgevoerd zonder technische bijstand van die andere lidstaat (in dit geval Duitsland). Deze kennisgeving moet gericht zijn aan de *bevoegde autoriteit* van de andere lidstaat (de 'in kennis gestelde lidstaat') en dient voorafgaand aan de interceptie plaats te vinden in gevallen waar de autoriteit van de intercepterende lidstaat weet dat de persoon zich in de andere lidstaat bevindt of zal bevinden op het moment van het geven van de interceptieopdracht. Indien de intercepterende lidstaat pas tijdens de interceptie ontdekt dat de persoon zich tijdens de interceptie in een andere lidstaat bevindt of heeft bevonden, kan de kennisgeving ook tijdens of na de interceptie plaatsvinden. Uit lid 3 volgt dat de bevoegde autoriteit van de in kennis gestelde lidstaat de mogelijkheid heeft om binnen uiterlijk 96 uur na ontvangst van de kennisgeving de interceptie te verbieden of te beëindigen als deze in een vergelijkbare binnenlandse zaak niet zou zijn toegestaan. In het geval dat dan al materiaal is geïntercepteerd, kan worden bepaald dat de reeds vergaarde gegevens niet mogen worden gebruikt (in de in kennis gestelde lidstaat), of dat deze enkel onder specifieke voorwaarden mogen worden gebruikt.

10. De in artikel 31 centraal staande notificatieverplichting, die overigens niet is gekoppeld aan een EOB, treedt dus pas in werking indien sprake is van de interceptie van *telecommunicatie*. Het BGH meende dat de EncroChat-operatie hier niet onder zou vallen. Het *Landgericht* heeft echter een andere opvatting en kwalificeert de Franse gegevensextractiemaatregel wel als interceptie van telecommunicatie (punt 43). Het HvJ EU roept ter beantwoording van deze vraag in herinnering dat volgens vaste rechtspraak elke term uit een Unierechtelijke bepaling die niet specifiek verwijst naar nationale wetgeving, op dezelfde manier moet worden uitgelegd in alle lidstaten. Ten behoeve van deze eenvormige uitleg moet niet alleen naar de woorden van de bepaling zelf worden gekeken, maar ook naar de context en het doel van de regeling waar zij deel van uitmaken (punt 109).[12] Het HvJ EU bevestigt vervolgens dat de term telecommunicatie autonoom en uniform moet worden geïnterpreteerd volgens het Unierecht, bij gebrek aan een definitiebepaling in de richtlijn of specifieke verwijzing naar het recht van de lidstaten, alvorens de term uit te leggen aan de hand van de hiervoor genoemde handvatten. Kijkend naar de bewoordingen verwijst telecommunicatie, naar 'het geheel van procedés voor de overdracht van informatie op afstand.' In de context van de bepaling waar de term in wordt gebezigd, valt op dat in een bijbehorende bijlage met betrekking tot telecommunicatie zowel een telefoonnummer, IP-nummer als een e|mailadres wordt genoemd. Tevens blijkt uit overweging 30 van de EOB-Richtlijn dat de samenwerking inzake de interceptie van telecommunicatie niet enkel de inhoud van deze communicatie betreft, maar ook de bijbehorende verkeers| en locatiegegevens. Uit deze argumentatie (punten 111-114) volgt de conclusie dat 'de infiltratie van eindapparatuur teneinde zowel communicatiegegevens als verkeers| en locatiegegevens van een internet-gebaseerde communicatiedienst te vergaren, een interceptie van telecommunicatie in de zin van artikel 31, lid 1, van de EOB-Richtlijn is.' Op basis van deze uitleg valt de EncroChat-operatie te kwalificeren als interceptie van telecommunicatie.[13] In dat geval was er dus een kennisgevingsverplichting waarbij de bevoegde Duitse autoriteit door Frankrijk op de hoogte moest worden gebracht van de operatie op Duits grondgebied. Maar wie is nu de bevoegde autoriteit?

11. Het *Landgericht* meent dat de in artikel 31 genoemde *bevoegde autoriteit* die de kennisgeving dient te ontvangen een rechterlijke instantie zou moeten zijn, die niet met enig onderzoek belast is en die geen belang heeft bij het verkrijgen van de gegevens (punt 44). Het HvJ EU merkt op dat de Uniewetgever in de richtlijn niet heeft gespecificeerd of de bevoegde autoriteit een administratieve of gerechtelijke instantie moet zijn. Daarnaast blijkt uit het kennisgevingsformulier uit de bijlage van de EOB-Richtlijn dat enkel 'de in kennis gestelde lidstaat' dient te worden ingevuld en niet ook de autoriteit. Op basis van het voorgaande – en dus voornamelijk het gebrek aan specifieke informatie over de autoriteit – maakt het HvJ EU op dat het de lidstaten vrijstaat om deze autoriteit aan te wijzen. Als de intercepterende

lidstaat niet weet wie de bevoegde autoriteit is, kan de kennisgeving aan een geschikte autoriteit van de in kennis gestelde lidstaat worden gestuurd. Deze autoriteit moet de kennisgeving ambtshalve doorsturen naar de juiste instantie als zij niet zelf bevoegd is, om de werking van artikel 31 van de EOB-Richtlijn te waarborgen (punten 116-119). Ook in § 91g, lid 6, IRG (*Gesetz über die internationale Rechtshilfe in Strafsachen*), waarin artikel 31 van richtlijn 2014/41 naar Duits recht is omgezet, wordt niet bepaald wie de juiste autoriteit is. Een kennisgeving aan een onderdeel van het openbaar ministerie (en de verplichting van dat ambt om de kennisgeving eventueel door te sturen) is derhalve voldoende om van een kennisgeving aan een *bevoegde autoriteit* te spreken.

12. Het derde onderdeel van de vierde prejudiciële vraag ziet niet op de uitleg van een begrip uit artikel 31 van de EOB-richtlijn, zoals de voorgaande onderdelen, maar op de vraag of dit artikel ook strekt tot de bescherming van de rechten van degene wiens telecommunicatie wordt geïntercepteerd en of die bescherming zich ook uitstrekt tot het gebruik van de vergaarde gegevens in een strafprocedure in de lidstaat op wiens grondgebied de interceptie heeft plaatsgevonden. Het HvJ EU benadrukt ten behoeve van de beantwoording van deze vraag eerst dat bij de in dit artikel bedoelde intercepties geen sprake is van een EOB, waardoor de hierbij behorende voorwaarden en waarborgen niet van toepassing zijn (punt 121). Volgens het HvJ EU is de beoogde bescherming van artikel 31 EOB-Richtlijn tweeledig. Zo volgt uit lid 3 een beoordelingsmarge voor de (bevoegde autoriteit van de) lidstaat, waar het gaat om de binnenlandse beoordeling of de interceptie in een vergelijkbare binnenlandse zaak zou zijn toegestaan, waar bij een negatieve uitkomst de in kennis gestelde lidstaat de intercepterende lidstaat kan informeren of de interceptie mag doorgaan of niet (en of eventueel al geïntercepteerd materiaal niet of enkel onder voorwaarden mag worden gebruikt). Deze bepaling beschermt hierdoor niet enkel de soevereiniteit van lidstaten, maar waarborgt ook het beschermingsniveau in de lidstaat met betrekking tot de interceptie van telecommunicatie. Aangezien de interceptie een inbreuk vormt op het recht op eerbiediging van het privéleven en communicatie (artikel 7 van het Handvest van de grondrechten van de EU), volgt volgens het HvJ EU dat artikel 31 zich ook uitstrekt tot de bescherming van de rechten van de betrokken personen en het gebruik van de verkregen gegevens in strafprocedures in de in kennis gestelde lidstaat. De wijze waarop deze bescherming precies werkt, blijft echter onduidelijk. Uit de beantwoording van de vraag blijkt immers niet wat de gevolgen (zouden moeten) zijn indien de kennisgeving niet (of te laat) heeft plaatsgevonden en of dit nog op enige wijze te repareren valt indien de interceptie naar nationaal recht mocht plaatsvinden en het materiaal gebruikt wordt in het strafproces tegen de betrokken persoon.

13. Het antwoord op dit derde aspect van de vierde vraag is wellicht het meest verrassend voor Nederland. Op het punt van de bescherming van artikel 31 EOB-Richtlijn is namelijk een

discrepantie te herkennen tussen de interpretatie van het HvJ EU en de Hoge Raad. Het HvJ EU is hier duidelijk in: de rechten van de desbetreffende persoon worden hierdoor ook beschermd, gezien de interceptie een inbreuk op zijn rechten vormt. De Hoge Raad meende dat 'de [..] regelingen niet zijn geschreven ter bescherming van specifieke belangen van de af te tappen of afgetapte persoon, maar verband houden met, kort gezegd, de soevereiniteit van de betrokken landen en het daaraan verbonden uitgangspunt dat het aan de autoriteiten van een land is om te bepalen welke opsporingsactiviteiten op het eigen grondgebied plaatsvinden, ook al hebben de activiteiten hun uitwerking mede in andere landen.'[14] Deze discrepantie tussen de uitleg van het HvJ EU en de Hoge Raad blijkt in de praktijk echter allesbehalve zaligmakend te zijn voor de advocaten die hier wellicht nieuwe kansen in zagen. Verschillende advocaten hebben ter onderbouwing van een onrechtmatigheidsverweer gewezen op de ontbrekende kennisgeving, waardoor de belangen van de verdachte ook niet zijn meegewogen bij de in het geheel ontbrekende toets of volgens het Nederlandse recht de interceptie doorgang kon vinden.[15] Artikel 31 van de EOB-Richtlijn is echter niet van toepassing op de in Nederland uitgevoerde interceptie van de EncroChat-data. Zoals eerder gesteld, was Nederland immers betrokken bij de *vergaring* van het bewijs en lag het initiatief voor de interceptie van de telecommunicatie mede bij Nederland, waardoor een kennisgeving niet vereist was. Desondanks heeft een Nederlandse rechter-commissaris wel toestemming verleend voor zowel het binnendringen van de geautomatiseerde werken als het hierop volgende aftappen van de telecommunicatie. Door deze rechterlijke toetsing voorafgaand aan de interceptie kan worden aangenomen dat de belangen van de personen waarbij de interceptie plaatsvond voldoende zijn gewaarborgd. Deze belangen spelen immers altijd een rol bij de afweging die voorafgaat aan het al dan niet verlenen van machtigingen voor het binnendringen van een geautomatiseerd werk en het hierop volgende opnemen/aftappen van telecommunicatie.[16]

14. Voor Duitsland zijn de antwoorden op alle onderdelen van de vierde vraag van belang. Uit de antwoorden op deze vraag blijkt dat, zoals het *Landgericht* al meende, de EncroChat-operatie wél als interceptie van *telecommunicatie* moet worden beschouwd (en hoogstwaarschijnlijk niet als onlinedoorzoeking ex §100b StPO kan worden bestempeld). Hierdoor bestond een notificatieplicht voor de intercepterende lidstaat – in dit geval Frankrijk –, voor de intercepties voorafgaand aan het uitvaardigen van het EOB (dus tussen 1 april en 2 juni). Naar aanleiding van het ontvangen van deze kennisgeving had de *bevoegde autoriteit*, die zoals het BGH van mening was niet per se een onafhankelijke rechterlijke autoriteit hoeft te zijn, een oordeel moeten vellen over of de interceptie op basis van het nationale recht zou zijn toegestaan en of de interceptie (onder voorwaarden) doorgang kon vinden. De interpretatie van het nationale recht is hier aldus van doorslaggevend belang. Dit is al een punt van discussie geweest in de Duitse rechtspraak: het *Landgericht* meende dat het *StPO* geen

bulkinterceptiebevoegdheid kent waarbij communicatie wordt afgeluisterd van personen waartegen geen verdenking bestaat, waarna het *Kammergericht*[17] deze beschikking vernietigde en meende dat er wel een geschikte grondslag bestaat en er ook (op enig moment) een verdenking bestond.[18] Deze discussie zal op nationaal niveau nu beslecht moeten worden.

15. Het moge duidelijk zijn: in Duitsland zal de discussie over EncroChat op basis van dit arrest verder worden gevoerd. De interpretatie van het nationale recht zal doorslaggevend zijn om te bepalen of het EOB voor de *overdracht* van het bewijs rechtmatig is uitgevaardigd.[19] Met betrekking tot de *vergaring* van het bewijs voorafgaand aan het uitgevaardigde EOB is duidelijk geworden dat de Franse autoriteiten een kennisgeving aan Duitsland hadden moeten sturen over de interceptie van telecommunicatie op Duits grondgebied, waarna de Duitse bevoegde autoriteit had moeten toetsen of deze interceptie in een soortgelijke binnenlandse zaak zou zijn toegestaan. Nu dit beide niet is gebeurd, zal ook hier de interpretatie van het nationale recht van belang zijn voor de (eventuele) gevolgen hiervan voor de Duitse EncroChat-zaken. In theorie is het arrest ook voor Nederland van belang. In tegenstelling tot een eerdere vaststelling van de Hoge Raad blijkt immers dat de rechtsbescherming van artikel 31 EOB-Richtlijn wel degelijk ook op de desbetreffende individuen is gericht en niet enkel op de soevereiniteit van de lidstaat. In de praktijk heeft het onderhavige arrest echter geen directe betekenis voor de EncroChat-zaken in Nederland gezien de Nederlandse betrokkenheid bij de *vergaring* van de data, waardoor enerzijds de beslissingen over de *overdracht* van het bewijs niet van belang zijn en anderzijds artikel 31 EOB-Richtlijn niet van toepassing is.

D.A.G. (Dave) van Toor

Universitair docent straf(proces)recht, Willem Pompe Instituut voor Strafrechtswetenschappen, Universiteit Utrecht

C.M. (Celine) Taylor Parkins-Ozephius

Docent-promovenda straf(proces)recht, Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtsstaat en Rechtspleging, Universiteit Utrecht

[1] J.J. Oerlemans & D.A.G. van Toor, 'Legal Aspects of the EncroChat Operation: A Human Rights Perspective', *European Journal of Crime, Criminal Law and Criminal Justice* 2022, 3-4, p. 309.

[2] Zie Oerlemans & Van Toor 2022 voor meer informatie over de operatie.

[3] Zie hierover uitgebreid D.A.G. van Toor, 'Het gebruik van resultaten uit de EncroChathack in de Duitse strafrechtspleging', *TBS&H* 2022, 2.

[4] *Landgerichte* zijn competent met betrekking tot de zwaardere strafzaken, terwijl de *Amtgerichte* competent zijn lichtere strafzaken (tot een maximumstraf van vier jaar gevangenisstraf) te behandelen.

[5] HvJ EU 2 maart 2021, ECLI:EU:C:2021:152, *Prokuratuur* (HvJ EU, C-746/18) – Differentiatie en beperkingen van dataretentie door telecommunicatieaanbieders en de vorderingsvoorwaarden, *EHRC Updates* maart 2021, m.nt. Van Toor.

[6] Overigens bestaat discussie of de handeling een onlinedoorzoeking (§100b StPO) betreft of interceptie van telecommunicatie aan de *bron* (§100a StPO). Zie bijv. OLG Schleswig, beslissing van 29 april 2021 - 2 Ws 47/21, r.o. II. Voor beide bevoegdheden is een machtiging van de rechter-commissaris (*Richtervorbehalt*) noodzakelijk.

[7] *Staatsanwaltschaft Graz (Dienst voor belastingstrafzaken van Düsseldorf)*, HvJ EU 2 maart 2023, C|16/22, ECLI:EU:C:2023:148, punten 27 en 28.

[8] *Staatsanwaltschaft Wien (Vervalste overschrijvingsopdrachten)*, HvJ EU 8 december 2020, C|584/19, ECLI:EU:C:2020:1002, punten 50 en 51.

[9] Oerlemans & Van Toor 2022; zie ook HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 6.7-6.11.

[10] Vgl. de rechtspraak van het EHRM op dit punt: *Yüksel Yalçinkaya t. Turkije*, EHRM 26 september 2023, zaaknr. 15669/20, ECLI:CE:ECHR:2023:0926JUD001566920, par. 312, *EHRC Updates* september, m.nt. Van Toor & Taylor Parkins-Ozephius.

[11] Zie voor een zaak waarin dat wel het geval was en de invloed daarvan op de beoordeling van verdedigingsrechten: *Yüksel Yalçinkaya t. Turkije*, EHRM 26 september 2023, zaaknr. 15669/20, ECLI:CE:ECHR:2023:0926JUD001566920, *EHRC Updates* september, m.nt. Van Toor & Taylor Parkins-Ozephius.

[12] *Ekro*, HvJ EU 18 januari 1984, 327/82, ECLI:EU:C:1984:11, punt 11, en *Staatsanwaltschaft Wien (Vervalste overschrijvingsopdrachten)*, HvJ EU 8 december 2020, C|584/19, ECLI:EU:C:2020:1002, punt 49.

[13] Het verdient in dit kader opmerking dat ondanks dat de Nederlandse wetgeving en de Hoge Raad in dit kader enkel spreken over het opnemen/aftappen van telecommunicatie en de wettelijke grondslag van de hackbevoegdheid niet in een kennisgevingsverplichting

voorziet – wat zou kunnen worden opgevat als een indicatie dat deze kennisgevingsverplichting niet van toepassing zou zijn op de hackbevoegdheid –, de kennisgevingsverplichting ook onverkort op de hackbevoegdheid van toepassing is. De memorie van toelichting bij de Wet Computercriminaliteit III (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 9-10 & 25) bevestigt dit: een aparte regeling werd niet nodig geacht, nu voor het opnemen van de telecommunicatie (ook na het binnendringen in een geautomatiseerd werk) hoe dan ook een apart bevel vereist is die wel voorziet in deze verplichting.

Tevens lijkt het HvJ EU hiermee een voorschot te nemen op de beslissing onder welke Duitse strafvorderlijke bepaling de opsporingshandeling valt. In rn. 3 en eindnoot 6 berichtten wij over de discussie of de handeling een onlinedoorzoeking is of de interceptie van telecommunicatie aan de bron. Het antwoord dat het HvJ EU op het eerste deel van de vierde vraag geeft, lijkt erop te duiden dat de handeling interceptie aan de bron is.

[14] HR 13 juni 2023, ECLI:NL:HR:2023:913, r.o. 6.23.4.

[15] Vgl. bijvoorbeeld Rb. Gelderland 28 mei 2024, ECLI:NL:RBGEL:2024:3241 inzake EncroChat-data, Rb. Gelderland 4 juli 2024 en Rb. Oost-Brabant 18 juli 2024, ECLI:NL:RBOBR:2024:3404 inzake EncroChat, SkyECC en Anom-data.

[16] Volgens de rechtbank Gelderland (28 mei 2024, ECLI:NL:RBGEL:2024:3241) blijkt dit ook uit de afgegeven machtigingen: “De rechtbank overweegt voorts dat uit de genoemde 126uba en 126t Sv-machtigingen door de rechter-commissaris ook blijkt dat er, mede vanwege de inbreuk op de persoonlijke levenssfeer die gemaakt zou kunnen worden en teneinde de belangen van de verdediging in de zin van artikel 6 EVRM te waarborgen, ten aanzien van Nederlandse gebruikers een extra rechterlijke toetsing naar Nederlandse maatstaven is aangelegd en dat er in dat kader ook (extra) voorwaarden aan de aangekondigde interceptie zijn gesteld. Daarmee is naar het oordeel van de rechtbank materieel voldaan aan hetgeen het Hof van Justitie in het arrest van 30 april 2024 vereist terzake waarborgen voor gebruikers van communicatiemiddelen waarvan interceptie plaatsvindt op het grondgebied van een lidstaat door opsporingsdiensten van een andere lidstaat, zonder technische bijstand van de lidstaat waar die gebruikers zich bevinden.”

[17] Het *Kammergericht* is de naam van de hogere instantie (*Oberlandesgericht*) van specifiek het *Landgericht* Berlijn.

[18] Van Toor 2022, p. 103-104.

[19] Het HvJ EU geeft overigens wel aan dat wanneer het EOB onrechtmatig is, de nationale rechter de verkregen bewijzen niet mag gebruiken als de verdediging geen doeltreffend

commentaar heeft kunnen leveren en het bewijs van doorslaggevende betekenis is (punt 131).