EHRC EUROPEAN HUMAN RIGHTS CASES UPDATES

ANNOTATIE

Yüksel Yalçinkaya t. Turkije (EHRM, 15669/20) – Digitaal bewijs: Unieke kenmerken, unieke toetsing?

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

Annotatie bij Europees Hof voor de Rechten van de Mens, 26-09-2023, ECLI:CE:ECHR:2023:0926JUD001566920 (EHRC-2023-0227)

1. De nasleep van de (vermeende) coup, georganiseerd door aanhangers van Fetullah Gülen (de organisatie wordt *Fetullahçi Terör Örgütü* (FETÖ) genoemd), heeft veel mensenrechtelijke vraagstukken opgeleverd. Al eerder publiceerde *EHRC Updates* annotaties over klachten van mensenrechtenschendingen naar aanleiding van het optreden van de autoriteiten tegen de organisatie en haar leden die verantwoordelijk voor de couppoging zouden zijn. Een stroom van klachten die het Hof heeft bereikt – er zijn nog meer dan 8.000 klachten aanhangig –,[1] heeft betrekking op het gebruik van de smartphone-applicatie *ByLock*.[2] Deze berichtenservice – die gebruik maakt van cryptografie, vergelijkbaar met gangbare services zoals *WhatsApp* en *Signal* – is, volgens de Turkse autoriteiten,[3] speciaal ontwikkeld voor FETÖ (als organisatie). Het (enkel) geïnstalleerd hebben van *ByLock* wordt daarom door de autoriteiten gezien als een duidelijke aanwijzing van betrokkenheid bij de als terroristische organisatie bestempelde beweging rondom Gülen.

2. In de door een van ondergetekenden geannoteerde zaak *Akgun*[4] gaat het om de vraag of het voorarrest van vermeende leden van FETÖ gerechtvaardigd was: meer specifiek over de vraag of het gebruik van de cryptocommunicatieapplicatie *ByLock* bewezen kan worden en, zo ja, of dat voldoende is om een redelijk vermoeden van schuld in de zin van artikel 5 lid 1 sub c EVRM aan te nemen. In de onderhavige zaak gaat het niet om het voorarrest van de klager – net zoals vele andere gearresteerden iemand met een openbare functie, *in casu* een docent –, maar om de *veroordeling* van de klager voor het lidmaatschap van een terroristische

organisatie op basis van het feit dat hij *ByLock* heeft gebruikt. Dat is een duidelijke stap verder dan in de eerdere *ByLock*-zaken. Net zoals in de voorarrest-zaken gaat het in de onderhavige zaak wel alleen over het *gebruik* van de applicatie. Inhoudelijke berichten die via de applicatie zijn uitgewisseld, liggen *niet* ten grondslag aan de veroordeling (par. 311).

3. Op basis van de hierboven genoemde uitspraken is het niet verwonderlijk dat Yalçinkaya klaagt over schending van het Verdrag door de omstandigheden waaronder hij is veroordeeld.[5] De *installatie* van een cryptocommunicatieapplicatie is namelijk onvoldoende gebleken voor het aannemen van een redelijk vermoeden van schuld (*Akgun*, par. 173). Die lijn doorredenerend zou het (met enig gevoel voor *understatement*) verrassend zijn dat het enkele *gebruik* hiervan wel voldoende belastend zou zijn voor een bewezenverklaring van deelname aan een criminele of terroristische organisatie. Yalçinkaya klaagt in de onderhavige zaak in het bijzonder op grond van artikel 6 lid 1 EVRM dat de gegevens met betrekking tot zijn gebruik van de *ByLock*-applicatie, die het doorslaggevende bewijs vormden voor zijn veroordeling, onrechtmatig zijn verkregen en daarom ontoelaatbaar hadden moeten worden verklaard (rns. 4-7).[6] Daarnaast beargumenteert klager dat de relevante gegevens waarop zijn veroordeling berust niet aan hem beschikbaar zijn gesteld om deze te onderzoeken of aan te vechten. Dit is in strijd met het *equality of arms*-beginsel (rns. 8-11). Beide punten – de beoordeling van het gebruik van onrechtmatig verkregen bewijs en het *equality of arms*-beginsel – komen samen in de laatste twee randnummers (rns. 12-13).

4. Alvorens de klachten over schending van artikel 6 EVRM inhoudelijk te behandelen, besteedt het EHRM aandacht aan het bijzondere karakter van digitaal bewijs, waarbij hij zich de vraag stelt of dit karakter een aanpassing vereist van het gebruikelijke toetsingskader voor de beoordeling van het gebruik van onrechtmatig verkregen bewijs. Het EHRM erkent (par. 312) dat digitaal bewijs, zoals de data van de *ByLock*-applicatie, een bijzondere status heeft, vanwege de unieke kenmerken en uitdagingen die het met zich brengt. Digitaal bewijs is immers inherent vatbaarder (in vergelijking met bijvoorbeeld het geheugen van een getuige [7]) voor vernietiging, beschadiging, wijziging of manipulatie. Bovendien kan de complexiteit van de technologie die nodig is voor het verzamelen, beveiligen, verwerken en analyseren van dergelijk bewijs het voor nationale instanties moeilijk maken om de authenticiteit, nauwkeurigheid en integriteit ervan vast te stellen. Desondanks stelt het Hof dat deze factoren geen aanleiding geven om de waarborgen uit artikel 6 lid 1 EVRM strenger of soepeler toe te passen. De kernvraag blijft, ook in deze onderhavige zaak, de vraag naar de *overall fairness of the proceedings* (par. 313). Uit bestendige rechtspraak van het EHRM volgt dat, wanneer klachten over het gebruik van onrechtmatig verkregen bewijs worden ingediend, die vervolgens worden beoordeeld op (i) of de verdediging de authenticiteit van het bewijs kon aanvechten; (ii) de kwaliteit van het bewijs; en (iii) of daarnaast ondersteunend bewijs

aanwezig was.[8]

5. Dat de kwaliteit van het bewijs (en de eventuele afwezigheid van ondersteunend bewijs) van belang zijn bij de beoordeling of het proces in zijn geheel eerlijk is geweest, is vreemd.[9] Met de kwaliteit van het bewijs, in onderlinge samenhang met andere bewijsmiddelen bezien, kan de *waarheidsgetrouwheid* van de aanklacht worden beoordeeld. In hoeverre kan met voldoende mate van zekerheid worden vastgesteld dat de verdachte het ten laste gelegde feit heeft gepleegd? Hoe hoger de (inherente) betrouwbaarheid van een bewijsmiddel of hoe meer verschillende bewijsmiddelen tot dezelfde conclusie leiden des te zekerder kan de rechter zijn in zijn vaststelling daaromtrent. De vaststelling van de waarheid is iets heel anders dan de beoordeling of een proces eerlijk is. De inherente kwaliteit van bewijsmiddelen heeft geenszins invloed op de uitoefening van verdedigingsrechten en op fundamentele belangen van de maatschappij bij onafhankelijke, onpartijdige en openbare rechtspraak. Sommige EHRM-rechters hebben zich in het verleden al kritisch uitgelaten over het vereenzelvigen van waarheidsgetrouwheid en eerlijkheid.[10] Vooralsnog ziet het EHRM geen aanleiding om die bestendige rechtspraak te wijzigen; ook niet als het gaat om digitaal bewijs.

6. Terug naar de kwaliteit van het bewijs. Volgens Yalçinkaya is de betrouwbaarheid van het bewijs in zijn zaak in het geding gekomen door het feit dat de Turkse autoriteiten de *ByLock*-gegevens heimelijk en zonder enige rechterlijke toetsing of andere procedurele waarborgen hebben verzameld (par. 314). Het Hof erkent dat de betrouwbaarheid van het bewijs eerder in twijfel kan worden getrokken wanneer de verzameling of verwerking van dit bewijs niet is onderworpen aan onafhankelijk toezicht, aan rechterlijke toetsing achteraf of als het niet gepaard gaat met andere procedurele waarborgen dan wel bevestigd wordt door ander bewijs (par. 315). De relevante gegevens zijn in de onderhavige zaak op enig moment verzameld door de MIT (de Turkse *national intelligence agency*), waarna deze maandenlang zijn bewaard alvorens deze aan de vervolgende autoriteiten zijn overgedragen. Nu uit de informatie uit het dossier blijkt dat bij het verzamelen van de data geen sprake was van *onafhankelijk toezicht* en feitelijk ook geen rechterlijke toetsing heeft plaatsgevonden voorafgaand aan of tijdens de verkrijging, meent het Hof dat de twijfels van Yalçinkaya over de betrouwbaarheid van het bewijs niet zomaar als ongegrond (of te abstract) hadden mogen worden afgedaan. Overigens laat het EHRM in het midden hoe dat toezicht vorm zou moeten worden gegeven. Dat is een gemiste kans: onafhankelijk toezicht *tijdens* de verkrijging – als dat praktisch is te organiseren – is een waarborg tegen (onbewuste) beschadiging of manipulatie van de bestanden. De toezichthouder zou dan kunnen checken of het bronbestand en het vergaarde bestand identiek zijn.

7. Omdat toezicht in de onderhavige zaak dus ontbreekt, gaat het EHRM over tot analyse van de omstandigheden waaronder de gegevens in beslag zijn genomen en of er maatregelen zijn

genomen door het MIT of de rechterlijke autoriteiten om de betrouwbaarheid van het bewijs te waarborgen (par. 317). Het EHRM meent echter dat hij niet zelf kan beoordelen of de door MIT genomen voorzorgsmaatregelen – o.a. de automatische vergaring, zonder menselijke tussenkomst; de hash-waarde werd vastgesteld voor de overdracht van de gegevens (par. 292-293) – de betrouwbaarheid en integriteit van het bewijs voldoende waarborgen, vooral omdat de nationale instanties deze beoordeling niet hebben uitgevoerd (par. 318). In de nationale procedure is de juistheid van de verkregen *ByLock*-gegevens wel op andere aanvullende manieren getest, waardoor op basis van metadata[11] kon worden geverifieerd dat de telefoon van klager daadwerkelijk verbinding heeft gemaakt met de applicatie (par. 319). De rechtmatigheid, nauwkeurigheid en betrouwbaarheid van deze metadata worden door de klager betwist, maar het Hof acht die argumenten niet voldoende (en niet voldoende specifiek onderbouwd) om de beoordeling van de nationale instanties in twijfel te trekken (par. 320-323). Hoe dan ook, de analyse van de authenticiteit van het digitale bewijs in de onderhavige zaak laat zien dat dit onderzoek anders plaatsvindt en plaats moet vinden dan bij traditioneel bewijs: bij een getuige wordt waarde gehecht aan directe ondervraging ter zitting om de kwaliteit van het bewijs vast te stellen, terwijl bij digitaal bewijs factoren als hash-waarden en verificatie via metadata worden gebruikt. Het valt daarom te betreuren dat het EHRM de kans heeft laten liggen om hierover stelliger een standpunt in te nemen en voorwaarden te scheppen voor onder meer de verkrijging en opslag van digitaal bewijs ten behoeve van de kwaliteitstoets (in aanvulling op de mogelijkheid om het bewijs te betwisten).[12]

8. Het is overigens niet het deel over de kwaliteit van het bewijs uit deze uitspraak waarover in de (Nederlandse) rechtspraktijk al veel te doen is geweest. Direct na publicatie hebben verschillende advocaten, verwijzend naar de onderhavige zaak, verweer gevoerd over de inzage in datasets afkomstig van gekraakte, afgeluisterde of in beslag genomen berichten van cryptocommunicatieaanbieders.[13] Nederlandse advocaten hebben (opportunistisch) geprobeerd de door de Hoge Raad ingezette lijn in *Ennetcom*[14] te wijzigen door te beargumenteren dat de onderhavige zaak een bredere mogelijkheid tot inzage in door de politie verzamelde berichten zou toestaan. Deze verzoeken worden steevast afgewezen: zo verwerpt de rechtbank Gelderland het verweer om inzage in de volledige EncroChat-dataset, omdat die dataset, anders dan de gefilterde dataset, niet van belang is om de betrouwbaarheid van de berichten in de zaak tegen de verdachte te onderzoeken.[15] Vooralsnog heeft het onderstaande arrest op dit punt tot een storm in een glas water geleid.

9. Uit de Nederlandse zaken – en dan gaat het niet alleen om zaken waarin een beroep op het onderhavige arrest is gedaan, maar eigenlijk om alle zaken waarin cryptocommunicatieberichten zijn gebruikt en de verdediging een verzoek tot vergaande inzage in de dataset heeft gedaan – blijkt heel duidelijk dat een onderscheid wordt gemaakt

tussen de ruwe data en de gefilterde data.[16] De ruwe dataset beslaat alle data die in het bezit van de autoriteiten is; dus de berichten van alle gebruikers van een applicatie. De gefilterde data is de data die door de autoriteiten als relevant voor (nog niet nader gespecificeerde) strafrechtelijke onderzoeken wordt bestempeld. Het kan dan bijvoorbeeld gaan om een gefilterde dataset bestaande uit berichten waarin het woord cocaïne is gebruikt. De standaardlijn in de rechtspraak, gebaseerd op *Rook* en *Sigurður Einarsson*, is dat de gefilterde dataset door de verdediging mag worden ingezien en onderzocht en dat (indirecte) inspraak mogelijk is op de samenstelling daarvan.[17]

10. In de onderhavige zaak beargumenteert klager dat hij inzage nodig heeft in de *ruwe* dataset (iets dat op basis van de eerder aangehaalde zaken *Rook* en *Sigurður Einarsson* niet als verplicht onder artikel 6 EVRM wordt gezien) om (i) de betrouwbaarheid en integriteit van de berichten te onderzoeken; (ii) naar ontlastend bewijs te zoeken; en (iii) onderzoek te kunnen verrichten naar de claim van de overheid dat *ByLock* inderdaad een door FETÖ gecreëerde en uitsluitend door hen gebruikte applicatie is (par. 325). Omdat de ruwe dataset, inclusief andere informatie over *ByLock*, is gebruikt om te bewijzen dat alleen FETÖ-leden de applicatie gebruiken en daardoor gebruikers van de applicatie onderdeel uitmaken van de organisatie van FETÖ, overweegt het EHRM dat klager mogelijk inzage moet krijgen in meer data dan alleen de berichten die zien op *zijn* betrokkenheid (par. 328). Hieruit wordt duidelijk dat de aard van de aanklacht – *in casu* deelname aan een terroristische organisatie, waarbij de applicatie onderdeel uitmaakt van de organisatie – invloed heeft in hoeverre inzage in de data moet worden gegeven. Ondanks dat in deze zaak het gebruik van de applicatie onderdeel van de aanklacht is, benadrukt het EHRM dat het inzagerecht niet absoluut is (par. 329). Uiteindelijk moet een *fair balance* worden getroffen tussen de verdedigingsrechten enerzijds en gegronde redenen om inzage te weigeren anderzijds (zoals bijvoorbeeld nationale veiligheid of de bescherming van rechten van derden). Daarbij is het van belang dat over de weigering tot inzage (par. 331) of contra-expertise (par. 333) naar de verdediging (gemotiveerd) wordt gecommuniceerd. Dat is in de onderhavige zaak niet gebeurd: bijna alle verzoeken van de verdediging zijn onbeantwoord gebleven. Dit stilzwijgen wordt door het EHRM als een van de redenen genoemd waarom van voldoende waarborgen voor een daadwerkelijke mogelijkheid om het bewijs te onderzoeken en te betwisten geen sprake is geweest en het proces in zijn geheel niet eerlijk is geweest (par. 341).

11. Hetgeen in randnummer 10 onder (ii) werd genoemd en in de meeste zaken de onderbouwing van het inzageverzoek is, is een verzoek tot het doen van zelfstandig onderzoek in de dataset. Vaak wordt hierbij genoemd dat de verdediging onderzoek wenst te verrichten naar ontlastend materiaal dat zich mogelijk in de dataset bevindt. Hierbij krijgt de verdediging vaak nul op het rekest: dit verzoek wordt veelal afgedaan op basis van een gebrekkige

motivering. Een andere optie via het *equality of arms*-beginsel is het indienen van een verzoek tot het verrichten van onderzoek naar de *aard* van de data. Dat verzoek lijkt op basis van dit arrest kansrijk, mits de resultaten van dat onderzoek bij kunnen dragen aan de beoordeling van de aanklacht. Dat zal wel het geval zijn als het communicatiemiddel – zoals in het onderhavige geval – essentieel is om te bewijzen dat de verdachte deel uitmaakt van een terroristische of criminele organisatie. Wanneer de aanklacht ziet op individuele delicten – zoals handelingen met betrekking tot overtreding van de Opiumwet of geweldsmisdrijven, waarbij de handelingen bewezen kunnen worden door de inhoud van de berichten – ligt het voor de hand dat ook dit verzoek wordt afgewezen.[18] Het verzoek tot nader onderzoek in een dataset naar de aard van de data is een fundamenteel ander verzoek dan hetgeen aan het begin van dit randnummer werd opgemerkt. Het gaat bij dit verzoek enerzijds om het vinden van nog onbekend gebleven, althans niet als zodanig geïdentificeerd, bewijs dat ontlastend kan werken – en waarvan dus de *inhoud* van het gegeven essentieel is – en anderzijds om het verrichten van onderzoek naar de kwaliteit van een gegeven. Bij dat laatste wordt de inhoud van het gegeven ter discussie gesteld door onderzoek te verrichten naar de inherente kwaliteit van het gegeven op basis van de *cia-triad*: is het gegeven vertrouwelijk (*confidential*) behandeld?; is het gegeven integer, in de zin van niet gemanipuleerd?; is het gegeven toegankelijk (*available*)?

12. Het zijn juist deze (en andere) aspecten van een gegeven (die kunnen worden gebruikt in een digitaal forensische analyse) die een andere invulling van het toetsingskader rechtvaardigen, althans waardoor de beoordeling van de kwaliteit van het bewijs in het licht van het overige bewijs overbodig is. Indien de verdediging in staat wordt gesteld om op basis van deze aspecten de authenticiteit van het bewijs aan te vechten is voldaan aan het eerste criterium (rn. 4). De kwaliteit van het digitale bewijs kan vervolgens worden getoetst door de inherente betrouwbaarheid van een gegeven vast te stellen op basis van de eigenschappen van het gegeven; een digitaal bestand heeft *inherente* kwaliteiten waardoor kan worden beoordeeld dat het bestand niet is gewijzigd, beschadigd of gemanipuleerd sinds de verkrijging. Dat is anders bij een getuige: er bestaat geen hersenonderzoek waarmee kan worden vastgesteld dat de getuige zich al dan niet bewust of onbewust heeft laten beïnvloeden bij het aanmaken, opslaan of reproduceren van een herinnering. Bij getuigenverklaringen is het daarom van essentieel belang om de feiten en omstandigheden waarover een getuige verklaart te verankeren in ondersteunend bewijs. Bij digitaal bewijs waarvan de inherente betrouwbaarheid is vastgesteld, is deze stap niet meer nodig om de kwaliteit van het bewijs vast te stellen. Het is daarom verrassend dat, zoals in randnummer 4 is besproken, het EHRM het opgestelde toetsingskader onverkort van toepassing verklaart op digitaal bewijs (terwijl hij zelf wel opmerkt dat digitaal bewijs unieke eigenschappen heeft).

13. We ronden af: Een aantal punten uit dit arrest – naast het grote aantal *dissents* – valt op. Ten eerste hinkt het EHRM nog op twee gedachten met betrekking tot het toetsingskader bij gebruik van digitaal bewijs. Enerzijds wordt terecht benoemd dat digitaal bewijs anders is dan traditioneel bewijs, terwijl anderzijds het traditionele toetsingskader wel onverkort van toepassing wordt verklaard. Het zou meer recht doen aan het bijzondere karakter van digitaal bewijs en aan het creëren van een daadwerkelijke mogelijkheid om het bewijs op betrouwbaarheid te onderzoeken om aspecten in de verslaglegging te verplichten zodat de *inherente* kwaliteit van digitaal bewijs te allen tijde kan worden beoordeeld. Ook de *dissenters* Ravarani en anderen benadrukken dit punt: het EHRM had de zaak kunnen beoordelen in het licht van de minimumeisen die worden gesteld aan de beoordeling van bewijs, namelijk of die beoordeling arbitrair of overduidelijk onredelijk is. Als volledig voorbij wordt gegaan aan digitaal forensische analyse, terwijl de veroordeling volledig berust op digitaal bewijs, dan is die beoordeling volgens ons evident onredelijk. Ten tweede valt op dat het laatste over inzage in datasets nog niet is gezegd of geschreven. Op basis van eerdere zaken leek te kunnen worden geconcludeerd dat de ruwe data niet behoort tot de categorie relevante stukken waartoe de verdediging het recht tot inzage kan ontlenen. In de onderhavige zaak lijkt aanleiding te kunnen worden gevonden om daarover anders te beslissen als de applicatie als middel – en dus niet de individuele inhoudelijke chatberichten – van belang is voor de beoordeling van de aanklacht.

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] Zie de gedeeltelijk *dissenting opinion* van Schembri Orland bij onderhavig arrest, rn. 11.

[2] Zie bijvoorbeeld: *Aydin Sefa Akay t. Turkije*, EHRM 23 april 2024, NR. 59/17, ECLI:CE:ECHR:2024:0423JUD0000005917); *Parildak* t. *Turkije*, EHRM 19 maart 2024, nr. 66375/17 ECLI:CE:ECHR:2024:0319JUD006637517; *Telek e.a. t. Turkije*, nrs. 66763/17, 66767/17 en 15891/18, EHRM 21 maart 2023, ECLI:CE:ECHR:2023:0321JUD006676317.

[3] Anders: Fox-IT, *Expert Witness Report on ByLock Investigation*, Delft: FoxIT 2017.

[4] *Akgün* t. *Turkije*, EHRM 20 juli 2021, nr. 19699/18, ECLI:CE:ECHR:2021:0720JUD001969918,– Het gebruik van een cryptocommunicatieapplicatie als voldoende grond voor een redelijk vermoeden van schuld, «EHRC Updates» april 2022, m.nt. Van Toor.

[5] We bespreken in deze annotatie alleen de klachten betreffende artikel 6 EVRM.

[6] Overigens is dit een standpunt dat door klagers vaker, maar altijd zonder succes, naar voren is gebracht. Zie bijv. *Rusu t. Roemenië*, EHRM 31 oktober 2017, nr. 22767/08, ECLI:CE:ECHR:2017:1031JUD002276708, «EHRC Updates» 2018/13, m.nt. Van Toor.

[7] Zie bijv. het nieuwsbericht over de professionele standaard voor het horen van getuigen. 'Rechtspsycholoog Annelies Vredeveldt: 'Geheugen is geen videocamera'. https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Rechtspsycholoog-Annelies-Vredeveldt-Geheugen-is-geen-videocamera.aspx.

[8] Bijv. *Bykov t. Rusland*, EHRM 10 maart 2009 (GK), nr. 4378/02, ECLI:CE:ECHR:2009:0310JUD000437802, «EHRC» 2009/69 m.nt. Ölçer.

[9] Van Toor schreef al vaker kritisch over het gebruiken van kwaliteitseisen in eerlijkheidsbeoordelingen. Zie *Rusu t. Roemenië*, EHRM 31 oktober 2017, nr. 22767/08, ECLI:CE:ECHR:2017:1031JUD002276708, «EHRC Updates» 2018/13, m.nt. Van Toor; *Ćwik* t. *Polen***,** EHRM 5 november 2020, nr. 31454/10, ECLI:CE:ECHR:2020:1105JUD003145410 – Bewijsuitsluiting na schending art. 3 EVRM, in het bijzonder bij onrechtmatigheid door andere burgers, EHRC Updates december 2022, m.nt. Van Toor.

[10] Zie de *dissenting opinions* van Loucaides (onder *Khan t. Verenigd Koninkrijk*), Tulkens (onder *P.G. & J.H. t. Verenigd Koninkrijk*), Spielmann (onder *Bykov t. Rusland*) en Rozakis, Tulkens, Jebens, Ziemele, Bianku en Power (over de doelredenering onder *Gäfgen t. Duitsland*).

[11] Deze metadata bestond uit CGNAT-data en HTS-records. CGNAT-data (*Carrier-Grade Network Address Translation data*) verwijst naar gegevens die worden gebruikt om netwerkverkeer van verschillende apparaten te beheren en te monitoren. Deze data maakt het mogelijk om te achterhalen welke gebruiker gekoppeld is aan een dynamisch en/of gedeeld IP-adres op een specifiek moment, ondanks dat meerdere gebruikers hetzelfde publieke IP-adres delen. HTS-records (*Historical Traffic Data records*) zijn gegevens die inzicht geven in

het communicatieverkeer van een specifieke gebruiker over een bepaalde periode.

[12] Vgl. de benadering van de Grote Kamer van het EHRM in de navolgende zaken: in deze zaken staan bulkinterceptie door inlichtingen- en veiligheidsdiensten en het recht op privacy ex. artikel 8 EVRM centraal. In deze arresten heeft het EHRM de nodige duidelijkheid verschaft met betrekking tot onder andere procedures en de wijze waarop met digitaal materiaal omgegaan moet worden door zelfs acht minimumwaarborgen voor deze specifieke situatie te schetsen: *Big Brother Watch t. Verenigd Koninkrijk*, EHRM 25 mei 2021, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, «EHRC Updates» september 2021, m.nt. Hagens en Oerlemans; *Centrum för Rättvisa* t. *Zweden*, EHRM 25 mei 2021, nr. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, «EHRC Updates» september 2021, m.nt. Hagens en Oerlemans.

[13] Een simpele zoekslag (d.d. 14 augustus 2024) naar *Yalçinkaya*, en als filter het rechtsgebied strafrecht, op rechtspraak.nl levert dertien hits op. Twaalf van deze zaken gaan over inzage in datasets.

[14] HR 28 juni 2022, ECLI:NL:HR:2022:900. Ook in EncroChat-zaken worden de verzoeken tot vergaande inzage afgewezen; zie 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* (30) 2022, p. 310-329.

[15] Rb. Gelderland 28 mei 2024, ECLI:NL:RBGEL:2024:3241.

[16] Zie voor gedetailleerde uiteenzetting over de verschillende soorten datasets: M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines: een suggesties voor uitbreiding', *BSb* 2021, 2.

[17] *Rook t. Duitsland*, EHRM 25 juli 2019, nr. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615, *Rook* t. *Duitsland*; *Sigurður Einarsson en anderen* t. *Ijsland*, EHRM 4 juni 2019, nr. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715.

[18] Zie bijv. Rb. Limburg 4 maart 2024, ECLI:NL:RBLIM:2024:1310: 'De verdediging heeft daarnaast op geen enkele wijze concreet onderbouwd waarom de beantwoording van de door de verdediging gestelde vragen omtrent de betrokkenheid van Europol en de beweerde ontbrekende of achtergehouden data van belang is voor enige door de rechtbank in deze concrete strafzaak te nemen beslissing'.