Eindelijk toegang tot datasets

(Erg) langzaam maar zeker naar een nieuw normaal

Desiree de Jonge & Sander Janssen[1]

Na de inbeslagneming van dataservers van Ennetcom in april 2016 deed een nieuw fenomeen zijn intrede in de Nederlandse strafrechtspleging: PGP-data. Oftewel de versleutelde inhoud van e-mailaccounts die de opsporing wist te ontsleutelen. In een snel toenemend aantal zaken wordt het door het Openbaar Ministerie gepresenteerde bewijs in doorslaggevende mate gebaseerd op een selectie van dergelijke data, terwijl de volledige datasets niet aan de verdediging worden verstrekt. Het toepassen van bestaande wetgeving, jurisprudentie en in de praktijk ontwikkelde uitgangspunten uit een tijd waarin in het geheel nog niet voorzienbaar was dat technologische ontwikkelingen zouden leiden tot dit type bewijsvoering staat inmiddels op gespannen voet met de adequate mogelijkheden die ook de verdediging moet hebben om die data in te zien, te onderzoeken en daaruit te selecteren wat ter verdediging van belang wordt geacht. Er zal een einde moeten worden gemaakt aan de sinds de introductie van dit fenomeen ontstane systemische ongelijkheid. Het Gerechtshof Arnhem-Leeuwarden nam in het onderzoek Bosnië-Brandberg na diverse eerdere verzoeken van de verdediging op 1 juli 2021 een baanbrekende beslissing die navolging verdient.

Inleiding

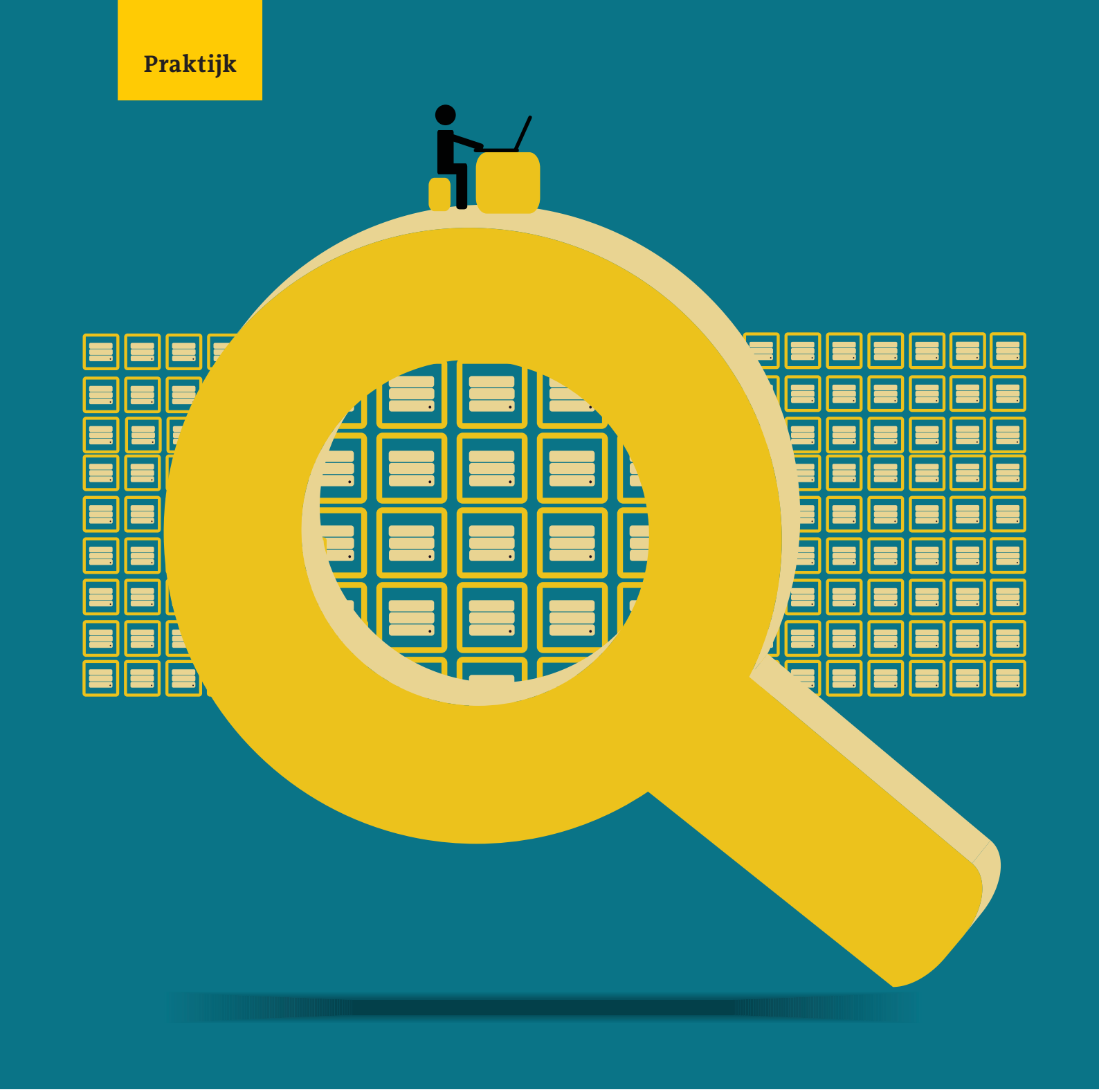
Ruim vijf jaar na de spraakmakende inbeslagname van serverdata van versleutelde berichtendienst Ennetcom en daarop gebaseerde uitgebreide opsporingsonderzoeken en strafvervolgingen waarin zeer langdurige gevangenisstraffen zijn geëist én opgelegd, moet worden geconstateerd dat er nog altijd geen sprake is van een effectieve inzagemodaliteit voor de verdediging. Het evenwicht tussen de mogelijkheden voor opsporing en verdediging om die data te onderzoeken is zoek, zo niet illusoir. Na aandringen van de verdediging en met de geplande inhoudelijke behandeling in hoger beroep van het liquidatieproces met de onderzoeksnaam Bosnië-Brandberg in zicht, kwam het Gerechtshof Arnhem-Leeuwarden op 1 juli 2021 tot een in de Nederlandse strafrechtspleging nog niet eerder genomen beslissing: de in dit onderzoek samengestelde datasets moeten voorzien van de benodigde software door het Openbaar Ministerie ter beschikking worden gesteld aan de verdediging. Een belangrijke doorbraak, maar wel eentje die komt in een zeer laat stadium in deze procedure en terwijl in diverse andere zaken al vonnissen en zelfs arresten zijn gewezen. In het licht van de centrale positie van deze versleutelde data in de verschillende bewijsconstructies dringt de vraag zich op of het uitgangspunt niet allang had moeten zijn dat datasets tijdig en actief aan de verdediging ter beschikking worden gesteld ter waarborging van het recht op een eerlijk proces, zoals in die zaken overigens ook regelmatig door de verdediging is gevraagd. In deze bijdrage komen wij tot een bevestigend antwoord op die vraag.

De intrede van versleutelde data in de Nederlandse strafrechtspleging

Na de inbeslagneming van dataservers van Ennetcom in april 2016 deed een nieuw fenomeen zijn intrede in de Nederlandse strafrechtspleging: PGP-data. Oftewel de middels 'Pretty Good Privacy'-software versleutelde inhoud van e-mailaccounts die (gedeeltelijk) bewaard bleek te zijn en waarvan de opsporing er gaandeweg in slaagde die te

Auteurs

1. Mr. D.N. de Jonge en mr. S.L.J. Janssen zijn beiden strafrechtadvocaat bij Cleerdin & Hamer Advocaten in Rotterdam. De tweede auteur is raadsman in de zaak *Bosnië-Brandberg* waarnaar wordt verwezen.



© Shutterstock

ontsleutelen. Sindsdien worden in toenemende mate omvangrijke strafzaken behandeld waarin opsporing voornamelijk heeft plaatsgevonden door analyse van grote hoeveelheden PGP-data en andere versleutelingsvarianten. Ennetcom bleek niet de enige versleutelde berichtendienst, ook PGP-Safe, Ironchat, Encrochat en Sky ECC kwamen in beeld als communicatienetwerken die een belangrijke rol vervulden in voornamelijk de zware, georganiseerde criminaliteit. Ook de data van die aanbieders worden onderzocht, welk onderzoek een scala aan potentiële bewijsmiddelen oplevert. Het varieert daarbij van bewijsmiddelen die nét nog nodig zijn om een volledig beeld te krijgen van strafbare feiten waarvoor op basis van ander bewijs al werd vervolgd, tot bewijsmiddelen die zicht geven op strafbare feiten en verdachten die zonder die data waarschijnlijk nooit bij politie en justitie in zicht zouden zijn gekomen.[2]

Zonder overdrijving kan worden gesteld dat nu en in de (nabije) toekomst in bijzonder veel zaken het door het Openbaar Ministerie gepresenteerde bewijs in doorslaggevende mate zal worden gebaseerd op dergelijke data en 'klassieke' bewijsmiddelen zoals getuigenverklaringen nog slechts een ondersteunende rol zullen spelen. Als gevolg daarvan worden strafzaken gedomineerd door discussies over de verkrijging, betrouwbaarheid en interpretatie van die data en over de in de processtukken gepresenteerde selectie daarvan. Die data zijn waar een verdachte zich tegen heeft te verdedigen. De vraag is of met toepassing van bestaande wetgeving, jurisprudentie en in de praktijk ontwikkelde uitgangspunten uit een tijd waarin in het

Een rechter in het EHRM signaleert terecht dat in dit type zaken op het kruispunt van nieuwe technologieën en bewijskwesties gecompliceerde vragen over *equality of arms* opdoemen

geheel nog niet voorzienbaar was dat technologische ontwikkelingen zouden leiden tot dit type bewijsvoering daartoe voldoende adequate mogelijkheden bestaan, of de complexiteit van de verdedigingspositie voldoende wordt erkend en wordt gewaarborgd dat tussen procespartijen geen ongelijke positie ontstaat. Een rechter in het EHRM signaleert terecht dat in dit type zaken op het kruispunt van nieuwe technologieën en bewijskwesties gecompliceerde vragen over *equality of arms* opdoemen en hij stelt dat *'the assumption that standard rules of disclosure ought to apply unchanged in this context is one that, at the very least, needs to be tested'.*[3]

Tot nu toe werd in alle zaken echter vastgehouden aan de standaard Nederlandse *disclosure*-route. De processtukken die aan de rechterlijke macht en verdediging worden verstrekt bestaan voornamelijk uit processen-verbaal van bevindingen met verslaglegging en interpretatie van een selectie van die data. Die selectie komt weer uit een samengestelde dataset waarin de resultaten zitten van door de opsporing gebruikte selectiecriteria. Zo'n dataset behelst een samenstel van relevant geachte communicatielijnen van potentiële verdachten, die uiteraard ook nog moeten worden geïdentificeerd als de gebruiker van het desbetreffende e-mailadres. Dit hele proces vindt doorgaans plaats voordat een verdachte wordt aangehouden en daarmee buiten zicht en zonder inspraak van de verdediging.

Ook na de aanhouding wordt de dataset niet verstrekt. Het dossier bestaat uit processen-verbaal met daarin relevant geachte ontsleutelde e-mailberichten en opgeslagen notities, veelal met een beschrijving van hoe die inhoud geïnterpreteerd moet worden of past bij overige onderzoeksbevindingen. Per definitie zijn de stukken zoals rechters en de verdediging die onder ogen krijgen daarmee een selectie van een selectie van de volledig veiliggestelde data van een server, welke data overigens in zichzelf weer niet volledig zijn.[4] Zonder inzage in het totaal lijkt niet altijd sprake te zijn van voldoende bewustheid dat het dus gaat om een (zeer) gefragmenteerde weergave. Kennisneming van meer data kan bijvoorbeeld zicht geven op mogelijke onderliggende conflicten waaruit strafbare feiten zijn voortgekomen, motieven voor het plegen van die feiten door anderen dan de verdachte en de mate van betrokkenheid van anderen. Een selectieve weergave maakt dat er reële risico's zijn dat informatie die relevant kan zijn voor de beoordeling van het gepresenteerde bewijs ontbreekt. De verdediging kan een bijdrage leveren door informatie aan het dossier toe te voegen die vanuit verdedigingsperspectief van belang wordt geacht, maar zal zich dus actief moeten opstellen om toegang te krijgen tot meer materiaal dan alleen de processtukken.

Inzagerecht, een Europeesrechtelijk perspectief

De in het recht op een eerlijk proces besloten liggende mogelijkheid het door het Openbaar Ministerie gepresenteerde bewijs te betwisten en daarbij feiten en omstandigheden die de verdediging voor de beoordeling van de zaak van belang acht te kunnen betrekken,[5] is een lege huls wanneer niet onderzocht zou mogen worden of die feiten en omstandigheden gevonden kunnen worden in materiaal waarover het Openbaar Ministerie beschikt en – in het geval van een dataset –door toepassing van door de opsporing relevant geachte selectiecriteria naar boven is gekomen. Hoewel door het Openbaar Ministerie inmiddels mondjesmaat wordt erkend dat de verdediging een inzagemogelijkheid moet worden geboden in de zaaksspecifieke dataset, bijvoorbeeld indien daartoe op basis van artikel 34 lid 2 Sv een verzoek wordt gedaan, moet worden geconstateerd dat inzage niet actief wordt gefaciliteerd en een inzagerecht niet in alle gevallen wordt erkend. Ook in de rechtspraak wordt daarin geen consistente lijn gehanteerd. Waar de Rechtbank Amsterdam recent in de zaak *Marengo* met zo veel woorden stelt dat de verdediging een recht op inzage heeft, zodat beoordeeld kan worden of er specifieke berichten zijn die zij toegevoegd zou willen zien aan de processtukken,[6] wees een Haagse rechter-commissaris in een zaak waarin Encrochat centraal staat een dergelijk verzoek nog als onvoldoende onderbouwd af nadat het Openbaar Ministerie zich verzette omdat er geen verdedigingsbelang zou bestaan.[7]

Noten

2. Denk aan strafbare voorbereidingshandelingen, maar ook aan opdrachtgevers van strafbare feiten die bij de uitvoering volledig buiten beeld blijven.

3. *Partly dissenting opinion* van rechter D. Pavli bij EHRM 4 juni 2019, nr. 39757/15 (*Sigurdur Einarsson e.a./IJsland*). Hier wordt ook nadrukkelijk aandacht voor gevraagd in: M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *Boom Strafblad*, 2021-2, p. 41-49.

4. Niet de volledige inhoud van PGP-accounts is op de servers bewaard gebleven en voorts is de mogelijkheid van ontsleuteling van meer veiliggestelde data afhankelijk gebleken van technologische ontwikkelingen van forensische zoekmachine Hansken. Zie Rb. Gelderland 26 juni 2019, ECLI:NL:RBGEL:2019:2833 waarin wordt verwezen naar een door een update van Hansken verkregen nadere dataset, waarvan de bruikbaarheid ter discussie werd gesteld wegens de incompleetheid van gegevens.

5. EHRM 16 februari 2000, nr. 27052/95 (*Jasper/het Verenigd Koninkrijk*); EHRM 16 februari 2000, nr. 28901/95 (*Rowe and Davis/het Verenigd Koninkrijk*); EHRM 24 april 2007, nr. 40412/98 (*V./Finland*).

6. Rb. Amsterdam 1 april 2021, ECLI:NL:RBAMS:2021:1507 en zie op min of meer vergelijkbare wijze Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113 waarin werd verzocht om inzage in datasets samengesteld in de zaken van medeverdachten die eveneens werden verdacht van deelname aan een criminele organisatie en de rechtbank ondanks verzet van het Openbaar Ministerie oordeelde dat de verdediging ook in die datasets inzage moet kunnen hebben.

7. Beschikking rechter-commissaris Rb. Den Haag, 25 augustus 2021, ECLI:NL:RBDHA:9368.

Het omvangrijke moderniseringsproject van het Wetboek van Strafvordering lijkt op dit punt helaas geen verbetering te brengen

De enige in het Wetboek van Strafvordering te vinden bepaling waarop de verdediging zich kan beroepen om inzage te krijgen is artikel 34 lid 2 Sv. Bezwaarlijk aan die bepaling is dat die inzage kan worden geweigerd indien de officier van justitie meent dat geen sprake is van processtukken. Ons wetboek loopt daarmee niet alleen achter op de ontwikkelingen van de afgelopen jaren maar ook op – bijvoorbeeld – de IJslandse wet, waarin met zoveel worden wordt bepaald dat de verdediging zo spoedig mogelijk een afschrift van processtukken moet krijgen, *alsmede faciliteiten om ander materiaal te onderzoeken*. Dat kan worden geweigerd wegens zwaarwegende (opsporings)belangen, maar niet wegens niet-relevantie van dat materiaal.[8] Het omvangrijke moderniseringsproject van het Wetboek van Strafvordering lijkt op dit punt helaas geen verbetering te brengen.

Een inzagerecht kan echter wel aan Europeesrechtelijke jurisprudentie worden ontleend.[9] Het EHRM beziet deze problematiek binnen de context van het recht op een eerlijk proces en stelt voorop dat niet alleen de mogelijkheid moet bestaan om kennis te kunnen nemen van direct bewijs dat ziet op tenlastegelegde gebeurtenissen, maar ook moet worden voorzien in toegang tot gegevens die van belang zijn voor de beoordeling van de *toelaatbaarheid, betrouwbaarheid en compleetheid* van aangeleverd bewijs.[10] Het gaat niet enkel om materiaal dat mogelijk relevant kan zijn voor de beslissing of de verdachte schuldig of onschuldig is, maar ook informatie die ziet op de mate van betrokkenheid en – zo volgt uit de uitspraak *Natunen/Finland* uit 2009 – op de op te leggen straf moet inzichtelijk zijn geweest.[11] In diezelfde uitspraak oordeelde het EHRM dat een procedure waarbij de opsporings- en vervolgende autoriteiten zélf proberen te beoordelen wat voor een verdachte en zijn verdediging mogelijk wel en niet relevant is, in zichzelf niet voldoet aan de eisen van artikel 6 lid 1 EVRM. Dat is niet anders indien op grond van de nationale regelgeving de vervolgende autoriteit verplicht is zowel het belastende als het ontlastende bewijs aan het dossier toe te voegen, zoals in Nederland het geval is.[12]

Het inzagerecht vloeit hieruit voort, nu politie en justitie anders *de facto* wel dat monopolie op de beoordeling van de relevantie van onderzoeksmateriaal en de samenstelling van de processtukken hebben. Deze uitgangspunten zijn recenter, in 2019, nog eens herhaald in de uitspraak *Rook/Duitsland* waarin het ging om het faciliteren van toegang tot grote hoeveelheden data.[13] Bij de vraag of de verdediging voldoende in de gelegenheid is gesteld inspraak te hebben bij de samenstelling van het dossier, wordt betrokken of kennis kon worden genomen van materiaal waar de verdediging zelf niet over kon beschikken. Het EHRM ziet die kennisname en de daarmee ontstane mogelijkheid om vervolgens onderbouwd te verzoeken tot toevoeging van gegevens aan het dossier als onderdeel van het in artikel 6 lid 3 onder b EVRM aan een verdachte en aan de verdediging gegarandeerde recht 'te beschikken over de tijd en faciliteiten die nodig zijn voor de voorbereiding van zijn verdediging.'[14]

Geboden inzagemodaliteiten

Het onderzoeksmateriaal afkomstig uit in beslag genomen versleutelde communicatie dat in de verschillende onderzoeken wordt ingebracht wordt als gezegd de dataset genoemd. Het gaat dan om de selectie die de opsporing al dan niet na toestemming van de rechter-commissaris uit het totale databestand van een aanbieder door het NFI aangeleverd krijgt. De opsporing kan die selectie vervolgens vanaf het eigen (politie)bureau doorzoeken middels het daartoe (verder) ontwikkelde programma Hansken en maakt vervolgens uit die dataset een selectie die in processen-verbaal wordt neergelegd. In die processen-verbaal wordt bijvoorbeeld de identificatie van een verdachte of de relevante communicatie rondom een strafbaar feit gerelateerd, en dat is wat rechters en advocaten vervolgens aangeleverd krijgen. Tot zo ver weinig nieuws: het is altijd al zo dat in het procesdossier dat wordt verspreid processen-verbaal staan opgenomen waarin de bevindingen van onderzoekshandelingen zijn neergelegd en het bronmateriaal dat in die processen-verbaal wordt beschreven wordt vaker niet dan wel bijgevoegd. Op het moment dat je als verdediging echter aangeeft dat te willen controleren, bijvoorbeeld door tapgesprekken of getuigenverhoren na te luisteren of van zendmastgegevens of ANPR-lijsten te mogen kennisnemen, dan wordt daar zeker de laatste jaren vrijwel altijd in voorzien.

Ook in het geval van versleutelde data wordt in veel zaken inmiddels erkend dat de verdediging – op verzoek – in ieder geval in de gelegenheid moet worden gesteld inzage te doen in de aan de verdachte toegeschreven communicatielijn(en) en doorgaans ook in de dataset van het onderzoek. Waar het voornamelijk wringt is in de wijze waarop die inzagemogelijkheden door het Openbaar Ministerie praktisch gezien worden ingevuld enerzijds en het feit dat daar ondanks veelvuldig geuite bezwaren vanuit de verdediging door rechters steeds genoegen mee wordt genomen anderzijds. Een blik op recente(re) gepubliceerde beslissingen en eigen ervaringen leert dat de tot nu toe geboden inzagemodaliteiten grofweg kunnen worden onderscheiden in twee varianten: inzage in de gehele dataset van een zaak, en inzage door verstrekking van de door het Openbaar Ministerie aan de verdachte toegeschreven berichten, ook wel aangeduid als de 'eigen PGP-lijnen', meestal in een omvangrijk Excel-bestand.

Voor inzage in de dataset moet de verdediging naar het NFI in Rijswijk, waar middels het genoemde programma Hansken kennis kan worden genomen van de ontsleutelde inhoud van e-mailaccounts maar ook van de metadata. Een geavanceerd zoekprogramma is bij de hoeveelheid data waar het in dit type onderzoeken om gaat in feite noodzakelijk om de te onderzoeken onderdelen tot behapbare proporties terug te brengen en relevant materiaal daarin te kunnen onderkennen.[15] Hansken kent tal van selectietools zodat – bijvoorbeeld – de inzage kan worden beperkt tot een mogelijk relevante periode, of tot

alleen de notities of contactenlijsten van accounts. Ook de verdediging kan – na enige instructie – daarvan gebruik maken en zoekslagen in de dataset doen.

Dat maakt niet dat op deze wijze op een efficiënte of zelfs maar zinvolle manier kennis kan worden genomen van de dataset. Nog los van het gegeven dat op het moment dat de verdediging begint met zoeken door de opsporingsautoriteiten met een grote hoeveelheid tijd, mankracht, kennis van het materiaal en onderzoeksmethoden al maanden, zo niet jaren, onderzoek is gedaan in diezelfde data en er per definitie een nauwelijks nog te overbruggen achterstand is ontstaan,[16] is het de verdediging bij zo een inzage niet toegestaan informatie te printen of op te slaan. Het vergt dus nauwgezette aantekeningen om vast te leggen welke berichten in die enorme berg data zijn gevonden en vooral waar deze zijn gevonden om deze op een later moment, bijvoorbeeld wanneer iets voorbijkomt dat bij die berichten lijkt aan te sluiten, terug te kunnen vinden. Andere dossierstukken, notities, samenvattingen, aantekeningen et cetera die de verdediging op kantoor heeft kunnen daar niet bij worden betrokken. En wellicht het belangrijkste bezwaar: deze inzagemogelijkheid kan niet tezamen met de (vaak gedetineerde) verdachte worden benut en de resultaten van het onderzoek kunnen dan ook niet op zinvolle wijze worden besproken tussen advocaat en de cliënt die niet bij het NFI aanwezig kan zijn. De cliënt zal dus alles uit tweede hand moeten vernemen. Dit terwijl die cliënt – de verdachte – in bepaalde zaken veel beter in staat kan worden geacht de relevantie of portee van bepaalde communicatie in te schatten dan de advocaat. Inzage kan bovendien alleen op afspraak en binnen de openingstijden van het NFI gedaan worden. Tot slot is van belang dat een strafrechtelijk onderzoek een dynamisch proces is, waardoor er in elk stadium, bij elke dossieraanvulling, na elke cliëntbespreking of anderszins verkregen informatie, belangen kunnen ontstaan die dataset te raadplegen, of dat nog eens opnieuw te doen. Het moeten afreizen naar het NFI beperkt de mogelijkheid daartoe.

Het verstrekt kunnen krijgen van de 'eigen PGP-lijnen' heeft als voordeel dat deze doorgaans ook aan de gedetineerde verdachte op een laptop kunnen worden verstrekt en dat de verdediging daar naar eigen inzicht en planning mee kan omgaan. De berichten worden echter omgezet in een Excel-bestand, wat de overzichtelijkheid en doorzoekbaarheid bepaald niet ten goede komt (dat is een understatement). Voorts wordt met de 'eigen PGP-lijnen' vaak maar een deel van de communicatie die met een bepaald account heeft plaatsgevonden verstrekt omdat die communicatie als gevolg van de structuur van de verkregen data vaak niet in het aan de verdachte toegeschreven account is aangetroffen, maar in een ander account van een al dan niet geïdentificeerde medeverdachte. Bovendien spreekt die medeverdachte dan weer met derden over zijn contacten met het aan de verdachte toegeschreven account en juist die communicatie met derden kan bijdragen aan het inzichtelijk krijgen van de juiste context waarbinnen gebeurtenissen zich hebben afgespeeld.

Een effectieve inzagemogelijkheid zou nu juist moeten voorzien in het kunnen bekijken en onderzoeken van gegevens die van belang kunnen zijn voor de vraag of de

Door het NFI werd er vanaf de ontwikkeling van Hansken in 2012 al rekening mee gehouden dat ook voor de verdediging inzage mogelijk zou moeten zijn. Tot *remote access* tot de data voor de advocatuur is het echter – bijna tien jaar na de ontwikkeling van de zoekmachine – nog steeds niet gekomen

8. Zie daarvoor de relevant domestic law zoals weergegeven in de zaak EHRM 4 juni 2019, nr. 39757/15 (*Sigurdur Einarsson e.a./IJsland*). De weigering die faciliteiten te bieden kan voorts ter beoordeling worden verwezen naar de rechtbank, een belangrijke procedurele waarborg.

9. Zo ook B. de Wilde e.a., *Digitale informatie in het strafproces - De noodzaak van aanpassing van strafvorderlijke wetgeving*, WODC, 2019, p. 68 waarin de rapporteurs stellen: *'Uit EHRM-jurisprudentie lijkt een recht om kennis te nemen van de meest directe bron voort te vloeien. Die kennisneming is van belang om de bronnen waarop het bewijs direct is gebaseerd effectief te kunnen betwisten.'* Zie hierover ook uitgebreid D.N. de Jonge, *Verdedigen in tijden van digitale bewijsvoering*, in: *Aan de slag, Liber Amicorum Gerard Hamer*, Sdu, 2018, p. 151.

10. EHRM 11 december 2008, nr. 6293/04 (*Mirilashvili/Rusland*).

11. EHRM 31 maart 2009, nr. 21022/04 (*Natunen/Finland*): *'Failure to disclose to the defence material evidence, which contains such particulars which could enable the accused to exonerate himself or have his sentence reduced would constitute a refusal of facilities necessary for the preparation of the defence.'*

12. Idem, par. 47: *'Even though the police and the prosecutor were obliged by law to take into consideration both the facts for and against the suspect, a procedure whereby the investigating authority itself, even when co-operating with the prosecution, attempts to assess what may or may not be relevant to the case, cannot comply with the requirements of Article 6 § 1.'*

13. EHRM 25 juli 2019, nr. 1586/15 (*Rook/Duitsland*).

14. EHRM 4 april 2017, nr. 2742/12 (*Matanovic/Kroatië*).

15. In onderzoek *Marengo* bestaat de dataset bijvoorbeeld uit bijna één miljoen berichten. In het genoemde onderzoek *Bosnië-Brandberg* is de dataset recent in pdf-versie verstrekt en beslaat in die vorm ruim 20.000 pagina's.

16. Zie daarover de in voetnoot 2 genoemde partly dissenting opinion: *'(…) even where the defence benefits from substantial access, the prosecution still holds distinct advantages: it will normally have had a longer period of time to analyse the evidence, generally greater analytical resources, and more intimate knowledge of the material, including in relation to any exculpatory elements. In view of these considerations, the current majority's conclusion that the prosecution "did not hold any advantage over the defence" in the circumstances of the current case (see paragraph 90) seems rather far-fetched.'*

in het dossier gemaakte selectie en interpretatie van berichten van aan de verdachte toegeschreven berichten betrouwbaar is én of er andere data zijn die een volledi-ger beeld geven. Dat kan niet alleen van groot belang zijn voor (de betwisting van) de identificatie van de gebruiker van die PGP-lijnen, maar ook voor een volledi-ger en daarmee juister beeld van de toedracht van strafbare feiten en de mate van betrokkenheid van de verdachte(n) daarbij.

Waar het kortom nog altijd aan ontbreekt – en dat is ruim vijf jaar na de intrede van het voor de opsporing en vervolging zo belangrijke fenomeen PGP-data een even teleurstellende als onacceptabele constatering – is het faciliteren van een inzagemodaliteit waarmee die data effectief, zonder restricties en bezwaren kunnen worden onderzocht en met de verdachte om wie het uiteindelijk allemaal gaat kunnen worden gedeeld; een modaliteit waarmee wordt voorzien in de benodigde waarborg van voldoende tijd én faciliteiten om de verdediging op effectieve wijze voor te bereiden, net zoals de opsporing al jarenlang vanaf de eigen werkplek van een dergelijke modaliteit gebruik heeft kunnen maken met uitvoerige onderzoeken waarin de inhoud van versleutelde communicatie uitgebreid wordt geanalyseerd tot gevolg.

Dat daar ook vanuit verdedigingsperspectief behoefte aan zou bestaan was uiteraard voorzienbaar en is in ieder geval duidelijk vanaf de daarover gevoerde discussies in de eerste zaken die op PGP-data werden gebaseerd. Sterker nog, door het NFI werd er vanaf de ontwikkeling van Hansken in 2012 al rekening mee gehouden dat ook voor de verdediging inzage mogelijk zou moeten zijn en werd nagedacht over de mogelijkheid vanaf advocatenkantoren gebruik te laten maken van Hansken.[17] Tot *remote access* tot de data voor de advocatuur is het echter – bijna tien jaar na de ontwikkeling van de zoekmachine – nog steeds niet gekomen, terwijl de vraag daarnaar sinds de intrede van PGP-data in 2016 gelet op het toenemende aantal daarop gebaseerde strafzaken uiteraard steeds indringender is geworden.

Het Openbaar Ministerie is ervoor verantwoordelijk de benodigde faciliteiten te bieden maar heeft kennelijk niet de urgentie gevoeld om naast alle capaciteit en middelen die zijn gestopt in het opsporen van strafbare feiten in die data er óók voor te waken dat vervolgens geen verregaand onevenwichtige strafprocessen worden gevoerd. De discussie in de Nederlandse rechtszalen gaan dan ook niet zozeer over de verkrijging, betrouwbaarheid en de inhoud van de data, maar over werkbare toegang daartoe zodat de benodigde controle op inhoud, selectie en interpretatie van die data zoals dat bij andere bewijsmiddelen als sinds jaar en dag gebeurt kan plaatshebben. Het is een legitieme vraag of dááraan wel zo veel tijd en zittingscapaciteit zou moeten worden gespendeerd.

In een omvangrijk rapport van het WODC over onder meer de digitalisering van bewijsvoering wezen de rapporteurs er in 2019 al op dat het niet alleen voor de verdediging maar ook voor de rechter van belang kan zijn het originele materiaal waarop processen-verbaal zijn gebaseerd (bronmateriaal) te kunnen interpreteren en pleiten zij ervoor de in het huidige Nederlandse strafproces vrijwel afwezige materiële onmiddellijkheid in ere te herstellen. In toekomstige digitale dossiers zou het daarom mogelijk moeten worden om, indien gewenst, ook het bronmateriaal te raadplegen.[18] Zo ver is het nog lang niet. De mogelijkheden van *remote access* tot datasets in PGP-zaken worden op dit moment nog onderzocht met de NVSA,[19] maar waarom zouden in de tussentijd verdachten voor wie bijzonder veel op het spel staat moeten accepteren dat hun strafzaak wordt behandeld zonder dat zij hun verdediging adequaat hebben kunnen voorbereiden op een wijze die voldoet aan de beginselen van een behoorlijk strafproces?

Rechtbank Amsterdam in Marengo vs. Hof Arnhem-Leeuwarden in Bosnië-Brandberg

Deze discussie werd begin dit jaar ook gevoerd in het bekende liquidatieproces *Marengo*. Het belang van de inzage en de grote problemen die daarbij nog altijd bestaan lijken daarbij door de Rechtbank Amsterdam maar in beperkte mate te zijn onderkend. Zelfs na een speciale 'PGP-inzagedag' en een regiezitting waarop alle beperkingen van de verdediging werden gedemonstreerd en besproken, werd vastgehouden aan het formalistische uitgangspunt dat de datasets geen processtukken zijn, dat daarmee geen recht bestaat op verstrekking daarvan en dat de geboden inzagemogelijkheden volstaan. De rechtbank benoemt daarbij het uitgangspunt dat geen afschrift wordt verstrekt van *alle* onderzoeksresultaten, een uitgangspunt dat zeker in zaken waarin de datasets grotendeels alle onderzoeksresultaten *zijn* en een grote hoeveelheid mogelijk relevant materiaal bevatten ter discussie zou moeten staan. Gewezen wordt op de centrale rol die de officier van justitie heeft als het gaat om de voorwaarden waaronder inzage kan plaatsvinden en waarbij rekening moet worden gehouden met privacygevoelige gegevens van derden die aan die PGP-communicatie deelnemen.[20]

Het privacy-argument komt in meerdere beslissingen van rechtbanken terug, maar overtuigt niet

Het privacy-argument komt in meerdere beslissingen van rechtbanken terug, maar overtuigt niet. Niet valt in te zien waarom de verdediging bij het NFI wel die volledige dataset met privacygevoelige informatie zou mogen inzien, maar die privacybelangen aan verstrekking van dezelfde dataset, al dan niet onder bepaalde strenge voorwaarden, in de weg zouden staan. Bovendien sluit het één het ander niet uit: hoewel niet ideaal bestaat de mogelijkheid daadwerkelijk door het Openbaar Ministerie als te privacygevoelig aangemerkte gegevens niet te verstrekken of onleesbaar te maken, zolang wordt aangegeven dat niet alle data voor de verdediging inzichtelijk zijn.[21] Hier lijkt sprake van een gelegenheidsargument om te voorkomen de het Openbaar Ministerie al die privacygevoelig geachte informatie uit de dataset

moet filteren, temeer nu ditzelfde privacy-argument er niet aan in de weg heeft gestaan dat het Openbaar Ministerie bij de verschillende aanbieders steeds *alle* data van *alle* gebruikers in beslag heeft mogen nemen, zonder concrete, laat staan geïndividualiseerde, verdenking. De achtergrond van het niet (willen) verstrekken van datasets lijkt vaak vooral gelegen in praktische problemen of de moeite die dat oplevert, in plaats van in een strikte noodzaak het faciliteren van de verdediging te beperken.[22] Als die indruk juist is dan zou dat uiteraard al snel in strijd komen met artikel 6 EVRM.[23]

Er lijkt echter eindelijk beweging te komen nu het Gerechtshof Arnhem-Leeuwarden in het onderzoek *Bosnië-Brandberg* na diverse eerdere verzoeken op 1 juli 2021 een in die zin baanbrekende beslissing heeft genomen dat voor het eerst in alle zaken die er rond versleutelde informatie hebben gelopen en nog lopen is besloten dat de verdediging niet alleen inzage moet kunnen hebben in de gehele dataset, maar die inzage ook op eigen gelegenheid en op zelf gekozen momenten moet kunnen plaatshebben én de daartoe benodigde software door het Openbaar Ministerie moet worden aangeleverd. En dat niet alleen: ook de verdachte dient in de penitentiaire inrichting, binnen de daar grenzende kaders, dezelfde gelegenheid te krijgen. Dit alles nadat de hierboven besproken problemen, bezwaren en jurisprudentie zeer uitgebreid waren besproken en dus met erkenning van niet alleen het belang dat een verdachte heeft bij kennisneming van deze data, maar ook van de verantwoordelijkheid die het Openbaar Ministerie heeft om te voorzien in een modaliteit die daadwerkelijke en zinvolle kennisname mogelijk maakt. Mogelijk dat de stand van het onderzoek in deze zaak – hoger beroep tegen een bij de rechtbank opgelegde levenslange gevangenisstraf waarbij de bewezenverklaring grotendeels, om niet te zeggen uitsluitend, is gebaseerd op PGP-communicatie – een rol heeft gespeeld bij de totstandkoming van die beslissing, maar dat doet aan de principiële aard daarvan niets af. In dit onderzoek zijn de data inmiddels in een aangepaste vorm aan zowel de verdediging als de verdachte in pdf verstrekt (dat bleek anders dan eerder was gecommuniceerd wel te kunnen).

Het is nu zaak dat ook door andere gerechten deze verantwoordelijkheid van het Openbaar Ministerie niet alleen wordt erkend maar ook wordt afgedwongen

Afronding

Zoals dat wel vaker zo is wordt onder druk alles vloeibaar en ook in andere zaken wordt nu bezien of daar op soortgelijke wijze sprake kan zijn van verstrekking van de dataset aan advocaten en verdachten, zonder dat daartoe vanuit de verdediging eindeloze verzoeken en smeekbedes hoeven te worden gedaan.[24] De datasets lijken daarbij eindelijk hun plek te gaan innemen als 'normaal' dossierstuk waarvan het niet alleen mogelijk maar zelfs voor de hand liggend is dat de weergave en interpretatie daarvan in de processen-verbaal in het procesdossier door de verdediging en de verdachte kunnen worden gecontroleerd. Het is nu zaak dat ook door andere gerechten deze verantwoordelijkheid van het Openbaar Ministerie niet alleen wordt erkend maar voor zover nog nodig ook wordt afgedwongen, zodat na meer dan vijf jaar eindelijk een einde komt aan de systemische ongelijkheid die er sinds de introductie van de PGP-data in de Nederlandse strafprocessen is ontstaan. •

17. In het onderzoek Tandem is daarover in 2018 door één van de ontwikkelaars van de zoekmachine verklaard, welke zoekmachine overigens niet naar aanleiding van PGP-data is ontwikkeld maar al eerder, om forensisch onderzoek van grote hoeveelheden digitale data mogelijk te maken.

18. B. de Wilde e.a., *Digitale informatie in het strafproces - De noodzaak van aanpassing van strafvorderlijke wetgeving*, WODC, 2019, par. 5.4.4 en 5.4.5 (p. 64 e.v.).

19. Zo volgt uit een weergegeven toelichting van het Openbaar Ministerie in Rb. Amsterdam 21 mei 2021, ECLI:NL:RBAMS:2021:2585. Zo ook dat dit zich nog in een pril stadium bevindt.

20. Rb. Amsterdam 1 april 2021, ECLI:NL:RBAMS:2021:1507.

21. Zo besliste het Gerechtshof Amsterdam op 8 juli 2020 in de zaak tegen Willem Holleeder (*Vandros*) op verzoek van de verdediging dat een zoekslag naar bepaalde zoektermen moest worden gemaakt in de volledige Ennetcom-data en is het onderzoek daartoe mede gelet op het voorkomen van een onnodige inbreuk op privacy van derden in handen gesteld van de raadsheer-commissaris, waarna de zoekresultaten gewoon aan de verdediging zijn verstrekt. Hof Amsterdam 8 juli 2020, ECLI:NL:GHAMS:2020:1904.

22. In het in voetnoot 7 genoemde WODC-rapport, p. 68, wordt gesteld dat op basis van gesprekken met respondenten uit de advocatuur, opsporing en vervolging kan worden vastgesteld dat de obstakels bij het toegankelijk maken van bronmateriaal vooral praktisch van aard zijn en er geen principiële bezwaren naar voren zijn gebracht.

23. Zie hierover ook M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *Boom Strafblad*, 2021-2. p. 45.

24. *Partly dissenting opinion* van rechter D. Pavli bij EHRM 4 juni 2019, nr. 39757/15 (*Sigurdur Einarsson e.a./IJsland*). *'(…) full electronic disclosure in high-volume criminal investigations must be provided by default, that is, as a matter of standard prosecutorial practice and without the need for the defence to initiate and litigate a litany of procedural requests.'*