EHRC EUROPEAN HUMAN RIGHTS CASES UPDATES

ANNOTATIE

Särgava t. Estland (EHRM, 698/19) – Procedurele waarborgen ter bescherming verschoningsrecht bij uitoefening digitale opsporingsbevoegdheden

D.A.G. van Toor en I.N. de Wit

Annotatie bij Europees Hof voor de Rechten van de Mens, 16-11-2021, ECLI:CE:ECHR:2021:1116JUD000069819 (EHRC-2021-0310)

1. Anno 2022 kunnen grote hoeveelheden data uit in beslag genomen gegevensdragers worden gebruikt om de waarheid aan het licht de brengen.[1] Zo hebben de autoriteiten in *Rook t. Duitsland*[2] en *Sigurdur Einarsson e.a. t. IJsland*[3] (hierna aangehaald als *Einarsson*) miljoenen gegevens in beslag genomen, namelijk de gehele digitale administratie van *Mediamarkt* (in *Rook*) en, de tijdens de financiële crisis van de begin jaren 2000 omgevallen, *Kaupping Bank* (in *Einarsson*). Tussen die data kan natuurlijk ook geprivilegieerde informatie verzeild raken, bijvoorbeeld communicatie tussen advocaat en cliënt. In zowel *Rook* als *Einarsson* gaat de klacht uiteindelijk alleen over de inzage in de dataset onder het *equality of arms*-beginsel,[4] terwijl het in de onderhavige zaak juist gaat om de bescherming van materiaal dat onder het verschoningsrecht valt dat op in beslag genomen gegevensdragers staat. Het EHRM oordeelt in de zaak *Särgava t. Esland* dat er toereikende waarborgen naar nationaal recht dienen te zijn om willekeurige of onevenredige inmenging in geprivilegieerde informatie te voorkomen. En dat is bij een gegevensdrager waarop privégegevens, zakelijke gegevens en gegevens die onderdeel uitmaken van een strafbaar feit staan niet zo eenvoudig.

2. In de onderhavige zaak staat de klacht van een advocaat centraal die, naast zijn werkzaamheden als jurist, ook bestuurder is van meerdere bedrijven. Die bedrijven lijken

(veelal) connecties te hebben met de onderwereld, waardoor de verdenking rijst dat Särgava als een soort *consigliere* optreedt (waarbij hij blijkbaar niet van, zoals Marlon Brando ons leerde, onbesproken gedrag is) (par. 6-7). Nadat klager in beeld van de autoriteiten komt, besluit justitie het kantoor van klager, zijn huis en zijn vervoersmiddel te doorzoeken. Blijkens het doorzoekingsbevel wil justitie met name gegevensdragers in beslag nemen (par. 9). Duidelijk is, dat de autoriteiten ervan op de hoogte zijn dat logischerwijs ook gegevens die geen onderdeel uitmaken van de strafbare feiten waarvoor klager wordt verdacht, maar van zijn legale juridische activiteiten, deel zullen uitmaken van de in beslag genomen goederen (par. 9). Hierover gaat dan ook de nationale rechtsgang (par. 17-29) en de klacht bij het EHRM.

3. Centraal in de beoordeling van het Hof staat hoe, wanneer tegen een verschoningsgerechtigde een verdenking is gerezen, geprivilegieerd materiaal wordt onderscheiden en gescheiden van materiaal waar geen beroep op het beroepsgeheim van de advocaat kan worden gedaan. De klager stelt expliciet dat hij niet klaagt over de eventuele onrechtmatigheid van de doorzoeking, maar alleen over de inbeslagname van zijn onder het verschoningsrecht vallende gegevensdragers (par. 73). Volgens klager vallen alle gegevensdragers onder de Estse absolute *inviolability rule*, terwijl de overheid beargumenteert dat doordat de klager zijn gegevensdragers voor zowel verschoningsgerechtigde werkzaamheden als illegale activiteiten gebruikte een situatie heeft gecreëerd ‘whereby the data contained therein would be seized as a result of a search’ (par. 18).

4. Deze discussie speelt breder:[5] gegevensdragers bevatten al snel ook niet tot het strafrechtelijke onderzoek behorend materiaal, waarbij de vermenging van onder het verschoningsrecht vallend materiaal en relevant bewijsmateriaal een bijzonder moeilijke kwestie is. In beginsel geldt voor informatie uitgewisseld tussen een persoon met een beroepsgeheim en zijn cliënt of patiënt namelijk een geheimhoudingsplicht en een daaraan gekoppeld verschoningsrecht. Op dit verschoningsrecht kan slecht bij (hoge) uitzondering een inbreuk worden gemaakt,[6] namelijk wanneer ‘zich zeer uitzonderlijke omstandigheden voordoen op grond waarvan het belang dat de waarheid aan het licht komt moet prevaleren boven het verschoningsrecht’.[7] Dat geldt naar Nederlands recht bijvoorbeeld voor de situatie dat de verschoningsgerechtigde zelf verdachte is van een ernstig strafbaar feit en als de verschoningsgerechtigde een crimineel samenwerkingsverband aangaat (zoals in het onderhavige geval). Ook het EHRM acht het verschoningsrecht niet absoluut en overweegt dat de advocatuur niet moet worden gebruikt om een vrijhaven te creëren (par. 89). Wel moet een strikte set van regels uit het nationale recht blijken, waarin enerzijds recht wordt gedaan aan de essentiële positie die rechtsgeleerden in de rechtspleging innemen terwijl het anderzijds mogelijk is om niet onder het verschoningsrecht vallend materiaal bij

verschoningsgerechtigde in beslag te nemen (par. 89).

5. In onderhavige zaak ontbrak het aan die waarborgen in het nationale recht van Estland. De juridische grondslag (art. 91 CCrp), op basis waarvan de gegevensdragers in beslag waren genomen, bevatte weliswaar enkele waarborgen, zoals dat de data alleen onderzocht mogen worden als er een redelijke verdenking bestaat dat de gezochte gegevensdrager op de te doorzoeken locatie aanwezig is – dit lijkt een eis die vergelijkbaar is met de *probable cause* uit het Amerikaanse constitutionele recht – en dat de te geven machtiging aan diverse eisen moet voldoen (par. 96). Maar, een praktisch kader om geprivilegieerd materiaal te onderscheiden van niet-geprivilegieerd materiaal, ook in het geval dat de advocaat zelf verdachte is, ontbreekt (par. 98). Ook had de onderzoeksrechter in deze zaak geen voorzieningen getroffen om het door het beroepsgeheim beschermd materiaal veilig te stellen. De laptop en telefoon van de advocaat zijn zelfs op basis van ruim geformuleerde trefwoorden doorzocht, zonder dat die methode uit de wet voortvloeit (par. 106). Dit levert dan ook een schending van art. 8 EVRM op, omdat de inbreuk niet in overeenstemming met het recht heeft plaatsgevonden.

6. Zoals al kort aangestipt, heeft onderhavige zaak betrekking op de situatie dat de advocaat zelf verdachte is. In dat soort zaken is het evident dat de gegevens die onderdeel uitmaken van het feitencomplex waarvoor de advocaat wordt verdacht, niet vallen onder het algemene belang dat wordt gediend met het verschoningsrecht. Verschoningsgerechtigde informatie kan echter ook, in vaker voorkomende gevallen, worden verkregen in geval dat gegevensdragers van een cliënt in beslag worden genomen. Zo is bijvoorbeeld in de zaak *Einarsson* de gehele administratie van de verdachte in beslag genomen en zijn gesprekken tussen advocaat en cliënt opgenomen.[8] Ook in de zaak *Rook* is de gehele administratie van de verdachte in beslag genomen.[9] In het arrest *Saber* laat het EHRM zich uitgebreid uit over de situatie dat vertrouwelijke informatie tussen een advocaat en cliënt toegankelijk is via een in beslag genomen smartphone van cliënt zelf.[10] In die zaak werd de smartphone van de cliënt in beslag genomen in het onderzoek naar twee personen die ervan verdacht werden hem te willen vermoorden. De politie maakte een kopie van de inhoud van de smartphone met het doel om het motief van de daders te achterhalen. Bij de inbeslagneming verklaarde de cliënt dat de smartphone correspondentie bevatte tussen hem en zijn advocaten, ook over een zaak waarin hij zelf verdachte was. Daarop is de data overhandigd aan de rechtbank Oslo om te bepalen welke data geprivilegieerd zou zijn. Dit zou geschieden aan de hand van door de rechtbank gekozen trefwoorden (par. 7-11). Uiteindelijk heeft de rechtbank besloten de selectie door de politie te laten uitvoeren, omdat een nieuwe uitspraak van het nationale hooggerechtshof dat toestond (par. 38). De cliënt wendde zich tot het EHRM. Ook in Noorwegen ontbrak het volgens het Hof aan duidelijke regelgeving inzake de bescherming van het professioneel verschoningsrecht. Het was voor Saber niet voorzienbaar geweest op

welke wijze het onderzoek aan de data plaats zou vinden, daar de regels pas na de inbeslagneming, en niet door de wetgever, werden gecreëerd. Het Hooggerechtshof in Noorwegen had in zijn uitspraak bovendien ook geen aanwijzingen gegeven over de wijze waarop de politie de data zou moeten filteren (par. 55-58).

7. In Nederland is er vooralsnog geen specifieke wettelijke grondslag voor de doorzoeking van gegevensdragers zoals de smartphone. Art. 126aa lid 2 Wetboek van Strafvordering (Sv) bepaalt enkel dat verschoningsgerechtigd materiaal dat onderdeel uitmaakt van de processtukken moet worden vernietigd. Dit gebeurt onder de verantwoordelijkheid van de officier van justitie. Het materiaal mag alleen aan de processtukken worden toegevoegd na voorafgaande machtiging door de rechter-commissaris. Om te bepalen welk materiaal onder het verschoningsrecht valt, zal de officier van justitie of een opsporingsambtenaar kennis moeten nemen van de inhoud van het materiaal. Een ander regime, maar dan onder de verantwoordelijkheid van de rechter-commissaris, volgt uit art. 98 Sv. Dit artikel bepaalt dat brieven of geschriften die onder het verschoningsrecht vallen, niet in beslag mogen worden genomen. Het stamt nog uit het tijdperk dat vooral schriftelijke bescheiden in beslag werden genomen, en omvat geen digitale gegevensdragers. Hieruit blijkt dat naar huidig recht schriftelijke bescheiden beter zijn beschermd dan digitale gegevens.

8. In de rechtspraak wordt het hierboven genoemde onderzoek aan smartphones toegestaan op basis van algemeen geformuleerde opsporingsbevoegdheden.[11] Er is in de Nederlandse strafrechtpraktijk bovendien weinig toezicht op de methoden die de politie daarbij gebruikt en hoe de privacy van betrokken smartphonegebruikers daarbij wordt gewaarborgd.[12] De vastgelegde werkwijze is, dat een officier van justitie, die niét betrokken is bij het betreffende onderzoek, kennis kan nemen van informatie in die zaak die mogelijk onder het verschoningsrecht valt. Er is geen duidelijke en specifieke filteringsprocedure ter bescherming van het professionele verschoningsrecht in het geval van inbeslagneming van een gegevensdrager, zoals het EHRM wel eist in onder meer *Särgava* en *Saber*. De rechter-commissaris is de bevoegde autoriteit die hierop toeziet en die, in de gevallen dat de verschoningsgerechtigde bezwaar maakt tegen inbeslagneming, de aannemelijkheid van die claim beoordeelt (zie art. 98 lid 5). Daarbij krijgt de rechter-commissaris in de praktijk hulp van geheimhouderfunctionarissen, opsporingsambtenaren die niet bij het desbetreffende onderzoek betrokken zijn. Een wettelijke grondslag hiervoor ontbreekt, maar de rechter-commissaris heeft zelf niet de tijd en digitale expertise om dergelijk onderzoek eigenhandig uit te voeren.[13] In gevallen met grote hoeveelheden data is het alleen niet altijd duidelijk waar de verschoningsgerechtigde gegevens zich bevinden, en hoe de gegevens kunnen worden geïdentificeerd en getraceerd en in hoeverre de geheimhouderfunctionarissen kennisnemen van de inhoud van de geprivilegieerde stukken.[14] Er lijkt in de genoemde rechtspraak van de

Hoge Raad geen aandacht te worden besteed aan de vastlegging van de wijze waarop bepaalde gegevens als (niet) onderdeel uitmakend van het verschoningsrecht is geselecteerd en welke informatie precies is ingezien.

9. Dit gebrek aan transparantie vergroot de kloof tussen advocaten en justitie. Zo oordeelde de voorzieningenrechter van de rechtbank Oost-Brabant in een procedure aangespannen door advocaten tegen de Staat dat het verschoningsrecht was geschonden.[15] De Staat mag niet langer de correspondentie van de betrokken advocaten inzien. Het openbaar ministerie had in die zaak 3.115 e-mails tussen een bedrijf, verdacht van witwassen en valsheid in geschrifte, en hun advocaten heimelijk bemachtigd. De opsporingsambtenaren hadden zelf een selectie gemaakt via zoektermen en pas een half jaar later de officier van justitie op de hoogte gebracht van de geprivilegieerde stukken. De officier van justitie besloot dat de stukken vernietigd moesten worden, maar dit heeft het onderzoeksteam niet gedaan. Ook had een opsporingsambtenaar 875 bestanden die niemand mocht inzien aan het opsporingsteam vrijgegeven.

10. Er zijn ook gevallen waar de verschoningsgerechtigde zelf niet in beeld is. Dit was bijvoorbeeld aan de orde bij onderschepte communicatie uit de versleutelde chatdiensten SkyECC en EnroChat. Het openbaar ministerie vroeg advocaten die de chatdiensten gebruikt hadden, zich te melden, zodat de reguliere protocollen voor verschoningsgerechtigden zou kunnen gevolgd.[16] Het kwaad is dan al geschied, de gegevens zijn dan al in beslag genomen en mogelijk al bekeken. Dit is juist bij cryptocommunicatieaanbieders een risico, omdat het op voorhand onmogelijk is voor de autoriteiten om te weten wie de gebruiker van een bepaald account is. Alleen middels een inhoudsanalyse zou dan kunnen worden achterhaald of bepaalde berichten onder het verschoningsrecht vallen.

11. De Modernisering van het Wetboek van Strafvordering zal een verbetering in de wettelijke regulering van digitale opsporing met zich meebrengen.[17] De nieuwe regeling ziet specifiek op het onderzoek naar digitale gegevens en maakt een onderscheid tussen onderzoek naar de verschoningsgerechtigde zelf en cliënten van verschoningsgerechtigden.[18] De rechter-commissaris krijgt in het nieuwe voorstel de verantwoordelijkheid om te beslissen over het vergaren en inzien van digitale gegevens in dergelijke onderzoeken en de bescherming van verschoningsgerechtigde gegevens daarbij. De rechter-commissaris kan volgens de Memorie van Toelichting een nieuw technologisch hulpmiddel gebruiken om verschoningsgerechtigde communicatie uit de data te filteren bij onderzoek naar niet verschoningsgerechtigden.[19] Wanneer het hulpmiddel gebruikt kan worden zonder de communicatie in te zien, staat de Memorie van Toelichting toe dat opsporingsambtenaren de data filteren. In welke mate deze software gegevens die onder het verschoningsrecht correct identificeert, zal nog moeten blijken. Daarnaast blijkt niet uit de Memorie van Toelichting hoe deze spilfunctie van de

rechter-commissaris zich verhoudt tot het in stand gebleven art. 126aa Sv, dat ook toestaat dat geheimhouderfunctionarissen kennisnemen van dergelijke communicatie. Het zou, in het licht van de genoemde recente uitspraken van het EHRM, aan te bevelen zijn dat de wetgever meer specifieke waarborgen opneemt om het verschoningsrecht te beschermen. Gedacht kan hierbij worden aan hoe die gegevens kunnen worden geïdentificeerd en getraceerd en in hoeverre de rechter-commissaris kennis mag nemen van de inhoud van de geprivilegieerde stukken. Ook zou er een verbaliseringsplicht opgenomen kunnen worden, zodat per zaak wordt vastgelegd op welke wijze tot een selectie is gekomen en welke informatie precies in gezien is.

I.N. (Iris) de Wit

Junior docente straf(proces)recht, Willem Pompe Instituut voor Strafrechtswetenschappen, Universiteit Utrecht

D.A.G. (Dave) van Toor

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

[1] 'Politie onderschept opnieuw massaal crimineel berichtenverkeer', Politie.nl 8 juni 2021, www.politie.

nl/nieuws/2021/juni/8/politie-onderschepopnieuw-massaal-crimineel-berichtenverkeer.html;

'Arrestaties na kraken Sky ECC: criminele communicatie is niet meer onbespied', NOS 9 maart 2021, https://nos.nl/artikel/2371961.

[2] EHRM 25 juli 2019, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook* t. *Duitsland*).

[3] EHRM 4 juni 2019, ECLI:CE:ECHR:2019:0604JUD003975715 (*Einarsson* t. *IJsland*).

[4] M. Galič, ' De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding'', *BSb* 2021/2, p. 41-49.

[5] D.A.G. van Toor & D. van Os, 'Partiële of geschoonde teruggave van gegevensdragers. Naar een gemoderniseerde beslagregeling voor elektronische gegevensdragers', *TBS&H* 2020, 5, p. 260-269.

[6] HR 27 mei 2008, ECLI:NL:HR:2008:BC1369, *NJ* 2008/407.

[7] HR 30 oktober 2007, ECLI:NL:HR:2007:BA5611, r.o. 4.3.

[8] EHRM 4 juni 2019, ECLI:CE:ECHR:2019:0604JUD003975715 (*Einarsson* t. *IJsland*).

[9] EHRM 25 juli 2019, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook* t. *Duitsland*).

[10] EHRM 17 december 2020, ECLI:CE:ECHR:2020 (*Saber* t. *Noorwegen*).

[11] Voor onderzoek in een bij aanhouding in beslag genomen smartphone geldt bijvoorbeeld het

Smartphone-arrest van de Hoge Raad, HR 4 april 2017, ECLI:NL:HR:2017:592, NJ 2017/230, m.nt. T. Kooijmans.

[12] B.J. Koops & B. Newell, 'From horseback to the moon and back: Comparative limits on police searches of smartphones upon arrest', Hastings Law Journal (72) 2020, afl. 1, p. 264-268.

[13] HR 16 oktober 2018, ECLI: NL:HR:2018:1960, HR 9 februari 2021, ECLI:NL:HR:2021:193, NJ 2021/119, r.o. 7.2.1, en D.R. Doorenbos & M.E. Rosing, 'Recht doen aan het verschoningsrecht', S&O 2020, afl. 5/4, p. 217-224.

[14] L. Stevens & M. Galič, 'Bescherming van het professionele verschoningsrecht in geval van doorzoeking van een smartphone: het EHRM eist een concrete basis en een praktische procedurele regeling in het recht', *Ars Aequi* 2021/845, p. 849.

[15] Rechtbank Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035.

[16] 'Advocaten kunnen zich bij OM melden als geheimhouder in versleutelde chatdiensten', advocatenorde.nl 23 april 2021, https://www.advocatenorde.nl/nieuws/advocaten-kunnen-zich-bij-om-melden-als-geheimhouder-in-versleutelde-chatdiensten#:~:text=Geheimhoudernummers-,Advocaten%20kunnen%20zich%20bij%20OM%20melden%20als%20geheimhouder%20in%20versleutelde,chatdiensten%20Sky%20ECC%20of%20EncroChat.

[17] L. Stevens & B.J. Koops, 'Naar een Strafvordering 2030 and beyond. Een visioen van toekomstbestendige

regulering van opsporingsbevoegdheden', in: M. Groenhuijsen e.a., *Op zoek naar evenwicht,* Deventer: Wolters Kluwer 2021, p. 701-714.

[18] Art. 2.7.67 en 2.7.68 nieuw Wetboek van Strafvordering. Zie ook Memorie van Toelichting

nieuw Wetboek van Strafvordering, p. 456 en p. 470-472. Doorzoeking bij de verschoningsgerechtigde zelf wordt geregeld in art. 2.7.62.

[19] Memorie van Toelichting nieuw Wetboek van Strafvordering, p. 470.