

Recht doen aan het verschoningsrecht

prof. mr. D.R. Doorenbos en mr. M.E. Rosing¹

1. Waarom men de kat niet op het spek moet binden

Een advocaat is wettelijk en gedragsrechtelijk verplicht tot geheimhouding van de communicatie met zijn cliënten. Die geheimhouding is buitengewoon belangrijk. Een advocaat kan zijn essentiële rol binnen de rechtsstaat niet vervullen indien hij zijn cliënt niet kan garanderen dat hun onderlinge communicatie vertrouwelijk en dus geheim zal blijven.²

Het verschoningsrecht van de advocaat beschermt diens vertrouwelijke communicatie met zijn cliënten tegen inzage door derden. Die derden staan buiten de advocaat-cliënt-relatie en zij behoren daar ook buiten te blijven. Dat geldt in het bijzonder voor opsporingsambtenaren. Het door hen te dienen belang van de waarheidsvinding moet wijken voor het belang van de vertrouwelijkheid van de advocaat-cliënt-communicatie.³

Het verschoningsrecht wordt geschonden zodra derden zich inzage verschaffen in de advocaat-cliënt-communicatie. Zo'n schending is per definitie onherstelbaar. Indien de inhoud van de geheime communicatie tussen advocaat en cliënt ter kennis is gekomen bij een derde, is deze inhoud buiten de sfeer van de vertrouwelijkheid geraakt. Dat valt niet meer ongedaan te maken.

Omdat kennisneming van verschoningsgerechtigde gegevens praktisch altijd zal plaatsvinden buiten het zicht van de betrokken advocaat en diens cliënt, is zo'n schending onzichtbaar. Zij laat voor de buitenwereld geen sporen na.

Voor de advocaat en zijn cliënt zal in de regel oncontroleerbaar zijn wat de derde met de verworven kennis heeft gedaan of nog zal doen. Dat geldt zeker indien die derde een opsporingsambtenaar is. De professionele tegenstander van de advocaat en diens cliënt zal immers wel de laatste zijn om inzicht te verschaffen in de wijze waarop binnen het opsporingsapparaat met de verworven kennis is

omgegaan resp. hoe deze (tactisch) is of zal worden gebruikt. En bij gebreke van evidente aanwijzingen van gebruik in dossierstukken, zal een rechter daar doorgaans geen onderzoek naar willen laten verrichten.

Kortom: een inbreuk op het verschoningsrecht is niet alleen onherstelbaar, maar ook onzichtbaar en oncontroleerbaar. Wie het verschoningsrecht wil waarborgen, zal dus zoveel mogelijk moeten voorkómen dat dergelijke inbreuken kunnen plaatsvinden, door de mogelijkheden voor zulke inbreuken maximaal te beperken. Niet de kat op het spek binden dus, maar het spek veilig buiten bereik van de kat houden. En daaruit volgt onder meer, dat aan opsporingsambtenaren uiteraard geen enkele rol mag worden toebedeeld bij het selecteren of beoordelen van verschoningsgerechtigde communicatie.

2. Probleem: het opsporingsapparaat verschaft zich toegang tot verschoningsgerechtigde gegevens

In het licht van de voorgaande paragraaf kan slechts met verbazing en ontzetting worden kennisgenomen van de werkwijze die OM en Fiod propageren in relatie tot de omgang met verschoningsgerechtigde communicatie. Zij menen immers dat zij wel degelijk een rol zouden moeten vervullen. En zij gaan zelfs zo ver dat zij betogen dat de huidige wet en rechtspraak hen notabene zou toestaan als regel kennis te nemen van verschoningsrechtelijke communicatie om te beoordelen of deze wel echt als zodanig moet worden gekwalificeerd.⁴

Daarbij maken zij gekunsteld onderscheid tussen de inbeslagneming van gegevens bij een doorzoeeking (art. 98 en 125i Sv) en de vordering van gegevens met behulp van bijzondere opsporingsbevoegdheden (art. 126nc e.v. Sv). De beoordeling van een beroep op het verschoningsrecht zou in het eerste geval aan de rechter-commissaris zijn, maar in het tweede geval primair aan de officier van justitie. Pas na diens beoordeling zou de rechter-commissaris eraan te pas kunnen komen. De verklaring van dit merkwaardige onderscheid wordt door OM en Fiod gezocht in de regeling omtrent de

1. Daan Doorenbos is advocaat bij Stibbe Amsterdam en hoogleraar Ondernemingsstrafrecht aan de Radboud Universiteit te Nijmegen. Muriel Rosing is advocaat bij Stibbe Amsterdam.

2. Zie EHRM 6 december 2012, ECLI:NL:XX:2012:BZ0945 (*Michaud tegen Frankrijk*), par. 118.

3. Zie reeds HR 1 maart 1985, ECLI:NL:HR:1985:AC9066 (*Notaris Maas*) en HR 6 mei 1986, NJ 1986/814 (*Advocaat is vertrouwensberoep*).

4. Zie M. van der Horst en R. Klein, Het verschoningsrecht, de toekomst met vertrouwen tegemoet?, *TvSO* 2019, 4, p. 150-170.

vernietiging van gegevens die door bijzondere opsporingsbevoegdheden zijn verkregen. Het feit dat daarin wordt onderkend dat een opsporingsambtenaar wel eens kan stuiten op een gegeven waarop verschoningsrecht van toepassing is, in welk geval de officier van justitie moet worden ingeschakeld om te voorkomen dat een dergelijk gegeven in het onderzoek zou worden betrokken, blijkt door het opsporingsapparaat te worden aangegrepen om een praktijk te rechtvaardigen waarin men *alle* verschoningsgerechtigde communicatie beoordeelt die door bijzondere opsporingsbevoegdheden wordt verkregen.

Dat OM en Fiod op deze wijze (willen) omgaan met verschoningsgerechtigde communicatie, blijkt onder meer uit de standpuntbepaling van de Staat der Nederlanden in een principiële discussie die wij daarover zijn aangegaan ten overstaan van de civiele rechter.⁵ Daarin hebben wij de Staat in de positie geplaatst dat hij namens OM en Fiod moet uitleggen hoe er in de praktijk wordt gewerkt en waarom dat volgens de Staat niet onrechtmatig zou zijn. Aldus is ons zeer veel duidelijk geworden over de feitelijk gevolgde werkwijze en de argumentatie met behulp waarvan men deze tracht te rechtvaardigen. Dankzij de kennis en ervaring die wij zodoende hebben opgedaan, kunnen wij de problematiek intussen vrij scherp neerzetten. Het beeld zal evenwel herkenbaar zijn voor elke advocaat die werkzaam is op het terrein van het ondernemingsstrafrecht in omvangrijke fraudeonderzoeken.

Het door OM en Fiod ingenomen standpunt omtrent 'standaard' kennisneming van verschoningsgerechtigde gegevens die zijn verkregen met behulp van bijzondere opsporingsbevoegdheden, is in menig opzicht ongerijmd. Zo is het nogal willekeurig met behulp van welk dwangmiddel de digitaal opgeslagen correspondentie of e-mail-communicatie tussen de advocaat en zijn cliënt in handen van het opsporingsapparaat belandt. Een e-mail bevindt zich per definitie op meer dan één locatie, namelijk bij de verzender en diens provider alsook bij de ontvanger en diens provider, terwijl er verschillende strafvorderlijke mogelijkheden bestaan om die e-mail te bemachtigen. Het zou dan kennelijk steeds van de keuze van het OM afhangen of het opsporingsapparaat een potentieel verschoningsgerechtigde e-mail zou mogen bekijken. Dezelfde e-mail van of aan de advocaat zou nu eens wel, dan weer niet kunnen worden beoordeeld, al naar gelang de aard van de ingezette opsporingsbevoegdheid. Is dit nu werkelijk een strafvorderlijk 'systeem' waar Fiod en OM in geloven?

5. Zie o.a. Rechtbank Oost-Brabant 26 februari 2019, ECLI:NL:RBOBR:2018:1804; Rechtbank Oost-Brabant 29 maart 2019, ECLI:NL:RBOBR:2018:1783; Rechtbank Oost-Brabant 5 juni 2019, ECLI:NL:RBOBR:2019:3107; Hof 's-Hertogenbosch 25 april 2019, ECLI:NL:GHSHE:2019:1545; Hof 's-Hertogenbosch 14 mei 2019, ECLI:NL:GHSHE:2019:1808; Hof 's-Hertogenbosch 6 augustus 2020, ECLI:NL:GHSHE:2020:2537.

Te vrezen valt van wel. Het wordt in elk geval opgeschreven en verdedigd alsof het heel normaal is. Maar het is onbegrijpelijk, omdat het impliceert dat het verschoningsrecht systematisch wordt geschonden. Zoals gezegd levert elke kennisneming – ook als die plaatsvindt door een willekeurige opsporingsambtenaar die 'geheimhouder-opsporingsambtenaar' heet – een onherstelbare inbreuk op het verschoningsrecht op. De tegenwerping dat deze opsporingsambtenaar de opgedane kennis wel geheim zal houden voor zijn collega's van het onderzoeksteam, is niet alleen oncontroleerbaar, maar miskent ook de essentie van het verschoningsrecht. Het vertrouwen van de rechtzoekende dat bij zijn hulpverlener geheim zal blijven wat zij onderling communiceren, zal niet in stand blijven wanneer de rechtzoekende beseft dat opsporingsambtenaren in voorkomend geval inzage zullen nemen in deze communicatie. De bezwering dat de opsporingsambtenaren die deze inzage hebben gehad daar dan verder niets mee doen – althans indien en voor zover zij het verschoningsrecht zouden willen erkennen – zal de rechtzoekende geenszins gerust stellen.

Kortom: wie betoogt dat opsporingsambtenaren een taak moeten hebben bij de selectie of de beoordeling van verschoningsgerechtigde communicatie, verliest uit het oog dat de grondslag van het verschoningsrecht het vertrouwen op geheimhouding is. Die grondslag wordt ondergraven zodra opsporingsambtenaren toegang hebben tot die communicatie. De advocaat zal zijn verdachte cliënt nooit kunnen uitleggen dat zijn geheim bij het opsporingsapparaat in goede handen is, al was het maar omdat hij dat ook helemaal niet weet.

Het standpunt van OM en Fiod is verder ongerijmd vanwege het feit dat zij hiermee een positie claimen die hen nota bene meer macht zou verschaffen dan de rechter. Terwijl de Hoge Raad leert dat zelfs een rechter uiterst terughoudend moet zijn in kennisneming van verschoningsgerechtigd materiaal waarover discussie loopt en daarbij slechts inzage mag nemen indien en voor zover dat strikt noodzakelijk is⁶, daar zouden opsporingsambtenaren en OM als regel alle verschoningsgerechtigde communicatie mogen bekijken en beoordelen, zonder dat iemand dat verder ooit zou kunnen zien of controleren. Er zit erg weinig logica in deze benadering.

3. Waar haalt men het vandaan?

Het uitgangspunt dat elke kennisneming van advocaat-cliënt-communicatie door derden een onherstelbare inbreuk op het verschoningsrecht impliceert, waardoor het algemene rechtsbeginsel waarop dat verschoningsrecht berust, geweld wordt aangedaan, wordt binnen het opsporingsap-

6. Zie o.a. HR 16 juni 2020, ECLI:NL:HR:2020:1048, r.o. 4.2.2.

paraat blijkbaar niet (meer) onderkend. Hoe heeft het zo ver kunnen komen?

De verklaring begint bij de technische ontwikkeling van de opsporingsbevoegdheden. Waar de techniek het mogelijk maakte om lopende communicatie op te nemen en af te luisteren, werd praktisch onvermijdelijk dat opsporingsambtenaren zouden kunnen worden geconfronteerd met communicatie van en aan verschoningsgerechtigden. Toen de wetgever aan het begin van deze eeuw het arsenaal aan bijzondere opsporingsbevoegdheden uitbreidde, waarmee de mogelijkheden voor het maken van geheime opnames substantieel werden vergroot, heeft hij daarmee rekening gehouden. Met het oog daarop werd het voorschrift van art. 126aa lid 2 Sv geïntroduceerd en nader uitgewerkt in art. 4 Besluit bewaren en vernietigen niet-gevoegde stukken. In die laatste bepaling staat te lezen dat de opsporingsambtenaar die door de uitoefening van een bijzondere opsporingsbevoegdheid kennis zou nemen van ‘mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder’ daarvan onverwijld de officier van justitie in kennis moet stellen. Indien de officier van justitie vervolgens vaststelt dat het inderdaad om verschoningsgerechtigde communicatie gaat, moet hij terstond de vernietiging bevelen van de processen-verbaal en andere voorwerpen voor zover die zulke communicatie behelzen.

De strekking van deze regeling is onmiskenbaar dat inbreuken op het verschoningsrecht zo beperkt mogelijk moeten blijven. Indien opsporingsambtenaren kennisnemen van ‘mededelingen door of aan verschoningsgerechtigden’ moet dat zo snel mogelijk leiden tot vernietiging van al hetgeen waarop en waarin die mededelingen zijn vastgelegd. Uitsluitend indien de mededelingen buiten het verschoningsrecht vallen – omdat de geheimhouder niet in zijn hoedanigheid optrad of in de uitzonderlijke omstandigheid dat de advocaat zelf als verdachte is aangemerkt – kan een nadere beoordeling door de rechter-commissaris plaatsvinden, bij voorkeur na raadpleging van een gezaghebbend lid van de beroepsgroep.

Dat de wetgever bij deze regeling ruimte heeft gelaten voor een afstemming tussen opsporingsambtenaar en officier van justitie over de aanwezigheid van verschoningsrechtige communicatie, valt te verklaren vanuit de gedachte dat het anno 2000 praktisch gesproken onvermijdelijk leek dat opsporingsambtenaren bij het afluisteren van gesprekken op zulke communicatie zouden kunnen stuiten. Daar heeft de wetgever destijds deze oplossing voor gekozen: bepaald niet ideaal, maar een beter alternatief had men nog niet bedacht.

Toen vervolgens de praktijk uitwees dat opsporingsambtenaren in het kader van het opnemen en afluisteren van telefoongesprekken maar al te vaak ook de communicatie met advocaten plachten uit te luisteren en vast te leggen, hetgeen in enkele zaken tot niet-ontvankelijkheid van het OM leidde, is in 2011 het systeem van nummerherken-

ning ingevoerd.⁷ Dat was een veel doeltreffendere oplossing en waarborg tegen inbreuken op de verschoningsrechtige telecomcommunicatie, omdat daarmee technisch wordt voorkómen dat kennisneming van zulke communicatie – althans indien gevoerd via een geregistreerd advocatennummer – nog kan plaatsvinden.

Terwijl het systeem van nummerherkenning dus een probleem oploste, was in de praktijk intussen een ander – veel ernstiger – probleem ontstaan. Dat betrof de hierboven al aangeduide werkwijze van opsporingsambtenaren en OM waarbij wordt gepretendeerd dat zij het ‘recht’ hebben om ten aanzien van e-mail-verkeer met advocaten, verkregen met behulp van een vordering tot gegevensverstrekking, inhoudelijk te beoordelen of e-mails wel of niet onder het verschoningsrecht vallen. De omstandigheid dat een e-mail afkomstig is van of gericht is aan het kantooradres van de advocaat is voor de opsporingsambtenaren op zichzelf blijkbaar nog geen reden om er geen kennis van te nemen, terwijl ook de aanduiding ‘advocaat-client-correspondentie’ of ‘*privileged*’ nog onvoldoende drempel vormt.⁸

In het civiele geding waarin wij procederen over de schending van ons verschoningsrecht door Fiod en OM, heeft de Staat der Nederlanden zeer expliciet gesteld dat art. 126aa lid 2 Sv in zijn opvatting meebrengt dat inhoudelijk kennisgenomen móet worden van correspondentie waarop mogelijk het verschoningsrecht rust. Uit die bepaling zou ook volgen dat de officier van justitie op grond van een inhoudelijke toets moet besluiten of sprake is van verschoningsrechtige communicatie. Kennisneming van dergelijke correspondentie door opsporingsambtenaren en de officier van justitie is toegestaan en is niet in strijd met art. 126aa Sv, het verschoningsrecht en internationale (mensenrechten)verdragen, aldus het betoog van de Staat.

Dit standpunt impliceert dat het verschoningsrecht in de opsporingspraktijk stelselmatig wordt geschonden: elke e-mail wordt bekeken door een opsporingsambtenaar en diens selectie wordt weer getoetst door een officier van justitie. Dat deze functionarissen worden getooid met de naam ‘geheimhouder-ambtenaar’ doet in wezen niet ter zake: het enkele feit dat deze opsporingsambtenaren de e-mail-communicatie inzien en beoordelen, is immers ruimschoots voldoende om de rechtzoekende te doen concluderen dat de correspondentie met zijn advocaat openbaar wordt gemaakt aan de partij die in de opsporing zijn grootste vijand is. Bij de huidige werkwijze heeft de rechtzoekende in veel gevallen zelfs de zekerheid van zodanige open-

7. Zie nader het Besluit van 8 augustus 2011, *Stb.* 380, houdende wijziging van het Besluit bewaren en vernietigen niet-gevoegde stukken (nummerherkenning).

8. Vgl. M. van der Horst en R. Klein, a.w., p. 157, waar zij schrijven dat wordt gekeken naar het briefhoofd en de onderwerpregel, maar dat ook wordt gezien of de informatie relevant is voor het onderzoek.

baarmaking, namelijk in al die gevallen waarin (een kopie of *image* van) zijn digitale administratie en correspondentie in handen van OM en Fiod terecht is gekomen.⁹

4. Regeling van art. 126aa Sv biedt geen grondslag voor schending van verschoningsrecht

Deze stand van zaken is meer dan zorgwekkend. Het is natuurlijk nooit de bedoeling van de wetgever geweest dat de regeling rondom de vernietiging van toevallig onderschepte verschoningsgerechtigde communicatie bij telefoontaps (de zgn. 'bijvangst') zou kunnen rechtvaardigen dat opsporingsambtenaren en officieren van justitie het e-mail-verkeer van en aan verschoningsgerechtigden zouden gaan 'screenen'. Uit niets blijkt dat de wetgever dat heeft willen toestaan: niet uit de tekst, niet uit de toelichting en ook niet uit de strekking van de regeling. Het Besluit bewaren en vernietigen niet-gevoegde stukken is ook geen regeling die enige opsporingsbevoegdheid creëert, laat staan een bevoegdheid waarmee inbreuk mag worden gemaakt op het verschoningsrecht.

Opmerking verdient dat de mogelijkheid tot het heimelijk vorderen van e-mail-verkeer pas werd geïntroduceerd in 2005. De desbetreffende bevoegdheid bestond dus nog niet eens ten tijde van de invoering van art. 126aa Sv en het Besluit bewaren en vernietigen niet-gevoegde gegevens. Reeds daarom kan de wetgever in 2000 niet hebben goed gevonden dat opsporingsambtenaren kennis zouden nemen van e-mails van en aan advocaten en/of die ter kennis zouden mogen brengen aan de officier van justitie. Tekst en toelichting van de regeling zijn dan ook duidelijk toegespitst op telefoongesprekken. Over kennisneming van e-mails, correspondentie, stukken of documenten is destijds in het geheel niet gesproken. De grensverleggende uitleg van OM en Fiod kan derhalve niet worden gebaseerd op de wetgeschiedenis of de bedoeling van de wetgever. Integendeel: bij gelegenheid van de wetwijziging van 2005 waarbij de vorderingen tot gegevensverstrekking aan derden werden geïntroduceerd, is juist expliciet gesteld dat deze nieuwe bevoegdheden niet waren bedoeld om verschoningsgerechtigde communicatie te bemachtigen: *'Gegevens die onder het verschoningsrecht vallen kunnen geen onderwerp zijn van de toepassing van de voorgestelde bevoegdheden. Dit betekent tevens dat de bevoegdheden niet zodanig mogen worden aangewend dat deze gege-*

*vens langs andere weg verkregen worden. (...) De ratio van een bepaling als artikel 96a, derde lid, onder b, verzet zich tegen de mogelijkheid dat de waarborg van deze bepaling zou worden omzeild door dezelfde gegevens bij een andere derde te vorderen.'*¹⁰

Klare taal, die geen ruimte biedt voor het in de redenering van OM en Fiod gemaakte onderscheid tussen e-mail-correspondentie die wordt verkregen door inbeslagneming en e-mail-correspondentie die wordt verkregen door uitlevering op een vordering tot gegevensverstrekking.

Die benadering vindt dus geen steun in de wetgeschiedenis – integendeel – en zij volgt evenmin uit tekst en strekking van de toepasselijke voorschriften.

Het betoog waarmee OM en opsporingsambtenaren verdedigen waarom zij verschoningsgerechtigde e-mails 'moeten' kunnen inzien en beoordelen, is zozeer strijdig met de strekking van de wettelijke regeling en zozeer gespeend van alle juridische logica, dat het een raadsel is hoe lang men dat heeft kunnen volhouden zonder dat een rechter hier korte metten mee heeft gemaakt. Hopelijk is dat een kwestie van tijd. In elk geval is het bepaald onjuist te menen dat de Hoge Raad de werkwijze van OM en Fiod ooit zou hebben goedgekeurd.¹¹ Dat laatste is geenszins het geval.

De Hoge Raad heeft daarentegen wél bij herhaling tot uitdrukking gebracht dat er geen grond is om het verschoningsrecht verschillend te benaderen al naar gelang het gaat om fysieke stukken of digitale gegevens.¹² Dat is ook volstrekt logisch, vanuit de gedachte dat het verschoningsrecht berust op een algemeen rechtsbeginsel dat meebrengt dat het maatschappelijk belang dat de waarheid aan het licht komt, moet wijken voor het maatschappelijk belang dat een ieder zich vrijelijk en zonder vrees voor openbaarmaking om bijstand en advies tot zijn advocaat moet kunnen wenden. Wie dat rechtsbeginsel wil respecteren, behoort strafvorderlijke voorschriften zodanig uit te leggen dat deze recht doen aan het verschoningsrecht. De werkwijze die in de opsporingspraktijk is ontwikkeld, waarbij kennis wordt genomen van communicatie die onder het verschoningsrecht valt en waarbij opsporingsambtenaren beoordelen of dat verschoningsrecht wel 'terecht' wordt ingeroepen, getuigt daarentegen allerminst van enig respect voor dat rechtsbeginsel. In die werkwijze wordt het verschoningsrecht volledig ondergeschikt gemaakt aan het belang van waarheidsvinding, waarbij het opsporingsapparaat bepaalt wat mag prevaleren. Men is dan ver afgedwaald van de weg die de Hoge Raad heeft gewezen.

De suggestie dat de Hoge Raad zich in een recente beschikking 'akkoord' zou hebben verklaard met een werkwijze waarbij opsporingsambtenaren inhoudelijk kennisnemen van potentieel verscho-

9. Voor de advocaat komt daar nog bij dat hij de 'geheimhouder-ambtenaar' in de ene zaak, in de volgende zaak weer gewoon zal tegenkomen als opsporingsambtenaar of zaakofficier. Dezelfde mensen dus, die dan intussen wel kennis dragen van zijn cliënt-advisering en verdedigingsstrategie in een voorgaande zaak. Hoe zouden OM en Fiod het vinden wanneer derden inzage hebben in hun opsporingstactiek en -strategie?

10. Zie *Kamerstukken II* 2003/04, 29441, 3, p. 16 en 22.

11. Zoals gesuggereerd door M. van der Horst en R. Klein, a.w., p. 158.

12. Zie o.a. HR 30 juni 2017, ECLI:NL:HR:2017:1205.

ningsgerechtigde communicatie, is niet juist.¹³ Daarover werd in die zaak niet geklaagd – de verdediging was meegegaan in de gekozen werkwijze – en dus hoefde de Hoge Raad zich daar niet over uit te spreken. Waar de Hoge Raad zich wel over uitsprak, blijft beperkt tot de concrete zaak en heeft geenszins de strekking de ‘geheimhouder-opsporingsambtenaar’ te legitimeren. In zijn conclusie noteerde A-G Knigge al expliciet dat de zaak daar niet over gaat:

‘In cassatie wordt niet geklaagd over de inschakeling door de rechter-commissaris van een zogenaamde geheimhouder-OvJ en van zogenaamde geheimhouder-opsporingsambtenaren. De vraag of die inschakeling toelaatbaar is en zo nee, wat daarvan de consequenties moeten zijn, is daarom niet aan de orde. Ik merk slechts op dat er naar het mij voorkomt weinig bezwaar tegen de inzet van geheimhouder-opsporingsambtenaren is als de door hen verrichte selectie van bestanden die mogen worden gebruikt voor het opsporingsonderzoek, uitsluitend plaatsvindt aan de hand van zoektermen en dus zonder dat van de inhoud van die bestanden wordt kennisgenomen. Van een schending van het beroepsgeheim is dan geen sprake. Problematisch wordt het als de opsporingsambtenaar die de selectie verricht wel van de inhoud van de bestanden kennisneemt. In deze zaak is daarvan, afgaande op het door de desbetreffende opsporingsambtenaar opgemaakte proces-verbaal, sprake geweest (zie hierna, onder 4.2). De vraag is of deze inbreuk op het beroepsgeheim wordt gerechtvaardigd door het feit dat zij plaatsvindt onder verantwoordelijkheid van de rechter-commissaris. Die vraag is zoals gezegd in deze zaak niet aan de orde.’

5. Het kan nog erger: ‘ontoegankelijk maken’ in plaats van vernietigen

Tot nu toe ging het nog slechts om de kennisneming van verschoningsgerechtigde communicatie. De omstandigheid dat opsporingsambtenaren en OM zich daartoe gelegitimeerd achten, door een wettelijke regeling die daar geen basis voor biedt en rechtspraak die daar geen ruimte voor geeft, is op zichzelf al ernstig genoeg. Maar ernstiger nog is de omstandigheid dat het opsporingsapparaat de verschoningsgerechtigde communicatie die het in handen krijgt, in strijd met de wet niet meer vernietigt. Want hoewel tekst en toelichting van de wettelijke regeling (art. 126aa Sv en art. 5 Besluit bewaren en vernietigen niet-gevoegde gegevens) er geen enkel misverstand over laten bestaan dat vernietiging betekent dat de gegevens niet meer –

i.e. nooit meer – kenbaar mogen zijn,¹⁴ meent men in de opsporingspraktijk dat het al wel voldoende is wanneer de gegevens niet meer toegankelijk zijn voor het betrokken onderzoeksteam. De norm ‘niet meer kenbaar’ wordt dan afgezwakt tot ‘niet meer kenbaar voor bepaalde opsporingsambtenaren’ – maar dus wel blijvend beschikbaar voor de opsporing als zodanig. Dat komt er dan op neer dat waar de wetgever spreekt over vernietigen, in feite wordt bedoeld op bewaren.

Omdat aan dit ‘ontoegankelijk maken’ van de verschoningsgerechtigde communicatie een proces van selectie, beoordeling en beschrijving voorafgaat, beschikken opsporingsambtenaren en OM over een nauwkeurige registratie van alle betrokken bestanden en individuele items daarbinnen. Indien later zou worden bedacht dat een zeker item toch wel kan worden ingezien – een nieuwe teamleider of officier van justitie heeft mogelijk weer een nieuw idee – dan is dat eenvoudig terug te halen. De databank met verschoningsgerechtigde gegevens is geduldig beschikbaar.

De praktijk van het ‘ontoegankelijk maken’ wordt door de opsporingsinstanties gelegitimeerd met de stelling dat de authenticiteit en integriteit van kopieën of *images* van beslagen of gevorderde gegevens te allen tijde moet worden gewaarborgd. Wanneer gegevens zouden worden vernietigd, zou de herkomst van deze gegevens niet langer controleerbaar zijn. Daarnaast wordt het standpunt ingenomen dat daadwerkelijk ‘vernietigen’ van digitale gegevens technisch gezien niet mogelijk zou zijn.

Welk (technisch) verhaal men hier ook bij zou willen vertellen: het kan niet deugen. Vernietigen moet een definitief karakter hebben en dat is natuurlijk ook mogelijk. Dat men moeite moet doen om het definitief kwijt te raken, is de keerzijde van het gemak waarmee het wordt verkregen. De kosten van vernietiging vormen de prijs die een rechtsstaat mag betalen voor het algemene rechtsbeginsel dat ten grondslag ligt aan het verschoningsrecht. Wanneer verschoningsgerechtigde communicatie die bij inbeslagneming en uitlevering wordt verkregen, te allen tijde beschikbaar blijft binnen het opsporingsapparaat, is vertrouwen op geheimhouding in de advocaat-cliënt-relatie uiteraard niet meer aan de orde. Dan is er nog slechts grond voor permanente vrees voor openbaarmaking van datgene wat met de verschoningsgerechtigde is gedeeld. Het is de doodsteek voor het verschoningsrecht.

Ook op dit punt is het een raadsel hoe dit zo ver heeft kunnen komen, zonder dat hier ooit in rechte de staf over is gebroken. Het feit dat het hier gaat om een onzichtbare praktijk, die als zodanig ook

13. Zie HR 16 juni 2020, ECLI:NL:HR:2020:1048.

14. De toelichting op art. 5 van het Besluit noemt de fysieke vernietiging (doorknippen, verbranden) van de gegevensdrager een trefzekere wijze van vernietiging. Als alternatief wordt gewezen op het opnieuw formatteren van een diskette. Het simpelweg wissen van bestanden is niet voldoende, aldus de toelichting. Er wordt duidelijk bedoeld op een definitieve vernietiging.

niet ter discussie zal (kunnen) komen in de individuele strafzaak, zal in belangrijke mate verklaren waarom dit fenomeen – het opsporingsapparaat bewaart al het verschoningsgerechtigd materiaal dat het tegenkomt – tot nog toe nauwelijks tot publieke discussie heeft geleid.¹⁵

6. Het verschoningsrecht in het nieuwe wetboek: goede uitgangspunten

Gelukkig vaart de wetgever intussen een juiste koers. Bij de voorstellen voor het nieuwe wetboek van strafvordering¹⁶ wordt ondubbelzinnig benadrukt dat het niet de bedoeling is dat opsporingsambtenaren kennisnemen van verschoningsgerechtigde communicatie. Die boodschap is niet nieuw, maar zij kan niet krachtig genoeg worden uitgedragen, gegeven de hiervóór geschetste ontsporing van de praktijk.

Het uitgangspunt in het nieuwe wetboek van strafvordering is dat voorwerpen of gegevens waarover het verschoningsrecht zich uitstrekt niet in beslag genomen en/of overgenomen mogen worden, respectievelijk dat van onder het verschoningsrecht vallende informatie geen kennis mag worden genomen. Het nieuwe wetboek onderscheidt daarbij de situatie dat de informatie wordt verkregen via de geheimhouder zelf¹⁷ en de situatie dat informatie wordt verkregen via een derde.¹⁸ Voor beide gevallen geldt dat alleen in streng genormeerde uitzonderingsgevallen door de rechter-commissaris kan worden beslist dat het OM kennis mag nemen van onder het verschoningsrecht vallende informatie. Die uitzonderingsgevallen betreffen de situaties waarin (i) de verschoningsgerechtigde toestemming geeft voor kennisneming, (ii) de voorwerpen of gegevens voorwerp uitmaken van het strafbare feit of tot het plegen daarvan hebben gediend dan wel (iii) sprake is van doorbrekingsgrond.

Ingeval dit noodzakelijk is voor zijn beslissing over de toepasselijkheid van het verschoningsrecht, kan alleen de rechter-commissaris kennisnemen van de informatie. Voor kennisneming door (geheimhouders)opsporingsambtenaren is op geen enkele wijze ruimte. Voordat de rechter-commissaris beslist, wordt de verschoningsgerechtigde gehoord. Daarnaast kan de rechter-commissaris advies inwinnen van een vertegenwoordiger van de beroepsgroep.¹⁹ De rechter-commissaris is verplicht dergelijk ad-

vies in te winnen indien hij – in afwijking van het standpunt van de verschoningsgerechtigde – overweegt te beslissen dat het OM van de betreffende informatie kennis mag nemen.

Een glasheldere boodschap dus. De officier van justitie die kennis wil nemen van verschoningsgerechtigde informatie, zal altijd éérst langs de rechter-commissaris moeten. Daarbij is niet van belang of de informatie door middel van een inbeslagneming of vordering zijn verkregen. In de opzet van het nieuwe wetboek zijn de bepalingen inzake de inbeslagneming van voorwerpen en het bevel tot verstrekking gegevens (de huidige ‘vordering’) allemaal in hoofdstuk 7 ‘Bevoegdheden met betrekking tot voorwerpen en gegevens’ ondergebracht. De inbeslagneming is geregeld in Titel 7.2 en het bevel tot verstrekking gegevens in Titel 7.3 genaamd ‘onderzoek van gegevens’. De hiervoor genoemde procedure betreffende de omgang met informatie die onder het verschoningsrecht valt, is van toepassing op zowel de inbeslagneming van voorwerpen als op het onderzoeken van gegevens. Daarmee komt nog beter tot uitdrukking dat de bescherming van het verschoningsrecht over de hele linie gelijkloopt.

In de nieuwe systematiek zal zo geen enkele ruimte zijn voor een betoog dat e-mails tussen advocaat en cliënt, die zijn verkregen via een bevel c.q. vordering bij een derde zoals een provider, door opsporingsambtenaren en officieren van justitie zouden mogen worden gelezen en beoordeeld op toepasselijkheid van het verschoningsrecht. In alle gevallen dient de rechter-commissaris te worden betrokken. Hij moet oordelen of het verschoningsrecht van toepassing is, of er sprake is van een uitzonderingsgeval en hij dient de verschoningsgerechtigde in de gelegenheid te stellen om zijn standpunt kenbaar te maken. Van die laatste stap mag alleen in uitzonderingsgevallen worden afgezien, dat is als de verschoningsgerechtigde na de nodige inspanningen onvindbaar blijkt, na herhaalde verzoek daartoe zijn standpunt niet kenbaar maakt of als de verschoningsgerechtigde overleden is. In al die gevallen moet het advies van een vertegenwoordiger van de beroepsgroep worden gevraagd. Het feit dat de verschoningsgerechtigde in het belang van het onderzoek (nog) niet op de hoogte is van de inbeslagneming of het overnemen van gegevens (zoals het geval kan zijn bij een bevel verstrekking gegevens waarvoor de officier van justitie net als onder huidig recht een geheimhoudingsplicht kan opleggen²⁰) kan geen reden zijn om het vragen van een standpunt van de verschoningsgerechtigde (tijdelijk) achterwege te laten en alvast kennis te nemen van de betreffende gegevens. In die gevallen zal de beslissing over de kennisneming van de gegevens moeten worden uitgesteld tot een moment waarop de verschoningsgerechtigde van de inbeslagneming of overname van de gegevens op de hoogte mag zijn.²¹

15. Wanneer het klimaat daar rijp voor is, leent deze problematiek zich voor een parlementaire enquête. Het gaat hier ook om de kwaliteit van onze rechtsstaat. Zie in dat verband de opinie van D.R. Doorenbos in *NRC Handelsblad* van 14 juni 2019 (‘OM en FIOD, stop met schenden van het verschoningsrecht’).

16. Ambtelijke versie wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, juli 2020, te raadplegen via www.rijksoverheid.nl.

17. Art. 2.7.63 en 2.7.64 Sv (ambtelijke versie, juli 2020).

18. Art. 2.7.67 en 2.7.68 Sv (ambtelijke versie, juli 2020).

19. Indien de verschoningsgerechtigde een advocaat is, kan hierbij aan de Deken worden gedacht.

20. Art. 2.7.37 Sv (ambtelijke versie, juli 2020).

21. Ambtelijke versie Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek

7. Een potentieel lek

Bestaat er onder het nieuwe wetboek van strafvordering dan geen risico meer op onterechte kennisname van informatie die onder het verschoningsrecht valt? Helaas wel.

Dat risico zal zich niet zozeer voordoen als de opsporingsambtenaren voorwerpen in beslag nemen of gegevens overnemen bij de verschoningsgerechtigde zelf of diens cliënt. In die gevallen is de verschoningsgerechtigde op de hoogte van de inbeslagneming of overname (althans: kan hij dat zijn). Hij kan zich dan direct op het standpunt stellen dat zich tussen de in beslag te nemen of over te nemen informatie verschoningsgerechtigde informatie bevindt. Hij kan vervolgens controle houden op de omgang met die informatie en voorkomen dat OM en/of opsporingsambtenaren kennisnemen van informatie die onder het verschoningsrecht valt.

Anders is het als sprake is van een inbeslagneming of een bevel verstrekking gegevens bij een derde, niet zijnde de cliënt. In dat geval zal de verschoningsgerechtigde niet altijd op de hoogte zijn van de inbeslagneming van voorwerpen of het onderzoek aan gegevens waarover zijn verschoningsrecht zich uitstrekt en kan hij zijn standpunt dus niet meteen kenbaar maken. Het wetsvoorstel schrijft voor dat de rechter-commissaris dient te beslissen over de voorwaarden waaronder de inbeslagneming of het onderzoek van die gegevens kan plaatsvinden, wanneer bij de inbeslagneming of het onderzoek het redelijke vermoeden ontstaat dat inzet van die bevoegdheden betrekking heeft op voorwerpen of gegevens die onder het verschoningsrecht vallen.²² Maar daarbij moet er dus maar op worden vertrouwd dat de betrokken opsporingsambtenaren dat vermoeden tijdig kenbaar maken en de rechter-commissaris bij de inbeslagneming of het onderzoek betrekken.

Zelfs als dat gebeurt, kan de verschoningsgerechtigde niet controleren op welke manier met verschoningsgerechtigde informatie wordt omgegaan. Dat is zorgelijk omdat op dit punt de concept-memorie van toelichting de deur op een kier lijkt te zetten voor het betrekken van – al of niet reeds betrokken – opsporingsambtenaren. Indien de rechter-commissaris namelijk zou beslissen dat de verschoningsgerechtigde informatie uit de in beslag te nemen of te onderzoeken gegevens gefilterd moet worden, zou hij dat uitfilteren volgens de memorie om redenen van efficiëntie c.q. gebrek aan adequate ondersteuning kunnen uitbesteden aan opsporingsambtenaren, mits dat mogelijk is zonder van die informatie kennis te nemen.²³ Zo zouden de opsporingsinstanties dus alsnog over informatie komen te beschikken die onder het verschoningsrecht valt.

Overigens kan het ook zo zijn dat het redelijke vermoeden dat het verschoningsrecht van toepassing is pas ontstaat als verschoningsgerechtigde informatie al in het bezit van de opsporingsambtenaren is. Weliswaar schrijft het wetsvoorstel voor dat in dat geval geen kennis mag worden genomen van informatie waarover het verschoningsrecht zich uitstrekt,²⁴ maar daarbij moet tegelijkertijd worden vastgesteld dat de huidige versie van het wetsvoorstel geen bepalingen kent die de vernietiging voorschrijven van gegevens waarover het verschoningsrecht zich uitstrekt. In eerdere conceptversies waren dergelijke bepalingen nog wel opgenomen, maar klaarblijkelijk hebben OM en Fiod de wetgever ervan kunnen overtuigen dat vernietigen niet mogelijk is, onder verwijzing naar het eerdergenoemde argument dat de integriteit van kopieën of *images* van beslagen of verstrekte gegevens na vernietiging niet langer vast zou staan. Voor die situatie heeft de wetgever kennelijk geen oplossing weten te vinden en heeft hij geoordeeld dat dan moet worden volstaan met het ontoegankelijk maken van de gegevens voor de opsporing.²⁵ Dit is de achilleshiel van het wetsvoorstel.

Alles overziend kunnen we concluderen dat het voorgestelde nieuwe wetboek van strafvordering weliswaar recht wil doen aan het verschoningsrecht, maar dat het daarin niet zal slagen zolang wordt gecapituleerd voor vermeende noden uit de praktijk (belasting kabinet RC, complexiteit van vernietiging, etc.). Dan blijft het mogelijk dat Fiod en OM kunnen beschikken over informatie die onder het verschoningsrecht valt, met alle risico's van dien.

8. Op weg naar een oplossing

De in dit artikel beschreven actuele opsporingspraktijk deugt niet. Opsporingsambtenaren behoren niet over informatie te kunnen beschikken die onder het verschoningsrecht valt. Ervaringen uit het verleden leren dat we niet kunnen vertrouwen op eerbiediging van en een rechtmatige omgang met informatie die onder het verschoningsrecht valt.

Dit betekent dat opsporingsambtenaren informatie waarover het verschoningsrecht zich uitstrekt niet moeten kunnen beslaan, overnemen of vorderen. Daartoe zien wij maar één oplossing: het aan de poort uitfilteren van informatie die onder het verschoningsrecht valt, vóórdat deze informatie in beslag wordt genomen, wordt overgenomen of wordt onderzocht. In dit verband zou gewerkt moeten worden met een systeem van herkenning van bij de Orde van Advocaten opgegeven e-mailadressen, naar voorbeeld van het reeds bestaande systeem van de nummerherkenning. In een recent gepubli-

van Strafvordering, p. 465 - 466.

22. Art. 2.7.67 Sv (ambtelijke versie, juli 2020).

23. Ambtelijke versie Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 471.

24. Art. 2.7.68 Sv (ambtelijke versie, juli 2020).

25. Ambtelijke versie Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 476.

ceerd artikel over dit onderwerp is gedetailleerd beschreven dat dit technisch mogelijk zou zijn.²⁶ Wat al helemaal niet moet gebeuren is het inschakelen van – al dan niet bij het opsporingsonderzoek betrokken – opsporingsambtenaren bij rechterlijke werkzaamheden die verband houden met het selecteren of beoordelen van geheimhoudersinformatie. Dat is principieel fout. Wanneer een rechter-commissaris moet oordelen over de toepasselijkheid van het verschoningsrecht op een grote hoeveelheid stukken of gegevens, zijn opsporingsambtenaren wel de laatste functionarissen aan wie de (voor)selectie kan worden opgedragen, eenvoudigweg omdat zij de meest direct belanghebbenden zijn bij kennisneming. Wij geloven niet dat de Hoge Raad daar anders over zou denken, reeds omdat de Hoge Raad heeft uitgesproken dat de hier bedoelde werkzaamheden dienen te worden verricht ‘door zodanige functionaris en op zodanige wijze dat is gewaarborgd dat het verschoningsrecht niet in het gedrang komt’. Het ligt veeleer voor de hand hierbij te denken aan medewerkers van het kabinet RC dan aan opsporingsambtenaren.²⁷

Indien de selectie of beoordeling bij opsporingsambtenaren wordt neergelegd, leidt dat tot de reeds besproken bewaarregistratie (zie onderdeel 5). Blind vertrouwen op geheimhouding of de toezegging dat van verschoningsgerechtigde informatie geen kennis zal worden genomen geeft geen enkele waarborg. Vooralsnog is er geen enkel zicht op een wijze van selecteren, laat staan beoordelen van gegevens zonder van deze gegevens kennis te nemen. Wanneer van gegevens kennis kan worden genomen, kan het verschoningsrecht worden geschon- den en is het retourneren van digitale gegevens door de Fiod een volstrekt loos gebaar indien en zolang de op de kopieën of *images* opgeslagen geheimhoudersinformatie, al dan niet ter waarborging van de veronderstelde integriteit en authenticiteit van die kopie of die *image*, niet daadwerkelijk wordt vernietigd, maar in de computersystemen aanwezig blijft. Het moge duidelijk zijn dat en waarom kopieën of *images* met beslagen of ontvangen gege-

vens niet door opsporingsambtenaren moeten worden bewaard. Dergelijke kopieën of *images* zouden moeten worden ondergebracht bij het kabinet RC. Indien discussie mocht ontstaan over de integriteit van gegevens – een discussie die naar onze indruk in de praktijk overigens zelden of nooit wordt gevoerd – dan kan deze worden beslecht onder regie van de rechter-commissaris. Daar moet de wetgever toch een eenvoudige voorziening voor kunnen treffen.

Indien het kabinet RC onverhoopt niet in staat zou zijn om zelf voldoende capaciteit en deskundigheid op te bouwen voor de selectie en beoordeling van geheimhoudersinformatie, kan een en ander wel elders worden ingehuurd dan bij de belanghebbende tegenstander van de verdachte en zijn raadsman. Er zullen zeker private partijen te vinden zijn die geen enkel belang hebben bij de uitkomst van het debat, maar wel in staat zijn met digitale zoekslagen en juridische expertise de voorselectie te doen.²⁸

Het belang van het verschoningsrecht vergt dat elk risico op schending van dat recht tot een minimum wordt beperkt. Daartoe moeten in het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering nog een paar cruciale wijzigingen worden aangebracht.

26. H.B.J. Sluijsmans en V.J.C. de Bruijn, ‘Mogelijkheden voor het beter waarborgen van het verschoningsrecht door beheerst gebruik van machine learning’, *TvBS&H* 2020, 3, p. 109.

27. Vgl. ook M. van der Horst en R. Klein, a.w., p. 169, waar zij erkennen dat de Hoge Raad in zijn beschikking van 22 december 2015, ECLI:NL:HR:2015:3714, inderdaad niet heeft gezegd dat de bedoelde functionaris ook een opsporingsambtenaar zou kunnen zijn. Tot op heden heeft de Hoge Raad nog nooit overwogen dat de inzet van opsporingsambtenaren bij het selecteren of beoordelen van geheimhoudersinformatie rechtmatig is. Recent nog in de beschikking van 16 juni 2020, ECLI:NL:HR:2020:1048 heeft de Hoge Raad zich hierover niet nader uitgesproken. Zoals hiervóór al werd opgemerkt, klaagde het middel ook niet over de inzet van een geheimhouder-officier van justitie en geheimhouder-opsporingsambtenaar in die zaak, maar over de omstandigheid dat de klager en geheimhouders (in casu artsen) niet bij de selectie en beoordeling van geheimhoudersstukken waren betrokken.

28. Zie ook in dit verband: H.B.J. Sluijsmans en V.J.C. de Bruijn, ‘Mogelijkheden voor het beter waarborgen van het verschoningsrecht door beheerst gebruik van machine learning’, *TvBS&H* 2020, 3, p. 113.