



Universiteit
Leiden
The Netherlands

Het verschoningsrecht van advocaten en het gebruik van extra beveiligde communicatiemiddelen

Lochs, M.; Klapwijk, J.A.; Crijns, J.H.; Sander, D.B.

Citation

Lochs, M., Klapwijk, J. A., Crijns, J. H., & Sander, D. B. (2024). Het verschoningsrecht van advocaten en het gebruik van extra beveiligde communicatiemiddelen. *Nederlands Juristenblad*, 99(21), 1608-1616. Retrieved from <https://hdl.handle.net/1887/4196307>

Version: Publisher's Version

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/4196307>

Note: To cite this publication please use the final published version (if applicable).

Het verschoningsrecht van advocaten en het gebruik van extra beveiligde communicatiemiddelen

Marianne Lochs, Hanne Klapwijk, Jan Crijns & David Sander¹

In zijn uitspraak van 12 maart 2024 heeft de Hoge Raad uitgangspunten geformuleerd voor de waarborging van het functionele verschoningsrecht, in het bijzonder dat van advocaten, bij inbeslagneming door politie en justitie van (grote hoeveelheden) gegevens onder aanbieders van communicatiediensten. In deze bijdrage wordt de betekenis van deze uitspraak geanalyseerd in het licht van de bevindingen uit eerder onderzoek van de auteurs naar het gebruik van extra beveiligde communicatiemiddelen door advocaten. Uiteengezet wordt welke extra beveiligde communicatiemiddelen (strafrecht)advocaten gebruiken, welke beweegredenen daaraan ten grondslag liggen en welke potentiële risico's dat gebruik met zich brengt. Daarna wordt ingegaan op de vraag of en, zo ja, in hoeverre de uitspraak in het licht van die risico's tot een betere waarborging van het functionele verschoningsrecht van advocaten zal leiden.

1. Inleiding

De waarborging van het verschoningsrecht van advocaten mag zich de laatste jaren in grote belangstelling verheugen. Een belangrijke aanleiding daarvoor is de veelbesproken *Castor*-zaak, waarin de discussie over het waarborgen van het functionele verschoningsrecht bij inbeslagneming van grote hoeveelheden (mogelijk) verschoningsgerechtigde gegevens onder derden tussen Openbaar Ministerie (OM) en advocatuur op scherp kwam te staan.² Kern van

de discussie betrof de werkwijze die het OM hanteerde bij het doorzoeken en filteren van deze gegevens, waarbij zogenoemde (bij het OM of de politie werkzame) geheimhouderfunctionarissen waren betrokken.³ Op 12 maart 2024 heeft de Hoge Raad uitspraak gedaan naar aanleiding van de door het Hof 's-Hertogenbosch in deze zaak gestelde prejudiciële vragen.⁴ De Hoge Raad constateert dat de wet onvoldoende handvatten biedt voor het waarborgen van het verschoningsrecht bij het vorderen van (digitale) gegevens onder derden en formuleert enkele uitgangspunten voor dergelijke gevallen, om inbreuken op het verschoningsrecht zoveel mogelijk te voorkomen. Zo is een uitgangspunt dat het oordeel over de vraag of het om geheimhouderinformatie gaat in beginsel bij de verschoningsgerechtigde zelf ligt.⁵ Wanneer niet zonder kennisneming van de inhoud van die informatie kan worden vastgesteld of sprake is van geprivilegieerde communicatie of wanneer daarover discussie bestaat, is de rechter-commissaris de aangewezen autoriteit om de procedure voor filtering van verschoningsgerechtigde informatie in goede banen te leiden.⁶ Het door de Hoge Raad gegeven kader sluit aan bij de regeling die voor het nieuwe Wetboek van Strafvordering is voorgesteld.⁷

De uitspraak maakt duidelijk dat de door het OM toegepaste en verdedigde handelwijze onverenigbaar is met de ratio en inrichting van de regeling rondom de waarborging van het verschoningsrecht

De uitspraak maakt duidelijk dat de door het OM toegepaste en (tot voor kort)⁸ verdedigde handelwijze onverenigbaar is met de ratio en inrichting van de regeling rondom de waarborging van het verschoningsrecht. Het gegeven kader is dan ook van principieel en praktisch belang voor een adequate werkwijze bij de omgang met onder derden in beslag genomen gegevens. Tegelijkertijd lijken daarmee de vaak complexe problemen rondom de waarborging van het verschoningsrecht niet zonder meer te zijn opgelost. Zo blijkt uit door ons uitgevoerd onderzoek naar het gebruik van extra beveiligde communicatiemiddelen door advocaten dat zij in de praktijk allerlei verschillende communicatiemiddelen gebruiken. Daarbij gaat het vooral om verschillende soorten extra beveiligde chatapplicaties en e-mailproviders en, in mindere mate, om cryptotelefoons.⁹ Communicatie via dergelijke middelen kan op verschillende manieren in een opsporingsonderzoek terechtkomen, waarbij niet altijd eenvoudig (op voorhand) vast te stellen is dat het communicatiemiddel door een geheimhouder is gebruikt, hetgeen de waarborging van het verschoningsrecht kan bemoeilijken.¹⁰ In dat verband is noemenswaardig dat de Hoge Raad voor eventuele sanctiëring van verschoningsrechtgerelateerde vormverzuimen via artikel 359a Sv, betekenis toekent aan de mate waarin de verschoningsgerechtigde ‘passende maatregelen heeft genomen om zijn informatiehuishouding zo in te richten dat de kans op inbreuken op het verschoningsrecht zo gering mogelijk blijft, in het bijzonder waar het de keuze betreft van de communicatiemiddelen’.¹¹ In ons onderzoek concluderen wij dat de eigen verantwoordelijkheid van advocaten om de vertrouwelijkheid van communicatie met cliënten te waarborgen, betekenis heeft voor hun keuze voor bepaalde (typen) communicatiemiddelen. Juist de wens om communicatie vertrouwelijk te houden kan aanleiding zijn om te kiezen voor minder conventionele middelen. Wantrouwen in de naleving van het verschoningsrecht door de strafvorderlijke overheid – veelal versterkt door de opstelling en werkwijze van het OM ten aanzien van dit onderwerp – speelt daarbij vaak een rol. Aldus constateren wij voor (strafrecht-) advocaten een zekere paradox: enerzijds gebruiken zij omwille van hun verschoningsrecht soms bepaalde minder conventionele communicatiemiddelen, anderzijds kan juist dat gebruik hun verschoningsrecht op de tocht zetten, namelijk als deze communicatie in opsporingshanden komt.¹²

In deze bijdrage reflecteren wij op de betekenis van de uitspraak van de Hoge Raad in het licht van de bevindingen uit eerdergenoemd onderzoek. In de volgende paragraaf staan het verschoningsrecht en de uitspraak van de Hoge Raad centraal. Vervolgens bespreken we in paragraaf 3 de uitkomsten van ons eerdere onderzoek naar het gebruik van (extra beveiligde) communicatiemiddelen door advocaten: welke zijn dat, waarom kiezen zij voor bepaalde communicatiemiddelen, welke dilemma’s spelen daarbij, en welke potentiële risico’s, in het bijzonder voor het verschoningsrecht, brengt dat gebruik met zich? In paragraaf 4 gaan we in op de vraag of en, zo ja, in hoeverre de uitspraak van de Hoge Raad gelet op die risico’s zal leiden tot een betere waarborging van het verschoningsrecht van advocaten. In paragraaf 5 sluiten we af met enkele concluderende opmerkingen en aanbevelingen.

2. Waarborgen voor het verschoningsrecht en de uitspraak van de Hoge Raad

Het verschoningsrecht van advocaten vloeit voort uit het algemene rechtsbeginsel dat burgers vertrouwelijk moeten kunnen communiceren met een advocaat.¹³ Bij het recht op vertrouwelijke communicatie wordt doorgaans onderscheid gemaakt tussen de uit het beroep van advocaat voortvloeiende geheimhoudingsplicht en het verschoningsrecht. Het strekt zich uit tot alle informatie die is verkregen in het kader van de normale beroepsuitoefening van de advocaat.¹⁴ Waarborgen voor het verschoningsrecht zijn op verschillende plekken in de wet geregeld en hebben tot doel dat advocaten geen vertrouwelijke informatie hoeven prijs te geven, bijvoorbeeld wanneer zij

Toen was gebleken dat verschoningsgerechtigde telefonische communicatie toch in het opsporingsonderzoek terechtkwam, werd in 2011 een systeem van automatische nummerherkenning ingevoerd

Auteurs

1. Mr. dr. M. Lochs, mr. J.A. Klapwijk, prof. mr. J.H. Crijns en mr. D.B. Sander zijn verbonden aan het Instituut voor Strafrecht & Criminologie van de Universiteit Leiden, respectievelijk als universitair docent, promovenda, hoogleraar en PhD-fellow.

Noten

2. Omwille van de leesbaarheid spreken we hierna van verschoningsrecht en verschoningsgerechtigde als we het functionele verschoningsrecht van de advocaat en de advocaat als functioneel verschoningsge-

rechtigde bedoelen (art. 218 Sv). De verschoningsrechten uit art. 217 en 218a-219b Sv vallen buiten de reikwijdte van dit artikel.
3. Zie onder meer Rb. Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035; Hof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329; CAG 8 december 2023, ECLI:NL:PHR:2023:1122; HR 12 maart 2024, ECLI:NL:HR:2024:375 en D.R. Doorenbos & M.E. Rosing, ‘Recht doen aan het verschoningsrecht’, *TvS&O* 2020/5-6, p. 217-224.
4. HR 12 maart 2024, ECLI:NL:HR:2024:375.

5. *Ibid.*, r.o. 6.5.7.

6. *Ibid.*, r.o. 6.5.4-6.5.5 en 6.6.7.

7. Vgl. de voorgestelde art. 2.7.58-2.7.66 (nieuw) Sv en *Kamerstukken II* 2022/23, 36327, nr. 3, i.h.b. p. 627-632.

8. Een erkenning dat de gevolgde procedure het verschoningsrecht onvoldoende waarborgde, kwam voor het eerst op 25 september 2023. Zie het nieuwsbericht ‘OM in gesprek met strafrechtketen over verschoningsrecht’ op OM.nl.

9. J.A. Klapwijk e.a., *Het gebruik van extra beveiligde communicatiemiddelen door advocaten*, Leiden: Universiteit Leiden 2023.

10. *Ibid.*, p. 72-81.

11. HR 12 maart 2024, ECLI:NL:HR:2024:375, r.o. 6.8.2.

12. Klapwijk e.a. 2023, p. 52-59, 73-82.

13. HR 1 maart 1985, ECLI:NL:HR:1985:AC9066, *NJ* 1986/173, m.nt. Haardt (*Notaris Maas*); zie ook EHRM 13 maart 2007, ECLI:CE:ECHR:2007:0313J UD002339305 (*Castravet/Moldova*), par. 49-51.

14. Vgl. N.A.M.E.C. Fanoy, *De geheimhoudingsplicht en het verschoningsrecht van de advocaat* (diss. Amsterdam UvA), Antwerpen/Apeldoorn: Maklu 2018, p. 204-207.



© Shutterstock

als getuige worden gehoord,¹⁵ of wanneer voorwerpen worden gevorderd¹⁶ of in beslag genomen.¹⁷ Waar het gaat om kennisneming van mogelijk verschoningsgerechtigde stukken geldt het uitgangspunt dat in eerste instantie de geheimhouder moet aangeven of de gegevens onder het verschoningsrecht vallen. Dit standpunt wordt geëerbiedigd, 'tenzij redelijkerwijze geen twijfel erover kan bestaan dat dit standpunt onjuist is'.¹⁸ Die beoordeling is aan de rechter-commissaris, die daarbij zoveel mogelijk het advies van een vertegenwoordiger van de beroepsgroep inwint. Voor zover noodzakelijk mag de rechter-commissaris voor dit oordeel kennisnemen van de betreffende stukken.¹⁹

In de loop der tijd zijn er steeds meer (bijzondere) opsporingsbevoegdheden gekomen waarmee politie en justitie toegang kunnen krijgen tot (grote hoeveelheden en/of digitale) gegevens. Daarom zijn de wettelijke waarborgen aangepast.²⁰ In het bijzonder is artikel 126aa Sv van belang, dat de beslissing over het selecteren en filteren van verschoningsgerechtigde informatie in eerste

instantie bij de officier van justitie belegt.²¹ Nadat was gebleken dat verschoningsgerechtigde telefonische communicatie toch in het opsporingsonderzoek terechtkwam, werd in 2011 een systeem van automatische nummerherkenning ingevoerd. De bedoeling daarvan is dat gesprekken met geregistreerde advocatentelefoonnummers automatisch worden gefilterd en de opname na afloop van het gesprek – zonder dat deze voor politie en justitie toegankelijk is – wordt vernietigd.²² Dit systeem kent echter zijn beperkingen; zo filtert het geen chatcommunicatie (bijvoorbeeld via WhatsApp of Signal) via het geheimhoudernummer.²³

De omgang met op grond van bijzondere opsporingsbevoegdheden gevorderde gegevens kwam in 2019 volop in de belangstelling te staan na door advocatenkantoor Stibbe aangespannen civiele rechtszaken tegen de Staat in verband met mogelijke schendingen van het verschoningsrecht in de *Castor*-zaak. Het ging in deze zaak om

informatie die het OM had verkregen via een vordering van gegevens van een aanbieder van een hostingbedrijf voor e-mailverkeer.²⁴ Uit die procedures kwam naar voren dat het OM en de Fiscale inlichtingen- en opsporingsdienst (FIOD) een werkwijze hanteerden waarbij de selectie en beoordeling van eventueel verschoningsgerechtigde informatie plaatsvond door of onder leiding van de officier van justitie. Niet de rechter-commissaris maar zogenoemde 'geheimhoudingsambtenaren' (opsporingsambtenaren) beslisten dus of sprake was van verschoningsgerechtigde informatie.²⁵

Over de verenigbaarheid hiervan met het verschoningsrecht gaat het arrest van de Hoge Raad van 12 maart 2024. In lijn met de uitgebreide conclusie van advocaat-generaal Hartevelt oordeelt de Hoge Raad dat in de wettelijke regeling thans niet is voorzien in een procedure die het verschoningsrecht waarborgt in gevallen dat, door middel van de inzet van bijzondere opsporingsbevoegdheden, grote hoeveelheden gegevens voor politie en justitie beschikbaar komen. Een dergelijke regeling is wel opgenomen in het wetsvoorstel voor een nieuw Wetboek van Strafvordering. Daarin is neergelegd dat de filtering van mogelijk verschoningsgerechtigde informatie steeds plaatsvindt door de rechter-commissaris.²⁶ Vooruitlopend op het wetgevingsproces formuleert de Hoge Raad voorlopige uitgangspunten voor de omgang met mogelijk verschoningsgerechtigd materiaal.

In de eerste plaats brengt een 'redelijk vermoeden' dat een vordering tot gegevensverstrekking zich mede zal uitstrekken tot geprivilegieerde informatie verplichtingen met zich voor politie en justitie, bijvoorbeeld om van een dergelijk vermoeden melding te maken wanneer de rechter-commissaris wordt gevraagd om een machtiging voor het inzetten van dergelijke opsporingsmethoden.²⁷ De vraag is wel wanneer in concreto kan worden gesproken van een dergelijk vermoeden. De Hoge Raad geeft weliswaar enkele gezichtspunten (zoals de reikwijdte van de gegevensvordering en de aard van de gegevens), maar overweegt ook dat het antwoord afhankelijk is van de feiten en omstandigheden van het geval. Daarbij is de enkele omstandigheid dat de verdachte wordt of is bijgestaan door een advocaat onvoldoende voor een dergelijk vermoeden. Hetzelfde geldt voor de enkele stelling van de verdachte dat de vordering zich mogelijk zal uitstrekken tot geheimhouderinformatie.²⁸

Een tweede uitgangspunt is dat de beoordeling of sprake is van verschoningsgerechtigde informatie plaatsvindt door of onder verantwoordelijkheid van de rechter-commissaris. Deze kan zich daarbij laten bijstaan door

andere functionarissen, maar gewaarborgd moet worden dat geprivilegieerde informatie dan niet bekend wordt bij degenen die zijn belast met het opsporingsonderzoek.²⁹ Daarvoor is onder meer een strikte taak- en functiescheiding noodzakelijk.³⁰ Alleen wanneer op voorhand duidelijk is dat filtering kan plaatsvinden zonder kennisneming van de gegevens, kan dit door of onder leiding van een officier van justitie worden verricht.³¹

Ten derde geldt ook in deze context dat het oordeel of sprake is van geprivilegieerde informatie in principe bij de verschoningsgerechtigde zelf ligt.³² Dat betekent dat diens standpunt in beginsel moet worden ingewonnen, tenzij klemmende redenen van onderzoeksbelang hieraan in de weg staan, of het inwinnen van het standpunt prak-

Bovendien moet het standpunt van de verschoningsgerechtigde dat het om geprivilegieerde informatie gaat worden geëerbiedigd, tenzij er redelijkerwijs geen twijfel over kan bestaan dat dit onjuist is

tisch redelijkerwijs niet mogelijk is. In die gevallen moet het oordeel van een gezaghebbend lid van de beroepsgroep of een andere deskundige worden ingewonnen, of moet de filtering worden uitgesteld.³³ Bovendien moet het standpunt van de verschoningsgerechtigde dat het om geprivilegieerde informatie gaat worden geëerbiedigd, tenzij er redelijkerwijs geen twijfel over kan bestaan dat dit onjuist is.³⁴

De Hoge Raad staat verder stil bij de taakverzwaring die deze werkwijze zal meebrengen voor de kabinetten rechter-commissaris en de wijze van vernietiging van verschoningsgerechtigde gegevens.³⁵ Ook bespreekt de Hoge Raad mogelijke gevolgen van het niet naleven van deze regels. Onder verwijzing naar artikel 359a Sv legt de Hoge Raad de nadruk op de vraag of (wezenlijk) nadeel is ontstaan voor de verdachte. Bij het oordeel of en, zo ja, welke sanctiëring gepast is, kan bovendien meespelen in hoeverre de verschoningsgerechtigde passende maatregelen

15. Art. 218 Sv.

16. Vgl. onder meer art. 96a lid 3 en 126nd lid 2 Sv.

17. Vgl. onder meer art. 96c, 98 en 125f Sv.

18. HR 2 juli 2013, ECLI:NL:HR:2013:CA0434, NJ 2014/12, m.nt. Schalken, onder meer herhaald in HR 18 februari 2020, ECLI:NL:HR:2020:277.

19. HR 2 juli 2013, ECLI:NL:HR:2013:CA0434, r.o. 3.4, NJ 2014/12, m.nt. Schalken.

20. Zie voor een historisch overzicht CAG 8 december 2023, ECLI:NL:PHR:2023:1122, onder 2.

21. Alleen in specifieke situaties is een rol voor de rechter-commissaris weggelegd, zie art. 126aa lid 2 Sv. Zie voor een uitgebreide uiteenzetting Conclusie A-G 8 december 2023, ECLI:NL:PHR:2023:1122, onder 6.

22. Vgl. 'Nummerherkenning politie', advocatenorde.nl; hierover uitgebreider Klapwijk e.a. 2023, p. 44.

23. Hierover uitgebreider Klapwijk e.a. 2023, p. 76-77.

24. O.g.v. art. 126ng lid 2 of art. 126ug lid 2 Sv.

25. Doorenbos & Rosing 2020, p. 217-224. Zie ook (onder meer) Rb. Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035, r.o. 4.19-4.20 en Hof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329.

26. Zie onder meer de voorgestelde art.

2.7.62 en 2.7.66 (nieuw) Sv.

27. HR 12 maart 2024, ECLI:NL:HR:2024:375, r.o. 6.5.1-6.5.3.

28. *Ibid.*, r.o. 6.5.2.

29. *Ibid.*, r.o. 6.5.4-6.5.6.

30. *Ibid.*, r.o. 6.6.8.

31. *Ibid.*, r.o. 6.6.6.

32. *Ibid.*, r.o. 6.5.7.

33. *Ibid.*, r.o. 6.6.4.

34. *Ibid.*, r.o. 6.6.3.

35. *Ibid.*, r.o. 6.6.9-6.7.2.

heeft genomen om inbreuken op het verschoningsrecht zoveel mogelijk te voorkomen. Dit gezichtspunt valt te relateren aan de ernst van het verzuim, een van de factoren die de rechter blijkens artikel 359a lid 2 Sv heeft te betrekken bij de keuze voor een bepaalde sanctie.³⁶

Deze uitspraak beslecht de soms hoogoplopende discussie over de wijze waarop het verschoningsrecht moet worden gewaarborgd bij inbeslagneming van gegevens die zijn verkregen via bijzondere opsporingsbevoegdheden. Ondanks de wettelijke lacune gelden hiervoor, aldus de Hoge Raad, geen andere uitgangspunten dan voor klassieke dwangmiddelen zoals doorzoeking en inbeslagneming.³⁷ De uitspraak biedt daarmee duidelijkheid en is van belang voor een effectievere waarborging van het verschoningsrecht. Tegelijkertijd is de uitspraak toegespitst op de specifieke context van deze zaak – de inbeslagneming van gegevens die zijn gevorderd van de aanbieder van een communicatiedienst – en kan verschoningsgerechtigde informatie op allerlei manieren in het opsporingsonderzoek terechtkomen. Hierna zullen wij, aan de hand van bevindingen uit ons eerdergenoemde onderzoek, ingaan op door advocaten gebruikte (extra beveiligde) communicatiemiddelen en de uiteenlopende wijzen waarop verschillende communicatiemiddelen risico's voor de vertrouwelijkheid met zich kunnen brengen.

3. Het gebruik van (extra beveiligde) communicatiemiddelen door advocaten en de risico's voor het verschoningsrecht

3.1. De gebruikte communicatiemiddelen en de beweegredenen daarvoor

Voor de communicatie met de cliënt gebruiken advocaten verschillende, al dan niet extra beveiligde, communicatiemiddelen.³⁸ Naast persoonlijk en telefonisch contact kiezen advocaten geregeld voor het gebruik van chatapplicaties zoals WhatsApp, Signal en Telegram, soms voor extra beveiligde e-maildiensten en – in beperkte mate – voor cryptotelefoons.³⁹ In zijn algemeenheid geldt dat het belang van geheimhouding in de keuze voor de wijze van communicatie een belangrijke rol speelt.⁴⁰ De geïnterviewde advocaten zijn zich sterk bewust van hun geheimhoudingsplicht en de daarbij horende verantwoordelijkheden, zoals onder meer genormeerd door het tuchtrecht.⁴¹ Andere beweegredenen voor de keuze voor een bepaalde wijze van communiceren zijn de wens of het initiatief van de cliënt, praktische aspecten (bijvoorbeeld gebruiksvriendelijkheid) en het imago van bepaalde communicatiemiddelen.⁴² Hierna wordt uitgebreider ingegaan op de verschillende communicatiemiddelen en de beweegredenen om deze (niet) te gebruiken.

Veel van de geïnterviewde advocaten geven de voorkeur aan uitwisseling van vertrouwelijke informatie in persoon. Er kunnen echter allerlei redenen zijn waarom een persoonlijke bespreking niet (altijd) mogelijk is: er moeten (omvangrijke) stukken worden gedeeld en mede daardoor valt er veel te bespreken, er moet met spoed worden overlegd, cliënten zijn gedetineerd, wonen ver weg of soms (permanent) in het buitenland. Die praktische realiteit brengt mee dat advocaten vaak kiezen voor een communicatiemiddel dat zowel praktisch goed bruikbaar is als (voldoende) veilig.⁴³

Telefonisch contact via de geheimhoudertelefoon wordt door veel advocaten gereserveerd om minder gevoelige (praktische) zaken te bespreken of afspraken te maken. Daarbij speelt mee dat veel advocaten een zekere reserve hebben ten aanzien van de werking van het herkenningssysteem van geheimhoudernummers, al dan niet ingegeven door bekende incidenten.⁴⁴ Er zijn ook advocaten met een uitgesproken gebrek aan vertrouwen in de

Voor het risico dat de communicatie via hacks of inbeslagname van servers bij de justitiële autoriteiten terechtkomt, is reden om geen cryptotelefoon (meer) te gebruiken

bescherming die het geheimhoudernummer biedt. Soms leidt dat ertoe dat zij – al dan niet op verzoek van de cliënt – bewust op een andere wijze bellen, namelijk met de belfunctie van chatapplicaties zoals WhatsApp en Signal. In de wijze waarop deze applicaties zijn beveiligd (met encryptie), zien zij een waarborg tegen overheidsinterceptie.⁴⁵ Dergelijke applicaties worden, mede omwille van het praktische gemak, ook veelvuldig gebruikt voor chatcontact met de cliënt.⁴⁶

Wat betreft communicatie via e-mail zagen wij relatief grote verschillen tussen advocaten. Anders dan in de commune strafrechtspraktijk is e-mail in de financieel-economische (strafrechts)praktijk een veelgebruikt communicatiemiddel, waarmee soms ook gevoelige informatie wordt gedeeld. Daarom wordt soms gekozen voor extra beveiligingsmaatregelen (encryptie) of het gebruik van een extra beveiligde e-mailprovider als Zivver of Proton Mail. Praktische overwegingen, vooral gebruiksenvriendelijkheid, maken echter dat veel advocaten minder vaak beveiligd e-mailen dan zij uit oogpunt van vertrouwelijkheid wenselijk achten. Wel zorgen de geïnterviewde advocaten ervoor dat uit het e-mailadres, de onderwerpregel en/of de ondertekening blijkt dat het om geprivilegieerde communicatie gaat.⁴⁷ Mocht deze dan door de autoriteiten worden onderschept, zal doorgaans zonder kennisneming van de inhoud duidelijk zijn dat het om verschoningsgerechtigde inhoud gaat.

Het meest controversiële communicatiemiddel onder de geïnterviewde advocaten is de cryptotelefoon. Slechts enkelen hebben verklaard een dergelijke telefoon te hebben gebruikt en ook uit andere bronnen ontstaat de indruk dat het om relatief weinig advocaten gaat.⁴⁸ Een belangrijke reden om een cryptotelefoon te gebruiken is een gebrek aan vertrouwen in de vertrouwelijkheid van andere communicatiemiddelen en de legitieme behoefte

van de cliënt om extra beveiligd te communiceren. Het initiatief voor het gebruik van een cryptotelefoon was dan ook doorgaans van de cliënt afkomstig, waarbij soms meespeelde dat (huidige en potentieel nieuwe) cliënten alleen op deze wijze bereikbaar waren. Veel advocaten zien echter risico's in het gebruik van cryptotelefoons. Soms wordt gewezen op het criminele imago en daarmee samenhangende integriteitskwesaties, maar vooral het risico dat de communicatie via *hacks* of inbeslagname van servers bij de justitiële autoriteiten terechtkomt, is reden om geen cryptotelefoon (meer) te gebruiken.⁴⁹

Bovenstaande maakt duidelijk dat advocaten bij de keuze voor bepaalde (extra beveiligde) communicatiemiddelen de nodige argumenten moeten afwegen, waarbij afzonderlijke argumenten niet zelden in uiteenlopende richtingen wijzen. Bij veel van de geïnterviewde advocaten speelt in meer of mindere mate mee dat niet zonder meer wordt vertrouwd op een juiste omgang met verschoningsgerechtigde informatie in het opsporingsonderzoek. Dat wantrouwen lijkt door de gang van zaken in de *Castor*-zaak bij veel advocaten stevig te zijn aangewakkerd.⁵⁰ In combinatie met de noodzaak van (technische) kennis over de verschillende communicatiemiddelen en de daarbij betrokken afwegingen, kan dit de keuze voor een bepaald communicatiemiddel voor een advocaat in een concreet geval lastig maken. Daarop gaan we hierna verder in door potentiële risico's van verschillende communicatiemiddelen te bespreken.

3.2. Knelpunten in het licht van het verschoningsrecht

Vanuit het perspectief van de waarborging van het verschoningsrecht kunnen bij het gebruik van de hiervoor besproken communicatiemiddelen verschillende knelpunten worden geïdentificeerd.⁵¹

Bij het gebruik van chatapplicaties geldt dat deze doorgaans zijn gekoppeld aan het telefoonnummer dat als geheimhoudernummer is opgegeven. Toch worden hiermee uitgewisselde berichten – anders dan sommige van de geïnterviewde advocaten denken – niet automatisch als geheimhoudercommunicatie geïdentificeerd. Wanneer dergelijke communicatie (doorgaans door inbeslagname van een telefoon) in het opsporingsonderzoek terechtkomt, bestaat het risico dat opsporingsambtenaren pas bij kennisneming van de inhoud van die communicatie constateren dat het om vertrouwelijke communicatie gaat. De herkenbaarheid van het geprivilegieerde karakter van de communicatie kan daarnaast (mede) afhangen van de naam die de cliënt er zelf, bij het opslaan van het

Daarbij moet worden bedacht dat bij onderzoek na inbeslagname van een gegevensdrager voorafgaande filtering op geheimhoudernummers niet standaard plaatsvindt

telefoonnummer, aan heeft gekoppeld. Daarbij moet worden bedacht dat bij onderzoek na inbeslagname van een gegevensdrager voorafgaande filtering op geheimhoudernummers niet standaard plaatsvindt. Vaak is niet bekend dat er is gecommuniceerd met een advocaat, terwijl het OM ook niet beschikt over een overzicht van de als geheimhoudernummer geregistreerde telefoonnummers. Bovendien is het praktisch ondoenlijk om bij iedere inbeslaggenomen gegevensdrager (standaard) een zoekslag te maken teneinde vertrouwelijke communicatie uit de gegevensdrager te filteren, niet alleen gelet op capaciteit en middelen, maar ook vanwege het feit dat voor een dergelijke zoekslag specifieke software gebruikt wordt die niet voor alle onderzoeken beschikbaar is.⁵²

De problematiek bij e-mailcommunicatie is enigszins vergelijkbaar, en speelt vooral bij inbeslagname van gegevensdragers of wanneer e-mailgegevens zijn verkregen na een vordering tot gegevensverstrekking. E-mailadressen van advocaten zijn doorgaans vrij eenvoudig als zodanig te herkennen.⁵³ De uitgangspunten van de Hoge Raad bieden bovendien een kader voor de omgang met grote hoeveelheden e-mailcommunicatie. Niettemin kleven er verschillende (technische) moeilijkheden aan het doorzoeken van grote datasets, waarvoor doorgaans de forensische softwaretool *Hansken* wordt gebruikt.⁵⁴ Deze tool biedt de mogelijkheid om te filteren op mogelijke geheimhouderinformatie aan de hand van vooraf – in overleg met de rechter-commissaris en/of de advocaat van de verdachte – vast te stellen zoektermen.⁵⁵ Daarbij is het kiezen van de juiste zoektermen geen sinecure. Het niet includeren van bepaalde zoektermen kan leiden tot het onterecht niet uitsluiten van geprivilegieerde informatie, waar tegelijkertijd het wel includeren van deze zoektermen kan leiden tot het onterecht uitsluiten van niet-geprivilegieerde informatie. Bovendien kunnen er complicaties optreden wanneer het gaat om zogenaamde 'samenhangende sporen', zoals bijlagen bij e-mails, of

36. *Ibid.*, r.o. 6.8.1-6.8.2.

37. *Ibid.*, r.o. 6.4.3, 6.5.5 en 6.5.7.

38. De empirische informatie is verzameld door middel van interviews en schriftelijke vragenlijsten, gehouden met c.q. uitgezet onder advocaten, deken, medewerkers van het OM en het NFI. De meeste geïnterviewde advocaten waren werkzaam in de strafrechtspraktijk. Zie nader Klapwijk e.a. 2023, p. 20-25.

39. *Ibid.*, p. 50-52.

40. *Ibid.*, p. 52-59.

41. Vgl. art. 10a en 11a Advocatenwet en regel 3 van de Gedragsregels advocatuur. Lid 2 van regel 3 schrijft voor dat de advocaat 'passende maatregelen' neemt om ervoor te zorgen dat de vertrouwelijkheid van de communicatie is gewaarborgd, in het bijzonder waar het gaat om de keuze van de communicatiemiddelen.

Zie uitgebreider Klapwijk e.a. 2023, p. 39-40.

42. Klapwijk e.a. 2023, p. 59-65.

43. *Ibid.*, p. 54-56, 65.

44. Zie bijvoorbeeld K. Pijnappels, 'Manco's aan systeem nummerherkenning DJI', *Advocatenblad* 13 december 2019.

45. Klapwijk e.a. 2023, p. 54-56.

46. *Ibid.*, p. 50, 55-56, 59.

47. *Ibid.*, p. 51, 56-57, 59, 64.

48. Schattingen lopen uiteen van vijf tot twintig gebruikers; *ibid.*, p. 51-52.

49. *Ibid.*, p. 57-59, 60-63.

50. *Ibid.*, p. 53-55, 65.

51. In ons onderzoek hebben wij ook andere potentiële risico's besproken, te weten

risico's voor de onafhankelijkheid, de integriteit en in relatie tot de documentatieplicht van advocaten; *ibid.*, p. 66-72.

52. *Ibid.*, p. 55-56, 76-77.

53. *Ibid.*, p. 77.

54. Nederlands Forensisch Instituut, *Informatieblad Vernietigen van digitale sporen met verschoningsgerechtigde informatie*, Den Haag: Nederlands Forensisch Instituut 2023.

55. Zie over die werkwijze bijvoorbeeld HR 19 september 2023, ECLI:NL:HR:2023:1268.

wanneer bestanden door middel van doorsturen en/of downloaden op meerdere plekken in het databestand voorkomen.⁵⁶ Inmiddels zijn door de Nederlandse orde van advocaten (NOvA) en het OM de eerste stappen gezet voor de ontwikkeling van een e-mailherkenningssysteem.⁵⁷ Als dat er inderdaad komt, zou dat de huidige problematiek voor een belangrijk deel kunnen oplossen.

De (on)herkenbaarheid als geheimhouder speelt het meest nadrukkelijk bij het gebruik van cryptotelefoons. Dat hangt samen met de *hacks* of inbeslagname van servers van cryptocommunicatiediensten als Ennetcom, EncroChat en Sky ECC, waarmee (buitenlandse) opsporingsautoriteiten de afgelopen jaren furore maakten en die in de strafrechtspraktijk en -wetenschap de nodige stof deden opwaaien.⁵⁸ Het feit dat dergelijke diensten voornamelijk door criminele netwerken zouden worden gebruikt en daardoor een doelwit van opsporingsdiensten zijn, maakt ze – ondanks de extra beveiligingsfunctionaliteiten – kwetsbaar voor overheidsinterceptie.⁵⁹ Daarbij komt dat de door advocaten gebruikte cryptotelefoonnummers doorgaans niet bij het OM bekend zijn en het gebruik van *nicknames* het herkennen van verschoningsgerechtigde communicatie bemoeilijkt. Daardoor bestaat het risico dat pas na kennisneming van de inhoud van de communicatie duidelijk wordt dat het gaat om advocaat-cliëntcontact.⁶⁰ Om de datasets te kunnen filteren op verschoningsgerechtigd materiaal heeft het OM in het verleden een oproep gedaan aan advocaten om zich te melden als zij een cryptotelefoon gebruik(t)en.⁶¹ Uit ons onderzoek blijkt dat hieraan maar zeer beperkt gehoor is gegeven.⁶² Het niet willen melden lijkt mede te zijn ingegeven door de vrees dat met het kenbaar maken van de gebruikte cryptotelefoongegevens de aandacht juist op vertrouwelijke – en (daarmee) voor justitie interessante – informatie wordt gevestigd. Wanneer het vertrouwen ontbreekt dat die informatie vervolgens (zonder daarvan kennis te nemen) onleesbaar wordt gemaakt, zou het melden immers strijd kunnen opleveren met de geheimhoudingsplicht. Zeker wanneer (ook of vooral) de cliënt niet vertrouwt op een juiste handelswijze bij de opsporing, kan dit voor de advocaat een lastige afweging zijn.⁶³

Uit deze beknopte bespreking volgt dat zich risico's kunnen voordoen bij het – doorgaans uit een volstrekt legitiem streven naar vertrouwelijkheid voortkomende – gebruik van extra beveiligde en soms minder conventionele communicatiemiddelen door advocaten. Vele daarvan houden verband met de (on)herkenbaarheid als geheimhouder. Bij het filteren van geprivilegieerde informatie uit grote hoeveelheden digitale data kunnen zich bovendien (technische) complicaties voordoen.

4. Terug naar de uitspraak van de Hoge Raad

In het licht van de bevindingen uit ons onderzoek kan het kader van de Hoge Raad worden verwelkomd. Het biedt duidelijke handvatten voor een betere waarborging van het verschoningsrecht bij de omgang met (digitale) gegevens in het opsporingsonderzoek. Het uitgangspunt dat de filtering van geprivilegieerde informatie door – of in ieder geval onder leiding van – de rechter-commissaris wordt verricht, betekent een belangrijke verbetering voor een effectieve waarborging van het verschoningsrecht. Daarmee wordt immers voorkomen dat opsporingsambtenaren kennisnemen van de inhoud van verschoningsgerechtigde informatie. Hetzelfde geldt voor het uitgangspunt dat het standpunt van de verschoningsgerechtigde wordt ingewonnen en geëerbiedigd. Tegelijkertijd maken de bevindingen uit ons onderzoek duidelijk dat in de praktijk spelende uitdagingen voor het verschoningsrecht ook bij gebruikmaking van dit nieuwe kader nog altijd aandacht behoeven.

Allereerst is duidelijk dat advocaten veel verschillende communicatiemiddelen gebruiken in het contact met de cliënt. De communicatie kan dan ook op allerlei verschillende wijzen in het opsporingsonderzoek terechtkomen. Mede gelet op de hiervoor al kort geschetste (praktische en technische) beperkingen en uitdagingen bij het doorzoeken van (grote hoeveelheden) digitale gegevens, zullen zich in de praktijk complexe vragen blijven aandienen, óók met betrekking tot het verschoningsrecht.

Verder kan de vraag opkomen hoe de eis van het 'redelijk vermoeden' van de aanwezigheid van geprivilegieerde informatie zal worden uitgelegd. Moeten de opsporingsdiensten concreet weet hebben van het feit dat advocaat en cliënt op een bepaalde wijze (bijvoorbeeld per e-mail) contact hebben gehad? En hoe komt deze wetenschap tot de opsporingsdiensten, in aanmerking nemende dat de verdachte noch diens advocaat doorgaans voorafgaand aan het doen van een vordering aan een communicatiedienst daarvan in kennis zullen worden gesteld? Iets vergelijkbaars geldt voor communicatie met een cryptotelefoon. Hoewel een (nieuwe) *hack* doorgaans publiekelijk bekend wordt gemaakt, heeft dat er in ieder geval in het verleden niet vaak toe geleid dat advocaten zich meldden als cryptotelefoongebruiker. En als dat wel gebeurt, of als het OM daar ambtshalve – bijvoorbeeld uit eerdere onderzoeken – van op de hoogte is, brengt dat dan mee dat de filtering onder leiding van de rechter-commissaris moet plaatsvinden?

Het is dan ook van belang dat de Hoge Raad benadrukt dat het redelijk vermoeden van de aanwezigheid

Waar juist het vertrouwen bij advocaten de afgelopen jaren een flinke deuk lijkt te hebben opgelopen, kan er niet zonder meer van uit worden gegaan dat met de uitspraak van de Hoge Raad ook een einde is gekomen aan de (felle) discussies tussen OM en advocatuur op dit thema

Het is bij de beoordeling van die ‘passende maatregelen’ van belang om ook de praktische realiteit niet uit het oog te verliezen

van geprivilegieerde informatie ook gaandeweg het opsporingsonderzoek kan ontstaan. De kwetsbaarheid in dit verband is evenwel dat dit vermoeden vaak pas zal ontstaan na ontvangst – en dus (mogelijk deels) inhoudelijke kennisname – van de gegevens door opsporingsambtenaren. Hoewel het kader van de Hoge Raad een duidelijk richtsnoer biedt voor de vervolgens te hanteren handelswijze, sluit het niet uit dat kennis wordt genomen van verschoningsgerechtigd materiaal door ambtenaren die daar eigenlijk geen toegang toe zouden moeten hebben. Bovendien valt of staat een juiste uitvoering – nog evenzeer als voorheen – met de integriteit van de betrokken opsporingsambtenaren. Waar juist het vertrouwen daarin bij advocaten de afgelopen jaren een flinke deuk lijkt te hebben opgelopen,⁶⁴ kan er niet zonder meer van uit worden gegaan dat met de uitspraak van de Hoge Raad ook een einde is gekomen aan de (felle) discussies tussen OM en advocatuur op dit thema.

Daarnaast rijst de vraag in welke gevallen op voorhand duidelijk is dat filtering kan plaatsvinden zonder kennisneming van het verschoningsgerechtigde materiaal, zodat dit onder leiding van het OM kan gebeuren. Dit is vooral van belang bij grote digitale datasets, omdat het uiterst complex is het proces van filtering zo in te richten dat (alle) geprivilegieerde informatie eruit wordt gefilterd, zonder het net zo wijd uit te gooien dat ook veel niet-geprivilegieerde informatie daarin verdwijnt. Bovendien kunnen zich complicaties voordoen wanneer informatie, bijvoorbeeld bijlagen bij een e-mail van een advocaat naar de cliënt, door de cliënt wordt doorgestuurd.⁶⁵ In dat licht is van betekenis dat de Hoge Raad expliciet overweegt dat ook andere gegevens dan de in artikel 126aa Sv genoemde ‘mededelingen door of aan’ een verschoningsgerechtigde onder het verschoningsrecht kunnen vallen.⁶⁶ Een werkwijze waarbij alleen op het e-mailadres van de advocaat wordt gefilterd is dan vaak niet toereikend, en de vraag naar de optimale wijze van filtering is dan al snel zo complex dat betrokkenheid van de rechter-commissaris en de verschoningsgerechtigde wenselijk moet worden geacht.

Omdat de uitspraak van de Hoge Raad is toegespitst op de problematiek rondom het vorderen van (grote hoeveelheden) digitale gegevens, bieden de daarin neergelegde uitgangspunten bovendien niet zonder meer een bruikbaar kader voor geprivilegieerde communicatie die op andere wijze in het opsporingsonderzoek terechtkomt. Met name in gevallen waarin meer ad hoc op dergelijke communicatie wordt gestuit – bijvoorbeeld door het uitlezen van gesprekken via een chatapplicatie op een inbeslaggenomen telefoon –, blijft het goed mogelijk dat opsporingsambtenaren eerst door kennisneming van die communicatie ontdekken dat het om verschoningsgerechtigd materiaal gaat. Omdat het geheimhoudernummer in deze context geen automatische bescherming biedt, is het waarschijnlijk afhankelijk van de wijze waarop het telefoonnummer van de advocaat in de telefoon van de cliënt is opgeslagen, of eenvoudig herkenbaar is dat het om advocaat-cliëntcontact gaat. Denkbaar is verder dat een advocaat na inbeslagname van de telefoon van een cliënt meldt dat in de telefoon mogelijk geprivilegieerde communicatie is opgeslagen. De vraag is vervolgens wanneer zo’n mededeling aanleiding zal moeten zijn voor het inschakelen van de rechter-commissaris, gelet op hetgeen de Hoge Raad overweegt over het ‘redelijke vermoeden’ dat inbeslaggenomen gegevens mede verschoningsgerechtigd materiaal bevatten.⁶⁷

Tot slot nog een enkele opmerking over de overwegingen van de Hoge Raad omtrent de consequenties van het niet naleven van de voorgeschreven procedure, in het bijzonder de betekenis die in dat verband wordt toegekend aan de vraag of de advocaat passende maatregelen heeft genomen om de vertrouwelijkheid van de communicatie te waarborgen. Volgens de Hoge Raad kan de keuze voor de communicatiemiddelen daarbij een rol spelen. Het is op grond van deze overweging voorstelbaar dat bij het gebruik van minder conventionele communicatiemiddelen, bijvoorbeeld cryptotelefoons, minder snel gevolgen hoeven te worden verbonden aan inbreuken op het verschoningsrecht dan bij het gebruik van meer conventionele communicatiemiddelen zoals e-mail. Gelet op de risico’s van cryptotelefoons voor het waarborgen van het verschoningsrecht⁶⁸ zou dat op zichzelf niet onbegrijpelijk zijn. Tegelijkertijd blijkt uit ons onderzoek dat het gebruik van een cryptotelefoon (mede) kan zijn ingegeven door het op zichzelf legitieme streven naar veilige communicatie.⁶⁹ Dat roept de vraag op of de intenties van de betrokken advocaat relevant zijn in het kader van de toepassing van artikel 359a Sv. Ligt het verbinden van een (zwaardere) sanctie aan een verschoningsrechtgerelateerd vormverzuim bijvoorbeeld eerder in de rede als de cryptotelefoon is gebruikt met de bedoeling zo veilig mogelijk te communiceren met de cliënt bij de

56. Nederlands Forensisch Instituut 2023 en Klapwijk e.a. 2023, p. 78-79.

57. ‘NOVA en OM willen verschoningsrecht beter waarborgen met mailherkenningsysteem’, 4 april 2024, advocatenorde.nl.

58. Vgl. daarover bijvoorbeeld de artikelen in afl. 2 van 2022 van TBS&H.

59. Klapwijk e.a. 2023, p. 32-36, 74.

60. *Ibid.*, p. 74-76.

61. ‘Advocaten kunnen zich bij OM melden als geheimhouder in versleutelde chatdiensten’, 23 april 2021, advocatenorde.nl.

62. Klapwijk e.a. 2023, p. 75.

63. *Ibid.*, p. 75-76.

64. Vgl. het slot van par. 3.1.

65. Het feit dat verschoningsgerechtigd materiaal onder een ander dan de advocaat wordt aangetroffen, doet immers geen afbreuk aan het verschoningsgerechtigde karakter van dat materiaal, vgl. HR 13 oktober 2015, ECLI:NL:HR:2015:3076, NJ 2016/8, m.nt. Vellinga-Schootstra.

66. Onder verwijzing naar HR 10 april 2018, ECLI:NL:HR:2018:553, r.o. 3.6; zie ook HR 19 september 2023, ECLI:NL:HR:2023:1268.

67. Vgl. par. 2.

68. Zie daarover par. 3.2.

69. Zie par. 3.1.

Dat OM en advocatuur elkaar in dit kader hebben weten te vinden valt positief te waarderen

normale beroepsuitoefening, dan wanneer dat gebruik ingegeven lijkt te zijn door minder zuivere motieven? En hoe zijn dergelijke intenties vast te stellen? Bovendien rijst de vraag hoe eventuele voorzorgsmaatregelen die advocaten kunnen treffen (zoals het melden van de cryptotelefoon bij de deken of het OM), in dit verband moeten worden gewaardeerd. Bepaalt het al dan niet treffen van dergelijke maatregelen (mede) de omvang en/of de ernst van het vormverzuim?

Ook ten aanzien van chatapplicaties zoals WhatsApp, Signal en Telegram rijzen in dit verband vragen: zijn dit op zichzelf passende communicatiemiddelen, of vereist het gebruik daarvan extra voorzorgsmaatregelen, en zo ja welke? Gelet op de aard van dergelijke communicatiemiddelen lijkt het minder eenvoudig dan bij e-mail om in afzender, aanhef en/of ondertekening (steeds) tot uitdrukking te brengen dat het om geprivilegieerde informatie gaat. Het is bij de beoordeling van die 'passende maatregelen' wat ons betreft van belang om ook de praktische realiteit niet uit het oog te verliezen, waarin advocaten te maken kunnen hebben met niet (altijd) goed bereikbare of in het buitenland verblijvende cliënten, terwijl advocaten en/of cliënten soms vanwege – op zichzelf niet onbegrijpelijk – wantrouwen in (strafvorderlijke) overheden specifieke opvattingen kunnen hebben over de wijze waarop zij wensen te communiceren. In combinatie met het gegeven dat er tot op heden geen eenduidige richtlijnen zijn voor de vraag welke communicatiemiddelen al dan niet als passend worden gezien,⁷⁰ kan de keuze voor de wijze van communiceren voor de advocaat dan ook ingewikkelde dilemma's met zich brengen.

5. Conclusie

Met de uitspraak van de Hoge Raad is veel aan duidelijkheid gewonnen waar het gaat om de waarborging van het verschoningsrecht bij het vorderen van (grote hoeveelheden) digitale gegevens. De Hoge Raad geeft heldere kaders waaraan de praktijk duidelijk behoefte had. In zoverre kan de uitspraak een positieve bijdrage leveren aan effectieve(re) waarborging van het verschoningsrecht en daarmee een stap zijn in de richting van herstel van vertrouwen tussen OM en advocatuur op dit thema. Tegelijkertijd zijn met de uitspraak niet alle vragen beantwoord. De Hoge Raad heeft een kader geschetst voor onderzoek aan grootschalige digitale datasets verkregen door een vordering tot gegevensverstrekking aan een derde. Of en in hoeverre dit kader ook bruikbaar is voor onderzoek aan mogelijk geprivilegieerde informatie die op andersoortige wijze is verkregen, zal nog moeten blijken. Voorts rijst de vraag hoe de door de Hoge Raad geformuleerde uitgangspunten in de praktijk hun beslag moeten krijgen, zowel bij onderzoek aan grootschalige datasets verkregen door middel van een vordering tot gegevensverstrekking of *hacks* van cryptocommunicatiediensten als bij meer incidenteel onderzoek aan inbeslaggenomen gegevensdragers. In dat kader komt mede betekenis toe aan de vraag of en in hoeverre de kabinetten rechter-commissaris in de praktijk in staat zullen blijken de hun toebedeelde taak adequaat te vervullen, zowel in termen van capaciteit als in termen van (technische) kennis en middelen.

Bij deze stand van zaken blijft het vanzelfsprekend van belang dat advocaten ook zelf de vertrouwelijkheid van hun communicatie zoveel mogelijk waarborgen. Deze verantwoordelijkheid vloeit niet alleen voort uit de beroepsvereisten voor de advocatuur, maar lijkt ook door de Hoge Raad nader te worden onderstreept in zijn overweging dat het niet voldoende nemen van passende maatregelen door de advocaat een relevante factor kan zijn bij de sanctiëring van verschoningsrechtgerelateerde vormverzuimen. Advocaten kunnen aan deze verantwoordelijkheid tegemoetkomen door het maken van een weloverwogen keuze voor bepaalde communicatiemiddelen (bijvoorbeeld het slechts in uitzonderlijke gevallen gebruiken van een cryptotelefoon) en door een zorgvuldig gebruik van het gekozen communicatiemiddel (bijvoorbeeld door te kiezen voor een herkenbare gebruikersnaam bij het gebruik van een cryptotelefoon of encryptie bij het gebruik van e-mail).

Deze verantwoordelijkheid voor het kiezen van passende communicatiemiddelen kan echter niet louter bij individuele advocaten zelf worden gelegd. Van de NOVA mag worden verwacht dat zij – waar aangewezen in samenwerking met het OM – advocaten de nodige hulp biedt bij het maken van de juiste keuze, bijvoorbeeld door middel van het formuleren van richtlijnen over te gebruiken communicatiemiddelen en eventuele passende voorzorgsmaatregelen. Hetzelfde geldt voor het bieden van de nodige faciliteiten aan advocaten. Voor wat betreft dit laatste kan onder meer worden gedacht aan het inrichten van een systeem van automatische e-mailherkenning, waarvoor inmiddels in overleg tussen OM en NOVA de eerste stappen zijn gezet.⁷¹ Dat OM en advocatuur elkaar in dit kader hebben weten te vinden valt positief te waarderen. Van beide mag worden verwacht dat zij in een constructieve dialoog met elkaar treden, gericht op het vormgeven van systemen en praktijken die tot een optimale waarborging van het verschoningsrecht leiden, waarbij wordt gewerkt aan herstel van het wederzijdse vertrouwen.⁷² Want tegen onderling wantrouwen is geen jurisprudentieel kader of gemoderniseerd wetboek opgewassen. •

⁷⁰ Zie uitgebreider Klapwijk e.a. 2023, p. 72-73, 101-102.

⁷¹ Vgl. 'NOVA en OM willen verschoningsrecht beter waarborgen met mailherkenningssysteem', 4 april 2024, advocatenorde.nl; C. Geukers, 'Advies: eigen mailsysteem

voor advocaten', *Advocatenblad* 2024, afl. 3, p. 16-17; 'Beveiligd mailsysteem voor advocaten moet eind maken aan wantrouwen tegen OM', *FD* 5 april 2024.

⁷² Zie voor deze en andere aanbevelingen Klapwijk e.a. 2023, p. 98-102.