Universiteit Leiden
Rechtsgeleerdheid

Het gebruik van extra beveiligde communicatiemiddelen door advocaten

J.A. Klapwijk

M. Lochs

D.B. Sander

J.H. Crijns

Met medewerking van:

B.H.M. Custers

B.W. Schermer

Inhoudsopgave

Voorwoord

In dit rapport zijn de bevindingen neergelegd van het onderzoek dat de Universiteit Leiden in opdracht van de Nederlandse orde van advocaten heeft verricht naar het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten. Het rapport biedt inzicht in de verschillende beweegredenen van advocaten om wel of niet van dergelijke communicatiemiddelen gebruik te maken. Daarnaast worden verschillende (potentiële) risico's geïdentificeerd die met het gebruik van dergelijke communicatiemiddelen gepaard kunnen gaan. Het onderwerp van dit rapport raakt aan andere actuele thema's, waaronder met name het recht op vertrouwelijke communicatie tussen advocaat en cliënt en de waarborging daarvan in de praktijk. Ook deze thema's komen, voor zover van belang voor de beantwoording van de onderzoeksvragen, in dit rapport aan de orde.

Graag spreken wij hier onze dank uit aan iedereen die de uitvoering van dit onderzoek mede mogelijk heeft gemaakt.

In de eerste plaats danken wij de Nederlandse orde van advocaten voor het verstrekken van de opdracht tot dit onderzoek en de bereidheid om ons tijdens het onderzoek te ondersteunen, onder meer bij het leggen van contacten met de buitenlandse balies.

Verder zijn wij veel dank verschuldigd aan alle respondenten en de organisaties waaraan zij zijn verbonden voor hun bereidheid om in uitgebreide interviews en door middel van schriftelijke vragenlijsten hun kennis van, ervaringen met en opvattingen over het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten met ons te delen. Evenzeer danken wij onze buitenlandse contacten die schriftelijk hebben gereageerd op de vragen die wij hen in het kader van het rechtsvergelijkend onderzoek hebben voorgelegd en ons in contact brachten met andere relevante personen.

Wij danken bovendien Joost Nan, Gert-Jan van Olst, Liselotte Postma en Karin van Wingerde van de Erasmus Universiteit, voor hun bereidheid om mee te denken bij de opzet van het onderzoek en mee te lezen bij conceptversie van dit rapport.

Tot slot spreken wij graag onze dank uit aan Stijn van den Wijngaard, die gedurende de eerste maanden van het project aan het onderzoeksteam was verbonden, Aimée Lijten, die als student-assistent onmisbaar was bij het transcriberen van de interviews, en Marc van Walsem, die als student-assistent heeft geholpen bij het redigeren van het rapport.

Leiden, 17 oktober 2023

Hanne Klapwijk, Marianne Lochs, David Sander en Jan Crijns

Samenvatting

In opdracht van de Nederlandse orde van advocaten heeft de Universiteit Leiden onderzoek gedaan naar het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten. In dit onderzoek staan de volgende vragen centraal:

1. *Worden of werden extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruikt door advocaten en, zo ja, welke middelen en waarom (niet)?*
2. *Hoe moet het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten worden bezien, mede in het licht van de risico's daarvan en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?*

Het onderzoek is uitgevoerd om inzicht te verkrijgen in de aard en omvang van het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen onder advocaten en de beweegredenen van advocaten om wel of niet van dergelijke middelen gebruik te maken. Daarnaast worden potentiële risico's voor advocaten die gebruik maken van extra beveiligde en/of identiteitsversluierende communicatiemiddelen in kaart gebracht. Tot slot strekt het onderzoek ertoe om relevante kennis over de praktijk, regelgeving en het beleid in het buitenland te vergaren.

Ter beantwoording van de hoofd- en deelvragen zijn verschillende onderzoeksmethoden gehanteerd. Allereerst zijn reeds bestaande bronnen waaronder wet- regelgeving, jurisprudentie, literatuur en (overige) openbaar toegankelijke informatie geanalyseerd met als doel de uiteenzetting van de relevante (technische) aspecten en juridische kaders (*desk research*). Daarnaast is informatie verzameld door middel van het uitsturen van schriftelijke vragenlijsten en het afnemen van diepte-interviews bij verschillende actoren werkzaam in de rechtspraktijk, waaronder zeventien advocaten, twee medewerkers van het OM, een medewerker van het NFI en drie (oud of huidig) dekens. Tot slot is ten behoeve van een blik over de grens relevante informatie opgevraagd bij academici, praktijkjuristen en advocatenbalies in diverse landen.

Het antwoord op de eerste onderzoeksvraag *(Worden of werden extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruikt door advocaten en, zo ja, welke middelen en waarom (niet)?)* is te vinden in hoofdstuk 5 en luidt als volgt. Advocaten gebruiken verschillende extra beveiligde communicatiemiddelen waaronder extra beveiligde chatapplicaties, extra beveiligde e-mailproviders en (zeer beperkt) cryptotelefoons. Uit het onderzoek blijkt dat de uiteindelijke keuze voor een (al dan niet) extra beveiligd communicatiemiddel afhangt van veel verschillende factoren, waarbij de voordelen daarvan moeten worden afgewogen tegen de mogelijke risico's, en waarbij de wens van de cliënt, eigen opvattingen van de advocaat en de praktische realiteit een rol spelen.

De belangrijkste reden voor het gebruik van extra beveiligde communicatiemiddelen is het streven om de advocaat-cliënt-communicatie vertrouwelijk te houden. Die drijfveer zorgt ervoor dat de meeste respondenten (zeer) vertrouwelijke informatie bij voorkeur in persoon bespreken, en is mede ingegeven

door een vrij breed gedeelde terughoudendheid ten aanzien van de vertrouwelijkheid van andere gebruikelijke communicatiemiddelen, waaronder de geheimhoudertelefoon. In algemene zin is geconstateerd dat bij veel respondenten in meer of mindere mate sprake is van wantrouwen in de goede naleving van de regels rondom het verschoningsrecht door opsporingsdiensten en het OM. Daarnaast is de wens of voorkeur van de cliënt voor veel advocaten een belangrijke factor bij de keuze voor een bepaald communicatiemiddel. Vaak zijn zij bereid om aan die wens tegemoet te komen, mits zij dit met hun eigen opvattingen en verplichtingen kunnen verenigen. Daarbij zijn er duidelijke verschillen tussen advocaten, met name waar het gaat om het gebruik van cryptotelefoons. Sommigen zijn (of waren in het verleden) bereid mee te gaan in de behoefte van de cliënt, soms mede gelet op het gegeven dat (huidige en potentieel nieuwe) cliënten alleen op deze wijze bereikbaar zijn of waren. Anderen geven aan dat zij dit middel niet willen gebruiken vanwege bijvoorbeeld het criminele imago ervan of vanwege zorgen om het niet kunnen bewaren van voldoende distantie tot de cliënt. Tot slot hangt de vraag of advocaten daadwerkelijk gebruikmaken van extra beveiligde communicatiemiddelen, en zo ja, welke, mede af van praktische aspecten waarbij vooral de gebruiks(on)vriendelijkheid van bepaalde communicatiemiddelen een rol kan spelen. Dit doet zich in het bijzonder voor bij extra beveiligde e-mailapplicaties, die door veel respondenten als onpraktisch worden ervaren.

De tweede onderzoeksvraag *(Hoe moet het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten worden bezien, mede in het licht van de risico's daarvan en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?)* wordt behandeld in hoofdstuk 6 en laat zich als volgt beantwoorden. Bij het gebruik van extra beveiligde communicatiemiddelen door advocaten kunnen verschillende risico's worden geïdentificeerd. Het meest op de voorgrond staan de risico's voor de vertrouwelijkheid van advocaat-cliënt-communicatie. Deze risico's houden verband met de herkenbaarheid van dergelijke communicatie als verschoningsgerechtigd en het identificeren en filteren hiervan in het opsporingsonderzoek. Wanneer met cryptotelefoon gevoerde communicatie in een opsporingsonderzoek terechtkomt (door een hack of inbeslagname van de server), is het niet altijd eenvoudig om eventuele verschoningsgerechtigde informatie te herkennen, laat staan er (op voorhand) uit te filteren. Dit geldt met name voor communicatie via een cryptotelefoon waarvan de gebruikersgegevens niet door de advocaat aan het OM zijn doorgegeven. Daarnaast zijn er risico's voor de geheimhouding waar het gaat om het gebruik van chatapplicaties zoals WhatsApp, Signal of Telegram. Hoewel de communicatie via deze applicaties door de *end-to-end* encryptie niet kan worden meegelezen c.q. afgeluisterd, kan deze wel door inbeslagname van een telefoon bij de opsporing terechtkomen. Een (voorafgaande) filtering op verschoningsgerechtigde informatie blijkt om verschillende redenen praktisch (en technisch) ingewikkeld of zelfs niet haalbaar. In relatie tot e-mailcommunicatie is geconstateerd dat juist het ontbreken van extra beveiliging soms risico's voor de geheimhouding meebrengt, nu deze communicatie minder beveiligingswaarborgen kent ten opzichte van derden. Wanneer (grote hoeveelheden) e-mails in het opsporingsonderzoek terechtkomen blijkt bovendien de filtering van verschoningsgerechtigde informatie in verschillende opzichten problematisch.

Vervolgens zijn in dit onderzoek risico's geïdentificeerd die samenhangen met andere kernwaarden van de advocaat, in het bijzonder onafhankelijkheid en integriteit. Deze risico's kunnen zich vooral manifesteren bij het gebruik van cryptotelefoons en hangen voor een belangrijk deel samen met het gegeven dat dergelijke telefoons vrijwel uitsluitend binnen het criminele milieu worden gebruikt. Zo kunnen zich risico's voordoen wanneer de advocaat bij de communicatie via een cryptotelefoon onvoldoende distantie kan bewaren tot (de criminele activiteiten van) de cliënt of de criminele groepering waarvan deze deel uitmaakt. Hierbij geldt wel dat op basis van de bevindingen van dit onderzoek niet kan worden gesproken van een direct verband tussen het gebruik van een cryptotelefoon en niet-integer of niet-onafhankelijk handelen. Het al dan niet ontstaan van onvoldoende distantie tot de cliënt is immers in de eerste plaats afhankelijk van het handelen van de betreffende advocaat die gebruikmaakt van dit communicatiemiddel. Met andere woorden, niet het communicatiemiddel op zichzelf, maar de wijze waarop de advocaat daarvan gebruik maakt, is bepalend is voor de vraag welke risico's zich voordoen. Wel vormt het gebruik van cryptotelefoons meer concreet een risico waar het gaat om de beeldvorming als onderdeel van de kernwaarde integriteit. Zelfs wanneer de advocaat in de communicatie via een cryptotelefoon immers handelt in overeenstemming met de kernwaarden en gedragsregels, brengt de beeldvorming rondom cryptotelefoons als exclusief communicatiemiddel voor criminelen mee dat het gebruik hiervan afbreuk kan doen aan het vertrouwen in (de integriteit van) de beroepsgroep. Een laatste aspect waarvoor het gebruik van extra beveiligde communicatiemiddelen problematisch kan zijn betreft de documentatieplicht van advocaten, omdat het door bepaalde kenmerken van de extra beveiligde communicatiemiddelen lastig(er) kan zijn om belangrijke (processtrategische) afspraken met de cliënt adequaat vast te leggen. Ook hier geldt echter dat het al dan niet ontstaan van risico's omtrent de documentatieplicht in de eerste plaats afhankelijk is van het handelen van de advocaat, en niet van het gekozen communicatiemiddel.

Na uiteenzetting van deze bevindingen volgt in hoofdstuk 7 een korte uitstap over de grens, waarbij is ingegaan op verschillende aspecten die in enkele andere landen anders zijn geregeld dan wel anders worden ingevuld. Daarbij gaat het om strafbaarstelling van cryptotelefoons, de wijze waarop aan advocaten uitgebreide en concrete richtlijnen en handvatten worden geboden om hun plicht tot geheimhouding te kunnen waarborgen, en technische oplossingen waar het gaat om de beveiliging van e-maildiensten voor advocaten.

In hoofdstuk 8 zijn de bevindingen samengebracht en is, na beantwoording van de hoofdvragen, een drietal aanbevelingen geformuleerd. Deze aanbevelingen strekken ertoe dat 1) in het licht van het geconstateerde wederzijds wantrouwen door betrokken actoren, in het bijzonder de NOvA en het OM, in onderling overleg wordt ingezet op het tegengaan en verminderen van de huidige polarisatie en het wantrouwen waar het gaat om het debat over de waarborging van de vertrouwelijkheid. In dat licht verdient niet alleen goede naleving van regels rondom het verschoningsrecht aandacht, maar ook (het creëren van) meer begrip voor elkaars rol en positie en de daarbij horende moeilijkheden en dilemma's. Voorts verdient aanbeveling dat 2) door de betrokken actoren wordt gewerkt aan effectieve(re) waarborgen voor het verschoningsrecht wanneer het gaat om communicatie via andere middelen dan (telefonisch contact met) de geheimhoudertelefoon. Daarbij valt te denken aan de ontwikkeling van een

beveiligd e-mailsysteem door de NOvA, de beperking van het aantal kanalen waarover vertrouwelijk kan worden gecommuniceerd en/of de ontwikkeling van een systeem van automatische e-mailherkenning. Tot slot is aan te bevelen dat 3) duidelijke kaders en richtlijnen worden gecreëerd om verstandig gebruik van de verschillende, al dan niet extra beveiligde communicatiemiddelen door advocaten te bevorderen. Daarbij gaat het om het gebruik van e-mail en chatapplicaties, maar ook om het gebruik van cryptotelefoons, welk gebruik gelet op de potentiële risico's voor de vertrouwelijkheid en (in wat mindere mate ook) voor de integriteit en onafhankelijkheid een extra zorgplicht voor de advocaat met zich brengt.

Afkortingenlijst

AA	:	Ars Aequi
aant.	:	aantekening
ABA	:	American Bar Association
Advw.	:	Advocatenwet
AIVD	:	Algemene Inlichtingen- en Veiligheidsdienst
appl.no.	:	application number
art.	:	artikel
College van P-G's	:	College van procureurs-generaal
CNB	:	Conseil National des Barreaux
diss.	:	dissertatie
DJI	:	Dienst Justitiële Inrichtingen
EHRM	:	Europees Hof voor de Rechten van de Mens
EU	:	Europese Unie
HR	:	Hoge Raad
i.w.tr.	:	inwerkingtreding
jo.	:	juncto
MIVD	:	Militaire Inlichtingen- en Veiligheidsdienst
m.nt.	:	met noot
NJ	:	Nederlandse Jurisprudentie
NOvA	:	Nederlandse orde van advocaten
nr.	:	nummer
OM	:	Openbaar Ministerie
par.	:	paragraaf
Rb.	:	rechtbank
RC	:	rechter-commissaris
red.	:	redactie
r.o.	:	rechtsoverweging
Sr	:	Wetboek van Strafrecht
Stb.	:	Staatsblad
Stcrt.	:	Staatscourant
Sv	:	Wetboek van Strafvordering
vgl.	:	vergelijk
Voda	:	Verordening op de advocatuur

1. Inleiding

1.1 Aanleiding

Het onderzoeksbureau I&O Research heeft in opdracht van de Nederlandse orde van advocaten (NOvA) onderzoek gedaan naar agressie en bedreiging tegen advocaten. Uit dit onderzoek is gebleken dat ongeveer de helft van de advocaten (50%) die de enquête heeft ingevuld, binnen een tijdsbestek van twaalf maanden ten minste één vorm van agressie heeft meegemaakt.[1] Vier op de tien (40%) advocaten maakten zelfs meerdere incidenten mee.[2] Naar aanleiding van de uitkomsten van dit onderzoek heeft de NOvA drie meer specifieke onderzoeken uitgezet in het kader van het door hen opgezette Taskforce Bescherming tegen Ondermijning.[3] Het voorliggende rapport vormt de verslaglegging van één van deze onderzoeken, namelijk het onderzoek naar het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen binnen de advocatuur.[4]

In het navolgende wordt eerst de achtergrond van dit onderzoek geschetst, waarbij met name wordt stilgestaan bij de mogelijke relatie tussen ondermijning en het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten (par. 1.1.1) en het verband tussen het waarborgen van de vertrouwelijkheid van advocaat-cliënt-communicatie en het gebruik van dergelijke middelen (par. 1.1.2). Vervolgens volgt een uiteenzetting van de doelstellingen van dit onderzoek (par. 1.2), de onderzoeksvragen (par. 1.3), belangrijke begrippen (par. 1.4) en de opbouw van het rapport (par. 1.5).

1.1.1 Ondermijning, extra beveiligde communicatiemiddelen en (het gebruik daarvan door) advocaten

Ondermijning ontstaat wanneer criminelen bij de uitvoering van hun criminele activiteiten gebruik maken van legale diensten of bedrijven, met als gevolg een verwevenheid tussen of vermenging van de boven- en onderwereld, een vervaging van normen, een verminderd gevoel van veiligheid en leefbaarheid en een ontwrichting van maatschappelijke structuren, waaronder de rechtsstaat.[5] De aanpak van ondermijnende criminaliteit staat al een aantal jaar hoog op de politieke agenda,[6] maar de nadruk op de rol van advocaten lijkt groter sinds de aanhouding van Youssef Taghi in oktober 2021. De voormalig minister voor Rechtsbescherming, Sander Dekker, zag de aanhouding van Youssef Taghi in

1 Van Miltenburg, Van Straaten & J. Bouwmeester 2022. Het gaat hier om verschillende vormen van agressie, waaronder zowel verbale- als fysieke agressie, bedreiging en intimidatie.
2 Van Miltenburg, Van Straaten & J. Bouwmeester 2022.
3 'Onderzoeken naar kroongetuigenregeling, PGP-telefoons en betalingen aan advocaten', advocatenorde.nl.
4 De andere twee onderzoeken betreffen de impact van de huidige en een eventuele toekomstige, uitgebreide kroongetuigenregeling op advocaten (Universiteit Leiden) en betalingen aan advocaten (Erasmus Universiteit Rotterdam).
5 Deze definitie is gebaseerd op de definities van Rijksoverheid, het Centrum voor Criminaliteitspreventie en Veiligheid en de Nationale Politie. 'Ondermijning', Rijksoverheid.nl.; 'Georganiseerde criminaliteit en ondermijning', hetccv.nl.; 'Wat is ondermijning?', politie.nl.
6 Zie in dit verband o.a. Boutellier, van Steden, Eski & Boelens 2020, p. 5-8.

de EBI als 'een signaal dat ook advocaten betrokken kunnen raken bij ondermijnende activiteiten'.[7] Sinds de aanhouding wordt gepleit voor verschillende maatregelen om het toezicht op en de weerbaarheid van de beroepsgroep te vergroten.[8] Dekker heeft destijds gepleit voor een harde aanpak van advocaten die betrokken raken bij dergelijke ondermijnende activiteiten en heeft daarnaast enkele voorstellen gedaan voor (preventieve) maatregelen, waaronder een vierogenprincipe bij bezoek aan gedetineerden, een periodieke screening en extra kwaliteitseisen waaraan advocaten moeten voldoen op het moment dat ze gedetineerden met een vlucht- en/of maatschappelijk risico (GVM) bijstaan.[9] De NOvA heeft, mede als alternatief voor de voorgestelde maatregelen van de minister voor Rechtsbescherming, eind 2021 de Taskforce Bescherming tegen ondermijning opgericht.[10] Een van de doelen van deze Taskforce is het versterken van de weerbaarheid van advocaten en het vergroten van de bewustwording omtrent de risico's die met de beroepsuitoefening kunnen samenhangen. In het kader van deze Taskforce wordt, naast het leveren van een bijdrage in de vorm van verschillende wetenschappelijke onderzoeken, ook geïnvesteerd in onder andere weerbaarheidstrainingen en vertrouwensadvocaten.[11]

De veronderstelling dat er een verband kan bestaan tussen criminele activiteiten en ondermijning enerzijds en het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen anderzijds, komt (deels) voort uit de gedachte dat criminelen over het algemeen zoeken naar mogelijkheden om onderlinge communicatie verborgen te houden voor de strafvorderlijke overheid. Sinds de komst van verschillende technologische ontwikkelingen maken criminele netwerken steeds meer gebruik van (online) communicatiemiddelen die zowel de inhoud van het bericht als de identiteit van de gebruiker kunnen afschermen.[12] Met name cryptotelefoons worden binnen criminele netwerken veel gebruikt om onderling te communiceren.[13] Mede gelet op de populariteit van dergelijke toestellen binnen het georganiseerde criminele milieu is het denkbaar dat onder leden van criminele netwerken de wens bestaat om via een cryptotelefoon ook met hun advocaat in contact te kunnen komen.[14] Uit berichtgeving van onder andere het OM blijkt dat in ieder geval een aantal Nederlandse (strafrecht)advocaten in het verleden, al dan niet op verzoek van de cliënt, gebruik heeft gemaakt van een cryptotelefoon in het contact met cliënten.[15]

Dit onderzoek beoogt in kaart te brengen in hoeverre advocaten gebruikmaken van verschillende extra beveiligde en/of identiteitsversluierende communicatiemiddelen, waaronder cryptotelefoons, en wat daarvoor de beweegredenen zijn. Een van de gedachten daarbij kan zijn dat dwang, drang of druk[16]

---

7 Brief van de Minister van Rechtsbescherming van 22 november 2021, 3647135 (rijksoverheid.nl).
8 Brief van de Minister van Rechtsbescherming van 22 november 2021, 3647135 (rijksoverheid.nl).
9 Brief van de Minister van Rechtsbescherming van 22 november 2021, 3647135 (rijksoverheid.nl). Zie voor de criteria GVM lijst: 'GVM-lijst', commissievantoezicht.nl.
10 'Taskforce Bescherming Tegen Ondermijning', advocatenorde.nl.
11 'NOvA zoekt Vertrouwensadvocaten', advocatenorde.nl.
12 Zie in dit verband o.a. Eurojust 2021, p. 29 en *SOCTA report* 2021, p. 32-33.
13 Eurojust 2022, par. 7.2 en *SOCTA report* 2021, p. 32-33.
14 Zie o.a. Droogleever Fortuyn 2022.
15 Meeus 2017 en 'Mededeling inzake PGP-toestellen', advocatenorde-middennederland.nl.
16 Met deze begrippen doelen wij op verschillende gradaties van beïnvloeding waarmee iemand wordt bewogen tot bepaald handelen of nalaten, of waarmee wordt gepoogd iemand tot zulk handelen of nalaten te bewegen. Met deze vormen van beïnvloeding wordt iemands keuzevrijheid beperkt of, bij toepassing van dwang, geheel weggenomen. Dwang vormt dan ook de sterkste gradatie, druk beschouwen wij als de minst sterke gradatie waarbij de keuzevrijheid in beperkte(re) mate wordt beïnvloed.

vanuit de cliënt een rol zou kunnen spelen bij de keuze van advocaten om een bepaald communicatiemiddel te gebruiken, een gedachte die mede voortkomt uit het groeiende besef dat agressie richting de beroepsgroep de afgelopen vijf jaar lijkt te zijn toegenomen.[17] Uit het onderzoeksrapport van I&O Research blijkt dat bij de helft van de incidenten de eigen (voormalig of huidige) cliënt de bron van agressie is.[18] Wanneer sprake is van agressief gedrag vanuit de cliënt richting de advocaat, bijvoorbeeld in de vorm van bedreigingen of intimidatie, kan de advocaat in kwestie onder druk worden gezet om iets te doen wat hij of zij niet wil doen. Dit kan gaan om het aanschaffen en gebruiken van een cryptotelefoon, maar ook (vervolgens) om het faciliteren van criminele activiteiten via deze cryptotelefoon. Het gebruik van dwang, drang of druk door cliënten kan in die context dus een indicatie zijn voor ondermijning.

Tegelijkertijd mag duidelijk zijn dat het gebruik van een cryptotelefoon door een advocaat geen indicatie hoeft te zijn van het bestaan van dwang, drang of druk vanuit de cliënt. De advocaat kan ook zelf de keuze hebben gemaakt om een cryptotelefoon aan te schaffen, bijvoorbeeld met het oog op het waarborgen van de vertrouwelijkheid van de communicatie (zie hierover meer in par. 1.1.2). Bovendien, het 'criminele imago' van de cryptotelefoon betekent niet dat een dergelijk toestel niet kan worden gebruikt voor legitieme doeleinden. Het bezitten en gebruiken van dergelijke toestellen is immers niet verboden, bovendien kunnen er verschillende (legitieme) argumenten zijn om van een cryptotelefoon gebruik te maken (zie hierover meer in par. 1.1.2 en par. 3.4.1). Dat cryptotelefoons inmiddels niet meer weg te denken zijn uit het georganiseerde criminele milieu, betekent dus niet dat de advocaten die dergelijke telefoons gebruiken in het contact met cliënten, zich ook (vrijwillig of gedwongen) bezighouden met criminele activiteiten.

1.1.2 Geheimhouding en (extra beveiligde) communicatiemiddelen

Hoewel dwang, drang of druk vanuit de cliënt een rol zou kunnen spelen bij de overweging van een advocaat om een bepaald communicatiemiddel te gebruiken, zijn er ook genoeg andere (legitieme) redenen om in de hoedanigheid als advocaat te kiezen voor extra beveiliging van de communicatie met een cliënt. Het algemene (legitieme) doel van extra beveiligde communicatie is het voorkomen dat ongeautoriseerde derden toegang kunnen krijgen tot verschillende onderdelen van de communicatie. Binnen verschillende specifieke beroepsgroepen is er voor het gebruik van extra beveiligde communicatiemiddelen steeds meer aandacht.[19] Als professional heb je immers de taak om de communicatie met cliënt, klant of burger vertrouwelijk te houden en te voorkomen dat ongeautoriseerde derden toegang kunnen krijgen tot de informatie. Ook advocaten worden aangemoedigd om versleuteld te e-mailen en privacy vriendelijke chatapplicaties te gebruiken.[20] Gelet op de algemene AVG-verplichtingen, cybersecurity en de geheimhoudingsplicht lijkt het dan ook niet meer dan

17 Van Miltenburg, Van Straaten & Bouwmeester 2022, p. 12. Zie in dit verband ook: J. van den Heuvel, 'Advocaten in nood om toename aantal bedreigingen: "We zitten op een kantelpunt"', *De Telegraaf* 20 mei 2023.

18 Van Miltenburg, Van Straaten & Bouwmeester 2022, p. 20.

19 Zo gelden voor informatie-uitwisseling via e-mail in de zorg- en welzijnssector verschillende normen. Zie: 'Veilig mailen', nen.nl.

20 'Tips voor vertrouwelijke internetcommunicatie', *Adv. bl.* 2022/7, p. 68-69.

vanzelfsprekend dat een advocaat extra beveiligingsmaatregelen treft om de communicatie met de cliënt vertrouwelijk te houden. Dit geldt in zijn algemeenheid waar het gaat om communicatie die persoonsgegevens van cliënten bevat. Bovendien zijn de gesprekken die gevoerd worden tussen een advocaat en een cliënt niet enkel interessant voor cybercriminelen en commerciële partijen, maar ook voor overheden. Hoewel deze communicatie (doorgaans) onder het verschoningsrecht valt en er verschillende waarborgen voor het recht op vertrouwelijke communicatie zijn neergelegd in de Nederlandse en internationale wet- en regelgeving, blijken er in de praktijk verschillende kwetsbaarheden te bestaan wat betreft de adequate waarborging van de vertrouwelijkheid.[21] Discussies over de naleving van het recht op vertrouwelijke advocaat-cliëntcommunicatie en mogelijke schendingen van het verschoningsrecht door de strafvorderlijke overheid hebben de afgelopen jaren gespeeld op verschillende terreinen en zouden voor advocaten een (extra) beweegreden kunnen zijn om hun communicatie met cliënten extra te beveiligen.[22]

In de zaak rondom advocaat Inez Weski lijken verschillende van de hierboven benoemde thema's bij elkaar te komen. Sinds haar aanhouding in april 2023 is zowel de discussie over ondermijning en het gebruik van cryptotelefoons door advocaten, als de discussie over schendingen van het verschoningsrecht door de strafvorderlijke overheid, opnieuw aangewakkerd en actueel geworden.[23] Weski wordt door het OM verdacht van deelname aan een criminele organisatie, ze zou als 'doorgeefluik' berichten in en uit de Extra Beveiligde Inrichting (EBI) hebben doorgegeven.[24] De verdenking is mede gebaseerd op de communicatie die verliep via cryptotelefoons,[25] waarvan Weski er zelf ook een in haar bezit zou hebben gehad en deze ook zou hebben gebruikt in het contact met de familie van Taghi.[26] In de media wordt gesproken van druk die werd uitgeoefend op Weski door de familie van de Taghi om berichten door te geven.[27] Tijdens het opsporingsonderzoek zouden vervolgens fouten zijn gemaakt door het OM. Een officier van justitie zou vertrouwelijke informatie uit de praktijk van Weski hebben verspreid onder collega's. Het OM stelt zich echter op het standpunt dat er geen inhoudelijke documenten zijn gedeeld en dat het verschoningsrecht niet is geschonden.[28]

Hoewel dit onderzoek is opgestart in het kader van de Taskforce Bescherming tegen Ondermijning, blijkt uit het bovenstaande dat dit onderzoeksonderwerp, 'het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen binnen de advocatuur', niet enkel kan worden onderzocht in relatie tot het bestaan van dwang, drang of druk vanuit de cliënt, omdat dit onderwerp tevens raakt aan andere actuele thema's, waaronder met name het recht op vertrouwelijke communicatie tussen advocaat en cliënt en de waarborging daarvan in de praktijk. Gegeven het feit dat de thematiek

21 Zie par. 4.3-4.4.
22 Zie par 4.3-4.4.
23 Mos & Polman 2023b.
24 Zie bijv. Haenen & Meeus 2023.
25 Zie bijv. Haenen & Meeus 2023.
26 Zie bijv. Laumans & Vugts 2023.
27 Zie o.a. 'Advocaat Weski onder druk gezet door familie Taghi om berichten door te sluizen', *rtlnieuws.nl* 29 april 2023 en Laumans & Vugts 2023.
28 Mos & Polman 2023b.

vanuit verschillende kanten kan worden belicht zijn zowel de doelstellingen als de onderzoeksvragen in dit rapport open geformuleerd.

1.2 Doelstelling

Belangrijke doelen van dit onderzoek zijn (1) inzicht verkrijgen in de aard en omvang van het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen onder advocaten en (2) inzicht verkrijgen in de beweegredenen van advocaten om wel of niet van dergelijke middelen gebruik te maken. Daarnaast betreft een van de doelen (3) het in kaart brengen van de potentiële risico's voor advocaten die gebruik maken van extra beveiligde en/of identiteitsversluierende communicatiemiddelen. Tot slot wordt getracht (4) kennis te vergaren over de praktijk, regelgeving en het beleid in het buitenland.

In dit verband is het van belang om op te merken dat dit onderzoek zich niet richt op de vraag of en in hoeverre advocaten betrokken zijn bij ondermijnende criminaliteit. Evenmin heeft dit onderzoek tot doel om uitspraken te doen over het verband tussen ondermijning en het gebruik van bepaalde extra beveiligde en/of identiteitsversluierende communicatiemiddelen. De achtergrond waartegen dit onderzoek (mede) plaatsvindt moet in zoverre nadrukkelijk worden onderscheiden van de concrete doelstellingen van dit onderzoek.

1.3 Onderzoeksvragen

In dit onderzoek staan de volgende vragen centraal:

1. *Worden of werden extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruikt door advocaten en, zo ja, welke middelen en waarom (niet)?*
2. *Hoe moet het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten worden bezien, mede in het licht van de risico's daarvan en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?*

Ter beantwoording van bovenstaande onderzoeksvragen zijn de volgende deel- en subvragen geformuleerd:

1. *Wat is het juridisch kader rondom de vertrouwelijke communicatie tussen advocaten en hun cliënten en hoe is dit uitgewerkt in de praktijk?*
    a. *Wat wordt verstaan onder vertrouwelijke communicatie tussen advocaten en cliënten en op wie heeft het recht op vertrouwelijke communicatie betrekking (bijv. medewerkers met een afgeleid verschoningsrecht)?*
    b. *Hoe is het recht op vertrouwelijke communicatie tussen advocaten en cliënten in de wet en de jurisprudentie geregeld?*

c. *Op welke manier wordt de vertrouwelijke communicatie tussen advocaten en cliënten in de praktijk gewaarborgd?*

d. *Welke kwetsbaarheden kunnen in het juridisch kader en/of in de praktische uitwerking daarvan worden geïdentificeerd?*

2. *In hoeverre maken advocaten voor hun contacten met cliënten gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen?*

   a. *Welke extra beveiligde en/of identiteitsversluierende communicatiemiddelen worden door advocaten gebruikt? Hoe werken deze communicatiemiddelen? Is er wet- en regelgeving van toepassing op deze communicatiemiddelen, en zo ja, wat houdt deze in?*

   b. *Hoe vaak en in welke gevallen (typen zaken, cliënten, onderwerpen) wordt gebruikgemaakt van extra beveiligde en/of identiteitsversluierende communicatiemiddelen?*

3. *Wat zijn de beweegredenen van advocaten om gebruik te maken van extra beveiligde en/of identiteitsversluierende communicatiemiddelen of om dit juist niet te doen?*

   a. *Op wiens initiatief (advocaat/cliënt/derden) wordt gebruik gemaakt van extra beveiligde en/of identiteitsversluierende communicatiemiddelen?*

   b. *Wat zijn de motieven om (al dan niet) gebruik te maken van deze vormen van extra beveiligde en/of identiteitsversluierende communicatiemiddelen?*

4. *Wat is bekend over regelgeving en praktijk met betrekking tot het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in andere landen?*

5. *Welke risico's brengt het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen mee voor advocaten en cliënten en hoe moet dit gebruik worden bezien in het licht van die risico's en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?*

6. *Welke conclusies kunnen worden getrokken met betrekking tot het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten? Welke aanbevelingen kunnen op basis van deze conclusies worden gedaan?*

1.4 Begrippen

Mede in het kader van de afbakening van dit onderzoek dient het begrip 'extra beveiligde en/of identiteitsversluierende communicatiemiddelen' nader te worden toegelicht. Onder 'extra beveiligde en/of identiteitsversluierende communicatiemiddelen' verstaan wij in dit rapport het volgende: communicatiemiddelen die door middel van verschillende beveiligingsfunctionaliteiten de vertrouwelijkheid van de communicatie en de privacy van de gebruiker beter (zouden moeten) kunnen

waarborgen dan conventionele communicatiemiddelen.[29] In dit onderzoek wordt onderscheid gemaakt tussen drie categorieën communicatiemiddelen: extra beveiligde chatapplicaties; extra beveiligde e-mail en cryptotelefoons.[30] Omwille van de leesbaarheid wordt soms alleen de term 'extra beveiligd' of 'identiteitsversluierend' gebruikt. Tenzij expliciet aangegeven wordt daarmee geen inhoudelijk verschil bedoeld.

1.5 Opbouw

Na een uiteenzetting van de methodologie in hoofdstuk 2 zal in hoofdstuk 3 het begrip 'extra beveiligde en/of identiteitsversluierende communicatiemiddelen' nader worden geduid. In dit hoofdstuk worden tevens verschillende categorieën communicatiemiddelen onderscheiden en wordt de verhouding tussen opsporing en het (toenemende) gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen uiteengezet. In hoofdstuk 4 wordt, ter beantwoording van de eerste deelvraag, eerst het juridisch kader rondom vertrouwelijke communicatie tussen advocaten en cliënten uiteengezet, vervolgens wordt beschreven hoe dit juridisch kader in de praktijk wordt toegepast. In hoofdstuk 5 worden, ter beantwoording van de tweede en derde deelvraag, de uitkomsten gepresenteerd van de interviews die zijn gehouden met advocaten over het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen. In dit hoofdstuk staan de beweegredenen, overwegingen en knelpunten vanuit het perspectief van de advocatuur centraal. In hoofdstuk 6 worden, mede ter beantwoording van de vijfde deelvraag, verschillende risico's en knelpunten van het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten opgesomd. Naast de knelpunten vanuit het perspectief van de advocatuur worden ook de knelpunten en potentiële risico's vanuit verschillende externe perspectieven, waaronder het perspectief van de opsporing, in dit hoofdstuk behandeld. In hoofdstuk 7 wordt, ter beantwoording van de vierde deelvraag, een blik geworpen op het beleid en de praktijk in andere landen. In hoofdstuk 8 volgt, ter beantwoording van de twee hoofdvragen, een analyse van de verschillende onderzoeksbevindingen tezamen. Dit hoofdstuk bevat tevens enkele afsluitende opmerkingen en aanbevelingen.

[29] Bij meer conventionele middelen valt te denken aan de (mobiele of vaste) telefoon, WhatsApp, het advocaten e-mailadres, Gmail of Hotmail. Zie verder par. 3.2.

[30] Zie in dit kader par. 3.3.

2. Methodologie

2.1 Inleiding

In dit rapport staan de volgende twee hoofdvragen centraal:

1. *Worden of werden extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruikt door advocaten en, zo ja, welke middelen en waarom (niet)?*
2. *Hoe moet het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten worden bezien, mede in het licht van de risico's daarvan en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?*

Ter beantwoording van deze twee hoofdvragen zijn verschillende deelvragen geformuleerd. In dit hoofdstuk wordt toegelicht hoe de beantwoording van de verschillende hoofd- en deelvragen in dit rapport tot stand is gekomen.

2.2 Opzet onderzoek

Het onderzoek is gestart op 1 oktober 2022 en op 17 oktober 2023 is het onderzoeksrapport door de Universiteit Leiden aan de NOvA aangeboden. Ter beantwoording van de hoofd- en deelvragen zijn verschillende onderzoeksmethoden gehanteerd. De methodiek kan grofweg in drie onderdelen worden opgedeeld. Een eerste onderdeel betreft de analyse van reeds bestaande bronnen waaronder wet-regelgeving, jurisprudentie, literatuur en (overige) openbaar toegankelijke informatie met als doel de uiteenzetting van de relevante (technische) aspecten en juridische kaders. Het verzamelen, raadplegen en analyseren van voornoemde bronnen zal in dit rapport worden aangeduid als *desk research*. Een tweede onderdeel betreft empirisch onderzoek, bestaande uit het afnemen, uitwerken en analyseren van interviews en het uitzetten van een tweetal schriftelijke vragenlijsten. De interviews zijn afgenomen bij verschillende actoren werkzaam in de rechtspraktijk, het merendeel advocaten, waarvan de meesten werkzaam zijn in de strafrechtspraktijk. Tot slot wordt ter beantwoording van de vierde deelvraag een blik over de grens geworpen door een combinatie van *desk research* en het opvragen van relevante informatie bij academici, praktijkjuristen en advocatenbalies in diverse landen. In het navolgende zullen de verschillende onderdelen nader uiteen worden gezet.

2.3 Desk research

De methode van *desk research* is gebruikt voor de beantwoording van verschillende deelvragen.

De eerste deelvraag luidt: *Wat is het juridisch kader rondom de vertrouwelijke communicatie tussen advocaten en hun cliënten en hoe is dit uitgewerkt in de praktijk?* Deze deelvraag is beantwoord aan de hand van raadpleging, selectie en analyse van relevante wet- en regelgeving, jurisprudentie, literatuur en (overige) openbaar toegankelijke informatie. Voornoemde analyse heeft geresulteerd in een juridisch

kader en een beschouwing van de uitwerking van dit kader in de praktijk. De resultaten van de analyse zijn neergelegd in hoofdstuk 4.

Ook voor de beantwoording van onderdeel a van de tweede deelvraag is de methode van *desk research* gebruikt. Dit onderdeel luidt: *Welke extra beveiligde en/of identiteitsversluierende communicatiemiddelen worden door advocaten gebruikt? Hoe werken deze communicatiemiddelen? Is er wet- en regelgeving van toepassing op deze communicatiemiddelen, en zo ja, wat houdt deze in?* Aan de hand van raadpleging, selectie en analyse van relevante literatuur en (overige) openbaar toegankelijke informatie is het begrip 'extra beveiligde en/of identiteitsversluierende communicatiemiddelen' nader geduid en is een categorisering gemaakt van drie typen communicatiemiddelen die in dit rapport centraal staan. Daarnaast wordt op basis van relevante literatuur de verhouding tussen opsporing en het (toenemende) gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen nader toegelicht en wordt de relevante wet- en regelgeving ter zake het aanbieden en gebruiken van dergelijke middelen uiteengezet. De resultaten van deze analyse worden uiteengezet in hoofdstuk 3.

Tot slot zijn, ter beantwoording van de vijfde deelvraag, empirische onderzoeksmethoden gecombineerd met *desk research*. Deze deelvraag luidt: *Welke risico's brengt het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen mee voor advocaten en cliënten en hoe moet dit gebruik worden bezien in het licht van die risico's en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?* Het voor de (gedeeltelijke) beantwoording van deze vraag uitgevoerde *desk research* bestond uit de analyse van wet- en regelgeving, verschillende werkwijzen, handleidingen en overige (beleids)documenten die (onder meer) inzicht geven in de opsporingspraktijk.[31] Deze bevindingen zijn, gecombineerd met de informatie die is verkregen door middel van empirisch onderzoek naar dit thema, uiteengezet in hoofdstuk 6.

2.4 Empirisch onderzoek

De tweede, derde en vijfde deelvraag zijn (mede) beantwoord aan de hand van empirisch onderzoek.

De tweede en derde deelvraag hebben betrekking op het gebruik van extra beveiligde en/of identiteitsversluierende middelen door advocaten en hun beweegredenen daarvoor, en luiden als volgt: *In hoeverre maken advocaten voor hun contacten met cliënten gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen?* en *Wat zijn de beweegredenen van advocaten om gebruik te maken van extra beveiligde en/of identiteitsversluierende communicatiemiddelen?* Ter beantwoording van deze deelvragen zijn advocaten geïnterviewd (N=17) over het al dan niet gebruiken van de verschillende communicatiemiddelen en hun beweegredenen daarvoor. Om beter zicht te krijgen op het gebruik van specifiek cryptotelefoons binnen de advocatuur zijn aanvullend schriftelijke vragenlijsten voorgelegd aan het landelijk dekenberaad en het OM.[32]

---

31 Zie ook par. 6.1.

32 Zie par. 2.4.2.2.

De vijfde deelvraag heeft betrekking op de risico's die met het gebruik van dergelijke middelen gepaard gaan en luidt als volgt: *Welke risico's brengt het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen mee voor advocaten en cliënten en hoe moet dit gebruik worden bezien in het licht van die risico's en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?* Risico's kunnen vanuit het perspectief van de advocaat zelf, vanuit het perspectief van de opsporing en vanuit het perspectief van de toezichthouder (deken) worden geïdentificeerd. Daarom is deze deelvraag beantwoord aan de hand van verschillende informatiebronnen, waaronder de bevindingen uit de hiervoor al genoemde interviews met advocaten en de informatie verkregen op basis van *desk research*. Verder zijn vragen voorgelegd aan het NFI, het OM en het landelijk dekenberaad: eerst door middel van een schriftelijke vragenlijst, vervolgens is met (een of meer) betrokkenen werkzaam bij deze partijen[33] doorgepraat over de verschillende risico's van het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten voor het recht op vertrouwelijke communicatie vanuit (technisch) opsporingsperspectief, respectievelijk gedragsrechtelijk perspectief.

In het navolgende wordt een nadere toelichting gegeven op de selectie van de respondenten (par. 2.4.1), en de wijze waarop de dataverzameling (door middel van semigestructureerde diepte-interviews en schriftelijke vragenlijsten) heeft plaatsgevonden (par. 2.4.2).

2.4.1 Selectie respondenten

De interviews zijn afgenomen bij zeventien advocaten, waarvan veertien advocaten die met name strafzaken behandelen, twee advocaten met een ondernemings- en/of insolventierecht praktijk en één advocaat die naast strafzaken ook personen- familie en jeugdrechtzaken behandeld. Daarnaast zijn twee medewerkers van het OM en één medewerker van het NFI geïnterviewd. Tot slot zijn drie (oud of huidig) dekens geïnterviewd. Alle respondenten zijn benaderd vanuit de gedachte dat een interview met hen bruikbare informatie zal opleveren voor de beantwoording van de onderzoeksvragen. De uiteindelijke selectie van respondenten betreft dus een zogeheten doelgerichte steekproef (*purposive sampling*), zoals gebruikelijk is in kwalitatief onderzoek.[34]

2.4.1.1 Advocaten

De advocaten zijn op twee verschillende manieren geworven. In het navolgende worden beide wervingswijzen nader uiteengezet. De NOvA heeft bijgedragen aan de werving van respondenten door het met toestemming overhandigen van een lijst met advocaten die in het kader van het eerder uitgevoerde I&O Research hebben aangegeven een bijdrage te willen leveren aan dit onderzoek.[35] Nadat de Universiteit Leiden in opdracht van de NOvA is gestart met dit onderzoek heeft de NOvA aan de advocaten die destijds hebben aangegeven dat ze bereid waren om een bijdrage te leveren aan het

33 Het gaat om één medewerker van het NFI, twee officieren van justitie en drie (oud-)dekens.

34 Mortelmans 2016, p. 111. In tegenstelling tot de steekproeftrekking in kwantitatief onderzoek, die veelal is gebaseerd op een toevalligheidsfactor, aangeduid als *random sampling*.

35 Van Miltenburg, Van Straaten & Bouwmeester 2022, p. 9-10.

vervolgonderzoek over identiteitsversluierende (communicatie)middelen (N=84) gevraagd of ze de gegevens mochten overhandigen aan de Universiteit Leiden. Dertig advocaten hebben aangegeven dat hun gegevens gedeeld mochten worden in het kader van dit onderzoek. Aan deze groep advocaten is per mail een korte enquête voorgelegd, met gebruikmaking van het digitale systeem Qualtrics. De enquête had tot doel te inventariseren of en in hoeverre deze advocaten gebruikmaken van verschillende extra beveiligde en/of identiteitsversluierende (communicatie)middelen. Met behulp van zes meerkeuzevragen en een open vraag is voor verschillende categorieën identiteitsversluierende (communicatie)middelen uitgevraagd of de advocaat wel of (bewust) niet gebruikmaakt van dergelijke middelen en of de advocaat weet dat collega's gebruik maken van dergelijke middelen. De advocaten zijn gevraagd naar het gebruik van (1) extra beveiligde chatapplicaties; (2) extra beveiligde e-mail (buiten het voorgeschreven beveiligde e-mailcontact met de Rechtspraak); (3) extra beveiligde belapplicatie; (4) extra beveiligde SMS-applicatie; (5) extra beveiligingsmiddelen voor het opslaan en/of delen van bestanden en het gebruik van een (6) extra beveiligde telefoon ofwel 'cryptotelefoon'. Tot slot kregen de advocaten de open vraag of ze (7) andere extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruiken, en zo ja, welke.[36]

De enquête is op 9 december 2022 verstuurd, tien dagen later hebben de advocaten die de enquête nog niet ingevuld hadden een rappel ontvangen (N=14). Op 23 december 2022 hadden twintig advocaten de lijst ingevuld. De resultaten van dit enquêteonderzoek waren te herleiden tot de persoonlijke link die de respondent had ontvangen toen z/hij[37] werd benaderd om de enquête in te vullen, en zijn gebruikt voor de selectie van te interviewen respondenten.[38]

Twaalf advocaten zijn op basis van hun enquêteantwoorden geselecteerd en uitgenodigd voor een interview. Teneinde een zo volledig mogelijk beeld te krijgen van (de beweegredenen voor) het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen, is gekozen voor heterogeniteit in de steekproef.[39] Bij het selecteren van advocaten is ervoor gezorgd dat de selectie zowel advocaten bevat die aangeven dat ze wel gebruikmaken van bepaalde extra beveiligde en/of identiteitsversluierende middelen, als advocaten die aangeven dat ze (bewust) geen gebruikmaken van dergelijke middelen.[40] Daarnaast is gezorgd voor enige diversiteit in het type praktijk waarin de

---

36 Bij elke soort communicatiemiddel werden ter verduidelijking van de vraag enkele voorbeelden gegeven. De antwoordopties waar de respondenten per middel uit konden kiezen waren (a) Ik gebruik dit middel of heb dit middel gebruikt; (b) Ik overweeg dit middel te gebruiken; (c) Ik weet dat collega's gebruikmaken van dit middel; (d) Ik ken dit middel, maar kies er bewust voor het niet te gebruiken (e) Ik ken dit middel, maar heb nooit serieus overwogen het te gebruiken (f) Ik ben niet bekend met dit middel.

37 In dit rapport wordt in algemene verwijzingen naar personen steeds gebruik gemaakt van zowel de vrouwelijke als de mannelijke vorm: 'z/hij', 'haar/hem', 'haar/zijn'. In het besef dat in de realiteit in individuele gevallen de meervoudsvorm ('zij/hen/hun') op zijn plaats zou zijn, wordt die omwille van de leesbaarheid van dit rapport niet expliciet gehanteerd, maar waar de vrouwelijke en mannelijke enkelvoudsvormen worden gebruikt, kunnen ook steeds die meervoudsvormen worden gelezen.

38 Deelname aan deze enquête was in zoverre niet anoniem. De respondenten zijn daarvan op de hoogte gesteld en hebben (in Qualtrics) een apart toestemmingsformulier getekend.

39 Zie over deze kwalitatieve steekproefmethode o.a. Mortelmans 2016, p. 113.

40 In de enquête is gevraagd naar het gebruik van verschillende soorten extra beveiligde middelen. Uiteindelijk is ervoor gekozen om dit onderzoek toe te spitsen op drie categorieën communicatiemiddelen: de extra beveiligde chatapplicatie, extra beveiligde e-mail en de cryptotelefoon. Deze categorieën worden in par. 3.3 toegelicht. Andere extra beveiligde communicatiemiddelen waar de advocaten in de enquête naar zijn gevraagd, zoals bel- en SMS-applicaties, worden niet of nauwelijks gebruikt, en zullen in het rapport niet verder aan de orde komen.

respondenten werkzaam zijn, met dien verstande dat het grote merendeel van de respondenten (ook) strafzaken behandelt, zowel op het gebied van het commune als het financieel-economische strafrecht. Van de twaalf geselecteerde advocaten hebben tien gereageerd op het verzoek tot een interview (N=10).

Aanvullend op bovenstaande wervingswijze zijn respondenten benaderd vanwege hun (verwachte) bijzondere kennis van en/of ervaring met het onderwerp. Die inschatting is in sommige gevallen gemaakt naar aanleiding van informatie die over respondenten in openbaar toegankelijke bronnen is gevonden (nieuwsartikelen, wetenschappelijke of opiniërende bijdragen, rechtspraak.nl). Enkele respondenten zijn (ook) naar voren gekomen in interviews met andere respondenten, en vervolgens benaderd.[41]

2.4.1.2 Overige respondenten: NFI, OM, Dekens

Voor dit onderzoek is van belang dat ook de expertise van andere betrokken en/of deskundige partijen wordt meegenomen. Met name bij het in kaart brengen van de risico's die gepaard kunnen gaan met het gebruik van extra beveiligde en/of identiteitsversluierende (communicatie)middelen door advocaten, is het niet enkel relevant om de advocatuur te spreken, maar ook deskundigen van andere organisaties, waaronder het OM, het NFI en de lokale dekens. Ook deze respondenten zijn doelgericht geselecteerd op basis van hun (verwachte) bijzondere kennis van en/of ervaring met bepaalde onderwerpen. Bij het OM is gesproken met twee officieren van justitie die in het kader van hun werkzaamheden bij het OM kennis en expertise hebben op het gebied van digitale opsporing en het filteren van vertrouwelijke communicatie uit het opsporingsonderzoek. Bij het NFI is een digitaal forensisch onderzoeker geïnterviewd die in het bijzonder kan vertellen over de technische (on)mogelijkheden van de analysetool Hansken. Tot slot zijn drie (oud en huidig) dekens benaderd die vanwege hun (voormalige) functie als toezichthouder vanuit dat perspectief naar de thematiek van dit onderzoek kunnen kijken.

2.4.2 Werkwijze dataverzameling en -analyse

In de periode van 7 februari 2023 tot en met 4 oktober 2023 zijn twee schriftelijke vragenlijsten beantwoord en drieëntwintig semigestructureerde diepte-interviews afgenomen.[42] Dat wil zeggen dat de interviews zijn afgenomen op basis van (gepersonaliseerde) topiclijst(en), maar dat de onderzoekers zich gedurende het interview ook hebben laten leiden door de antwoorden van respondenten door vervolgvragen te stellen. Het diepte-interview is een geschikte (kwalitatieve) onderzoeksmethode voor het analyseren van beslissingsprocessen en derhalve goed bruikbaar om de verschillende beweegredenen voor het gebruik van een bepaald communicatiemiddel in kaart te brengen.[43]

---

41 Zie over deze kwalitatieve steekproefmethode, veelal aangeduid als de sneeuwbalsteekproef, o.a. Mortelmans 2016, p. 114.

42 Brent & Kraska 2021, p. 405-411 en Beyens, Kennes & Tournel 2016, p. 187-222.

43 Beyens, Kennes & Tournel 2016, p. 192.

2.4.2.1 Interviews

Doel en inhoud

Tijdens de semigestructureerde interviews met advocaten (N=17) stonden de beweegredenen om wel of (bewust) niet gebruik te maken van verschillende extra beveiligde en/of identiteitsversluierende (communicatie)middelen centraal. Voorts is aan de respondenten gevraagd of zij differentiëren in het gebruik van de middelen en, indien dit het geval is, bij welke type zaken en/of cliënten zij gebruikmaken van welk middel en waarom. De antwoorden die door de respondent waren gegeven in het kader van de eerder afgenomen enquête zijn gebruikt als leidraad voor het interview. De respondenten die niet via de enquêteprocedure geselecteerd zijn, hebben tijdens het interview de enquêtevragen voorgelegd gekregen. Aan de hand van de gegeven antwoorden in de enquête kon gericht worden uitgevraagd naar de motieven voor het wel of niet gebruiken van de verschillende middelen. Wanneer de respondent in de enquête had aangegeven een communicatiemiddel niet te kennen, werden vervolgvragen over het gebruik van dit middel achterwege gelaten.

Met de advocaten is gesproken over eventuele verzoeken vanuit cliënten om een bepaald communicatiemiddel te gebruiken. Meer specifiek is doorgevraagd naar het al dan niet aanwezig zijn van een bepaalde druk die gepaard zou kunnen gaan bij een dergelijk verzoek van de cliënt. Voorts is met de respondenten gesproken over de keuze van een communicatiemiddel in relatie tot het waarborgen van het recht op vertrouwelijke communicatie, meer specifiek overwegingen omtrent de geheimhoudingsplicht en overwegingen omtrent (potentiële inbreuken op) het verschoningsrecht. Tot slot kwamen ook enkele praktische overwegingen, met name overwegingen omtrent kosten en gebruiksvriendelijkheid van verschillende communicatiemiddelen, aan bod tijdens de interviews.

Tijdens het interview met de medewerkers van het OM stonden verschillende onderwerpen centraal. Met de respondenten is vooral gesproken over de verschillende risico's voor de geheimhouding die zich kunnen voordoen bij het gebruik van verschillende communicatiemiddelen door advocaten.

In het interview met de medewerker van het NFI stonden met name de technische mogelijkheden en onmogelijkheden van de analysetool Hansken centraal. Deze analysetool wordt door de opsporing gebruikt om grote hoeveelheden data te analyseren en heeft tevens een functie om vertrouwelijke communicatie uit de dataset te filteren.

Tijdens de interviews met (oud en huidig) dekens stonden de potentiële risico's van het gebruik van verschillende (extra beveiligde en/of identiteitsversluierende) communicatiemiddelen centraal. Met de respondenten is vooral gesproken over de over potentiële risico's betreffende de geheimhouding, integriteit, onafhankelijkheid en documentatieplicht van advocaten.

Werkwijze en waarborgen

De interviews met alle respondenten zijn auditief vastgelegd met opnameapparatuur. Na afloop van een interview is het door een onderzoeker verbatim getranscribeerd of neergelegd in een verkort gespreksverslag. Als de respondent daar prijs op stelde, is het transcript of gespreksverslag vervolgens

aan haar/hem ter goedkeuring voorgelegd. Die goedkeuring werd soms direct verleend, soms onder de voorwaarde dat door de respondent aangegeven passages uit het transcript verwijderd of op een bepaalde manier aangepast zouden worden. Die wens is door de onderzoekers steevast gehonoreerd. De – al dan niet op verzoek van de respondent aangepaste – transcripten zijn daarna gefinaliseerd.

Over deze gang van zaken zijn de respondenten vóór het interview per brief geïnformeerd. Indien nodig is een en ander voorafgaand aan het interview (en soms nadien ter herhaling) mondeling (nader) toegelicht. Alle respondenten hebben voor de beschreven gang van zaken hun toestemming verleend door een van tevoren toegestuurd *informed consent*-formulier te ondertekenen. Zo'n formulier is ook steeds door een van de interviewende onderzoekers ondertekend.

Na de finalisering van de transcripten en gespreksverslagen zijn deze door de onderzoekers geanalyseerd en gecodeerd. Daarbij is gebruikgemaakt van Atlas TI. Hierbij is door de onderzoekers een *a-priori*-benadering gehanteerd door voorafgaand aan het coderen verschillende codes op te stellen aan de hand van de topiclijst en de verschillende thema's die in het interview aan de orde kwamen.[44] Bij het coderen is gebruikgemaakt van verschillende thematische codes die samenhangen met (1) de beweegredenen van advocaten om wel of niet gebruik te maken van bepaalde communicatiemiddelen en (2) de risico's die met het gebruik van bepaalde communicatiemiddelen kunnen samenhangen.

De resultaten van dit empirische onderzoek staan beschreven in hoofdstuk 5 en – voor zover het gaat over risico's – ook in hoofdstuk 6. De bevindingen uit het interview met een medewerker van het NFI zijn verwerkt in hoofdstuk 3 en 6. Gezien de gevoeligheid van het thema van dit onderzoek zullen alle respondenten anoniem blijven. Om dezelfde reden zullen bepaalde bevindingen of uitlatingen niet worden toegeschreven aan individuele respondenten door middel van een nummer. Deze werkwijze is ook de basis waarop de respondenten hun medewerking aan ons onderzoek hebben verleend.

2.4.2.2 Schriftelijke vragenlijsten

Daarnaast is schriftelijk informatie ingewonnen bij het OM en bij het landelijk dekenberaad. Bij beide is, ter beantwoording van deelvraag 2, informatie opgevraagd over de hoeveelheid advocaten die hebben gemeld gebruik te maken of te hebben gemaakt van een cryptotelefoon. Aan het landelijk dekenberaad zijn daarnaast, ter beantwoording van deelvraag 3, vragen voorgelegd over de beweegredenen van advocaten om al dan niet gebruik te maken van een cryptotelefoon. Aan het OM zijn, ter beantwoording van deelvraag 5, tevens vragen voorgelegd over de potentiële risico's die gepaard kunnen gaan met het van het gebruik extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten.

2.5 'Rechtsvergelijkend' onderzoek

De vierde deelvraag luidt: *Wat is bekend over regelgeving en praktijk met betrekking tot het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in andere landen?*

[44] Decorte 2016, p. 483.

Voor de beantwoording van deze vraag, die in hoofdstuk 7 centraal staat, is op verschillende wijzen informatie verzameld. Om een beeld te krijgen van wat er bekend is over het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in andere landen zijn de onderzoekers bij wijze van inventarisatie begonnen te onderzoeken of dit onderwerp leeft in het maatschappelijke, politieke of juridische debat in andere landen. Daartoe is het nodige *desk research* gedaan door buitenlandse literatuur en nieuwsberichten over gebeurtenissen die raken aan de onderzoeksthematiek, te analyseren. Daarbij ging het overigens niet zozeer om een literatuurstudie (laat staan een systematische), als wel om een exploratieve blik op (mogelijk) relevante buitenlandse literatuur en nieuwsberichten. Daarnaast hebben de onderzoekers schriftelijk contact gezocht met professionals in het buitenland om daar hun licht op te steken voor wat betreft de vraag of en in hoeverre de thematiek van dit onderzoek ook daar speelt.[45] Dat betroffen nu eens contacten die al tot het eigen netwerk van (collega's van) de onderzoekers behoorden en in de regel zelf ook academici zijn, dan weer 'contacten' in de zin van personen, veelal academici, die blijkens gevonden literatuur affiniteit hebben met het onderwerp.

Na een eerste exploratieve zoekslag is een brief uitgegaan namens de onderzoekers vanuit de NOvA naar een aantal buitenlandse balies. De balies van Australië, België, Canada, Duitsland, Frankrijk, Italië, Roemenië, Spanje, de Verenigde Staten, het Verenigd Koninkrijk en Zweden zijn benaderd en verzocht te reageren op een aantal vragen. Aan de balies werd de vraag voorgelegd of het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in dat land werd gereguleerd door wetten, regelgeving of beleid. Daarnaast werd gevraagd naar het al dan niet bestaan van een sociaal, politiek en/of juridisch debat rondom het gebruik van dergelijke middelen door advocaten. Tot slot werd aan de balies een doorverwijzing naar (potentieel) relevante bronnen verzocht. Op die brief is – ook na het herhaaldelijk versturen van herinneringen – slechts door enkele balies gereageerd, meestal kort en tamelijk algemeen.[46]

De informatie die is verzameld door middel van *desk research* en/of het aanschrijven van buitenlandse contacten is uiteindelijk voornamelijk gebruikt ter oriëntatie op het onderwerp. Vervolgens is gekozen voor een thematische aanpak bij de beantwoording van de vierde deelvraag. Een aantal van de in hoofdstuk 6 geïdentificeerde risico's en knelpunten betreffende het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten is als vertrekpunt gebruikt. Daarbij is gekozen voor een nadere uitwerking van drie thema's waarover in het exploratieve onderzoek al relevante inzichten waren verkregen. In hoofdstuk 7 is de voor die onderwerpen meest relevante informatie bijeen gebracht, met als doel het in kaart brengen van de wijze waarop in andere landen met vergelijkbare problematiek wordt omgegaan. Vervolgens is in openbaar toegankelijke bronnen nog nader onderzoek verricht om bepaalde aspecten meer gedetailleerd of diepgaander te kunnen uitwerken. Van een klassiek rechtsvergelijkend onderzoek kan derhalve niet worden gesproken.[47] Er wordt dan ook nadrukkelijk niet gepretendeerd om een min of meer volledig beeld te schetsen van de regelgeving en

[45] Contacten zijn aangeschreven in de volgende landen: Duitsland, België, Zweden, Verenigd Koninkrijk, Spanje. Van de contacten uit Duitsland en België is een inhoudelijke reactie ontvangen.

[46] Vanuit de balies in België, Canada, Frankrijk, Spanje en Zweden is informatie gekomen.

[47] Vgl. over deze onderzoeksmethode Kestemont 2018, par. 3.3.

praktijk ten aanzien van dit onderwerp in enkele specifieke buitenlanden. Evenmin wordt een overzicht gegeven van alle informatie die hierover in het kader van dit onderzoek is verzameld. Voor de meer gefragmenteerde, thematische benadering is om verschillende redenen gekozen. In de eerste plaats leent deze deelvraag zich niet goed voor een klassieke rechtsvergelijking, alleen al omdat over dit onderwerp ook in andere landen niet of nauwelijks wet- of regelgeving voorhanden is. Bovendien richt de deelvraag zich deels op de praktijk in andere landen. Ook dat deel van de vraag laat zich niet (alleen) met klassiek rechtsvergelijkend onderzoek beantwoorden. In de tweede plaats, en in samenhang met het voorgaande, is gebleken dat de verkregen informatie vaak fragmentarisch van aard was en er over bepaalde aspecten weinig (empirische) informatie bekend was. Een meer traditionele aanpak waarin niet zozeer de thema's maar de onderzochte landen centraal worden gesteld zou daarom hoe dan ook een beperkt beeld opleveren. De meer op relevante thema's gerichte benadering waarvoor in dit rapport is gekozen, biedt ten opzichte daarvan het voordeel dat deze zich concentreert op de onderwerpen die in de Nederlandse situatie vragen of knelpunten opleveren en waarover in andere landen zinvolle inzichten zijn opgedaan. De op deze manier gepresenteerde informatie kan dan ook worden gebruikt bij het nadenken over en formuleren van mogelijke oplossingsrichtingen.

3. Extra beveiligde en/of identiteitsversluierende communicatiemiddelen

3.1 Inleiding

In dit hoofdstuk wordt uiteengezet wat in dit rapport wordt bedoeld met de term 'extra beveiligde en/of identiteitsversluierende communicatiemiddelen' (par. 3.2). Daarnaast worden verschillende categorieën communicatiemiddelen onderscheiden (par. 3.3). Vervolgens wordt ingegaan op de verhouding tussen de opsporing van strafbare feiten en het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen in relatie tot criminele activiteiten, waarbij de nadruk zal liggen op cryptotelefoons (par. 3.4). Tot slot wordt kort ingegaan op de op deze communicatiemiddelen van toepassing zijnde wet- en regelgeving (par. 3.5). Dit hoofdstuk dient er aldus toe om in zijn algemeenheid duidelijk te maken waar het om gaat bij het centrale onderwerp van dit onderzoek, en meer in het bijzonder ter (gedeeltelijke) beantwoording van deelvraag 2a (waar het gaat om de soorten extra beveiligde en/of identiteitsversluierende communicatiemiddelen, hun werking en de toepasselijke wet- en regelgeving).

3.2 Wat zijn extra beveiligde en/of identiteitsversluierende communicatiemiddelen?

Onder extra beveiligde en/of identiteitsversluierende communicatiemiddelen wordt in dit rapport verstaan: communicatiemiddelen die door middel van verschillende beveiligingsfunctionaliteiten de vertrouwelijkheid van de communicatie en de privacy van de gebruiker beter (zouden moeten) kunnen waarborgen dan de reguliere communicatiemiddelen. Het overkoepelende doel van de extra beveiliging is het voorkomen dat ongeautoriseerde derden toegang kunnen krijgen tot verschillende onderdelen van de communicatie. De beveiligingsfunctionaliteiten kunnen gericht zijn op het beveiligen van de inhoud van de communicatie, bijvoorbeeld hetgeen dat wordt besproken over de telefoon of via de e-mail. Daarnaast kunnen de beveiligingsfunctionaliteiten ook gericht zijn op het beveiligen van de metadata van de communicatie. Metadata zijn gegevens die de eigenschappen van andere gegevens beschrijven.[48] Het gaat om informatie over communicatie die niet te maken heeft met de inhoudelijke boodschap van het bericht, denk aan gebruikersinformatie over de verzender en de ontvanger, de datum en tijd van het bericht, de frequentie van berichten of de IP-adressen gelinkt aan de betrokken toestellen.[49] Wanneer het gaat om de opsporing van strafbare feiten is niet alleen de inhoud van communicatie, maar ook de metadata van potentieel belang. De vaststelling dát, wanneer, en waar personen met elkaar communiceren kan bewijsrechtelijk immers van betekenis zijn. [50]

Zowel de inhoudelijke communicatie als de metadata kunnen op verschillende manieren worden beveiligd. Encryptie is een veelgebruikte methode om de inhoud van een e-mail, telefoongesprek of chatbericht te beveiligen. Een ander woord voor encryptie is 'versleuteling'. Dit begrip duidt op een

48 *Cybersecurity Woordenboek* 2021, p. 49.
49 Zie in dit verband o.a. Jansen e.a. 2023, p. 70 en 72.
50 Jansen e.a.2023, p. 72 en 86-87.

wiskundig proces waarbij, meestal op basis van een algoritme, informatie wordt omgezet in een code en op deze manier onleesbaar wordt gemaakt voor derden.[51] Enkel de ontvanger van het bericht heeft de 'sleutel' waarmee het bericht leesbaar kan worden geopend. Het doel van encryptie is de inhoud van een bericht (of bestand) beschermen tegen ongeautoriseerde toegang, teneinde de vertrouwelijkheid en integriteit van informatie te waarborgen.[52] Pretty Good Privacy (PGP) is een bekende standaard in bijvoorbeeld e-mailverkeer om informatie voor derden onleesbaar te maken door middel van versleuteling.[53]

Naast versleuteling zijn er ook andere manieren waarop de communicatie extra beveiligd kan worden, bijvoorbeeld door het gebruik van (extra) wachtwoorden of door het (automatisch) verwijderen van berichten nadat deze zijn ontvangen. Voorts kan ook de locatie van de server of provider, en daarmee het land waar de berichtgeving wordt verzameld en opgeslagen, van belang zijn in het kader van de beveiliging van communicatie. Dit heeft onder andere te maken met verschillen in privacywetgeving en (opsporings-)bevoegdheden van overheidsinstanties tussen landen. Met name in de Verenigde Staten kunnen overheidsinstanties, waaronder inlichtingendiensten, veel informatie bij providers opvragen in het kader van de nationale veiligheid en opsporingsonderzoeken.[54] De servers van online platformen bevatten vaak niet alleen persoonlijke informatie over de gebruikers van dit platform maar ook grote hoeveelheden e-mailberichten en bestanden. In een land met strengere privacywettenkunnen overheidsinstanties niet of minder gemakkelijk de informatie bij de provider opvragen. Wanneer het gaat om digitale gegevens kunnen overigens meerdere routes worden gevolgd bij het opvragen van gegevens, namelijk via het bedrijf dat de communicatiedienst aanbiedt, maar ook via de serverbeheerder.[55]

3.3 Categorieën extra beveiligde en/of identiteitsversluierende communicatiemiddelen

In dit rapport zal de focus liggen op de middelen die worden gebruikt voor het digitale communicatieverkeer tussen advocaat en cliënt en de maatregelen die daarbij worden genomen. Daarbij wordt onderscheid gemaakt tussen drie categorieën extra beveiligde en/of identiteitsversluierende communicatiemiddelen die advocaten kunnen gebruiken om te communiceren met hun cliënt(en): cryptotelefoons, extra beveiligde chatapplicaties en extra beveiligde e-mailapplicaties. In het navolgende worden deze drie categorieën uiteengezet.

---

51 Kerr & Schneier 2018, p. 993. zie ook: *Cybersecurity Woordenboek* 2021, p. 24. Europol & Eurojust 2019, p. 19.

52 Jansen e.a. 2023, p. 24.

53 *Cybersecurity Woordenboek* 2021, p. 56.

54 Naef 2022, p. 78-79.

55 Dit vloeit voort uit het in de AVG gemaakte onderscheid tussen verwerken en verwerkingsverantwoordelijke. Wanneer bedrijf en server in verschillende landen zijn gevestigd kan dan gekozen worden voor een aanvraag in het land met de minst strenge privacywetgeving.

3.3.1 Cryptotelefoons

In dit rapport verstaan we onder een cryptotelefoon een toestel waarvan zowel de software als de hardware zo zijn ontworpen dat ze de communicatie zo veilig en vertrouwelijk mogelijk kunnen overbrengen en bewaren.[56] Er bestaan veel verschillende soorten cryptotelefoons met verschillende soorten beveiligingseigenschappen, voorbeelden zijn de telefoons van Ennetcom, PGP-Safe, EncroChat en Sky-ECC. Dergelijke telefoons bieden een hogere mate van privacy en anonimiteit aan hun gebruikers dan andere telefoons door onder andere de software die op de telefoons is geïnstalleerd. Deze software maakt het mogelijk om versleuteld chatberichten, bestaande uit tekst en/of afbeeldingen, te versturen en versleuteld te bellen.[57] Daarnaast draagt de hardware van de toestellen vaak ook bij aan de garantie voor anonieme en niet-traceerbare communicatie. Bepaalde onderdelen van het toestel, waaronder de camera, microfoon en/of USB-poort, zijn vaak verwijderd ofwel onbruikbaar gemaakt met als gevolg dat het gebruik van en de communicatie via deze toestellen niet gevolgd of getapt kan worden.[58] Tot slot bieden de telefoons vaak ook andere functionaliteiten om de communicatie zoveel mogelijk te versluieren. Zo bevatten de telefoons vaak een functionaliteit waarmee berichten na enige tijd automatisch verwijderd worden,[59] kunnen gebruikers daarnaast zelf met één handeling alle informatie op het toestel verwijderen (*Emergency Wipe* of *Panic Wipe*) of dit op afstand (laten) doen (*Wipe- or kill*-verzoek of *Remote wipe*).[60]

Aan de hogere mate van beveiliging en anonimiteit zit wel een prijs verbonden. De gemiddelde cryptotelefoon zelf kost 800 tot 1000 euro, maar de kosten voor de aan het toestel verbonden abonnement en/of licentie kunnen variëren van 800 tot 1500 euro per zes maanden.[61]

3.3.2 Chatapplicaties

Anno 2023 zijn online chatapplicaties (hierna: chatapps) niet meer weg te denken uit het digitale communicatieverkeer. In dit rapport spreken wij van een chatapplicatie wanneer er tussen (kleine groepen) individuen besloten gecommuniceerd kan worden via internet door middel van een op een smartphone geïnstalleerde applicatie. Voorbeelden van chatapps zijn WhatsApp, Threema, Telegram, Signal en Wire. Bij de meeste chatapps worden berichten verstuurd met *end-to-end* encryptie, een 'sterke' vorm van versleuteling waarmee de inhoud van berichten onleesbaar wordt gemaakt voor derden, doordat enkel de ontvanger de sleutel heeft om het bericht te 'ontsleutelen'. Het verschil met berichten die niet met *end-to-end* encryptie worden verstuurd zit daarbij in het sleutelbeheer: bij niet *end-to-end*

---

56 Royer & Van Leeuw 2022, p. 90.

57 Zie voor EncroChat: Rb. Midden-Nederland 12 april 2022, ECLI:NL:RBMNE:2022:1389, r.o. 3.4.1. Zie ook: Jansen e.a. 2023, p. 27.

58 Zie in het kader van EncroChat o.a. 'Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe', *Europol.europa.eu*, 2 juli 2020.

59 Zie voor EncroChat: Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2.

60 Zie in het PGP-Safe: Rb. Rotterdam 20 januari 2022, ECLI:NL:RBROT:2022:363, r.o. 9.2. Zie voor EncroChat: Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2. Zie voor Sky-ECC toestellen: Rb. Amsterdam 21 november 2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3. Zie voor ANOM toestellen: HR 8 november 2022, ECLI:NL:HR:2022:1589, r.o. 2.2.2.

61 Zie o.a. Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2.

encryptie wordt het bericht versleuteld naar de server gestuurd, maar daar wordt het ontsleuteld opgeslagen, hetgeen betekent dat de provider (en daarmee onder omstandigheden uiteindelijk ook de opsporingsdiensten) kennis kunnen nemen van de inhoud. Bij *end-to-end* versleutelde communicatie wordt het bericht lokaal versleuteld, versleuteld verstuurd en opgeslagen en weer lokaal ontsleuteld. Dit betekent dat de provider géén toegang heeft tot de inhoud van de berichten. Daarnaast bieden chatapps veelal extra optioneel te gebruiken functionaliteiten die ervoor zorgen dat de inhoud van de berichten privé blijft. Hierbij kan gedacht worden aan de mogelijkheid om het gehele account of bepaalde gesprekken te beveiligen met een extra wachtwoord,[62] mechanismen waardoor ontvangers chatberichten niet naar derden kunnen doorsturen,[63] mechanismen waardoor derden inkomende berichten op het telefoonscherm niet kunnen bekijken,[64] of instellingen om berichten na enige tijd automatisch te verwijderen.[65]

Hoewel er in Nederland nog steeds veelvuldig gebruik wordt gemaakt van WhatsApp,[66] stappen steeds meer mensen vanwege privacyoverwegingen over op alternatieve chatapps zoals Signal, Telegram of Threema. WhatsApp maakt, net als veel andere chatapps, gebruik van *end-to-end* encryptie en biedt daarnaast ook een aantal extra beveiligingsmechanismen.[67] De keuze om een alternatieve chatapplicatie te gebruiken is daarom veelal gebaseerd op de andere privacywaarborgen en beveiligingsfunctionaliteiten die alternatieve chatapps wel bieden, maar WhatsApp niet. Zo gaan Signal, Threema, Telegram en Wire anders om met het verzamelen, opslaan en/of delen van metadata dan WhatsApp.[68] Deze chatapps bieden daarmee dus meer waarborgen voor de privacy van de gebruiker richting de aanbieder van de communicatiedienst. Daarnaast bieden deze chatapps verschillende extra mogelijkheden om de communicatie privé en vertrouwelijk te houden.

Hoewel ook de communicatie via WhatsApp op verschillende manieren beveiligd is of kan worden, zal binnen dit rapport de nadruk met name liggen op de verschillende andere chatapps die extra waarborgen bieden omtrent het veilig en/of anoniem online communiceren.

3.3.3 Extra beveiligde e-mail

Anders dan de meeste chatapplicaties bieden veel e-mailproviders (nog) geen (standaard) *end-to-end* versleutelde communicatie aan hun gebruikers.[69] Wanneer een e-mail zonder (goede) versleuteling of andere extra beveiliging wordt verstuurd, is de correspondentie makkelijker toegankelijk voor

62 Zie functionaliteit Threema 'Private chats'.
63 Zie functionaliteit Telegram 'secret chats'.
64 Zie functionaliteit Signal 'Meekijkpreventie'; Telegram 'Secret chats'.
65 Mogelijkheid verwijderen berichten: WhatsApp 'Dissapearing messages'; Signal 'Verlopende berichten' en Telegram 'Self-destructing messages'.
66 Zie o.a. Nationaal Social Media Onderzoek 2023.
67 Zie: 'Message privately', whatsapp.com. Extra beveiligingsfunctionaliteiten die door WhatsApp worden aangeboden zijn bijvoorbeeld *Chat lock* en *Disappearing messages*.
68 Zie o.a. : 'Why Threema instead of WhatsApp', Threema.ch.; 'Signal Terms & Privacy Policy', Signal.org. en 'Signal: hoe veilig is deze privacyvriendelijke chat-app?', vpngids.nl; 'Telegram Privacy Policy', telegram.org; 'Privacy Policy', wire.com.
69 Lewis, Zheng & Carter 2017, p. 10.

ongeautoriseerde derden, bijvoorbeeld hackers. Bovendien, ook de e-mailprovider zelf kan de correspondentie op de server inzien en potentiële derden, bijvoorbeeld inlichtingendiensten, toegang geven tot de berichten. Onder een extra beveiligde e-mailprovider verstaan we in dit rapport een e-mailprovider die extra waarborgen biedt ter bescherming van de e-mailcorrespondentie door middel van sterke encryptie, multifactorauthenticatie of andere beveiligingsfunctionaliteiten.[70] Voorbeelden van extra beveiligde e-mail zijn Proton Mail, Zivver en HubSpot. In het geval van Zivver en Proton Mail wordt de correspondentie versleuteld voordat deze op de server komt. Dit betekent dat providers zelf de e-mails niet kunnen inzien en ook iemand anders geen toegang tot de e-mailcorrespondentie kunnen geven.[71] Daarnaast bieden extra beveiligde e-mailproviders ook andere functionaliteiten aan zoals het terughalen van e-mails, het gebruik van afleverbewijzen en multifactorauthenticatie.[72]

3.4 Opsporing en extra beveiligde en/of identiteitsversluierende communicatiemiddelen

3.4.1 Het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen binnen criminele netwerken

Veel van de hierboven benoemde beveiligingsfunctionaliteiten, denk aan encryptie of multifactorauthenticatie, zijn inmiddels ingebed in de alledaagse digitale communicatie en spelen een cruciale rol bij het waarborgen van de integriteit en vertrouwelijkheid van informatie en de privacy van gebruikers. Hoewel de wens om zo afgeschermd mogelijk te communiceren niet direct een indicatie voor crimineel gedrag hoeft te zijn, worden bepaalde extra beveiligde en/of identiteitsversluierende communicatiemiddelen wel geassocieerd met de betrokkenheid bij criminele activiteiten. Dit geldt met name voor de cryptotelefoons.[73] Deze telefoons lijken vooral gebruikt te worden binnen criminele netwerken.[74] Cryptotelefoons en andere vormen van versleutelde communicatie geven criminelen de mogelijkheid om anoniem, beveiligd en buiten het zicht van strafvorderlijke overheden te communiceren. De telefoons lijken voornamelijk te worden gebruikt binnen de georganiseerde misdaadstructuren, een groot deel van de communicatie gaat over drugshandel en daaraan gerelateerde delicten zoals fraude, witwassen, corruptie, gijzeling en moord.[75] Kortom, het gebruik van een cryptotelefoon (of een andere vorm van versluierende communicatie) lijkt inmiddels een belangrijke rol te vervullen als onderdeel van de modus operandi van criminelen. Zodoende hebben cryptotelefoons

70 Duò 2023.

71 'Security', proton.me.

72 'Zivver Secure Email', zivver.com en 'Security, Privacy, and Control', legal.hubspot.com.

73 Vgl. Van Toor 2022, p. 78-80. Zie ook *SOCTA report* 2021, p. 22 en 32-33 en *IOCTA report*, 2021, p. 18.

74 Ennetcom was in 2016 de grootste aanbieder van versleutelde communicatie aan criminelen. EncroChat was in begin 2020 een van de grootste aanbieders van digitaal versleutelde communicatie. Na de inbeslagname van de server werd duidelijk dat een groot aandeel van de EncroChat telefoon-gebruikers vermoedelijk betrokken was bij criminele activiteiten. *Criminal justice across borders in the EU* 2020, para. 7.2. Zie ook: Oerlemans & Van Toor 2022, p. 309-328 en p. 312. Zie ook Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085, waarin wordt gerefereerd aan een analyse van de Nederlandstalige berichten in de Ennetcomdata, waaruit bij een steekproef van de inhoud gemiddeld zo'n 75% van de berichten crimineel gerelateerd bleek te zijn.

75 Zie o.a. de communicatie PGP-Safe: Vermeulen, Soudijn & Van der Leest 2021, p. 197 en 'Ontsleutelde berichtgeving crypto-gsm's cruciaal in zaak vergismoord', *om.nl* 11 december 2017. Zie in dit verband ook de communicatie EncroChat: Europol & Eurojust 2021, p. 27.

een 'crimineel imago' gekregen, wat onder andere blijkt uit berichtgeving in de media waarin bijvoorbeeld wordt gesproken van 'internationaal chatnetwerk criminelen'[76] (EncroChat) en 'WhatsApp van de onderwereld'[77] (Ennetcom). Hoewel niet alle gebruikers zich bezighouden met criminele activiteiten en het hebben of gebruiken van een cryptotelefoon op zichzelf niet strafbaar of verboden is,[78] spreekt Europol over een 'grijze infrastructuur' die wordt geboden door cryptotelefoonproviders omdat deze een dienst aanbieden die het mogelijk maakt om criminele activiteiten optimaal verborgen te houden voor de strafvorderlijke autoriteiten. Gelet op de aanzienlijke hoeveelheid criminele activiteiten die met dergelijke diensten in verband wordt gebracht, kunnen cryptotelefoonproviders volgens Europol worden aangemerkt als een criminele organisatie 'after finding enough evidence of criminal abuse'.[79] Of inderdaad van een criminele organisatie kan worden gesproken zal steeds in concrete strafzaken moeten worden vastgesteld. In de Nederlandse context is dat tot op heden in ieder geval gebeurd in een zaak tegen Ennetcom en de oprichter c.q. middellijk bestuurder hiervan.[80] Ook kan worden gedacht aan andere mogelijke strafbare feiten, zoals witwassen en begunstiging.[81]

Zowel in Nederland als in een aantal andere landen zijn er voorbeelden van advocaten die betrokken zijn geweest bij de strafbare feiten van een criminele organisatie en in het contact met deze organisatie – die vermoedelijk voor een deel bestaat uit hun cliënten – een cryptotelefoon hebben gebruikt.[82] Op basis van deze incidenten kan evenwel niet worden aangenomen dat alle advocaten die in het bezit zijn van een cryptotelefoon, deze ook gebruiken voor criminele doeleinden en/of onder druk zijn gezet om dit toestel te schaffen. Een cryptotelefoon kan immers ook door de advocaat zijn aangeschaft om andere redenen, bijvoorbeeld om in contact te kunnen blijven met cliënten, wanneer deze cliënten andere communicatielijnen niet willen gebruiken.[83] Daarnaast hoeft ook de verkoop en ontwikkeling van cryptotelefoons niet per definitie in het criminele circuit te gebeuren. In 2018 heeft een Nederlandse advocaat een legitiem bedrijf opgericht gericht op de verkoop van cryptotelefoons voor geheimhouders. Het doel van deze advocaat was een mogelijkheid creëren om veilig te communiceren, zonder dit in de 'schimmige sfeer' te hoeven doen. Vijftien advocaten hebben in dit kader een speciale cryptotelefoon ontvangen.[84]

---

76 '6558 arrestaties sinds oprollen internationaal chatnetwerk criminelen', *RTL nieuws* 27 juni 2023.

77 'OM denkt dat Eindhovenaar achter 'WhatsApp van de onderwereld' zit', *NOS (in samenwerking met Omroep Brabant)* 12 oktober 2022.

78 Zie over de toepasselijke wet- en regelgeving ook par. 3.5.

79 *IOCTA report*, 2021, p. 18. Zie ook: Oerlemans 2021. Ook het OM spreekt van 'facilitators' van criminelen en criminele organisaties. 'Ontsleutelde berichtgeving crypto-gsm's cruciaal in zaak vergismoord', om.nl, 11 december 2017.

80 Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085, zie ook ECLI-nummers 9086 en 9087 (in de laatste zaak werd de boekhoudster van Ennetcom vrijgesproken van deelname aan een criminele organisatie). Zie ook de annotatie bij deze uitspraak: Oerlemans 2022a, p. 138-142.

81 Vgl. Rb. Rotterdam 20 januari 2022, ECLI:NL:RBROT:2022:363. Hier ging het om een verkoper van cryptotelefoons. Er volgde onder meer een bewezenverklaring van feitelijk leidinggeven aan begunstiging, voor witwassen volgde vrijspraak. Deelname aan een criminele organisatie was in deze zaak niet tenlastegelegd.

82 Zie o.a. Raad van Discipline 's-Hertogenbosch 23 april 2021, ECLI:NL:TADRSHE:2021:73, r.o. 2.5.; 'Onderschepte berichten tonen hoe opgepakte advocaten zich bezighielden met criminele praktijken', *nieuwsblad.be* 12 maart 2021 en 'Advocaat mag gevangenis verlaten met enkelband na arrestatie in dossier Sky ECC', *gva.be* 21 juni 2021.

83 Droogleever Fortuyn 2022.

84 Gloudemans-Voogd 2018 en Rietbroek 2018.

Omdat leden van criminele organisaties lang in de veronderstelling waren dat bepaalde cryptocommunicatiediensten niet te hacken zouden zijn, werd via de cryptotelefoons (en andere cryptocommunicatiediensten) vrijuit gecommuniceerd over het produceren, transporteren en verhandelen van grote hoeveelheden harddrugs.[85] Daarnaast werd vrijuit gesproken over liquidaties, witwassen en fraude. Door het neerhalen van cryptocommunicatiediensten (zie hierna par. 3.4.2) hebben opsporingsautoriteiten de communicatie tussen criminelen kunnen inzien.

3.4.2 Cryptotelefoon-operaties

Extra beveiligde en/of identiteitsversluierende communicatiemiddelen zorgen voor nieuwe uitdagingen binnen de opsporing. Door de extra beveiliging, bijvoorbeeld encryptie, is er minder directe toegang tot (potentieel) bewijs, het bericht is immers in principe onleesbaar voor iedereen behalve de ontvanger(s).[86] Het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen kan het identificeren en lokaliseren van relevante personen,[87] het vaststellen van samenwerkingsverbanden en criminele activiteiten en het vergaren van bewijsmateriaal binnen het opsporingsonderzoek, bemoeilijken.[88] Omdat de inhoud van communicatie tussen verdachten relevant kan zijn binnen een opsporingsonderzoek, heeft de strafvorderlijke overheid er belang bij om berichten te ontsleutelen, opdat de inhoud daarvan gelezen kan worden. Encryptie, en de omzeiling daarvan speelt een steeds grotere rol in verschillende onderdelen van het opsporingsonderzoek.[89] Naast de inhoud van berichten kunnen ook verschillende soorten metadata, zoals locatiegegevens, gebruikersnamen en informatie over het moment of de frequentie van de communicatie, relevant zijn binnen het opsporingsonderzoek, met name bij het identificeren en lokaliseren van relevante personen.[90]

Vanwege het veelvuldig gebruik van cryptotelefoons binnen de criminele markt hebben de afgelopen jaren meerdere cryptotelefoon-operaties plaatsgevonden. Opsporingsautoriteiten van verschillende landen werken in het kader van dergelijke operaties samen om de servers van cryptodiensten, waaronder Ennetcom, PGP-safe, Ironchat, EncroChat en Sky-ECC, neer te halen.[91] Doormiddel van inbeslagname, interceptie en/of overname van de servers kon de communicatie tussen gebruikers van dergelijke telefoons worden veiliggesteld, gekopieerd, ontsleuteld en soms zelfs live worden meegelezen.[92] Naast het neerhalen van bestaande aanbieders van cryptocommunicatie, werd in 2019

---

85 Zie voor analyse van de communicatie van PGP-Safe: Vermeulen, Soudijn & Van der Leest 2021, p. 197.

86 Jansen e.a. 2023, p. 70.

87 Jansen e.a. 2023, p. 72.

88 Zie in dit verband o.a. Jansen e.a. 2023, p. 73; Europol & Eurojust 2019, p. 23-24 en Europol & Eurojust 2021, p. 16-26.

89 Jansen e.a. 2023 en Europol & Eurojust 2021.

90 Jansen e.a. 2023, p. 5, 72 en 86-87.

91 Zie bijv. 'Twintig miljoen geheime berichten onderschept, honderd arrestaties in Nederland', *nos.nl* 2 juli 2020 (over Encrochat) en Vugts & Laumans 2021 (over Sky-ECC). Zie voor een overzicht van de verschillende cryptotelefoon-operaties: Oerlemans 2022b.

92 Zie voor wat betreft de werkwijzen in de verschillende cryptotelefoon-operaties: Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504, r.o. 3.1.1 en 3.1.2. (Ennetcom); Rb. Rotterdam 11 april 2022, ECLI:NL:RBROT:2022:2674, r.o. 5.2.1. (PGP-Safe); Rb. Overijssel 23 april 2020, ECLI:NL:RBOVE:2020:1563, r.o. 4.1.1 en Rb. Overijssel 23 april 2020, ECLI:NL:RBOVE:2020:1587, r.o. 4.2. (Ironchat/Ironphone); Rb. Rotterdam 25

door het Amerikaanse Federal Bureau of Investigation (FBI) het ANOM-platform opgericht.[93] Vanuit dit platform werden cryptotelefoons aangeboden en verspreid binnen criminele organisaties en werd vervolgens, in het kader van *Operation Trojan Shield*, de communicatie van de gebruikers onderschept.[94]

Het neerhalen van cryptocommunicatiediensten lijkt niet beperkt tot de aanbieders van aparte (hardware geprepareerde) cryptotelefoons. Dit blijkt onder andere uit de meer recente hack van Exclu-Messenger, een vorm van cryptocommunicatie waarbij de gebruiker een app op de eigen smartphone kan installeren en activeren tegen betaling van 800 euro per zes maanden.[95] Uit berichtgeving blijkt niet dat voor het gebruik van Exclu-Messenger een apart geprepareerde telefoon aangeschaft diende te worden. Technisch gezien lijkt het daarom ook niet te gaan om een cryptotelefoon-operatie. Hoewel het hier gaat om een app die gedownload kan worden en niet om een apart geprepareerde telefoon zonder microfoon, camera en/of USB poort, wordt Exclu-Messenger door het OM in hetzelfde rijtje geplaatst als Ennetcom, Encrochat en Sky-ECC.[96] Over de veronderstelling dat de app enkel gebruikt wordt door criminelen lijkt in de berichtgeving geen twijfel over te bestaan. Exclu-Messenger wordt aangeduid als 'een criminele communicatieapp',[97] 'een cryptocommunicatiedienst van criminelen'[98] of 'een versleutelde berichtendienst die door de onderwereld wordt gebruikt'.[99]

De cryptotelefoon-operaties kunnen worden aangemerkt als een vorm van 'datagedreven opsporing': bij de strafzaken die uit de operaties voortvloeien gaat het veelal om het verwerken en analyseren van data die op een eerder moment, in het kader van een ander onderzoek reeds is verzameld.[100] In het kader van de cryptotelefoon-operaties gaat het om grote hoeveelheden berichten die vrijwel in één keer worden verzameld door een hack of inbeslagname van een server, en vervolgens (in delen) worden geanalyseerd en gebruikt in verschillende strafrechtelijke onderzoeken. Ten behoeve van het snel en efficiënt doorzoeken van grote hoeveelheden data uit digitale gegevensdragers (bijvoorbeeld computers of telefoons) heeft het NFI de softwaretool Hansken ontwikkeld.[101] Hansken wordt onder andere bij de cryptotelefoon-operaties gebruikt om grote hoeveelheden data inzichtelijk en toegankelijk te maken voor de opsporingsambtenaren die met deze data moeten werken,[102] en biedt verschillende functionaliteiten om sporen met geheimhouderinformatie uit te sluiten van het onderzoek.[103] Hansken

---

juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3. en Rb. Midden-Nederland 12 april 2022, ECLI:NL:RBMNE:2022:1389, r.o. 3.4.2.1. (EncroChat); Rb. Amsterdam 21 november 2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3. (Sky-ECC).

93 '800 criminals arrested in biggest ever law enforcement operation against encrypted communication', europol.europa.eu, 8 juni 2021.

94 Zie voor wat betreft de werkwijze o.a. HR 8 november 2022, ECLI:NL:HR:2022:1589, r.o. 2.2.2.; Oerlemans 2022c; '800 criminals arrested in biggest ever law enforcement operation against encrypted communication', europol.europa.eu, 8 juni 2021.

95 'Politie leest vijf maanden mee met versleutelde berichten, 42 arrestaties', *nos.nl* 3 februari 2023. Zie ook Laumans & Vugts 2022.

96 'Politie leest opnieuw mee met criminelen: cryptocommunicatiedienst Exclu ontmanteld, *om.nl*, 3 februari 2023.

97 'Primeur: eerste verdachte in gekraakte criminele app Exclu voor de rechter', *rtvoost.nl*, 7 februari 2023.

98 'Politie lees opnieuw mee met criminelen: cryptocommunicatiedienst Exclu ontmanteld', *om.nl*, 3 februari 2023.

99 'Mega-operatie politie met 1200 agenten: 42 arrestaties, liquidaties voorkomen', *rtlnieuws.nl*, 3 februari 2023.

100 Hirsch Ballin & Oerlemans 2023, p. 18.

101 'Hansken', forensischinstituut.nl ; Zie ook de website Hansken: 'An introduction to Hansken', hansken.nl en 'Why Hansken', hansken.nl.

102 *Vision Statement Hansken* 2021, p. 1.

103 *Hansken – Informatieblad Geheimhouderinformatie NFI* 2020, p. 2. Zie over de werkwijze met Hansken ook: Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504, r.o. 3.1.3.

wordt gebruikt door de Politie, FIOD, NVWA, Koninklijke Marechaussee en Inspectie Leefomgeving en Techniek en heeft inmiddels in meer dan 700 zaakonderzoeken een rol gespeeld bij het inzichtelijk maken en analyseren van gegevens.[104]

3.5 Wet- en regelgeving

Op het aanbieden van extra beveiligde en/of identiteitsversluierende communicatiediensten zijn de algemene wettelijke regelingen rondom dataverwerking van toepassing, in het bijzonder de Algemene verordening gegevensbescherming (AVG)[105] en de daarop gebaseerde nationale wetgeving.[106] Daarnaast bevat de Telecommunicatiewet – mede op Europese regelgeving[107] gebaseerde – bepalingen voor de aanbieders van dergelijke diensten, waaronder strafbepalingen die zowel bestuurs- als strafrechtelijk gehandhaafd kunnen worden.[108] Daarbij gaat het onder meer om verplichtingen met betrekking tot het bewaren van verkeers- en locatiegegevens en het op vordering van overheidsdiensten verstrekken van deze gegevens.[109] Waar het gaat om het strafrecht is verder van belang dat het aanbieden en verkopen van cryptotelefoons op zichzelf niet strafbaar is. Onder omstandigheden kan wel strafrechtelijke vervolging plaatsvinden wegens daarmee samenhangende strafbare feiten zoals deelname aan een criminele organisatie, witwassen en begunstiging.[110] Omdat de focus in dit onderzoek ligt op het gebruik van dergelijke communicatiediensten door advocaten zal hier verder niet worden ingegaan op de normering van de ontwikkeling en aanbieding van dergelijke communicatiediensten en de handel in cryptotelefoons.

Voor wat betreft de wet- en regelgeving ter zake het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen volstaat een korte opmerking, nu dit wettelijk niet specifiek is genormeerd. Hoewel in ieder geval het gebruik van cryptotelefoons vaak met strafbare feiten in verband wordt gebracht, is het enkele gebruik van een dergelijke telefoon niet strafbaar.[111] Wel klinken er stemmen om bepaalde communicatiemiddelen aan banden te leggen. Zo is door een Amsterdams

---

104 'Hansken Community Partners', hansken.nl; *Vision Statement Hansken* 2021, p. 1.

105 Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (*PbEU* 2016, L 119).

106 Zoals de Uitvoeringswet Avg (*Stb.* 2018, 144).

107 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*PbEU* 2002, L 201) (richtlijn betreffende privacy en elektronische communicatie).

108 Vgl. art. 1 WED en voor de verhouding tussen bestuurs- en strafrechtelijke handhaving de OM Aanwijzing handhaving Telecommunicatiewet (*Stcrt.* 2016, 19418).

109 Vgl. in het bijzonder hoofdstuk 13 Telecommunicatiewet, gebaseerd op de destijds geldende Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (*PbEU* 2006, L 105) (Richtlijn dataretentie). In dat verband brengt ook de – deels nog in werking te treden – Digital Services Act (Verordening 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (*PbEU* 2022, L 277)) nadere verplichtingen mee voor dergelijke aanbieders.

110 Zie daarvoor ook par. 3.3.1.

111 Het rechtvaardigt op zichzelf evenmin een redelijke verdenking van deelname aan een criminele organisatie, aldus Rb. Amsterdam 26 november 2021, ECLI:NL:RBAMS:2021:6866. Zie uitgebreider Van Toor 2022.

gemeenteraadslid opgeroepen tot een verbod op de chatapplicatie Telegram omdat de dienst criminele communicatie zou faciliteren.[112] Bij de huidige stand van zaken gelden echter ook voor advocaten dus geen strafrechtelijke beperkingen voor het gebruik van dergelijke communicatiemiddelen. Wel kunnen voor advocaten gedragsrechtelijke verplichtingen, in het bijzonder de geheimhoudingsplicht, hiervoor van betekenis zijn. Dit komt in het volgende hoofdstuk nader aan de orde.

[112] Rensen 2023.

4. Het recht op vertrouwelijke communicatie tussen advocaat en cliënt

4.1 Inleiding

Het recht op vertrouwelijke communicatie tussen advocaten en cliënten vloeit voort uit het maatschappelijk belang dat burgers een advocaat kunnen raadplegen zonder bang te hoeven zijn dat de informatie die zij hierbij delen bij derden terechtkomt. Het wordt beschouwd als een onderdeel van het recht op een eerlijk proces als bedoeld in artikel 6 EVRM[113] en vormt tevens een uitwerking van het recht op bescherming van de persoonlijke levenssfeer zoals onder meer neergelegd in artikel 10 Grondwet en artikel 8 EVRM.[114]

Het recht op vertrouwelijke communicatie is niet als zodanig in de wet neergelegd, maar is door de Hoge Raad sinds 1985 aanvaard als algemeen rechtsbeginsel.[115] Het beginsel komt voorts tot uitdrukking in verschillende wettelijke bepalingen, waaronder het recht op vrij verkeer tussen raadsman en gedetineerde cliënt (art. 45 Sv) en het verschoningsrecht van artikel 218 Sv, op grond waarvan advocaten niet gehouden zijn als getuige vragen te beantwoorden over hetgeen hun in het kader van hun beroepsuitoefening is toevertrouwd. Het strekt zich uit tot alle informatie die wordt uitgewisseld in het kader van de beroepsuitoefening.[116] Bovendien komt een zogenaamd afgeleid verschoningsrecht toe aan het personeel van een advocatenkantoor, zoals secretariële medewerkers, boekhouders en schoonmakers.[117]

Hierna zal nader worden ingegaan op de inhoud van het recht op vertrouwelijke communicatie tussen advocaat en cliënt en de wijze waarop dat in de wet en de jurisprudentie is geregeld (par. 4.2). Vervolgens wordt uiteengezet hoe het recht op vertrouwelijke communicatie in de praktijk wordt gewaarborgd (par. 4.3). Tot slot zal aandacht worden besteed aan de vraag welke kwetsbaarheden in het juridisch kader en/of in de praktische uitwerking daarvan kunnen worden geïdentificeerd (par. 4.4). Dit hoofdstuk strekt aldus tot beantwoording van deelvraag 1 (*Wat is het juridisch kader rondom de vertrouwelijke communicatie tussen advocaten en hun cliënten en hoe is dit uitgewerkt in de praktijk?*).

4.2 Vertrouwelijke communicatie in de wet- en regelgeving en jurisprudentie

4.2.1 Reikwijdte van het recht op vertrouwelijke communicatie

Het recht op vertrouwelijke communicatie is beperkt tot hetgeen de advocaat in het kader van zijn beroepsuitoefening wordt toevertrouwd. Het gaat daarbij om informatie die is verkregen in de context

---

113 Het recht wordt als zodanig niet in art. 6 EVRM genoemd, maar in de jurisprudentie wel als onderdeel daarvan aanvaard, zie o.m. EHRM 13 maart 2007, ECLI:CE:ECHR:2007:0313JUD002339305 (Castravet/Moldova), par. 49-51.

114 Vgl. EHRM 16 december 1992, ECLI:CE:ECHR:1992:1216JUD00137108888 (Niemietz/Austria), par. 27-33.

115 HR 1 maart 1985, ECLI:NL:HR:1985:AC9066, *NJ* 1986/173 m.nt. Haardt (*notaris Maas*).

116 Vgl. de formulering in art. 218 Sv: 'hetgeen waarvan de wetenschap aan hen *als zodanig* is toevertrouwd' (cursivering toegevoegd).

117 Vgl. Mannheims & Felix 2021. Zie ook HR 23 november 1990, ECLI:NL:HR:1990:ZC0052, *NJ* 1991/761 m.nt. Vranken; HR 7 april 2012, ECLI:NL:HR:2012:BV3426, *NJ* 2012/408 m.nt. Zwemmer.

van de werkzaamheden die behoren bij de normale uitoefening van de functie van advocaat.[118] Dit gaat echter niet zo ver dat het verschoningsrecht zich automatisch uitstrekt tot alle informatie die door de cliënt bij de advocaat in bewaring is gegeven.[119] Voor informatie die de advocaat uit anderen hoofde krijgt, bijvoorbeeld omdat z/hij getuige is van een misdrijf of een bestuursfunctie bij een vereniging vervult, geldt dat dit evenmin onder zijn geheimhoudingsplicht valt.[120] Ook wanneer een advocaat bij communicatie wordt betrokken, zowel in persoon als via e-mail, met geen ander doel dan die communicatie als vertrouwelijk te kunnen aanmerken, kan niet worden gesproken van informatie die haar/hem in het kader van zijn beroepsuitoefening is toevertrouwd en die onder het verschoningsrecht valt.[121] Het is aan de advocaat zelf om te bepalen ten aanzien van welke informatie z/hij een geheimhoudingsplicht heeft. Wanneer hierover discussie ontstaat, is het uiteindelijk aan de (tucht)rechter of de deken om te bepalen of de advocaat zich terecht op zijn verschoningsrecht beroept.[122]

4.2.2 De geheimhoudingsplicht

Bij het recht op vertrouwelijke communicatie wordt doorgaans een onderscheid gemaakt tussen de geheimhoudingsplicht die voortvloeit uit het beroep van advocaat, en het verschoningsrecht dat de advocaat kan inroepen wanneer van haar/hem informatie wordt gevorderd die onder de geheimhoudingsplicht valt.[123]

De geheimhoudingsplicht van advocaten strekt ter bescherming van de belangen van de cliënt om op vertrouwelijke wijze juridische bijstand te kunnen inroepen en is zowel in het tuchtrecht als in het strafrecht geregeld. Tuchtrechtelijk werd de plicht tot geheimhouding tot 2015 beschouwd als onderdeel van de algemene betamelijkheidsnorm van artikel 46 Advocatenwet (oud). De verplichting was daarnaast neergelegd in Gedragsregel 6 (oud).[124] Met de wijziging van de Advocatenwet per 1 januari 2015 is de verplichting tot geheimhouding opgenomen in artikel 10a als een van de kernwaarden voor advocaten, en is daarnaast expliciet gecodificeerd in artikel 11a Advocatenwet.[125] De verplichting tot geheimhouding is thans tevens neergelegd in Gedragsregel 3. Die Gedragsregel codificeert in de eerste plaats de plicht tot geheimhouding over – onder meer – bijzonderheden van door haar/hem behandelde zaken, de persoon van zijn cliënt en de aard en omvang van diens belangen (lid 1). Daarnaast schrijft de bepaling 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

118 Vgl. Fanoy 2022, p. 13-22.
119 Vgl. HR 9 februari 2021, ECLI:NL:HR:2021:193, waarin het ging om een aan de advocaat gegeven mobiele telefoon.
120 Mannheims & Felix 2021.
121 Toelichting bij gedragsregel 3 van de Gedragsregels Advocatuur 2018.
122 Toelichting bij gedragsregel 3 van de Gedragsregels Advocatuur 2018; zie voor een voorbeeld Hof van Discipline 22 juni 2018, ECLI:NL:TAHVD:2018:124; HR 18 februari 2020, ECLI:NL:HR:2020:277 en HR 9 april 2021, ECLI:NL:HR:2021:532, *NJ* 2022/48 m.nt. Klaassen.
123 Zie uitgebreider Fanoy 2018.
124 Mannheims & Felix 2021.
125 Art. 10a lid 1 aanhef en onder e Advw.: 'In het belang van een goede rechtsbedeling draagt de advocaat zorg voor de rechtsbescherming van zijn cliënt. Daartoe is de advocaat bij de uitoefening van zijn beroep: (..) e. vertrouwenspersoon en neemt hij geheimhouding in acht binnen de door de wet en het recht gestelde grenzen'.

de communicatiemiddelen (lid 2). In dat verband adviseert de NOvA advocaten om de telefoon alleen te gebruiken voor het uitwisselen van algemene informatie en om afspraken te maken. Hetzelfde advies geldt voor het gebruik van onbeveiligde e-mail en chatapps, waarbij in het geval van chatapps nog in het bijzonder wordt gewaarschuwd voor het risico dat derden via de chatapps toegang hebben tot op de telefoon opgeslagen gegevens.[126]

Ondanks de geheimhoudingsplicht staat het de advocaat soms vrij om vertrouwelijke informatie naar buiten te brengen (Gedragsregel 3, lid 3). Daarbij dient de advocaat altijd een zorgvuldige belangenafweging te maken en heeft z/hij een eigen verantwoordelijkheid om te bepalen of bekendmaking in het belang is van de cliënt. In ieder geval dient te zijn voldaan aan drie cumulatieve voorwaarden: bekendmaking is gerechtvaardigd met het oog op een juiste taakvervulling, er is instemming van de cliënt en het is in overeenstemming met de goede beroepsuitoefening.[127] Wanneer belanghebbenden, zoals de (oud-)cliënt, menen dat de advocaat heeft gehandeld in strijd met haar/zijn geheimhoudingsplicht, kan daarover tuchtrechtelijk worden geklaagd.

Schending van de geheimhoudingsplicht is daarnaast ook strafrechtelijk gesanctioneerd. Artikel 272 Sr stelt strafbaar het opzettelijk schenden van de uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep voortvloeiende plicht tot het bewaren van enig geheim, waarvan hij weet of redelijkerwijs moet vermoeden dat hij het dient te bewaren.

4.2.3 Het verschoningsrecht

Nauw verbonden met de geheimhoudingsplicht is het verschoningsrecht van de advocaat, neergelegd in artikel 218 Sv. Waar de geheimhoudingsplicht van advocaten in de eerste plaats strekt tot bescherming van de rechten van de cliënt, wordt het verschoningsrecht gezien als een recht van de advocaat. De advocaat heeft dan ook een eigen verantwoordelijkheid in de uitoefening van dat recht, hetgeen meebrengt dat de opvatting van de cliënt over de uitoefening van het verschoningsrecht niet leidend is. Gelet op de geheimhoudingsplicht zal het feit dat de cliënt niet instemt met het vrijgeven van informatie in beginsel meebrengen dat de advocaat zijn verschoningsrecht ook daadwerkelijk zal moeten inroepen.[128]

Het verschoningsrecht betekent in de eerste plaats dat een advocaat kan weigeren om informatie die haar/hem in het kader van zijn beroepsuitoefening is toevertrouwd prijs te geven, bijvoorbeeld wanneer z/hij als getuige wordt opgeroepen om te verklaren. Daarnaast biedt het verschoningsrecht de advocaat de mogelijkheid om medewerking aan bepaalde opsporingshandelingen te weigeren, zoals het inzage geven in gevorderde stukken.[129] Ook normeert het verschoningsrecht het opsporingsonderzoek in andere opzichten, in die zin dat politie en justitie in hun optreden het verschoningsrecht dienen te respecteren. Daartoe zijn in wet- en regelgeving verschillende waarborgen opgenomen. Voor de inlichtingen- en

126 'Tips voor vertrouwelijke internetcommunicatie', *Adv. bl.* 2022/7, p. 68-69.
127 Zie ook de toelichting bij Gedragsregel 3.
128 Mannheims & Felix 2021, par. 3.6.
129 Een dergelijk bevel tot uitlevering kan worden gegeven op grond van art. 96a Sv.

veiligheidsdiensten geldt hetzelfde uitgangspunt, zij het dat de wet meer ruimte biedt voor uitzonderingen.[130] Hierna volgt een beknopt overzicht van de wijze waarop de naleving van het verschoningsrecht op hoofdlijnen is vormgegeven. Gelet op de focus van dit onderzoek zal de regeling rondom de inlichtingen- en veiligheidsdiensten hierbij grotendeels buiten beschouwing worden gelaten.

In de eerste plaats is in het Wetboek van Strafvordering op verschillende plekken geregeld hoe moet worden omgegaan met de inzet van opsporingsbevoegdheden in het geval sprake is van een (mogelijk) verschoningsrecht.[131] Zo schrijft artikel 98 Sv voor dat bij doorzoeking en inbeslagneming onder geheimhouders steeds de rechter-commissaris moet worden ingeschakeld en dat geen brieven of geschriften waarover de geheimhoudingsplicht zich uitstrekt in beslag worden genomen (lid 1). Voor de vraag of bepaalde stukken onder het verschoningsrecht vallen geldt als uitgangspunt dat het standpunt van de verschoningsgerechtigde dat dit het geval is, in beginsel door politie en justitie wordt geëerbiedigd, 'tenzij redelijkerwijze geen twijfel erover kan bestaan dat dit standpunt onjuist is'.[132] Die beoordeling is aan de rechter-commissaris, die daarbij zoveel mogelijk het advies van een vertegenwoordiger van de beroepsgroep inwint.[133] Voor zover noodzakelijk mag de rechter-commissaris voor dit oordeel kennisnemen van de betreffende stukken.[134] Wanneer sprake is van een grote hoeveelheid (digitale) stukken of gegevens die volgens de beslagene onder het verschoningsrecht vallen maar waarin niet eenvoudig is vast te stellen of dat het geval is – bijvoorbeeld omdat sprake is van verschillende geheimhouders van wie de identiteit of een contactgegevens onbekend zijn –, heeft de Hoge Raad geoordeeld dat 'het in de rede ligt dat onder leiding van de rechter-commissaris een schifting wordt gemaakt tussen stukken of gegevens die wel en die niet onder het verschoningsrecht kunnen vallen, bijvoorbeeld door gebruik te maken van een lijst met zoektermen die betrekking hebben op het deel van het materiaal waarover het verschoningsrecht zich mogelijk uitstrekt, zoals namen en e-mailadressen of termen die specifiek kunnen duiden op het voorwerp van het ingeroepen verschoningsrecht'.[135] De rechter-commissaris moet ervoor zorgen dat voldoende wordt gewaarborgd dat het verschoningsrecht niet door het strafrechtelijk onderzoek kan worden geschonden. Dat sluit niet uit dat zogenaamde 'geheimhouder-politieambtenaren' een selectie maken, zij het dat de verschoningsgerechtigde zoveel mogelijk moet worden betrokken bij de daarbij te gebruiken zoektermen.[136] In beginsel wordt de verschoningsgerechtigde in de gelegenheid gesteld zich uit te laten over de toelaatbaarheid van het gebruik van de door de rechter-commissaris geselecteerde stukken, met dien verstande dat hiervan kan

130 Vgl. art. 27 lid 2, art. 30 lid 3 en art. 66 Wiv 2017.

131 Zie voor een uitgebreid overzicht van het juridisch kader de conclusie van AG Silvis, 12 januari 2021, ECLI:NL:PHR:2021:18. Een en ander is ook uitgewerkt in de Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten (*Stcrt.* 2011, 4981).

132 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.

133 De NOvA heeft een handleiding opgesteld voor zowel advocaten als dekens: Handleiding voor advocaten bij strafrechtelijke doorzoeking, februari 2018, en Handleiding voor dekens bij strafrechtelijke doorzoeking, februari 2018, beide raadpleegbaar via advocatenorde.nl.

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

135 HR 16 juni 2020, ECLI:NL:HR:2020:1048, r.o. 4.3.1, *NJ* 2021/117, m.nt. Kooijmans.

136 HR 16 juni 2020, ECLI:NL:HR:2020:1048, r.o. 4.3.1, *NJ* 2021/117, m.nt. Kooijmans.

worden afgeweken indien het onduidelijk en niet eenvoudig te achterhalen is in relatie tot welke mogelijke verschoningsgerechtigden de in beslag genomen stukken of gegevens staan.[137]

Tegen een beslissing van de rechter-commissaris dat de stukken in beslag mogen worden genomen, kan de verschoningsgerechtigde beklag instellen (lid 4). Totdat daarop is beslist mag geen kennis worden genomen van de inbeslaggenomen stukken (lid 3). Wel kan de raadkamer van de rechtbank, evenals de rechter-commissaris voor zover dat noodzakelijk is kennis nemen van de betreffende stukken.[138]

Uit de jurisprudentie volgt dat het verschoningsrecht zich ook kan uitstrekken tot stukken die niet onder de geheimhouder, maar bijvoorbeeld bij de cliënt worden aangetroffen: ook dan gelden de waarborgen van artikel 98 Sv.[139] Uit artikel 98 lid 5 Sv vloeit overigens voort dat het verschoningsrecht zich niet uitstrekt tot brieven en geschriften die voorwerp van het strafbare feit zijn of tot het begaan daarvan hebben gediend. Voorts heeft de Hoge Raad aanvaard dat het verbod op inbeslagname ook in andere gevallen in zeer uitzonderlijke omstandigheden terzijde kan worden geschoven.[140]

Waar het gaat om bevelen tot uitlevering van voorwerpen en gegevensdragers is eveneens voorzien in een waarborg op grond waarvan verschoningsgerechtigden hun medewerking hieraan kunnen weigeren (vgl. art. 96a lid 3 sub b en art. 105 lid 3 Sv). Hetzelfde geldt voor verschillende bijzondere opsporingsbevoegdheden, zoals de verplichting tot het verstrekken van gegevens aan de officier van justitie (art. 126nd lid 2 Sv). Ook aan een bevel tot decryptie hoeven verschoningsgerechtigden geen gevolg te geven (art. 125k lid 3 Sv). Artikel 125l Sv bepaalt bovendien dat geen onderzoek plaatsvindt naar gegevens die vallen onder de geheimhoudingsplicht in de 'geautomatiseerde werken' van verschoningsgerechtigden (art. 125l Sv).

Voor de praktijk is verder artikel 126aa lid 2 Sv van groot belang. Dit artikel bepaalt dat informatie die door aanwending van bijzondere opsporingsbevoegdheden is verkregen en die valt onder het verschoningsrecht, dient te worden vernietigd. Andere informatie die wel door of aan de verschoningsgerechtigde is verstrekt maar die niet valt onder het beroepsgeheim, wordt slechts na een machtiging van de RC bij de processtukken gevoegd (art. 126aa lid 2 Sv). Een nadere uitwerking van deze bepaling is te vinden in het Besluit bewaren en vernietigen niet-gevoegde stukken.[141] Artikel 4 van dit Besluit bepaalt onder meer dat de opsporingsambtenaar die kennisneemt van mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder, de officier van justitie hiervan onverwijld in kennis stelt (lid 1). Wanneer de officier van justitie vaststelt dat het inderdaad gaat om geheimhouderinformatie, beveelt hij onmiddellijk de vernietiging hiervan (lid 2). Dit is slechts anders wanneer het gaat om een geheimhouder die zelf als verdachte is aangemerkt. In dat geval wint de officier van justitie het oordeel in van 'een gezaghebbend lid van de beroepsgroep waartoe de geheimhouder behoort'. In het geval van advocaten zal dat doorgaans de deken zijn. De officier van

137 HR 16 juni 2020, ECLI:NL:HR:2020:1048, r.o. 4.3.2, *NJ* 2021/117, m.nt. Kooijmans.
138 HR 28 juni 2016, ECLI:NL:HR:2016:1324, r.o. 2.3.2, *NJ* 2016/378, m.nt. Vellinga-Schootstra.
139 HR 22 september 2015, ECLI:NL:HR:2015:2783, *NJ* 2016/55, m.nt. Vellinga-Schootstra.
140 Vgl. HR 9 mei 2006, ECLI:NL:HR:2006:AV2386, *NJ* 2006/622, m.nt. De Boer. Zie over dit 'uitzonderlijke omstandigheden-regime' in een zaak waarin sprake was van een verdachte advocaat HR 18 februari 2022, ECLI:NL:HR:2022:223.
141 Besluit van 15 december 1999 (*Stb.* 1999, 548), laatstelijk gewijzigd Besluit van 27 oktober 2016 (*Stb.* 2016, 411).

justitie kan gemotiveerd afwijken van het oordeel van de deken (lid 3). Over de naleving van artikel 126aa lid 2 Sv is door de jaren heen veel discussie gevoerd. Dit heeft geleid tot verschillende aanpassingen in de (lagere) regelgeving en de praktijk, waarop hierna in paragraaf 4.3 wordt ingegaan.

4.2.4 Het verschoningsrecht in het nieuwe Wetboek van Strafvordering

Voor wat betreft het wettelijk kader kan hier tot slot nog worden gewezen op de voorstellen die thans in het kader van de modernisering van het Wetboek van Strafvordering aanhangig zijn.[142] Hier wordt volstaan met een korte bespreking van enkele, voor dit onderzoek relevante voorgestelde wijzigingen. In het nieuwe wetboek wordt het verschoningsrecht met een codificatie van de hiervoor besproken rechtspraak van de Hoge Raad steviger in de wet verankerd.[143] Voorts wordt voorzien in een procedure voor de situatie dat mogelijk verschoningsgerechtigde voorwerpen of gegevens worden aangetroffen bij een ander dan de verschoningsgerechtigde.[144] Belangrijk is verder het in de voorgestelde regeling neergelegde uitgangspunt dat filtering van mogelijk verschoningsgerechtigde informatie steeds plaatsvindt door de rechter-commissaris.[145] Anders dan gebeurt in de huidige praktijk – zie daarover par. 4.3 – is filtering door daartoe aangewezen geheimhoudermedewerkers van opsporingsdiensten of het OM dus niet toegestaan.[146] Hoewel de voorgestelde regeling door veel van de in het wetgevingsproces geconsulteerde organisaties overwegend positief is ontvangen,[147] is ook kritiek geleverd. Daarbij gaat het bijvoorbeeld vanuit de NOvA om de wijze waarop is gewaarborgd dat de verschoningsgerechtigde gelegenheid krijgt een standpunt in te nemen ten aanzien van de vertrouwelijkheid van het in beslag genomen materiaal, en de inrichting van de beklagprocedure na een beslissing van de RC tot kennisneming van de mogelijk verschoningsgerechtigde informatie.[148] Door het OM zijn onder meer bezwaren opgeworpen tegen het feit dat de praktijk waarin geheimhoudingsopsporingsambtenaren betrokken zijn bij de (eerste) filtering van mogelijk verschoningsgerechtigd materiaal niet meer mogelijk is met de nieuwe regeling.[149] Een met dat laatste bezwaar samenhangend punt van zorg is de capaciteit en (technische) kennis bij de kabinetten RC.[150] In het advies van de universiteiten over de aanhangige wetsvoorstellen is bovendien gewezen op technische beperkingen en is de vraag opgeworpen of en wanneer het mogelijk is 'om filtersoftware te ontwikkelen die met voldoende precisie grote gegevensbestanden op verschoningsgerechtigde informatie kan filteren'.[151]

142 Zie in het bijzonder Titel 6.2. van Boek 1 en Titel 7.5 van Boek 2, *Kamerstukken II* 2022/23, 36327, nr. 2.
143 Onder meer in de voorgestelde art. 2.7.61 en 2.7.62.
144 Voorgesteld art. 2.7.65 en 2.7.66.
145 Zie onder meer de voorgestelde art. 2.7.62 en 2.7.66.
146 Zie ook de MvT, *Kamerstukken II* 2022/23, 36 327, nr. 3, p. 646.
147 NOvA 2017, p. 46-51.
148 NOvA 2017, p. 50-51. Zie uitgebreider Fanoy 2017.
149 OM 2017, p. 34-35.
150 Zie voor een uitgebreidere uiteenzetting en een overzicht van de verschillende consultatie-adviezen ook Project bijstand TK Modernisering Sv 2023, p. 78-85.
151 Project bijstand TK Modernisering Sv 2023, p. 83-85.

4.3 Vertrouwelijke communicatie in de praktijk

Hoewel het recht op vertrouwelijke communicatie dus stevig is verankerd in de Nederlandse wet- en regelgeving en is omgeven met verschillende waarborgen, blijkt de praktijk soms weerbarstig. Al in 2001 werd in een kort geding, aangespannen door onder meer de NOvA en de Nederlandse Vereniging van Strafrechtadvocaten, geconstateerd dat er fouten werden gemaakt bij de uitvoering van de wettelijke bepalingen, in het bijzonder waar het ging om het gebruik van getapte telefonische communicatie.[152] Naar aanleiding daarvan publiceerde het OM de 'Instructie vernietiging geïntercepteerde gesprekken met geheimhouders', die moest zorgen voor een meer uniforme en volledige uitvoering van de regelgeving.[153] Om de geheimhouding beter te waarborgen werd in 2011 ook een systeem van automatische nummerherkenning ingevoerd, waarmee geregistreerde telefoonnummers van advocaten automatisch worden gefilterd en de opname na afloop van het gesprek – en zonder dat het voor politie en justitie toegankelijk is – wordt vernietigd.[154] Ook sms-verkeer wordt op deze wijze gefilterd.[155] Advocaten zijn op grond van artikel 6.10 van de Verordening op de advocatuur (Voda) verplicht hiervoor hun geheimhoudernummer(s) aan te leveren aan de Orde van Advocaten. Op grond van artikel 6.11 lid 1 Voda dienen zij dit geheimhoudernummer te gebruiken voor de vertrouwelijke communicatie, 'tenzij zwaarwegende omstandigheden zich daartegen verzetten'. Daarbij moet echter worden opgemerkt dat de NOvA (inmiddels) adviseert om telefonische communicatie te beperken tot het maken van afspraken en het uitwisselen van algemene informatie.[156] In 2013 is dit nummerherkenningssysteem ook ingevoerd voor de DJI, waarbij het systeem bij herkenning van het nummer een opname automatisch blokkeert.[157] Mede naar aanleiding van berichten over schendingen van de regels rondom het afluisteren van vertrouwelijke communicatie door de inlichtingen- en veiligheidsdiensten[158] is er de afgelopen jaren gewerkt aan een vergelijkbaar systeem voor de inlichtingen- en veiligheidsdiensten.[159] Dat heeft op 20 september 2023 geleid tot het tekenen van het 'Convenant Nummerherkenning Geheimhouders' waarin afspraken staan over het nieuwe systeem van nummerherkenning bij de AIVD en de MIVD.[160] De NOvA houdt op haar website een overzicht bij van incidenten waarbij mogelijk sprake is van schendingen van de vertrouwelijkheid.[161]

De discussie over de naleving van het recht op vertrouwelijke advocaat-cliëntcommunicatie is in 2019 weer in alle hevigheid opgelaaid, na door advocatenkantoor Stibbe aangespannen civiele rechtszaken tegen de Staat in verband met vermeende schendingen van het verschoningsrecht in de zogenoemde

152 Rb. Den Haag 19 december 2001, ECLI:NL:RBSGR:2001:AD7315, *NbSr* 2002/26.
153 Instructie van College van PG's, 2002I003, i.w.tr. 1 april 2002.
154 'Nummerherkenning politie', advocatenorde.nl. Dit leidde tot de invoering van een nieuw art. 4a in het Besluit van 8 augustus 2011 bewaren en vernietigen niet-gevoegde stukken (*Stb.* 2011, 380).
155 'Veelgestelde vragen geheimhoudernummer', advocatenorde.nl.
156 'Tips voor vertrouwelijke internetcommunicatie', *Adv. bl. 2022/7*, p. 68-69. Zie ook par. 4.2.2.
157 'Nummerherkenning DJI', advocatenorde.nl.
158 *Toezichtsrapport CTIVD* 2017. Zie ook Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.
159 'In ontwikkeling: nummerherkenning AIVD en MIVD', advocatenorde.nl. Zie voor de thans geldende wettelijke waarborgen art. 27, 30 en 66 Wiv 2017.
160 'NOvA en AIVD/MIVD tekenen convenant over nummerherkenning', *advocatenorde.nl* 25 september 2023.
161 'Nummerherkenning politie' en 'Nummerherkenning DJI', advocatenorde.nl. Zie ook *Rapport van de Commissie Telefonie Voor Justitiabelen* 2009.

Castor-zaak.[162] Uit die rechtszaken bleek dat de werkwijze bij de FIOD en het OM inhoudt dat in grote fraudeonderzoeken door een zogenoemde 'geheimhoudingsambtenaar' van de FIOD kennis wordt genomen van de inhoud van alle – ook mogelijk verschoningsgerechtigde – e-mailcorrespondentie die op grond van bijzondere opsporingsbevoegdheden is verkregen. De constatering dat een e-mail afkomstig is van of is gericht aan een advocatenkantoor leidt op zichzelf niet tot vernietiging. Wanneer de geheimhoudingsambtenaar tot de conclusie komt dat de correspondentie verschoningsgerechtigd is, legt z/hij deze voor aan de 'geheimhouder officier van justitie', die uiteindelijk beslist over de vraag of de informatie inderdaad moet worden vernietigd. Die 'vernietiging' houdt vervolgens slechts in dat de gegevens voor het opsporingsteam ontoegankelijk worden gemaakt ('uitgegrijsd').[163] Deze werkwijze is gebaseerd op de opvatting dat bij toepassing van artikel 126aa Sv de selectie en beoordeling van eventuele verschoningsgerechtigde informatie niet door of onder leiding van de rechter-commissaris, maar door of onder leiding van de officier van justitie kan plaatsvinden. Met andere woorden: wanneer het gaat om informatie die is verkregen door middel van de inzet van bijzondere opsporingsmiddelen zou een ander regime gelden dan wanneer het gaat om bij een doorzoeking inbeslaggenomen materiaal.[164]

Na verschillende – deels ook thans nog lopende – rechtszaken[165] oordeelde de voorzieningenrechter in februari 2022 dat de beschreven werkwijze grotendeels onrechtmatig is en hij verplichtte het OM tot openbaarmaking van de bij deze werkwijze gehanteerde Handleiding verwerking geheimhoudersinformatie.[166] Ten aanzien van de vervolgens gepubliceerde Handleiding heeft de NOvA het standpunt ingenomen dat de in de – met name over artikel 98 Sv gewezen – jurisprudentie ontwikkelde normen ten onrechte niet worden toegepast in gevallen waarin buiten het kader van een doorzoeking vermoedelijke geheimhouderinformatie wordt aangetroffen. Daarmee is de Handleiding wat de NOvA betreft op veel onderdelen in strijd met het verschoningsrecht.[167] De nadien opgestelde concept Aanwijzing omgang met verschoningsgerechtigd materiaal acht de NOvA betreft weliswaar een verbetering, maar biedt nog altijd onvoldoende bescherming aan het verschoningsrecht.[168] Op 2 mei 2023 oordeelde ook het hof 's-Hertogenbosch in het door het OM tegen de uitspraak van de voorzieningenrechter ingestelde hoger beroep, dat de toegepaste werkwijze ten aanzien van op de voet van artikel 126aa Sv verkregen informatie, in strijd is met regelgeving en jurisprudentie rond het verschoningsrecht en het verschoningsrecht bovendien onvoldoende waarborgt.[169] Om duidelijkheid te krijgen over de juiste uitleg van artikel 126aa Sv heeft het hof prejudiciële vragen gesteld aan de Hoge

162 Naar deze zaak wordt ook vaak verwezen als 'Box-' of 'Box Consultants-affaire', naar het van strafbare feiten verdachte bedrijf dat in deze kwestie centraal stond.

163 Zie uitgebreider Doorenbos & Rosing 2020.

164 Vgl. Rb. Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035, r.o. 4.19-4.20; zie ook Doorenbos 2022 en De Bree & Buruma 2022.

165 Zie o.a. Rb. Oost-Brabant 29 maart 2019, ECLI:NL:RBOBR:2019:1783; Hof 's-Hertogenbosch 14 mei 2019, ECLI:NL:GHSHE:2019:1808; Rb. Oost-Brabant 5 juni 2019 ECLI:NL:RBOBR:2019:3107; HR 19 februari 2021, ECLI:NL:HR:2021:273 en Hof 's-Hertogenbosch 10 februari 2022, ECLI:NL:GHSHE:2022:365.

166 Rb Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035.

167 'Reactie NOvA op Handleiding OM', 9 februari 2023, advocatenorde.nl.

168 *Advies Aanwijzing omgang verschoningsgerechtigd materiaal* 2023. In de tussentijd wordt gehandeld krachtens het 'Voorlopig Beleid Uitspraak Kort Geding Verschoningsrecht', *om.nl.*

169 Hof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329, r.o. 3.6.

Raad.[170] Daarnaast is in afwachting van de beantwoording van deze vragen een tijdelijke maatregel getroffen, op grond waarvan het OM wordt verplicht om de selectie en beoordeling van (mogelijke) geheimhouderinformatie over te laten aan de rechter-commissaris.[171] De NOvA zal ten behoeve van de beantwoording van deze vragen schriftelijke opmerkingen indienen en zal daarbij het belang van het verschoningsrecht als algemeen geldend en fundamenteel rechtsbeginsel nader belichten.[172] Dat de omgang met verschoningsgerechtigde informatie in de tussentijd nog altijd onderwerp is van discussie blijkt bijvoorbeeld uit berichtgeving rondom de aanhouding van advocaat Inez Weski.[173] Wel heeft het OM inmiddels erkend dat de procedures rond het verschoningsrecht niet altijd voldoende waarborgen hebben geboden.[174] De in dat kader gemaakte fouten zijn in ieder geval de aanleiding geweest om in de Castor-zaak tot seponering over te gaan.[175]

4.4 Kwetsbaarheden

Uit het voorgaande volgt al dat de waarborging van de vertrouwelijkheid van advocaat-cliëntcommunicatie geen rustig bezit is. De spanning die bestaat tussen het opsporingsbelang en de waarheidsvinding enerzijds, en het fundamentele recht op vertrouwelijkheid anderzijds, maakt dat zich allerlei moeilijkheden kunnen voordoen en een adequate waarborging van de vertrouwelijkheid kwetsbaarheden kent. De kwetsbaarheden lijken niet in de eerste plaats gelegen in het juridisch kader: in de wet en de jurisprudentie komt het fundamentele belang van vertrouwelijkheid duidelijk tot uitdrukking, terwijl daaruit eveneens een heldere werkwijze kan worden afgeleid om inbreuken op de vertrouwelijkheid zoveel te mogelijk te voorkomen of beperken. De hiervoor geschetste problematiek maakt daarentegen duidelijk dat vooral uit de wijze waarop het in de wet en jurisprudentie neergelegde kader in de (opsporings)praktijk wordt uitgevoerd, risico's voortvloeien voor de waarborging van de vertrouwelijkheid. Daarbij kan een onderscheid worden gemaakt tussen verschillende soorten vertrouwelijke informatie.

4.4.1 Telefonische communicatie

Ten aanzien van telefonische communicatie voorziet het systeem van automatische herkenning van geheimhoudernummers in een op zichzelf effectieve waarborg tegen inbreuken op de vertrouwelijkheid van telefoongesprekken door de strafvorderlijke overheid.[176] Kwetsbaarheden zijn gelegen in de praktische uitvoering waar het bijvoorbeeld gaat om het bijhouden van een volledige en geactualiseerde

170 Zie voor de aankondiging daarvan Hof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329, r.o. 3.7.3 en 3.7.4; de uiteindelijk gestelde vragen zijn te vinden in Hof 's-Hertogenbosch 5 september 2023, ECLI:NL:GHSHE:2023:2816. Op het moment van opleveren van dit rapport (16 oktober 2023) heeft de Hoge Raad nog geen uitspraak gedaan.

171 Hof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329, r.o. 3.8.

172 'NOvA meldt zich bij Hoge Raad over prejudiciële vragen verschoningsrecht', *advocatenorde.nl* 18 september 2023.

173 Zie hierover Mos & Polman 2023a en de reactie daarop van het OM: 'Openbaar Ministerie en het verschoningsrecht', *om.nl* 20 juli 2023.

174 'OM in gesprek met strafrechtketen over verschoningsrecht', *om.nl* 25 september 2023.

175 'OM seponeert strafrechtelijk onderzoek naar Brabantse vermogensbeheerder', *om.nl* 6 oktober 2023.

176 Zoals al genoemd in par. 4.2.3 werkt het systeem niet bij afluisteren door de inlichtingen- en veiligheidsdiensten.

lijst van geheimhoudernummers, terwijl in het verleden is gebleken dat ook technische onvolkomenheden tot schendingen van de vertrouwelijkheid hebben geleid.[177] Een belangrijke beperking van het gehanteerde systeem is verder dat het zich beperkt tot telefoongesprekken en sms-berichten. Wanneer het gaat om – met het geheimhoudertoestel gestuurde – berichten via diensten als WhatsApp, Signal en Telegram, biedt het systeem geen bescherming in de zin van automatische herkenning. Daar staat tegenover dat deze communicatiediensten op andere wijze zijn beveiligd en de daarmee gevoerde communicatie voor opsporingsdiensten in beginsel niet toegankelijk is.[178] Wel kunnen dergelijke data door de inbeslagname van mobiele telefoons in een strafrechtelijk onderzoek terechtkomen. Omdat dergelijke chatapplicaties zijn gekoppeld aan een telefoonnummer kunnen deze vervolgens wel worden gelinkt aan een geheimhoudernummer, uiteraard mits de chatapplicatie op de geheimhoudertelefoon is geïnstalleerd. Dit vergt echter een menselijke handeling, bijvoorbeeld een zoekslag op het betreffende geheimhoudernummer. Wanneer een dergelijke zoekslag niet voorafgaand aan het onderzoek aan de gegevens wordt uitgevoerd, zal pas bij inhoudelijke kennisneming van de informatie kunnen worden vastgesteld dat het om vertrouwelijke communicatie gaat.[179]

Ook voor – via *hacks* of beslag – beschikbaar gekomen communicatie via cryptotelefoons geldt dat geen automatische filtering op geheimhouderinformatie mogelijk is. Bovendien wordt de uitfiltering van vertrouwelijke communicatie mogelijk bemoeilijkt door het feit dat hierbij veelal aliassen of zelfgekozen *nicknames* worden gebruikt en de identiteit van de gebruiker juist zoveel mogelijk wordt afgeschermd.[180] In zulke gevallen kan dus eerst door kennisneming van de inhoud van de communicatie het vermoeden ontstaan dat het mogelijk gaat om vertrouwelijke communicatie. Naar aanleiding van de *hacks* van verschillende aanbieders van versleutelde telefonische communicatie heeft het OM advocaten daarom opgeroepen zich te melden wanneer zij hiervan gebruik hebben gemaakt.[181] Gelet op deze risico's voor de vertrouwelijkheid adviseert de NOvA dan ook 'zoveel mogelijk' gebruik te maken van geheimhoudernummers.[182]

4.4.2 Fysieke documenten en voorwerpen

Waar het gaat om fysieke documenten en voorwerpen[183] geldt dat met name risico's bestaan wanneer dergelijke stukken onder anderen dan de geheimhouder zelf worden aangetroffen en in beslag genomen. Wanneer het gaat om doorzoeking bij een geheimhouder is immers voorzien in een duidelijke procedure waarbij in beginsel steeds de rechter-commissaris en de deken aanwezig zullen zijn en de geheimhouder zelf in de gelegenheid is direct aan te geven welke stukken naar zijn mening onder het verschoningsrecht

177 'Opnieuw signalen van opgenomen telefoongesprekken bij DJI', advocatenorde.nl.

178 Overigens wordt wel gewerkt aan juridische mogelijkheden om toegang tot dergelijke gegevens te kunnen krijgen, zie daarover onder meer *Aanhangsel Handelingen II* 2021/22, nr. 2095.

179 Zie hierover uitgebreider par. 6.5.2.3.

180 Zie hierover uitgebreider par. 6.5.2.2.

181 'Advocaten kunnen zich bij OM melden als geheimhouder in versleutelde chatdiensten', *advocatenorde.nl* 23 april 2021.

182 'Geheimhoudingplicht niet goed te waarborgen met cryptotelefoon', *advocatenorde.nl* 20 mei 2021.

183 In de context van de advocaat-clientrelatie kan daarbij bijvoorbeeld worden gedacht aan usb-sticks en andere gegevensdragers. Zie over de omgang met de daarop opgeslagen digitale informatie ook de navolgende paragraaf.

vallen.[184] Worden de stukken onder derden in beslag genomen dan zal in beginsel eerst na (oppervlakkige) kennisneming van de stukken duidelijk zijn of het om vertrouwelijke informatie gaat. Daarbij geldt wel dat de advocaat ervoor kan zorgen dat in ieder geval de stukken die van haar/hem afkomstig zijn eenvoudig als zodanig te herkennen zijn, bijvoorbeeld door gebruikmaking van (brief)papier waarop de naam van de advocaat of het advocatenkantoor duidelijk zichtbaar is. In algemene zin blijft de waarborging van de vertrouwelijkheid in dergelijke gevallen niettemin afhankelijk van de wijze waarop door de betrokken opsporingsambtenaren en officieren van justitie met de gegevens wordt omgegaan. Omdat de advocaat niet bij de inbeslagneming aanwezig is en hier vaak ook niet direct van op de hoogte raakt, staat of valt de waarborging van de vertrouwelijkheid bij de handelswijze die in de praktijk door politie en justitie wordt beproefd. Zoals is gebleken in de strafzaken die het onderwerp waren van de civiele procedures tussen de Staat en Stibbe, is die handelswijze in ieder geval geruime tijd niet (geheel) in overeenstemming met het recht op vertrouwelijkheid geweest.

4.4.3 Digitale gegevens

Die in de opsporingspraktijk ontstane handelswijze vormt meteen ook de belangrijkste kwetsbaarheid waar het gaat om digitale (e-mail)communicatie en digitale gegevens. Dergelijke gegevens worden doorgaans verkregen door inbeslagneming van gegevensdragers en door het vorderen van informatie bij derden, zoals hostingservices en internetproviders. Daarbij kan het gaan om zeer omvangrijke datasets, die veelal slechts met technische hulpmiddelen zoals het door het NFI ontwikkelde zoekprogramma Hansken effectief kunnen worden doorzocht.[185] Inbreuken op het verschoningsrecht kunnen in dergelijke gevallen deels worden voorkomen door bij het vorderen van zulke gegevens aan te geven dat de derde zelf een selectie maakt waarbij vertrouwelijke informatie op voorhand wordt uitgefilterd.[186] Uiteraard moet dan wel ten tijde van de vordering al bekend zijn dat sprake kan zijn van communicatie met één of meer geïdentificeerde verschoningsgerechtigden, en moet de derde (technisch) in staat zijn een dergelijke selectie uit te voeren. Ook kunnen advocaten er zelf voor zorgen dat hun e-mailcorrespondentie eenvoudig als vertrouwelijke communicatie te identificeren valt, door gebruikmaking van een als zodanig herkenbaar e-mailadres en het gebruik van termen als 'geprivilegieerd' of 'advocaat-cliënt-correspondentie' in de onderwerpregel. Het gebruik van e-mailversleuteling is eveneens een manier om de vertrouwelijkheid te beschermen en wordt door de NOvA dan ook aangemoedigd.[187] Tot nog toe bleek een belangrijk obstakel echter dat in de opsporingspraktijk weinig bezwaren werden gezien tegen het zelf maken van een selectie in het verkregen materiaal, waarbij veelal niet werd volstaan met kennisneming van bijvoorbeeld afzender of geadresseerde en onderwerp, maar vaak ook de inhoud van dergelijke communicatie werd bekeken om te beoordelen of het daadwerkelijk om geheimhouderinformatie ging.[188] Daarbij wordt gewerkt met

184 Dat zich ook dan problemen kunnen voordoen blijkt evenwel uit de controverse rondom het beslag in de zaak Weski, zie bijv. Mos & Polman 2023b.
185 Zie voor meer informatie Hansken – Informatieblad Geheimhoudersinformatie 2020.
186 Zie in die zin ook Rb Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035.
187 'Vertrouwelijke internetcommunicatie', advocatenorde.nl.
188 Doorenbos & Rosing 2020, p. 219.

zogenaamde medewerkers geheimhouding, die geen onderdeel uitmaken van het onderzoeksteam en als taak hebben te beoordelen of sprake is van geheimhouderinformatie.[189] Bovendien bleek de gehanteerde handelswijze ook op andere aspecten – zoals het voorleggen van mogelijk vertrouwelijke communicatie aan de verschoningsgerechtigde en het zo nodig inschakelen van de RC – niet in lijn met het juridisch kader.[190] Tot slot moet in dit kader worden gewezen op de beperkingen die samenhangen met de technische eigenschappen van inbeslaggenomen digitale data, waardoor het in praktisch opzicht niet eenvoudig of (zonder meer) mogelijk is om alle verschoningsgerechtigde informatie (voorafgaand aan doorzoeking) uit een databestand te filteren.[191]

Hoewel in de (opsporings)praktijk inmiddels deels anders te werk wordt gegaan, hebben (de onthullingen over) de door politie en openbaar ministerie gehanteerde methoden geleid tot een groot wantrouwen onder advocaten en een over en weer zeer gespannen sfeer.[192] Net zoals de misstanden in 2001 rondom het afluisteren van telefoons leidden tot het stelsel van nummerherkenning, is al gepleit voor een systeem van automatische e-mailherkenning.[193] Dat neemt niet weg dat een breed gedragen indruk onder advocaten dat de strafvorderlijke overheid in de kern niet te vertrouwen is wanneer het gaat om de naleving van de regels rondom vertrouwelijke communicatie, ertoe kan leiden dat men zijn toevlucht zoekt tot andere methoden, zoals het gebruik van versleutelde communicatiediensten. Uit het voorgaande blijkt echter dat daaraan – in ieder geval waar het gaat om cryptotelefoons – ook weer eigen risico's kleven.

189 Vgl. Openbaar Ministerie, *Handleiding verwerking geheimhouderinformatie aangetroffen in inbeslaggenomen voorwerpen en in digitale bestanden*, juni 2014. Deze wordt inmiddels niet meer gebruikt.

190 Zie uitgebreider Rb. Oost-Brabant 22 maart 2022, ECLI:NL:RBOBR:2022:1035 en Hof 's-Hertogenbosch 2 mei 2023, ECLI:NL:GHSHE:2023:1329.

191 Zie hierover uitgebreider *Informatieblad NFI* 2023 en hierna par. 6.5.2.4.

192 Vgl. Brouwer 2022; Pijnappels 2022 en Doorenbos 2022.

193 Spronken 2022.

5. Het gebruik van extra beveiligde en/of identiteitsversluierende (communicatie)middelen door advocaten

5.1 Inleiding

Belangrijke doelen van dit onderzoek zijn het in kaart brengen van de verschillende extra beveiligde en/of identiteitsversluierende communicatiemiddelen die door advocaten worden gebruikt in het contact met hun cliënten (deelvraag 2), en het in kaart brengen van de beweegredenen van advocaten om dergelijke middelen wel of niet te gebruiken (deelvraag 3). De beantwoording van deze vragen vindt plaats aan de hand van de bevindingen uit de interviews met zeventien advocaten. Waar mogelijk worden deze bevindingen aangevuld met informatie verkregen uit de schriftelijke reacties van het OM en het landelijk dekenberaad. In dit hoofdstuk worden deze bevindingen uitgewerkt. In paragraaf 5.2 wordt uiteengezet welk beeld ontstaat over het type extra beveiligde communicatiemiddelen dat door advocaten wordt gebruikt en de mate waarin dit gebeurt. In de daaropvolgende paragrafen wordt ingegaan op de beweegredenen om al dan niet gebruik te maken van extra beveiligde communicatiemiddelen. Aan de hand van de bevindingen uit de interviews is daarbij een thematische onderverdeling gemaakt. In paragraaf 5.3 wordt uiteengezet op welke wijze de geheimhoudingsplicht doorwerkt in de keuze voor het gebruik van extra beveiligde communicatiemiddelen. Paragraaf 5.4 bespreekt welke rol de wens of voorkeur van de cliënt daarbij speelt. In paragraaf 5.5 worden enkele overige beweegredenen behandeld. In paragraaf 5.6 volgt een conclusie.

5.2 De gebruikte communicatiemiddelen

In het derde hoofdstuk zijn drie categorieën extra beveiligde communicatiemiddelen besproken. Tijdens de interviews stond het gebruik van deze drie categorieën middelen centraal. Andere extra beveiligde communicatiemiddelen waar de advocaten in de enquête naar zijn gevraagd, zoals bel- en SMS-applicaties, worden niet of nauwelijks gebruikt, en zullen hierna dan ook niet verder aan de orde komen.

5.2.1 Chatapplicaties

Uit de interviews blijkt dat advocaten geregeld gebruikmaken van extra beveiligde chatapps.[194] De chatapplicaties die het meeste worden gebruikt zijn Signal en Telegram, een enkeling geeft aan Threema gebruikt te hebben. Andere chatapplicaties, bijvoorbeeld Wire of Element, worden niet gebruikt. Signal, Telegram of Threema worden door de meeste advocaten naast WhatsApp gebruikt. Over het algemeen worden chatapplicaties gebruikt voor het uitwisselen van praktische informatie over afspraken, zittingen en de stand van zaken, al zijn er ook advocaten die aangeven dat zij met cliënten meer inhoudelijke informatie en bestanden via chatapps uitwisselen.

[194] Ongeveer de helft van de geïnterviewde advocaten gaf aan gebruik te maken van een extra beveiligde chatapplicatie (al dan niet naast het gebruik van WhatsApp).

5.2.2 Extra beveiligde e-mail

Extra beveiligde e-mail(providers) – anders dan het verplichte gebruik van Veilig Mailen via Zivver in het contact met de Rechtspraak – worden door de respondenten ook geregeld gebruikt, zij het in mindere mate dan chatapps.[195] De extra beveiliging van de e-mailcorrespondentie, bijvoorbeeld door (een provider die gebruik maakt van) encryptie, wordt veelal niet standaard toegepast, maar enkel wanneer de advocaat dit noodzakelijk acht, bijvoorbeeld in verband met de gevoeligheid van de inhoud van het bericht of de bijlagen, of wanneer een cliënt hierom vraagt. In zijn algemeenheid valt op dat het gebruik van e-mail in de contacten met cliënten verschilt al naar gelang het soort praktijk. Vooral in de commune strafpraktijk loopt cliëntcontact maar tot op zekere hoogte via e-mail, bijvoorbeeld omdat cliënten zelf niet goed overweg kunnen met e-mail, of omdat zij gedetineerd zijn. In de financieel-economische (straf)praktijk is e-mail daarentegen een belangrijk en veelgebruikt communicatiemiddel. Daarnaast worden, met name voor het delen van bestanden, soms specifieke applicaties gebruikt of andere beveiligingsmaatregelen getroffen.[196] In dat geval hoeven de (gevoelige) bestanden niet via (extra beveiligde) e-mail te worden verzonden. Extra beveiligde e-mailapplicaties en extra beveiligd delen van bestanden zullen in het navolgende samen worden besproken, gelet op de overeenkomstige strekking van en beweegredenen voor het gebruik van deze middelen.

5.2.3 Cryptotelefoons

Voor wat betreft het gebruik van cryptotelefoons door advocaten zijn aantallen opgevraagd bij zowel het OM als bij het landelijk dekenberaad. Door beide organisaties is bevestigd dat de dekens van het OM eerder dit jaar (2023) een lijst hebben ontvangen met daarop de namen van advocaten die, zo blijkt uit dossieronderzoek, gebruik maken en/of hebben gemaakt van een cryptotelefoon.[197] Het is niet bekend hoeveel advocaten er precies op deze lijst staan, maar vanuit het OM wordt aangegeven dat ze vijf tot vijftien geheimhouders hebben geïdentificeerd in verschillende cryptotelefoon-operaties.

De dekens hebben gesproken met verschillende advocaten die gebruik hebben gemaakt van een cryptotelefoon.[198] Alle advocaten die met de dekens hebben gesproken hebben aangegeven op dit moment geen gebruik meer te maken van een dergelijk toestel, zo blijkt uit de schriftelijke reactie van het landelijk dekenberaad.

Binnen de steekproef van respondenten hebben drie advocaten aangegeven dat zij (kort) een cryptotelefoon in hun bezit hebben gehad en/of hebben gebruikt. Drie andere advocaten geven aan dat

---

195 Proton Mail is een voorbeeld van een beveiligde e-mailprovider die door de respondenten (incidenteel) wordt gebruikt.

196 Bijvoorbeeld Fileshar, FileCap, een digitale kluis of beveiligd digitaal platform.

197 Dit blijkt uit de schriftelijke reactie van het OM en de schriftelijke reactie van het landelijk dekenberaad.

198 Het is onduidelijk met hoeveel advocaten de dekens precies hebben gesproken.

ze direct of meer indirect weleens het verzoek hebben gekregen van cliënt(en) om een cryptotelefoon te gebruiken, maar dat ze dit verzoek hebben geweigerd.[199]

De respondenten die zelf een cryptotelefoon in het bezit hebben gehad of (indirect) een verzoek hebben gekregen van een cliënt om met een cryptotelefoon te communiceren, verlenen zonder uitzondering (overwegend) bijstand in georganiseerde misdaadzaken. Met name bij deze groep advocaten lijkt geen twijfel te bestaan over het feit dat een deel van hun collega's (in het verleden) gebruik heeft gemaakt van cryptotelefoons.

> 'dat was ook geen geheim dat advocaten dat ook wel gebruikten.'
>
> 'Minimaal 15 tot 20.'
>
> 'Maar ja, meer dan tien.'

In de paragrafen hierna zal worden ingegaan op de beweegredenen voor het al dan niet gebruiken van extra beveiligde communicatiemiddelen. Daarbij zal waar relevant een onderscheid worden gemaakt naar het type middel, omdat specifieke beweegredenen hierbij uiteen kunnen lopen.

5.3 Waarborging van de geheimhoudingsplicht

5.3.1 Inleiding

Uit de interviews met advocaten blijkt een duidelijk besef van het belang van vertrouwelijkheid en geheimhouding. Veel respondenten zijn zich zeer bewust van de gevoeligheid van de informatie waar zij mee te maken hebben en van het principiële recht van de cliënt op volstrekte vertrouwelijkheid. Mede gelet op de eisen die door onder meer de NOvA worden gesteld, hebben respondenten dan ook maatregelen getroffen om de vertrouwelijkheid van communicatie te waarborgen. In de interviews wordt bijvoorbeeld verwezen naar algemene maatregelen zoals het gebruik van een beveiligde server. Ook valt te denken aan de keuze voor bepaalde communicatiemiddelen of voor het zoveel mogelijk bespreken van vertrouwelijke informatie in persoon. In de hiernavolgende paragrafen worden de door advocaten gemaakte afwegingen en keuzes per type communicatiemiddel behandeld. Eerst worden in paragraaf 5.3.2 echter enkele algemene observaties besproken die samenhangen met het feit dat er verschillende soorten risico's voor de geheimhouding kunnen worden geïdentificeerd.

5.3.2 Typen risico's voor vertrouwelijkheid

Bij de waarborging van de vertrouwelijkheid spelen verschillende aspecten een rol, waarbij in de eerste plaats van belang is uit welke hoek de mogelijke risico's voor vertrouwelijkheid komen. Zo is er het risico van inbreuken door (commerciële) derde partijen, bijvoorbeeld doordat (meta)data voor een commerciële aanbieder van communicatiediensten inzichtelijk zijn, of via een hack of bij een derde partij belanden. De mate waarin advocaten zich hierover zorgen maken of zich hiertegen wapenen loopt

[199] Een van de advocaten die weleens een verzoek heeft gekregen, maar daar niet op in is gegaan geeft aan dat de cliënt de cryptotelefoon (die werd aangeboden aan de advocaat) al had meegenomen naar het kantoor.

uiteen, en lijkt deels afhankelijk van het type zaken waarin bijstand wordt verleend. Zo zijn er advocaten die zich nadrukkelijk bewust zijn van de (commerciële) gevoeligheid van de hen toevertrouwde gegevens en die om die reden bijvoorbeeld geen of minder gebruikmaken van bepaalde applicaties of diensten.[200] Anderzijds zijn er ook respondenten die het risico op datalekken in zijn algemeenheid wel onderkennen, maar voor wie dit geen aanleiding is om specifieke aanvullende maatregelen te treffen. Daarbij speelt soms een inschatting van de gevoeligheid van de behandelde zaken een rol. In dat verband zijn sommige respondenten vooral beducht voor menselijke fouten, zoals het gebruiken van een verkeerd telefoonnummer of e-mailadres.

Een deel van de respondenten heeft (ook) zorgen over mogelijke inbreuken door buitenlandse overheden en veiligheidsdiensten, bijvoorbeeld omdat zij een praktijk hebben met een internationale component. Voor sommige respondenten bepaalt dat (mede) de keuze voor het gebruik van bepaalde (chat- of e-mail)applicaties. Ook door advocaten die naar aanleiding van het gebruik van een cryptotelefoon contact hebben gehad met de dekens wordt de wens om veilig te kunnen communiceren met cliënten in het buitenland soms genoemd als reden om een cryptotelefoon te gebruiken.[201] In een enkel geval zijn ook andere voorzorgsmaatregelen getroffen, zoals het meenemen van een geschoonde telefoon of laptop naar het buitenland. Verder kan ook het mogelijk meeluisteren door binnenlandse inlichtingendiensten een reden zijn om bepaalde informatie niet via een (digitaal) communicatiemiddel te delen, bijvoorbeeld in terrorismezaken.

In de strafpraktijk speelt ten slotte het risico van inbreuken op de vertrouwelijkheid door de strafvorderlijke overheid nadrukkelijk een rol.[202] Het is juist dit risico en de noodzaak om hiervoor maatregelen te treffen dat in de interviews het meest op de voorgrond staat. Uiteraard speelt daarbij mee dat het overgrote merendeel van de respondenten werkzaam is in de strafrechtspraktijk.[203] Vooral bij die respondenten valt vaak scepsis of zelfs wantrouwen in de naleving van het verschoningsrecht door de strafvorderlijke autoriteiten waar te nemen. De mate waarin sprake is van wantrouwen loopt daarbij wel sterk uiteen en lijkt tot op zekere hoogte samen te hangen met het type praktijk. Het wantrouwen is over het algemeen het grootst bij advocaten die werkzaam zijn in de commune strafpraktijk waarin ook grotere strafzaken met al dan niet georganiseerde (drugs)criminaliteit worden behandeld, en bij advocaten die bijstand verlenen in de grotere financieel-economische strafzaken. Met name advocaten die optreden in zaken waarin het belang van de overheid om inbreuk te maken op het verschoningsrecht als minder groot wordt ingeschat, geven blijk van meer vertrouwen in de huidige waarborgen. Daarbij wordt er soms op gewezen dat verschoningsgerechtigd materiaal hoe dan ook niet bruikbaar is als bewijs in de strafzaak. Verschillende respondenten benadrukken in dat verband ook de plicht van de advocaat om zichzelf altijd als zodanig kenbaar te maken. Nu in de interviews zo sterk de nadruk heeft gelegen op de waarborging van de vertrouwelijkheid in relatie tot mogelijke inbreuken door de strafvorderlijke

200 Daarbij gaat het bijvoorbeeld om een voorkeur om (bepaalde) informatie niet via WhatsApp, maar bijvoorbeeld via Signal te delen.

201 Zo blijkt uit de schriftelijke reactie van het landelijk dekenberaad

202 Dit blijkt uit de interviews met advocaten en wordt tevens expliciet benoemd in de reactie van het landelijk dekenberaad.

203 Van de zeventien geïnterviewde advocaten, behandelen vijftien (ook) strafzaken. Zie voor de selectie van respondenten meer uitgebreid: par. 2.4.1.

overheid, zal dat bij de hiernavolgende bespreking ook het meeste aandacht krijgen. Waar relevant zal ook worden ingegaan op maatregelen die advocaten treffen om andersoortige risico's voor de vertrouwelijkheid te beperken.

5.3.3 Bespreking in persoon

In het algemeen beweegt de geheimhoudingsplicht advocaten ertoe om bewuste keuzes te maken over hoe bepaalde informatie wordt gedeeld. Een veel gehoord geluid is dan ook dat advocaten er bewust voor kiezen om bepaalde, erg gevoelige informatie alleen in persoon – op kantoor, in de penitentiaire inrichting of zelfs buiten – te bespreken. Enkele respondenten geven aan dat er bij besprekingen op kantoor soms ook, en doorgaans op verzoek van de cliënt, voor wordt gekozen om de telefoon op te bergen in een speciale – niet afluisterbare – box of hoes, of om de telefoon bij de receptie te laten liggen.

Voor wat betreft de breed gedeelde voorkeur voor het voeren van vertrouwelijke besprekingen in persoon is nog vermeldenswaardig dat de spreekkamers op politiebureaus en in penitentiaire inrichtingen niet zonder meer worden vertrouwd. Enkele respondenten geven aan dat zij tijdens gesprekken met gedetineerde cliënten bepaalde dingen niet mondeling bespreken, maar schriftelijk, om te voorkomen dat erg gevoelige informatie bij de strafvorderlijke overheid of bij inlichtingendiensten terechtkomt.[204] Zij refereren in dat verband aan de ophef die is ontstaan over deze wijze van corresponderen in de zaak van Youssef T., en weerspreken nadrukkelijk dat dit een signaal is van normoverschrijdend of zelfs strafbaar gedrag.

5.3.4 Telefoon

Telefonisch contact wordt door veel respondenten gereserveerd voor wat minder gevoelige besprekingen, bijvoorbeeld over praktische zaken of voor het maken van afspraken. Vooral in de financieel-economische (straf)praktijk is het echter gebruikelijk om ook meer inhoudelijk te communiceren via de telefoon of een digitaal communicatiemiddel zoals Teams, waarbij praktische aspecten een rol spelen: er moet nu eenmaal veel worden besproken, en cliënten zitten niet dichtbij of zelfs in het buitenland.

De vertrouwelijkheid van telefonisch contact ten opzichte van de strafvorderlijke overheid en DJI wordt gewaarborgd door het herkenningssysteem van geheimhoudertelefoonnummers. Verschillende respondenten geven aan op zichzelf wel vertrouwen te hebben in een goede werking van dit systeem. Sommigen wijzen in dat verband ook op de aard van hun praktijk. Zij maken de inschatting dat de meeste zaken niet van dien aard zijn dat justitie erg veel inspanningen zal verrichten om mee te kunnen luisteren. Niettemin valt bij veel respondenten ten minste een zekere reserve te bespeuren, al is het maar met een verwijzing naar (technische) incidenten in het verleden, of vanwege de mogelijkheid van (onbewuste) menselijke fouten. Daarnaast zijn er verschillende respondenten die een uitgesproken

[204] De respondenten die aangeven dit zelf te doen geven tevens aan dat dit niet ongebruikelijk is en dat collega's dit naar hun weten ook doen.

gebrek aan vertrouwen hebben in de bescherming die het geheimhoudernummer biedt. Bij deze respondenten ziet dat wantrouwen meestal niet zozeer op de technische aspecten van het herkenningssysteem, maar vooral op het handelen van de overheid. Men gaat ervan uit dat gesprekken toch worden afgeluisterd, alleen niet opgenomen of uitgewerkt, of houdt er rekening mee dat politie en justitie de waarborgen omzeilen, bijvoorbeeld door het gebruik van andere technische middelen zoals IMSI-catchers. Verschillende respondenten verwijzen in dat verband naar de Box-affaire: de handelswijze van de strafvorderlijke overheid in die kwestie geeft hen (extra) aanleiding voor wantrouwen in de naleving van de waarborgen voor het verschoningsrecht in het algemeen.

> 'want toen ik als advocaat begon stond ik daar redelijk bleu in, ik dacht van "ja ik heb toch mijn telefoonnummer doorgegeven dus dan is alles goed, dan kan ik gaan communiceren". Maar dat soort voorbeelden maken wel, dat je denkt van "nou, dan ben ik toch terughoudender".'

De onzekerheden over de vertrouwelijkheid van telefonisch contact zijn voor vrijwel alle respondenten reden om belangrijke, inhoudelijke zaken bij voorkeur in persoon te bespreken. [205] Dat geldt ook voor respondenten die aangeven op zichzelf wel vertrouwen te hebben in het systeem van de nummerherkenning, of die erop vertrouwen dat eventueel (al niet opzettelijk) onderschepte informatie toch niet zal worden gebruikt in de strafzaak. Daarnaast benoemen enkele respondenten in dit verband ook dat zij steeds duidelijk maken dat het gaat om een advocaat-cliënt-gesprek. Voor verschillende advocaten zijn hun zorgen over de vertrouwelijkheid van gesprekken die via de geheimhoudertelefoon worden gevoerd, echter een reden om bij voorkeur niet via de geheimhoudertelefoon te bellen. Zij kiezen er bewust voor om telefonische gesprekken met (familieleden van) cliënten en andere advocaten waar mogelijk via Signal te voeren. Wanneer de cliënt in het buitenland verblijft is het niet of in veel mindere mate mogelijk om besprekingen in persoon te voeren, zodat advocaten tot op zekere hoogte zijn aangewezen op telefonisch contact. Het is juist voor die situaties dat de noodzaak wordt gevoeld om te zoeken naar andere veilige manieren van communiceren, zoals bellen via Signal of met cryptotelefoons.

5.3.5 Chatapplicaties

Vrijwel alle respondenten maken in het contact met hun cliënten gebruik van chatapplicaties, zoals WhatsApp, Signal, Telegram of Threema. Belangrijke redenen hiervoor zijn de behoefte aan een laagdrempelige mogelijkheid voor communicatie, het praktische gemak van deze chatapps en het gegeven dat vrijwel niemand meer communiceert via SMS. Wanneer het gaat om de geheimhouding van deze communicatie ten opzichte van de strafvorderlijke overheid, wordt over het algemeen aangenomen dat dit ten aanzien van al deze chatapps adequaat is gewaarborgd. Een veelgenoemde reden daarvoor is dat deze diensten zo algemeen worden gebruikt dat de overheid geen toegang tot de servers kan krijgen met het argument dat deze diensten alleen of voornamelijk door criminelen worden gebruikt. Hoewel

[205] Onzekerheden over de vertrouwelijkheid van telefonisch contact spelen ook een rol bij de keuze van advocaten om een cryptotelefoon te gebruiken, zo blijkt uit de schriftelijke reactie van het landelijk dekenberaad. Het gebruik van het geheimhoudernummer bleek niet altijd een waterdicht systeem om vertrouwelijk met cliënt te kunnen communiceren.

sommige respondenten een duidelijke voorkeur hebben voor het gebruik van Signal boven WhatsApp, heeft dat doorgaans niet zozeer te maken met de mogelijkheid van inbreuken door de strafvorderlijke overheid, maar met de beveiliging van gegevens ten opzichte van (commerciële) derden. Een dergelijke voorkeur komt soms voort uit een onderzoek naar de eigenschappen van dergelijke berichtendiensten, maar is ook geregeld gebaseerd op een 'gevoel', of is ontstaan nadat respondenten van collega's of cliënten hebben gehoord dat zij dit gebruiken, bijvoorbeeld omdat het veiliger zou zijn. Niettemin vormen de extra beveiligingsfuncties van bepaalde berichtendiensten, zoals de mogelijkheid om berichten na verloop van tijd automatisch te laten verwijderen, in een enkel geval wel een reden om bewust voor het gebruik van zo'n dienst te kiezen. Dat hangt samen met de mogelijkheid dat de communicatie wordt ingezien bij inbeslagname van de telefoon van een cliënt. Hoewel de chatapplicaties gekoppeld zijn aan een telefoonnummer en respondenten aangeven dat zij hiervoor hun geheimhoudernummer gebruiken, wordt deze informatie niet automatisch vooraf uitgefilterd.[206] Niet alle advocaten lijken zich bewust van het feit dat bij kennisneming van communicatie op een in beslag genomen telefoon vaak niet direct inzichtelijk zal zijn wanneer het om verschoningsgerechtigde informatie gaat. Sterker nog, er zijn respondenten die in de veronderstelling verkeren dat verschoningsgerechtigde communicatie er automatisch of in ieder geval eenvoudig uitgefilterd kan worden. Toch geven veel advocaten aan dat zij gevoelige informatie (zekerheidshalve) in beginsel niet via chatapplicaties delen, maar dit communicatiemiddel vooral gebruiken voor uitwisseling van praktische informatie en het maken van afspraken.

5.3.6 E-mail en delen van bestanden

Veel respondenten houden bij het gebruik van e-mail en/of het op andere wijze (digitaal) delen van bestanden, rekening met de mogelijkheid dat deze informatie in handen komt van derden. Daarbij gaat het vooral om het risico dat deze informatie bij de strafvorderlijke overheid terechtkomt, bijvoorbeeld doordat deze communicatie bij de cliënt of bij derden wordt aangetroffen. Voor justitie minder interessante stukken, zoals dagvaardingen of stukken uit het dossier, worden wel geregeld via e-mail doorgestuurd. Het risico dat de gegevens bij derde partijen terechtkomen wordt soms ook betrokken bij de afweging om informatie al dan niet via e-mail te delen, of geeft aanleiding om gebruik te maken van versleuteling (bijvoorbeeld met Zivver), of een platform voor het delen van bestanden (bijvoorbeeld Fileshare). Voor wat betreft het gebruik van e-mail kan een onderscheid worden gemaakt tussen advocaten die werkzaam zijn in de commune strafpraktijk, en advocaten die zich bezighouden met financieel-economische strafzaken.

In de commune strafpraktijk lijkt het uitgangspunt om terughoudend om te gaan met het delen van informatie via e-mail. Het middel wordt vooral gebruikt voor het delen van dagvaardingen, dossierstukken en andere – in relatie tot het eventuele inzien door justitie – minder gevoelige informatie. Sommige respondenten gebruiken voor bepaalde correspondentie Proton Mail, bijvoorbeeld wanneer toch meer gevoelige informatie moet worden verstuurd, of omdat de cliënt daaraan de voorkeur geeft.

[206] Zie hierover uitgebreider par. 6.5.2.3.

Daarbij is de gedachte dat Proton Mail beter beveiligd is tegen inbreuken door buitenlandse overheden of inlichtingendiensten, of door de strafvorderlijke overheid.[207]

In de financieel-economische strafzaken is e-mail echter een veelgebruikt communicatiemiddel, ook voor uitwisseling van meer inhoudelijke en voor justitie potentieel interessante informatie. Tegelijk speelt juist in deze zaken de problematiek rondom de inbeslagname van grote hoeveelheden digitale gegevens, waaronder e-mailberichten. De Box-affaire heeft bij veel respondenten, maar zeker bij degenen die werkzaam zijn in het financieel-economische strafrecht, dan ook tot grote zorgen en soms zelfs onverholen achterdocht geleid. Desalniettemin blijft e-mail om praktische redenen een belangrijk communicatiemiddel. Enkele respondenten geven aan dit met het oog op de waarborging van het verschoningsrecht weliswaar problematisch te vinden, maar geen goede andere mogelijkheid te zien. Soms wordt wel gebruik gemaakt van een extra beveiligde e-mailapplicatie zoals Zivver, maar doorgaans niet standaard. Dat heeft vooral te maken met ervaren gebruiksonvriendelijkheid, of het feit dat cliënten het onhandig vinden of er niet goed mee om kunnen gaan.[208] Wel wordt soms gekozen voor het delen van bestanden via een daarvoor ingericht middel, bijvoorbeeld een beveiligd platform of een digitale kluis.

Om de vertrouwelijkheid van e-mailcorrespondentie zoveel mogelijk te waarborgen zorgen de advocaten ervoor dat de communicatie als geheimhouderinformatie herkenbaar is. E-mailadressen bevatten in de domeinnaam vaak een verwijzing naar het feit dat het om een advocatenkantoor gaat, en veel advocaten vermelden dit ook in de onderwerpregel of maken dit zichtbaar door het gebruik van een digitale handtekening of watermerk. Geregeld wordt ook in het onderwerp expliciet vermeld dat het gaat om vertrouwelijke advocaat-cliënt-communicatie. Ook de advocaten die soms via Proton Mail communiceren geven aan dat zij in de naam van het e-mailadres, in het onderwerp en/of de ondertekening (expliciet) tot uitdrukking brengen dat het bericht afkomstig is van een advocaat.

5.3.7 Cryptotelefoons

Een gebrek aan vertrouwen in de vertrouwelijkheid van de hiervoor besproken communicatiemiddelen heeft sommige advocaten aanleiding gegeven om (tijdelijk) een of meerdere cryptotelefoons te gebruiken.[209] Daarbij moet worden opgemerkt dat de wens of het initiatief om hiervan gebruik te maken met name van de cliënt afkomstig was (zie hierna ook par. 5.4). De meeste respondenten – ook degenen die zelf geen cryptotelefoon hebben gebruikt – delen de zorgen van cliënten over geheimhouding en hebben begrip voor de wens om extra beveiligd te communiceren, ook als dat met een cryptotelefoon is. Het waarborgen van de vertrouwelijkheid wordt ook door de advocaten die contact hebben gehad met de dekens genoemd als een van de argumenten voor het gebruik van een cryptotelefoon.[210] Niettemin is

---

207 Zie m.b.t. (de beveiligingsfunctionaliteiten van) Proton Mail uitgebreider par. 3.3.3 en 'Security', proton.me.

208 Zie hierover uitgebreider par. 5.5.2.

209 In de steekproef ging het om drie geïnterviewde advocaten die (kort) een cryptotelefoon in hun bezit hebben gehad en/of hebben gebruikt.

210 Uit de schriftelijke reactie van het landelijk dekenberaad blijkt dat onzekerheden over de vertrouwelijkheid van meer conventionele communicatiemiddelen een rol spelen bij de keuze van advocaten om een cryptotelefoon te gebruiken. Het gebruik van het geheimhoudernummer bleek niet altijd een waterdicht systeem om vertrouwelijk met cliënt te kunnen communiceren.

iedereen zich (inmiddels) ook bewust van de risico's voor de vertrouwelijkheid die (kunnen) ontstaan wanneer een server wordt gehackt of in beslag wordt genomen in het kader van een cryptotelefoon-operatie.[211]

De respondenten die aangeven een cryptotelefoon te hebben gebruikt zijn werkzaam in de commune strafpraktijk, waarbij zij zich voornamelijk of uitsluitend bezighouden met zaken die betrekking hebben op georganiseerde (drugs)criminaliteit. Uit de interviews komt het beeld naar voren dat door veel verdachten in dergelijke zaken gebruik werd of wordt gemaakt van cryptotelefoons, om meeluisteren door de strafvorderlijke overheid te voorkomen. Geregeld was dit ook (vrijwel) het enige middel waar deze cliënten mee communiceerden. De advocaten die in dergelijke zaken bijstand verlenen geven dan ook vrijwel allemaal aan dat zij op enig moment van cliënten het (directe of indirecte) verzoek hebben gekregen om een dergelijke telefoon te gebruiken, of dat hen zelfs een telefoon werd aangeboden. Een respondent heeft de ervaring dat de aanbieders van de verschillende cryptocommunicatiediensten telefoons aan advocaten aanboden, waarschijnlijk met de bedoeling om ervoor te zorgen dat ook hun (potentiële) cliënten een dergelijke telefoon zouden aanschaffen. De in dit onderzoek betrokken respondenten die daadwerkelijk een (of meerdere) cryptotelefoon(s) zijn gaan gebruiken geven aan alleen gebruik te hebben gemaakt van een door hen zelf aangeschafte cryptotelefoon, om afhankelijkheid van cliënten zoveel mogelijk te voorkomen.

Waar de wens om geheimhouding te verzekeren de belangrijkste reden is om een cryptotelefoon te gebruiken, wordt geheimhouding tegelijkertijd juist ook als het grootste risico gezien. Uit de verschillende *hacks* of inbeslagname van servers van aanbieders van cryptocommunicatiediensten, is immers gebleken dat de vertrouwelijkheid van deze communicatie allerminst gegarandeerd is. Voor advocaat-cliënt-communicatie bestaat dan het risico dat deze niet (onmiddellijk) als zodanig herkenbaar is. Veel respondenten zijn zich hiervan bewust en benoemen de *hacks* van cryptodiensten en de daaraan verbonden risico's voor de geheimhouding van advocaat-cliënt-communicatie expliciet als argument(en) om geen gebruik (meer) te maken van een cryptotelefoon.[212] Hetzelfde geldt voor de advocaten die in gesprek zijn gegaan met de dekens: een aantal van hen is gestopt met het gebruik van cryptotelefoons nadat duidelijk werd dat de servers inbeslaggenomen of gehackt konden worden.[213]

> 'Los van het feit dat ik het niet wil gebruiken, ben ik er ook niet van overtuigd dat die communicatie afgeschermd blijft.'

Degenen die een cryptotelefoon hebben gebruikt geven aan dat zij herkenbaarheid als geheimhouder van groot belang vinden. Om die reden kan bijvoorbeeld in de gekozen *nickname* tot uitdrukking worden gebracht dat het om een advocaat gaat. Een andere maatregel is het betrachten van transparantie over de gebruikte cryptotelefoonnummers richting de deken en/of het OM. Uit het onderzoek blijkt evenwel dat dit er niet altijd toe lijkt te hebben geleid dat verschoningsgerechtigde communicatie ook daadwerkelijk,

211 Dit blijkt uit zowel de interviews alsook uit de schriftelijke reactie van het landelijk dekenberaad.
212 Dit geldt zowel voor de advocaten die bewust geen gebruik hebben gemaakt van cryptotelefoons, als voor de advocaten die in het verleden wel gebruik hebben gemaakt van cryptotelefoons.
213 Dit blijkt uit de schriftelijke reactie van het landelijk dekenberaad.

voorafgaand aan kennisneming daarvan, is verwijderd. In ieder geval in één geval heeft het OM dergelijke communicatie doorgestuurd naar de lokale deken.

5.4 Wens, verzoek of initiatief van cliënt

In zijn algemeenheid geldt dat de communicatievoorkeuren van de cliënt door de respondenten worden meegenomen in de keuze voor een bepaald (extra beveiligd) communicatiemiddel. Met name de respondenten die werkzaam zijn binnen de commune strafrechtspraktijk geven aan dat hun cliënten over het algemeen weinig vertrouwen hebben in bepaalde communicatiemiddelen, bang zijn voor eventuele overheidsinterceptie (in binnen- en buitenland) en daarom specifieke voorkeuren hebben wat betreft extra beveiligde communicatiemiddelen. In de hiernavolgende paragrafen wordt nader ingegaan op de verschillende verzoeken van cliënt(en) om via een extra beveiligde chatapplicatie of extra beveiligde e-mail te communiceren (par. 5.4.1), de verzoeken van cliënt(en) om met een cryptotelefoon te communiceren (par. 5.4.2) en de vraag of dergelijke verzoeken gepaard gaan met een vorm van dwang, drang of druk (par. 5.4.3).

5.4.1 Chatapplicaties en extra beveiligde e-mail

Een deel van de respondenten gebruikt op verzoek van een of meerdere cliënten Signal of Telegram in plaats van WhatsApp. Door enkele van deze respondenten wordt aangegeven dat ze Signal, Telegram of Threema op verzoek van een cliënt hebben gedownload. Ook het bellen of verzenden van stukken via een chatapplicatie gebeurt soms op verzoek van cliënten. Hetzelfde geldt voor het gebruik van beveiligde e-mail. Een deel van de advocaten geeft aan dat sommige cliënten de voorkeur geven aan het gebruik van extra beveiligde mail, zoals Proton Mail of het delen van bestanden via een digitale dataroom. Dit verzoek lijkt met name afkomstig van in het buitenland verblijvende cliënten.

Voor wat betreft bovenstaande verzoeken geldt dat de betrokken advocaten aangeven dat ze geen moeite hebben met het tegemoetkomen van een cliënt in diens verzoek om een specifieke (extra beveiligde) chatapplicatie of e-mailprovider te gebruiken. Dit geldt niet voor alle advocaten: twee advocaten geven aan bewust geen gehoor te geven aan het verzoek van cliënten om te communiceren via een (bepaalde) chatapplicatie. Eén van hen geeft aan niet afhankelijk te willen zijn van de communicatiemiddelen die een cliënt uitzoekt.

De voorkeuren van de cliënt kunnen onder omstandigheden ook resulteren in het gebruik van een minder beveiligde vorm van communicatie. Zo blijkt uit de gesprekken met enkele advocaten dat zij zelf soms de voorkeur geven aan bepaald extra beveiligd communicatiemiddel, bijvoorbeeld Signal of Zivver, maar dat onkunde of weerstand vanuit de cliënt communicatie via dit middel kan belemmeren. Bijvoorbeeld omdat cliënten het gebruik van Zivver onhandig vinden of een bepaalde extra beveiligde chatapplicatie, zoals Signal, niet op hun telefoon hebben.

5.4.2 Cryptotelefoons

Hoewel de meeste respondenten bereid lijken te zijn om tegemoet te komen aan de wens van cliënt daar waar het gaat om het gebruik van specifieke extra beveiligde e-mailproviders of chatapplicaties, ligt dit voor een aantal respondenten anders wanneer het gaat om het verzoek om een cryptotelefoon te gebruiken.

Verschillende advocaten gaven aan dat ze bekend zijn met het feit dat (een deel van hun) cliënten cryptotelefoons gebruiken of hebben gebruikt. Eén van deze advocaten geeft aan dat cliënten enkel hebben gepeild of communicatie met een cryptotelefoon mogelijk is, vier andere advocaten hebben van hun cliënten weleens een cryptotelefoon aangeboden gekregen. Tenslotte geeft een enkele advocaat aan dat deze een cryptotelefoon in het bezit heeft gehad op initiatief van een collega en niet van een cliënt. Deze groep advocaten is werkzaam in strafzaken die betrekking hebben op georganiseerde (drugs-)criminaliteit. Een deel van de advocaten die in gesprek zijn gegaan met de dekens geeft aan dat het gebruik van een cryptotelefoon op initiatief van cliënt is gebeurd.[214]

Twee van de vijf advocaten die direct of meer indirect het verzoek van een of meer cliënt(en) kregen om te communiceren door middel van een cryptotelefoon, hebben een tijd gebruik gemaakt van dergelijke telefoons.[215] Deze advocaten geven aan dat (huidige en potentieel nieuwe) cliënten op enig moment enkel nog communiceerden via een cryptotelefoon. De drie andere advocaten geven aan dat ze het verzoek hebben geweigerd. Door deze advocaten worden verschillende argumenten opgesomd die ten grondslag liggen aan de keuze om geen cryptotelefoon te willen gebruiken. Hierbij spelen onder andere overwegingen omtrent integriteit en het criminele imago van cryptotelefoon een rol.[216] Daarnaast wordt door alle drie de advocaten verwezen naar de recente cryptotelefoon-operaties en de daarmee gepaarde risico's voor het waarborgen van de vertrouwelijkheid van de communicatie.

5.4.3 Druk, dwang of drang vanuit de cliënt?

Druk, dwang of drang ontstaat op het moment dat een advocaat zelf een bepaald communicatiemiddel niet wil gebruiken, maar het gevoel heeft dat hij of zij tegen de wens of het verzoek van de cliënt geen 'nee' kan zeggen. De gesprekken met de advocaten geven geen aanleiding om aan te nemen dat er bij de keuze voor een bepaald communicatiemiddel sprake is van een dergelijke druk, dwang of drang vanuit de cliënt(en).

---

214 Zo blijkt uit de schriftelijke reactie van het landelijk dekenberaad, een ander deel van de advocaten die met de dekens in gesprek zijn gegaan heeft (kort) een cryptotelefoon in het bezit gehad en/of gebruikt op initiatief van een collega. In dit kader wordt in de schriftelijke reactie verwezen naar het in 2018 opgestarte initiatief om speciale cryptotelefoons te ontwikkelen voor advocaten. Zie in dit verband uitgebreider: par. 3.4.1 en Gloudemans-Voogd 2018.

215 Zie voor wat betreft de beweegredenen van deze twee advocaten: par. 5.4.3. De derde advocaat die een cryptotelefoon in het bezit heeft gehad, geeft aan dat dit niet op initiatief van cliënt, maar op initiatief van een collega was.

216 Zie hierover ook par. 5.5.1.

Zoals blijkt uit de bovenstaande paragrafen spelen de voorkeuren van cliënten een rol bij keuze voor extra beveiliging en kan onder omstandigheden de wens van cliënt zelfs leidend zijn bij het kiezen voor een specifieke chatapplicatie of e-mailprovider. Wat betreft deze twee typen communicatiemiddelen lijken zowel de advocaten die instemmen met een verzoek van cliënt tot extra beveiligde communicatie, als de advocaten die een dergelijk verzoek weigeren, geen druk te ervaren vanuit de cliënt. De geïnterviewde advocaten die instemmen met verzoeken van cliënt geven aan geen probleem te hebben met de keuze voor een bepaalde chatapplicatie of e-mailprovider. Sterker nog, een deel van de advocaten erkent zelf ook de noodzaak van extra beveiligde communicatie en kan zich inleven in de wens van cliënt om extra beveiligingsmaatregelen te treffen. Dergelijke verzoeken vanuit de cliënt worden derhalve door de advocaten niet als ongeoorloofd ervaren.

> 'Omdat het nog steeds reguliere communicatiemiddelen zijn, andere varianten van hetzelfde, het zijn niet die Encrochat telefoons, zie ik geen belemmering en ervaar bij mijzelf ook geen weerstand om aan dat simpele verzoek tegemoet te komen. Dus ik ervaar ook geen druk.'

Voor de advocaten die indirect of direct het verzoek van cliënt hebben gehad om een cryptotelefoon te gebruiken geldt ook dat deze aangeven geen druk, dwang of drang vanuit de cliënt te hebben ervaren. Dit geldt zowel voor de advocaten die het verzoek hebben geweigerd, als voor de advocaten die wel een tijd met een cryptotelefoon hebben gecommuniceerd. Door de cliënt uitgeoefende druk lijkt evenmin een rol te hebben gespeeld bij de advocaten die een cryptotelefoon hebben gebruikt en daarover met de lokale dekens in gesprek zijn geweest.[217]

> 'En op het moment dat klanten zeggen, daar willen we niet over praten, dan kunnen we geen zaken doen met elkaar, "oké, dan ga je naar een ander".'

> 'Nou ja, dat heeft er dan meer mee te maken dat cliënten ook in het buitenland verblijven en dat ze dan zeggen "omdat we in het buitenland verblijven vinden we het prettiger om op deze manier te communiceren" en dan zeg ik "nee, doe ik niet".'

Enkele strafrechtadvocaten geven tijdens de gesprekken over druk voorbeelden van andersoortige verzoeken die niet gerelateerd zijn aan de keuze voor een bepaald communicatiemiddel, maar potentieel wel druk kunnen opleveren. Door een van de respondenten wordt bijvoorbeeld de situatie geschetst waarin een cliënt vanuit de PI met een mobiele telefoon contact zoekt. Een andere respondent geeft aan dat er wel eens iemand in het kantoor heeft gestaan die bepaalde dossiers in wilde zien.

> 'Dan kan je soms wel eens een soort van druk voelen, dat je denkt "dit voelt niet echt goed aan" en dan zeg je "nou, dit doe ik niet".'

---

217 Dit blijkt uit de schriftelijke reactie van het landelijk dekenberaad, waarin wordt vermeld dat geen van de advocaten heeft aangegeven dat invloed is uitgeoefend door de cliënt. Of door de dekens specifiek is gevraagd naar de aanwezigheid van dwang, drang of druk is echter onduidelijk.

Voor zover besproken lijken advocaten goed in staat om dergelijke verzoeken, waar potentieel een bepaalde druk van uit zou kunnen gaan, te weigeren. Meer in het algemeen wordt het weigeren van verzoeken, die al dan niet betrekking hebben op de keuze voor een bepaald communicatiemiddel, door verschillende advocaten verbonden aan de vrijheid om ervoor te kiezen een (potentiële) cliënt niet bij te staan.

> 'Dus als ik zeg "we gaan het zo doen" en zij zeggen "nou dat denk ik niet", dan zeg ik "daar is de deur". Heel simpel.'

Wel laten enkele respondenten doorschemeren dat het niet gebruiken van een cryptotelefoon (in het verleden) gevolgen zou kunnen hebben (gehad) voor hun praktijk. Zo geven de twee advocaten die wel gebruik hebben gemaakt van cryptotelefoons aan dat ze een dergelijk toestel hebben gebruikt omdat ze anders niet meer bereikbaar zouden zijn voor cliënten. Deze cliënten zouden op enig moment enkel nog maar via cryptotelefoon communiceren. Beide advocaten hebben destijds, vanwege de noodzaak om met hun cliënten in contact te blijven of de wens om bepaalde nieuwe cliënten bij te kunnen staan, een of meerdere cryptotelefoon(s) aangeschaft of aangenomen van een cliënt. Eén van deze respondenten spreekt in dat verband van een zekere 'commerciële druk' om een cryptotelefoon te gebruiken. Het gebruiken van een dergelijke telefoon zou een commercieel voordeel kunnen opleveren:

> 'Stel bijvoorbeeld, er wordt tienduizend kilo in beslaggenomen en men is op zoek naar advocaten, en jij hebt dus geen beveiligde telefoon, dan word je overgeslagen.'

> 'Anders waren ze niet bereikbaar en anders had je ze niet als cliënt. En dat waren écht wel interessante cliënten, dus die wilde je wel als cliënten. Ik wilde ze wel als cliënten en ik denk ook wel mijn collega's […] "Jaa, maar dat is geen druk, dat is geld verdienen".'

Dit beeld lijkt bevestigd te worden door twee andere advocaten die bijstand verlenen in zaken met betrekking tot georganiseerde criminaliteit maar bewust geen gebruik maken van cryptotelefoons om te communiceren met cliënten. Eén van hen meent dat advocaten die wel gebruik maken van cryptotelefoons een betere concurrentiepositie kunnen verkrijgen ten opzichte van de advocaten die dat niet doen. Een ander wijst op de mogelijkheid dat je als advocaat in sommige zaken niet of minder snel wordt ingeschakeld:

> 'Nou ja kijk als je ambitieus bent en je wil meedoen met dit soort zaken, dan zet je jezelf buiten spel als je principieel bent en zegt "ik doe dat niet".'

Tegelijkertijd lijkt het niet gebruiken van een cryptotelefoon niet direct gevolgen te hebben voor de (bestaande) praktijk van advocaten, zo blijkt uit de interviews met twee advocaten die allebei verzoeken van cliënten om een cryptotelefoon te gebruiken hebben geweigerd. Zo blijkt uit de interviews dat de keuze van sommige respondenten om geen cryptotelefoon te gebruiken niet tot gevolg heeft gehad dat bestaande cliënten bij hen zijn weggegaan.

> ‘Ik merk toch ook gewoon dat op het moment dat jij als advocaat gewoon goed kan uitleggen dat je de belangrijkste en meest vertrouwelijke dingen echt gewoon op kantoor, *face to face* moet bespreken, en dat dit ook in hun belang is, dat je daar uiteindelijk heel erg ver mee komt.’

5.5 Overige beweegredenen en overwegingen

5.5.1 Imago en integriteit

Een deel van de respondenten benoemt het criminele imago van de cryptotelefoons en/of de daarmee samenhangende (potentiële) integriteitskwesties expliciet als argument(en) om geen cryptotelefoon te gebruiken in het contact met cliënt(en). Deze respondenten wijzen op het feit dat de toestellen met name worden gebruikt binnen criminele organisaties, ‘het is echt voor boeven’, en geven aan dat dit imago voor hen een van de redenen is om niet met een dergelijk toestel te willen communiceren.

> ‘Beeldvorming, je komt ineens in een massa van gesprekken terecht, wat eigenlijk alleen maar criminelen zijn, daar zit jouw berichtje dan tussen.’

> ‘Omdat het in een kwade reuk staat, vanuit het Openbaar Ministerie wordt gezegd en uit rechtspraak blijkt dat het eigenlijk alleen wordt gebruikt, met name wordt gebruikt door criminelen en wordt opgezet door criminelen. Dus als je daar aan meedoet dan ga je al mogelijk de grens over.’

Het gebruik van een cryptotelefoon wordt door een deel van deze respondenten geassocieerd met de (de schijn van) betrokkenheid bij criminele activiteiten. Ze wijzen op het gevaar dat een advocaat te dicht op zijn of haar cliënt(en) zou komen te staan door met een cryptotelefoon te communiceren. Door het gebruik van een cryptotelefoon zou de schijn worden gewekt dat de advocaat betrokken is bij ‘het voortraject’ van criminele activiteiten of bereid is om cliënten van ‘verdergaande adviezen’ te voorzien. Enkele advocaten geven aan dat ze collega’s kennen die zich ‘zorgen maken’ over de cryptotelefoon-operaties.

> ‘Alleen krijgt het natuurlijk al wel vrij snel een beetje de schijn van "bespreek je nou nog meer vertrouwelijk dan waar de vertrouwelijkheid voor bedoeld is?" en daar heb ik wel bij willen wegblijven denk ik.’

> ‘Wij staan mensen bij die verdacht worden van strafbare feiten en verhoord worden mogelijk, maar we geven geen advies aan criminele organisaties.’

> ‘En nogmaals, er zijn er ook een aantal waarvan ik weet dat zij zich zorgen maken of er nog iets gaat komen ofwel vanuit de orde, ofwel vanuit het OM.’

> ‘De collega's die ik ken die het hebben gebruikt die doen of alsof ze niet meer weten wat hun adres is richting de orde, dan weet je hoe laat het is.’

Andere respondenten zijn zich bewust van het criminele imago van de cryptotelefoon maar geven aan dat dit imago niet direct gepaard hoeft te gaan met risico’s betreffende de integriteit of onafhankelijkheid

van een advocaat. Immers, cliënten kunnen belang hebben bij extra beveiligde communicatie en het zoeken naar manieren en middelen om de communicatie met cliënten vertrouwelijk en uit de handen van de strafvorderlijke overheid te houden, is inherent aan het werk van een (strafrecht)advocaat. Het imago van de cryptotelefoon zou op zichzelf voor deze respondenten daarom geen argument zijn om een dergelijk toestel niet te gebruiken. Deze respondenten onderkennen wel andere gevaren van het communiceren met een cryptotelefoon en noemen de recente cryptotelefoon-operaties als argument om niet met een cryptotelefoon te willen communiceren. Wanneer de server van een cryptodienst door overheden is gehackt of in beslag is genomen, bestaat het risico dat de communicatie tussen advocaat en cliënt er niet uit wordt gefilterd als vertrouwelijke communicatie. Dit risico kan onder andere ontstaan wanneer een advocaat heeft gecommuniceerd onder een (identiteitsversluierende) *nickname* en daardoor niet herkenbaar is als geheimhouder.[218]

5.5.2 Praktische overwegingen: kosten en gebruiksvriendelijkheid

Tot slot zijn de geïnterviewde advocaten gevraagd naar overige praktische overwegingen om bepaalde extra beveiligde communicatie middelen wel of niet te gebruiken.

Kosten lijken geen rol te spelen bij de overweging om een extra beveiligd communicatiemiddel wel of niet te gebruiken. Aan de meeste extra beveiligde chatapplicaties en e-mailproviders die door de advocaten worden gebruikt zijn geen of relatief weinig kosten verbonden. Financiële overwegingen spelen daarom logischerwijs bij dit soort middelen vaak geen rol. De kosten voor (het gebruik van) een cryptotelefoon kunnen daarentegen oplopen tot achthonderd tot duizend euro per half jaar. Hoewel advocaten op de hoogte zijn van deze hoge kosten, geven alle bevraagde advocaten aan dat kosten geen rol spelen bij de (hypothetische) overweging om een cryptotelefoon wel of niet aan te schaffen. Kosten zouden ofwel op de cliënt kunnen worden verhaald ofwel als bedrijfskosten kunnen worden weggeschreven.

In tegenstelling tot de kosten kan gebruiksvriendelijkheid wel een rol spelen bij het kiezen voor een wel of niet beveiligde optie. Dit geldt met name waar het gaat om het versturen van extra beveiligde e-mails. Een groot deel van de respondenten geeft aan Zivver onhandig te vinden in het gebruik. Zo geeft een van de advocaten aan niet goed met Zivver te kunnen werken, de 'gebruiksonvriendelijkheid' van de e-mailprovider zou hierbij een rol spelen. Een andere advocaat geeft aan 'gemakshalve zonder Zivver' e-mails te versturen en door vier andere advocaten wordt het mailen met Zivver omschreven als 'gedoe', 'irritant', 'praktisch heel onhandig' of zelfs 'een ramp'. De gebruiksonvriendelijkheid van Zivver speelt, met name bij de advocaten die veel e-mailcontact hebben met hun cliënten, een rol bij de keuze om niet (altijd) beveiligd te mailen. Het mailen met Zivver, dat gebruik maakt van extra wachtwoorden, zou te veel tijd en moeite kosten. Daarbij kan bovendien meespelen dat e-mails of bestanden die via Zivver worden verstuurd niet rechtstreeks in het door de advocaat gebruikte dossiersysteem kunnen worden opgeslagen.

---

218 Zie over dit risico uitgebreider par. 6.5.

5.6 Conclusie

Uit de interviews met advocaten komt het beeld naar voren van een beroepsgroep die zich sterk bewust is van het recht op en het belang van vertrouwelijke communicatie. Daarbij ligt de nadruk op het voorkomen van inbreuken op de geheimhouding door de strafvorderlijke overheid. De advocaten maken bewuste keuzes in de wijze waarop zij informatie delen. Als uitgangspunt geldt daarbij voor de meeste respondenten dat zij er de voorkeur aan geven om gevoelige informatie in persoon te bespreken. Er kunnen echter allerlei redenen zijn waarom een persoonlijke bespreking niet (altijd) mogelijk is. Deels afhankelijk van het type praktijk kiezen respondenten dan voor een communicatiemiddel dat zowel praktisch goed bruikbaar is, als (voldoende) veilig. De wens van de cliënt speelt daarbij voor veel advocaten een belangrijke rol. Omdat de meesten de behoefte van hun cliënten aan (extra) beveiligde communicatie als volstrekt legitiem ervaren, zijn zij vaak bereid om een communicatiemiddel te gebruiken waaraan de cliënt de voorkeur geeft. Daarbij speelt mee dat veel advocaten ten minste een zekere scepsis, zo niet een uitgesproken wantrouwen hebben ten opzichte van de naleving van de waarborgen rondom het verschoningsrecht door de (strafvorderlijke) overheid. Bij de beslissing om al dan niet mee te gaan in de wens van de cliënt geldt wel als voorwaarde dat zij dit kunnen verenigen met hun eigen – uit onder meer de gedragsregels voortvloeiende – (geheimhoudings)verplichtingen. Dat vergt soms een afweging van verschillende belangen, waarbij zich dilemma's kunnen voordoen.

Een eerste dilemma hangt samen met het feit dat optimale geheimhouding op gespannen voet kan staan met de praktische realiteit. Zo blijkt de ervaren gebruiksonvriendelijkheid van extra beveiligde e-mailapplicaties een zodanig obstakel dat het niet of minder wordt gebruikt dan (sommige) advocaten eigenlijk noodzakelijk of wenselijk vinden. Ook kan worden gedacht aan de situatie dat een cliënt in het buitenland verblijft, waardoor advocaten moeten teruggrijpen op communicatiemiddelen die zij uit oogpunt van vertrouwelijkheid minder veilig achten (zoals telefoon of e-mail).

Een ander spanningsveld is gelegen in de – uit (soms terecht) wantrouwen in de vertrouwelijkheid van gangbare communicatiemiddelen voortkomende – vraag naar extra beveiliging, en het risico dat daarmee juist de waarborging van het verschoningsrecht in het geding komt. Hoewel het minder eenvoudig is om toegang te krijgen tot de inhoud van extra beveiligde communicatie, kan de extra beveiliging onder omstandigheden er ook voor zorgen dat het niet direct duidelijk is dat het gaat om communicatie met een geheimhouder. Die spanning is met name zichtbaar bij het gebruik van cryptotelefoons nu de afgelopen jaren verschillende servers zijn gehackt. In zoverre moet uit oogpunt van vertrouwelijkheid dus een onderscheid worden gemaakt tussen inhoud en identiteit: waar de inhoud van de communicatie in hoge mate kan worden afgeschermd, moet de identiteit van de betrokken advocaat zoveel mogelijk kenbaar zijn om de waarborgen rondom het verschoningsrecht te kunnen naleven. Dat is bij sommige extra beveiligde communicatiemiddelen niet vanzelfsprekend.

6. Knelpunten en risico's

6.1 Inleiding

Naast het krijgen van inzicht in het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten en hun beweegredenen hiervoor, beoogt dit onderzoek een beeld te geven van de risico's die hiermee samenhangen, mede in het licht van de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten (deelvraag 5). Verschillende uit die interviews voortvloeiende inzichten worden in dit hoofdstuk nader tegen het licht gehouden. Verder wordt het beeld van die risico's en knelpunten in dit hoofdstuk uitgediept en aangevuld met informatie uit andere bronnen. Zo zijn verschillende documenten geanalyseerd, waaronder de Gedragsregels advocatuur en werkwijzen, handleidingen en overige (beleids)documenten die inzicht geven in de opsporingspraktijk. Daarnaast wordt geput uit het interviews met lokale dekens en de interviews met de medewerker(s) van het NFI en het OM, en uit de schriftelijke informatie van het landelijk dekenberaad en het OM. De op basis van deze gecombineerde bevindingen geïdentificeerde risico's en knelpunten worden hierna besproken. Daarbij is duidelijk geworden dat deze zich vooral voordoen bij het gebruik van cryptotelefoons, zodat daarop in de navolgende bespreking de nadruk zal liggen. Wanneer de risico's (ook) betrekking hebben op andere communicatiemiddelen wordt dit steeds aangegeven. In paragraaf 6.2 wordt ingegaan op de integriteit van advocaten. Paragraaf 6.3 behandelt de risico's voor de onafhankelijkheid. In paragraaf 6.4 worden de risico's voor de documentatieplicht van advocaten uiteengezet, in paragraaf 6.5 komt de geheimhoudingsplicht aan bod.

6.2 Integriteit

In artikel 10a Advocatenwet zijn de kernwaarden van de advocaat neergelegd. Naast de in dit onderzoek al meermaals genoemde plicht tot geheimhouding worden daar onafhankelijkheid, partijdigheid, deskundigheid en integriteit genoemd. Hierna wordt eerst uiteengezet wat wordt verstaan onder integriteit (par. 6.2.1), vervolgens wordt op de in dit verband relevante risico's en knelpunten ingegaan (par. 6.2.2).

6.2.1 Betekenis integriteit

De kernwaarde van integriteit wordt in verband gebracht met de norm dat iedere advocaat zich 'betamelijk' dient te gedragen.[219] Integriteit kent verschillende aspecten en het is dan ook niet goed mogelijk om hiervan een eenduidige definitie te geven.[220] Het begrip hangt in ieder geval samen met het uitgangspunt dat beroepsbeoefenaars zich gedragen in overeenstemming met de verantwoordelijkheid die zij uit hoofde van hun functie en positie dragen, waarbij taken adequaat, zorgvuldig, en betrouwbaar

219 Zie ook (het negatief geformuleerde) art. 46 Advw. als grondslag voor tuchtrechtelijke aansprakelijkheid.
220 Vgl. uitgebreider Heuvel, Huberts & Muller (red.) 2012, i.h.b. deel I.

worden uitgevoerd en rekening wordt gehouden met alle in het geding zijnde belangen.[221] Voor advocaten betekent dit onder meer dat de advocaat zich richt op de belangen van de cliënt, z/hij onafhankelijk is en z/hij zich kan verantwoorden voor de gemaakte keuzes, mede gelet op bredere belangen zoals een goede rechtsbedeling, waaraan z/hij immers een belangrijke bijdrage levert.[222] Integriteit hangt dus sterk samen met andere advocatuurlijke kernwaarden, en betekent vanzelfsprekend ook dat een advocaat handelt binnen de kaders die het recht, waaronder het tucht- en strafrecht, bieden. Een ander belangrijk kenmerk van integriteit is dat het sterk is verbonden met het vertrouwen dat in beroepsbeoefenaars wordt gesteld.[223] Het gaat dan nadrukkelijk om het maatschappelijke belang van een betrouwbare en fatsoenlijke advocatuur en de noodzaak dat er vertrouwen is in het goede functioneren van de beroepsgroep, mede gelet op de bijzondere rechten en verplichtingen die aan het beroep van advocaat zijn verbonden.[224] Eén van de in dit verband relevante privileges is het verschoningsrecht, waar de noodzaak van integer handelen zich dan ook nadrukkelijk laat voelen.[225]

6.2.2 Risico's en knelpunten voor integriteit

Risico's met betrekking tot de kernwaarde integriteit kunnen zich bij het gebruik van cryptotelefoons door advocaten op verschillende manieren voordoen. Deze risico's hangen sterk samen met het gegeven dat cryptotelefoons vooral binnen criminele netwerken worden gebruikt en daardoor een bepaald imago hebben gekregen. Sommige geïnterviewde advocaten wijzen bijvoorbeeld op de schijn van ontoelaatbaar of zelfs strafbaar handelen die kan ontstaan wanneer advocaten (ook) met dergelijke toestellen communiceren (zie par. 5.5.1) of de schijn dat de advocaat te dicht bij de cliënt komt, bijvoorbeeld doordat de advocaat kennis krijgt van zaken die z/hij voor het vervullen van haar/zijn rol als rechtsbijstandverlener eigenlijk niet wil of hoeft te weten.

> 'Maar het heeft nog een ander heel vervelend effect en dat is dat klanten denken dat ze op een lijn zitten waarop ze alles kunnen maken. Dus ze gaan jou dingen schrijven die jij helemaal niet wil horen, die je helemaal niet wil weten. En daar moet je dan weer op reageren en wat kan er dan gebeuren, dan kan zo'n berichtje van jou opeens doorgestuurd worden in een andere PGP-chat en dan gaat jouw bericht een eigen leven leiden.'

> 'Het is een manier van omgaan met cliënten die ik überhaupt niet ambieer. Ik heb niets te maken met de snode plannetjes van deze mensen.'

Voornoemde potentiële risico's die samenhangen met het criminele imago van cryptotelefoons zouden in mindere mate ook aan de orde kunnen zijn bij het gebruik van bepaalde chatapps. Zo wordt het gebruik van Telegram soms wel in verband gebracht met criminaliteit. Een van de respondenten verwijst

---

221 Karssing 2006, p. 12.

222 Vgl. *Kamerstukken II* 2009/10, 32382, nr. 3, p. 10.

223 Karssing 2006, p. 17-18. Zie voor dat verband tussen het vertrouwen in de beroepsgroep en de onbetamelijkheid van het handelen bijv. ook Hof van Discipline 2 juni 2023, ECLI:NL:TAHVD:2023:59, par. 5.42.

224 Zie ook 'Integriteit', advocatenorde.nl.

225 Vgl. *Een maatschappelijke orde* 2006, p. 20. Het was onder meer dit rapport dat aanleiding gaf tot het in 2015 opnemen van de vijf kernwaarden in de Advocatenwet (met de Wet positie en toezicht advocatuur (*Stb.* 2014, 354)).

naar door de politie opgemaakte processen-verbaal waarin de constatering dat een verdachte gebruikmaakt van Telegram wordt gepresenteerd als ondersteuning van de verdenking van betrokkenheid bij strafbare feiten. Ook werd recent nog opgeroepen tot een verbod op Telegram omdat dit platform criminele gedragingen zou faciliteren.[226]

Tegelijkertijd wordt door de dekens en vanuit de zijde van het OM aangegeven dat eventuele risico's voor de integriteit toch vooral los van het gebruik van een extra beveiligd communicatiemiddel moeten worden gezien. Zij zien, met andere woorden, geen duidelijke relatie tussen een al dan niet integere rolvervulling en de wijze waarop wordt gecommuniceerd. Er zullen immers altijd advocaten zijn die niet integer handelen. Bovendien, of een advocaat al dan niet integer zal handelen is niet afhankelijk van het communicatiemiddel maar van de wijze waarop de advocaat met dit communicatiemiddel omgaat. Daarbij wordt ook gewezen op de mogelijkheid dat dit te maken heeft met uitgeoefende druk. Zo wordt het voorbeeld genoemd van advocaten die onder dwang hun geheimhoudertelefoon door (relaties van) hun cliënten laten gebruiken. Daarnaast zouden cliënten zich ook vrijer kunnen voelen om via een afgeschermde communicatielijn, zoals een cryptotelefoon, druk op de advocaat te kunnen uitoefenen. Inmiddels is de mate van beveiliging en afscherming van andere communicatiemiddelen (in het bijzonder bepaalde chatapplicaties) echter ook van dien aard, dat dit risico niet beperkt is tot cryptotelefoons.

Dit betekent niet dat het gebruik van cryptotelefoons helemaal geen risico's voor de integriteit mee kan brengen. Mogelijke risico's hangen vooral samen met het feit dat ook het waarborgen van het vertrouwen in de beroepsgroep onderdeel is van de kernwaarde integriteit. Ook wanneer de advocaat de vereiste zakelijke distantie in de communicatie met een cryptotelefoon weet te bewaren en zich daarbij beweegt binnen de tucht- en strafrechtelijke grenzen, blijft een risico bestaan voor de integriteit. De beeldvorming van cryptotelefoons als communicatiemiddel van criminelen en het (mogelijk geheel misplaatste) onderbuikgevoel dat de advocaat die van een dergelijk middel gebruikmaakt ook over grenzen gaat, kan het vertrouwen in de advocatuur immers schaden. Daarbij komt dat het voor advocaten gelet op de geheimhoudingsplicht vaak niet goed mogelijk is om een dergelijke zweem van verdachtmaking weg te nemen.

> 'Je roept toch een beeld op dat je deel gaat uitmaken van een groep die maar één reden heeft om dat instrument te gebruiken.'[227]

6.3 Onafhankelijkheid

6.3.1 Betekenis onafhankelijkheid

Iedere advocaat wordt geacht in zijn beroepsuitoefening onafhankelijk te zijn, zo schrijft artikel 10a lid 1 sub a Advocatenwet voor. Het gaat daarbij om onafhankelijkheid van de (strafvorderlijke) overheid,

---

226 Rensen 2023. Het vermeende 'criminele imago' van Telegram lijkt echter van een andere orde dan dat van cryptotelefoons.

227 Quote afkomstig van een van de geïnterviewde (oud of huidig) dekens.

de rechterlijke macht, andere (proces)partijen én van de cliënt. Door de NOvA wordt onafhankelijkheid als eerste kernwaarde omschreven en in verband gebracht met de eerlijkheid van het proces en een efficiënte rechtsbedeling.[228] Het uitgangspunt is ook neergelegd in Gedragsregel 2 en wordt voorts in verschillende internationale documenten erkend.[229] Waar het gaat om de onafhankelijkheid ten opzichte van de cliënt wordt deze kernwaarde zo uitgelegd dat de advocaat voldoende afstand bewaart tot de cliënt en zijn persoonlijke belangen geen rol spelen bij de behandeling van een zaak. Deze onafhankelijkheid zorgt ervoor dat de advocaat grenzen kan trekken en stelt hem/haar in staat om te beslissen op welke wijze de belangen van de cliënt het beste kunnen worden behartigd. Daarbij hoort ook dat de advocaat ervoor zorgt dat de hem/haar toegekende privileges op de juiste wijze worden gebruikt.[230] Een te hechte persoonlijke relatie kan afbreuk doen aan de onafhankelijkheid, maar in algemene zin is ook gewezen op de invloed van de toegenomen marktwerking en commercialisering. Het daarmee gepaard gaande belang van werving en behoud van cliënten kan de ruimte voor advocaten om grenzen te stellen en de koers te bepalen beperken.[231]

6.3.2 Risico's en knelpunten voor onafhankelijkheid

Risico's voor de onafhankelijkheid kunnen zich bij het gebruik van cryptotelefoons vooral manifesteren waar het gaat om de situatie dat advocaten dergelijke toestellen van hun cliënten of van cryptotelefoonaanbieders ontvangen. In zaken waarin het gaat om de grotere onderzoeken naar georganiseerde (drugs)criminaliteit en daarmee samenhangende (gewelds)delicten werden zulke telefoons inderdaad aan advocaten aangeboden, zo blijkt uit de interviews (zie par. 5.4.2). Wanneer advocaten zo'n telefoon aannemen kan dat in verschillende opzichten afbreuk doen aan hun onafhankelijkheid ten opzichte van de cliënt.

In de eerste plaats lijkt het vaak de cliënt die aangeeft van welke cryptocommunicatiedienst z/hij gebruikmaakt. Daarbij is van belang dat veel cryptocommunicatiediensten (op enig moment) de functionaliteit van het toestel zo hebben ingericht dat uitsluitend communicatie met toestellen van dezelfde aanbieder mogelijk is. Om te kunnen blijven communiceren met alle cliënten moet een advocaat dan dus meerdere toestellen hebben. Er kan dan dus een situatie ontstaan waarin niet de advocaat maar de cliënt bepaalt op welke wijze er wordt gecommuniceerd.

> 'En het andere punt is, en dat raakt er natuurlijk wel een beetje aan, dat ik uiteindelijk niet afhankelijk wil zijn van mijn cliënten en de wijze waarop zij willen communiceren. Uiteindelijk wil ik gewoon zelf de controle ook daarover houden.'

---

228 'Onafhankelijkheid', advocatenorde.nl.

229 O.m. art. 16 United Nations Basic Principles on the Role of Lawyers, adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August to 7 September 1990, U.N. Doc. A/CONF.144/28/Rev.1 at 118 (1990)2; art. 1 Model Code of Conduct for European Lawyers, Council of Bars and Law Societies of Europe (CCBE).

230 *Kamerstukken II* 2009/10, 32382, nr. 3, p. 9.

231 Vgl. *Een maatschappelijke orde* 2006, p. 25-26.

Een tweede manier waarop de onafhankelijkheid in het gedrang kan komen hangt samen met het aannemen van een door de cliënt aangeboden telefoon, nu zowel het toestel als het daarbij horende abonnement een zekere financiële waarde vertegenwoordigt. Wanneer deze kosten (deels) door de cliënt worden gedragen kan dat vragen oproepen over hoe deze vergoeding moet worden gewaardeerd en verantwoord, in aanmerking genomen dat het de advocaat niet altijd vrij staat om zo'n vergoeding aan te nemen, bijvoorbeeld wanneer sprake is van door de Raad voor Rechtsbijstand gefinancierde bijstand.[232] Wordt zo'n telefoon toch aangenomen, dan maakt de advocaat zich in zekere zin afhankelijk van zijn cliënt en wordt z/hij bovendien in integriteitsopzicht kwetsbaar.

Ten derde kan hier worden gewezen op een mogelijk risico voor de onafhankelijkheid dat weliswaar niet rechtstreeks wordt veroorzaakt door het gebruik van cryptotelefoons, maar daarmee door enkele respondenten wel in verband wordt gebracht. Het gaat daarbij om de situatie dat je als advocaat niet zozeer één client bijstaat maar in meer of mindere mate diensten verleent aan een criminele organisatie. Dit risico zou groter kunnen zijn bij het gebruik van cryptotelefoons omdat de advocaat daarbij met leden van zo'n criminele groepering in een afgeschermde chatgroep terecht kan komen. Een risico voor de onafhankelijkheid is dan gelegen in het feit dat daarbij zoveel verschillende – en mogelijk met de belangen van de cliënt strijdige – aspecten een rol gaan spelen, dat de advocaat niet of minder goed in staat is om grenzen te stellen en de in zijn optiek (voor de individuele cliënt) beste koers te varen. Dat risico is vanzelfsprekend nog sterker wanneer er van die criminele organisatie druk, drang of dwang uitgaat. Overigens zal duidelijk zijn dat een dergelijke situatie, waarin de advocaat mogelijk niet (alleen) de belangen van de individuele cliënt dient, ook problematisch kan zijn in het licht van de kernwaarde partijdigheid.[233] Tegelijkertijd is ook dit risico niet beperkt tot cryptotelefoons, een advocaat kan immers ook in een afgeschermde appgroep van Telegram terechtkomen en via deze appgroep een criminele organisatie bijstaan. Bovendien geldt ook bij dit potentiële risico dat er geen duidelijke relatie bestaat tussen een al dan niet onafhankelijke rolvervulling en de wijze waarop wordt gecommuniceerd. Of een dergelijk risico voor de onafhankelijkheid ontstaat is immers niet afhankelijk van het communicatiemiddel, maar van de wijze waarop de betreffende advocaat gebruik maakt van dit communicatiemiddel.

6.4 Documentatieplicht

6.4.1 Inhoud documentatieplicht

Advocaten zijn gehouden belangrijke informatie en afspraken vast te leggen en te bewaren in een dossier. Deze verplichting vloeit voort uit Gedragsregel 16 lid 1, dat luidt: 'De advocaat dient zijn cliënt op de hoogte te brengen van belangrijke informatie, feiten en afspraken. Ter voorkoming van misverstand, onzekerheid of geschil, dient hij belangrijke informatie en afspraken schriftelijk aan zijn cliënt te

[232] Zie gedragsregel 18 lid 2 Gedragsregels advocatuur. Een dergelijke telefoon is ook als gift niet toelaatbaar, nu de advocaat slechts giften van 'geringe financiële waarde' mag aannemen, zoals een bos bloemen of een fles wijn, vgl. Hof van Discipline 7 december 2018, ECLI:NL:TAHVD:2018:214.

[233] Omdat de partijdigheid bij het gebruik van extra beveiligde communicatiemiddelen in het algemeen veel minder (potentieel) in het geding is, wordt deze kernwaarde hier verder niet uitgewerkt.

bevestigen.' Het gaat daarbij in ieder geval om informatie over de kansen, risico's en kosten van door de advocaat verleende bijstand, alsook afspraken over de gekozen processtrategie.[234] Achtergrond hiervan is dat onduidelijkheid over wat er tussen advocaat en cliënt is afgesproken zoveel mogelijk wordt voorkomen.[235] In geval adequate vastlegging ontbreekt en daardoor in een eventuele tuchtzaak niet kan worden vastgesteld of de cliënt voldoende is geïnformeerd, is dat een omstandigheid die voor risico van de advocaat komt.[236] Vastlegging kan overigens ook gebeuren met behulp van 'digitale media, zoals e-mail', blijkt uit de toelichting op Gedragsregel 16. Daarnaast dienen advocaten ervoor zorg te dragen dat dossiers snel vindbaar zijn en dat relevante gegevens daarin overzichtelijk en toegankelijk zijn weergegeven (art. 31 Regeling op de advocatuur).[237]

6.4.2 Risico's en knelpunten voor de documentatieplicht

De hiervoor beschreven documentatieplicht kan in het geding zijn wanneer advocaten over belangrijke zaken met hun cliënten communiceren via cryptotelefoons en bepaalde chatapps. Op zichzelf is dit een vorm van digitale communicatie die kán worden vastgelegd, zodat het gebruik van deze middelen niet per definitie strijdig is met de documentatieplicht. Wel kan het vastleggen van deze communicatie praktisch minder eenvoudig zijn, bijvoorbeeld wanneer sprake is van verdwijnende berichten.[238] Bovendien bieden niet alle chatapps de mogelijkheid om chats eenvoudig te exporteren en vervolgens in het dossier op te slaan. Zodanige vastlegging kan dan nog steeds door middel van bijvoorbeeld het maken van screenshots, maar is wel omslachtig. Zeker wanneer veel communicatie op deze wijze plaatsvindt, laat het zich goed denken dat adequate vastlegging in de praktijk niet of niet optimaal plaatsvindt. Bij het gebruik van cryptotelefoons geldt nog als bijkomende complicatie dat het gaat om verschillende aanbieders, waarbij doorgaans kortdurende abonnementen worden verstrekt, zodat gebruikers geregeld meerdere (tijdelijke) toestellen hebben.

> 'Ik heb van alle advocaten die PGP-berichten hadden te horen gekregen "die heb ik niet meer want ik heb die telefoon weggedaan, dus het is niet meer te achterhalen wat ik heb gedaan". Ook dat moet je als toezichthouder zeggen, in strijd met je verplichting om een volledig dossier bij te houden. Geldt overigens ook voor WhatsApp wat vaak verdwijnt.'[239]

Dit risico kan enigszins worden gerelativeerd doordat de advocaat allerminst verplicht is om alle communicatie met een cliënt te bewaren. Daarbij komt dat het gebruik van een cryptotelefoon of chatapplicatie voor het uitwisselen van (inhoudelijke) informatie er op zichzelf niet aan in de weg staat dat belangrijke afwegingen, keuzes en afspraken vervolgens op een andere schriftelijke wijze (per brief of

---

234 Zie de toelichting op regel 16 Gedragsregels advocaat, bijv. Raad van Discipline Arnhem-Leeuwarden 10 juli 2023, ECLI:NL:TADRARL:2023:193.

235 Toelichting op regel 16 Gedragsregels advocatuur.

236 Bijv. Hof van Discipline 21 januari 2022, ECLI:NL:TAHVD:2022:7.

237 Zie verder voor verplichtingen met betrekking tot het dossier- en zaaksbeheer art. 6.4 Voda en art. 32 sub f Regeling op de advocatuur.

238 Bijvoorbeeld de mogelijkheid om automatisch berichten na enige tijd te verwijderen bij WhatsApp *'Dissappearing messages'*; Signal 'Verlopende berichten' en Telegram '*Self-destructing messages*'.

239 Quote afkomstig van een van de geïnterviewde (oud of huidig) dekens.

e-mail) aan de cliënt worden bevestigd. Of dat praktisch gezien ook haalbaar is valt evenwel te betwijfelen: de cliënt moet dan immers wel op andere wijze te bereiken zijn en ermee instemmen dat afspraken zo worden vastgelegd. Nu een belangrijke reden om cryptotelefoons te gebruiken is dat de cliënten alleen deze communicatiemiddelen nog vertrouw(d)en, lijkt dat niet zonder meer aannemelijk.

6.5 Geheimhoudingsplicht

6.5.1 Geheimhoudingsplicht en communicatiemiddelen

De geheimhoudingsplicht is onder andere neergelegd in Gedragsregel 3 en schrijft voor dat advocaten 'passende maatregelen' dienen te nemen teneinde de vertrouwelijkheid van de communicatie te waarborgen. Voor een meer algemene uiteenzetting van de geheimhoudingsplicht van advocaten wordt verwezen naar paragraaf 4.2.2. Hierna wordt vooral ingegaan op de geheimhoudingsplicht in relatie tot de keuze voor een bepaald communicatiemiddel.[240] Uit de toelichting op Gedragsregel 3 blijkt dat van de advocaat zorgvuldigheid mag worden verlangd bij het maken van de keuze voor een specifiek medium en het niveau van beveiliging. De vraag rijst wat onder die zorgvuldigheid moet worden verstaan en welk communicatiemiddel, met het oog op de mate van beveiliging, het beste gebruikt kan worden. Het lijkt niet goed mogelijk om hierop een eenduidig antwoord te formuleren. Daarbij speelt mee dat er grote verschillen zijn in de praktijkvoering van advocaten die samenhangen met onder meer het rechtsgebied waarop de advocaat werkzaam is en het type cliënt waarmee de advocaat te maken heeft. Ook het soort informatie dat wordt uitgewisseld lijkt daarbij relevant. Wel schrijft artikel 6.11 Voda voor dat de advocaat voor vertrouwelijke communicatie gebruik maakt van het opgegeven geheimhoudernummer, 'tenzij zwaarwegende omstandigheden zich daartegen verzetten'. Op wat voor soort zwaarwegende omstandigheden wordt gedoeld is niet duidelijk. Bovendien lijkt de verplichting om voor vertrouwelijke communicatie het geheimhoudernummer te gebruiken te worden afgezwakt door een aantal door de NOvA gegeven tips voor vertrouwelijke internetcommunicatie, waarin onder meer wordt aangegeven dat de telefoon geschikt is 'voor het maken van afspraken en dergelijke, niet voor het delen van inhoudelijke en vertrouwelijke informatie'.[241] Andere verplichtingen voor advocaten om van een specifiek medium wel of geen gebruik te maken zijn er niet. Wel wordt door de NOvA in de hiervoor al genoemde tips voor vertrouwelijke internetcommunicatie onder andere aangeraden om als advocaat gebruik te maken van een privacy-vriendelijke chatapplicatie, en wordt afgeraden om vertrouwelijke informatie uit te wisselen via onbeveiligde e-mail. Dit zijn echter, aldus de NOvA, vrijblijvende suggesties die advocaten naar eigen inzicht kunnen gebruiken.[242] Bovendien worden er geen specifieke privacy vriendelijke chatapplicaties of (beveiligde) e-mailproviders aangeraden.

Uit de interviews blijkt dat er onder advocaten verschillend wordt gedacht over de mate van beveiliging en de risico's van verschillende communicatiemiddelen. Een deel van de respondenten kiest bewust voor Signal in plaats van WhatsApp omdat Signal meer waarborgen zou bieden. Andere respondenten zijn

240 Regel 3 lid 2 Gedragsregels advocatuur.
241 'Vertrouwelijke internetcommunicatie', advocatenorde.nl.
242 'Vertrouwelijke internetcommunicatie', advocatenorde.nl.

van mening dat het gebruik van Signal geen toegevoegde waarde heeft. Een groot deel van de advocaten lijkt echter niet te beschikken over grondige (technische) kennis over de beveiligingswaarborgen- en risico's van bepaalde communicatiemiddelen. In combinatie met bepaalde – soms door wat afwijkende motieven ingegeven – voorkeuren van cliënten kan dat ertoe leiden dat advocaten soms enigszins onzeker zijn over waar zij bij de keuze voor een communicatiemiddel goed aan doen. Er is bovendien geen consensus over de vraag welke chatapplicatie het beste gebruikt kan worden.

Het OM lijkt, zo blijkt uit de gegeven schriftelijke reactie, vraagtekens te stellen bij het gebruik van bepaalde (extra beveiligde en/of identiteitsversluierende) communicatiemiddelen door advocaten. Het is, aldus het OM, niet enkel de vraag of het gebruik van cryptotelefoons, WhatsApp, Signal, Telegram, Skype en bepaalde e-mailproviders zoals Gmail of Hotmail 'voldoen aan de mate van afscherming die op grond van de gedragsregels vereist is'. In de schriftelijke reactie wordt gewezen op het feit dat de verzamelde data veelal wordt opgeslagen bij derden en dat daaraan risico's zijn verbonden in het kader van het waarborgen van de vertrouwelijkheid.[243] Het OM werpt in de schriftelijke reactie de vraag op of het gebruik van andere communicatiemiddelen dan de geheimhoudertelefoon 'past binnen de geheimhoudingsplicht van de advocaat'. Advocaten zouden zelf kiezen voor 'een minder zekere afscherming' wanneer zij, in plaats van bellen via het systeem van nummerherkenning, bellen, chatten en/of mailen via een ander communicatiemiddel. Uit het interview met het OM blijkt dat de 'minder zekere afscherming' ook te maken heeft met verschillende (technische en/of praktische) onmogelijkheden om geheimhouderinformatie uit bepaalde communicatielijnen te filteren.

Dat de geheimhoudingsplicht met zich meebrengt dat advocaten zorgvuldig moeten omgaan met digitale communicatie en de beveiliging daarvan, daar lijken alle partijen het met elkaar over eens te zijn. Wat deze zorgvuldigheid vervolgens in concrete gevallen inhoudt en welke communicatiemiddelen advocaten het beste kunnen gebruiken om de vertrouwelijkheid van de communicatie te waarborgen, daarover lijkt nog geen duidelijkheid te bestaan.

6.5.2 Risico's geheimhoudingsplicht: inbreuken op het verschoningsrecht door overheidsinstanties

Het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen kan verschillende risico's voor de geheimhouding met zich mee brengen. Uit de interviews met advocaten blijkt dat men zich binnen de strafrechtadvocatuur met name bewust is van de potentiële inbreuken op het verschoningsrecht door de strafvorderlijke overheid. In het navolgende volgt daarom allereerst een opsomming van verschillende risico's voor de geheimhouding, geïdentificeerd vanuit het perspectief van de opsporing (OM), de techniek (NFI) en de advocatuur zelf. In paragraaf 6.5.3 worden vervolgens verschillende risico's voor de geheimhouding behandeld die verband houden met potentiële inbreuken op de vertrouwelijkheid door derde partijen, niet zijnde overheidsinstanties.

---

[243] Het OM lijkt te doelen op het gevaar van potentiële inbreuken door derde partijen, niet zijnde overheidsinstanties. Zie par. 6.5.3 over de risico's met betrekking tot het waarborgen van de vertrouwelijkheid tegenover derden.

6.5.2.1 'Criminele communicatiemiddelen' als opsporingsdoelwit

Het omzeilen van extra beveiliging, met name encryptie, speelt een steeds grotere rol in de opsporing van strafbare feiten en heeft de afgelopen jaren tot grote doorbraken geleid in meerdere strafrechtelijke onderzoeken.[244] Binnen (georganiseerde) criminele netwerken worden bepaalde extra beveiligde en/of identiteitsversluierende communicatiemiddelen, met name cryptotelefoons, veel gebruikt.[245] In het kader van de opsporing en vervolging van strafbare feiten en, meer specifiek, de aanpak van georganiseerde criminaliteit, zijn de afgelopen jaren verschillende servers van cryptocommunicatiediensten inbeslaggenomen of gehackt.[246] De strafvorderlijke overheid heeft interesse in het neerhalen van bepaalde cryptocommunicatiediensten omdat die veel binnen criminele netwerken worden gebruikt. Dergelijke diensten (EncroChat, Sky-ECC, Exclu-Messenger) zullen dus sneller onderwerp worden van een hack of inbeslagname dan de meer reguliere platformen die (ook of met name) voor legitieme doeleinden worden gebruikt (WhatsApp, Signal etc.). Op het moment dat een advocaat gebruikmaakt van een platform waarvan de strafvorderlijke overheid meent dat die (vooral) door criminelen wordt gebruikt, is er dus een kans dat dit platform wordt neergehaald, waardoor de communicatie tussen advocaat en cliënt in de 'gehackte', 'inbeslaggenomen' of 'meegelezen' dataset zit en in opsporingsonderzoeken terechtkomt. In dergelijke gevallen zorgt het gebruik van een communicatiemiddel met sterke beveiligingsfunctionaliteiten juist voor minder veilige en vertrouwelijke communicatie tussen advocaat en cliënt. Advocaten kunnen, gelet op de geheimhoudingsplicht, vanuit deze optiek beter gebruik maken van een meer conventioneel communicatiemiddel dat wellicht minder beveiligingsfunctionaliteiten biedt, maar tegelijkertijd minder snel het doelwit zal worden van een hack of inbeslagname door opsporingsautoriteiten.

6.5.2.2 Herkenbaar als verschoningsgerechtigde 'aan de poort' bij gebruik (crypto)telefoon

Verschillende risico's houden verband met de herkenbaarheid van advocaten als zijnde verschoningsgerechtigde en het identificeren en filteren van verschoningsgerechtigde informatie in het opsporingsonderzoek. Teneinde verschoningsgerechtigde informatie goed uit een opsporingsonderzoek te kunnen filteren, dient het duidelijk te zijn dat het gaat om vertrouwelijke communicatie tussen advocaat en cliënt. Voor wat betreft telefonisch contact zorgt het systeem van nummerherkenning voor het uitfilteren van verschoningsgerechtigde informatie 'aan de poort'. Het OM benadrukt dat dit systeem het onmogelijk maakt om verschoningsgerechtigden te tappen.

In relatie tot het gebruik van cryptotelefoons door advocaten wijzen zowel de geïnterviewde dekens als (de medewerkers van) het OM en het NFI op de risico's voor de geheimhouding die ontstaan wanneer een advocaat gebruikmaakt van een cryptotelefoon met een pseudoniem of *nickname*. Indien de advocaat het gebruik van een cryptotelefoon niet formeel heeft gemeld en diens *nickname* niet heeft doorgegeven,

244 Zie ook par. 3.4.2.
245 Zie par. 3.4.1.
246 Zie par. 3.4.2.

is het voor de opsporingsautoriteiten bij een potentiële cryptotelefoon-operatie niet direct duidelijk dat het om communicatie van een verschoningsgerechtigde gaat. Het filteren van verschoningsgerechtigde communicatie voorafgaand aan het opsporingsonderzoek op basis van de gemelde *nickname*, is in dat geval niet mogelijk. Er bestaan ook andere manieren om een dataset te schonen voordat deze ter beschikking wordt gesteld aan een opsporingsteam. Het OM heeft in het kader van verschillende cryptotelefoon-operaties met behulp van software en een lijst met zoekwoorden geheimhouders onderkend en de geheimhouderinformatie uit de dataset gefilterd.

'[..] omdat we geen reacties hadden en er wel voor vreesden dat er geheimhoudersdata in zou zitten.'

De zaaksofficier en de rest van het onderzoeksteam kunnen, door een preventieve schoning, geen kennisnemen van de op basis van de woordenlijst gemarkeerde communicatie. Enkel de geheimhouderofficier kan deze communicatie inzien. Door het gebruik van een woordenlijst kon geheimhouderinformatie worden gefilterd, ondanks het feit dat geheimhouders zichzelf niet hadden gemeld. Een dergelijke filtering op basis van zoekwoorden is echter aanzienlijk ingewikkelder (en daardoor vermoedelijk ook minder volledig) dan een filtering op basis van gemelde gebruikersgegevens. Door de geïnterviewde dekens wordt dan ook benadrukt dat het gebruiken van een cryptotelefoon, zonder dat dit gemeld is, in strijd kan zijn met de geheimhoudingsplicht.

Hoeveel advocaten de gegevens van hun cryptotelefoon daadwerkelijk hebben aangeleverd bij het OM in het kader van de geheimhoudingsregeling, is niet geheel duidelijk geworden. Het gaat in ieder geval om niet meer dan enkele advocaten, zo blijkt uit de informatie van het landelijk dekenberaad en het OM. Ook een van de respondenten geeft aan dat veel collega's zich niet hebben willen melden.

'De meeste collega's waren heel erg bang, en achteraf gezien snap ik dat wel, om zich aan te melden.'

Bij het niet willen melden lijkt wantrouwen richting het OM en de werkwijze van het OM wat betreft verschoningsgerechtigde informatie, een rol te spelen. Door het OM wordt tevens gewezen op het feit dat meerdere advocaten zich op het standpunt hebben gesteld dat de gedragsregels zich verzetten tegen het formeel melden en doorgeven van de gebruikte *nickname*. Kenbaar maken van de gebruikte cryptotelefoongegevens zou er in die gedachtegang mogelijk toe leiden dat daarmee juist de aandacht op vertrouwelijke – en (daarmee) voor justitie interessante – informatie wordt gevestigd, waarbij het vertrouwen ontbreekt dat die informatie vervolgens (zonder daarvan kennis te nemen) onleesbaar wordt gemaakt. In zoverre zou juist het wél melden van deze gegevens 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. Ook zorgen om de eigen veiligheid kunnen daarbij een rol spelen, waarbij door een respondent wordt gewezen op de mogelijkheid dat cliënten verhaal komen halen bij de advocaat wanneer blijkt dat verschoningsgerechtigde communicatie toch is afgeluisterd of meegelezen. Daarbij moet wel worden opgemerkt dat er in dit onderzoek geen concrete voorbeelden van dit soort incidenten zijn gezien. Het niet willen melden hoeft dus geen signaal te zijn voor ontoelaatbaar handelen, maar dat kan wel. Ook zorgen over eventuele gevolgen wanneer advocaten in die communicatie gedrags- of strafrechtelijke normen hebben geschonden, kunnen immers

een reden zijn om de gebruikte cryptotelefoongegevens niet te delen. Uit de informatie van het OM blijkt dat er signalen zijn dat hiervan wel eens sprake is (geweest), maar in ieder geval niet op erg grote schaal. Duidelijk is in ieder geval dat wanneer de door advocaten gebruikte cryptotelefoongegevens niet worden gemeld, het risico bestaat dat pas na inhoudelijke kennisneming van de communicatie blijkt dat het om verschoningsgerechtigde informatie gaat.

6.5.2.3 Herkenbaar als verschoningsgerechtigde 'aan de poort' bij gebruik chatapplicatie en e-mail

Uit de interviews met advocaten blijkt dat advocaten naast telefonisch contact via het systeem van nummerherkenning, ook gebruik maken van andere communicatielijnen, zoals e-mail en chatapplicaties. Hoewel vanuit verschillende hoeken reeds is gepleit voor een systeem van automatische herkenning van geheimhouders-e-mailadressen,[247] geeft het OM in zijn schriftelijke reactie aan dat het systeem van nummerherkenning, zoals we dat op dit moment hebben voor telefonisch contact, 'niet toepasbaar' is op andere communicatielijnen. Dit betekent dat e-mailcorrespondentie of communicatie via een chatapplicatie tussen advocaat en cliënten niet automatisch 'aan de poort' wordt uitgefilterd. Dit geldt ongeacht de mate van beveiliging die bij deze communicatiemiddelen wordt gebruikt.

Waar het gaat om chatapplicaties is relevant dat deze kunnen worden gekoppeld aan het telefoonnummer dat als geheimhoudernummer is geregistreerd. De geïnterviewde advocaten geven ook aan dat zij de door hen gebruikte chatapplicaties inderdaad aan hun geheimhoudernummer hebben gekoppeld. Sommigen gaan er dan ook van uit dat zij gebruikmaken van hun geheimhoudernummer en dat deze communicatie automatisch of in ieder geval gemakkelijk als geheimhoudercommunicatie zou moeten (kunnen) worden geïdentificeerd. Het systeem van automatische nummerherkenning werkt echter alleen voor telefonisch contact en sms-contact, niet bij het gebruik van chatapplicaties. Omdat deze applicaties gebruikmaken van *end-to-end* encryptie is aftappen weliswaar niet mogelijk, maar de inhoud van de communicatie kan wel bij de opsporing terechtkomen door bijvoorbeeld de inbeslagname van een telefoon. Omdat de chatapplicaties gekoppeld zijn aan een telefoonnummer en respondenten aangeven dat zij hiervoor hun geheimhoudernummer gebruiken, zou bij kennisname van deze communicatie via een inbeslaggenomen telefoon in beginsel herleidbaar kunnen zijn dat het hier om geheimhouderinformatie gaat. Nu deze informatie niet automatisch wordt uitgefilterd bestaat echter het risico dat dit pas duidelijk wordt na kennisneming van de inhoud van de communicatie, of wanneer door opsporingsinstanties bij het uitlezen van de telefoon op voorhand wordt gezocht op een bepaald telefoonnummer. Dat laatste zal vaak niet gebeuren, alleen al omdat niet altijd bekend is dat er gecommuniceerd is met een advocaat, en welke advocaat dit dan is. Daar komt bij dat het OM niet beschikt over een overzicht van de als geheimhoudernummer geregistreerde telefoonnummers, een algemene zoekslag of filtering op basis van een standaardlijst met telefoonnummers is om deze reden ook niet mogelijk. Bovendien is het toepassen van een dergelijke werkwijze praktisch gezien onhaalbaar, zo wordt door het OM aangegeven. Wanneer bij iedere inbeslaggenomen gegevensdrager (standaard) een zoekslag moet worden gemaakt legt dit een enorm beslag op capaciteit en middelen. Dat is praktisch

247 Spronken 2022 en *Advies Aanwijzing omgang verschoningsgerechtigd materiaal* 2023, p. 3.

gezien alleen al ondoenlijk omdat voor het toepassen van een zodanige filtering specifieke software nodig is die niet beschikbaar is voor alle onderzoeken. Hetzelfde geldt voor de menskracht om deze zoekslagen uit te voeren.[248]

Voor e-mail bestaat evenmin een automatisch herkenningssysteem. Bij inbeslagname van gegevensdragers of bij het verkrijgen van e-mailgegevens na een vordering tot gegevensverstrekking, moet eventuele filtering van verschoningsgerechtigde informatie dus ook handmatig plaatsvinden. Dat kan doordat vooraf bepaalde zoektermen of e-mailadressen worden ingevoerd, maar kan ook gaandeweg een onderzoek plaatsvinden. Advocatenmailadressen zijn, ten opzichte van telefoonnummers bij het gebruik van chatapplicaties, doorgaans eenvoudiger als zodanig te herkennen. Dat het niet altijd goed is gegaan blijkt echter uit de al vaker genoemde Castor-zaak. De werkwijze van het OM wordt aangepast, maar mede gelet op de thans nog lopende juridische procedures is op dit moment niet geheel duidelijk hoe die eruit zal komen te zien.[249]

Die hierboven omschreven problematiek omtrent de herkenbaarheid van geheimhouderinformatie bij communicatie via chatapplicaties en e-mail wordt ook door het OM zelf onderkend. Het gebruik van veel verschillende soorten communicatiemiddelen door advocaten heeft als gevolg dat de filtering van verschoningsgerechtigde informatie steeds ingewikkelder wordt en steeds meer tijd vraagt. Elk medium kan in principe worden gebruikt in het contact tussen advocaat en cliënt, wat betekent dat de verschoningsgerechtigde informatie op heel veel plekken (in een gegevensdrager) kan zitten. Bovendien is om zowel technische als praktische redenen niet alles mogelijk en kan niet elke communicatielijn even gemakkelijk worden geschoond. Met name het filteren van verschoningsgerechtigde informatie uit chatapplicaties blijkt ingewikkeld. Vanuit het OM wordt gepleit voor een vertrouwelijke communicatiestandaard voor advocaten waardoor de vertrouwelijke informatie niet via alle communicatielijnen in het opsporingsonderzoek terecht kan komen. Een communicatiestandaard, een aparte (nieuw ontwikkelde) app of een elektronische handtekening uitgegeven door de NOvA zou een oplossing kunnen bieden. In dat kader wordt door het OM gewezen op de aanpak van andere beroepsgroepen met eenzelfde geheimhoudingsplicht. Artsen hebben Zorgmail en notarissen kunnen gebruik maken van een beschermde digitale omgeving aangeboden door de Koninklijke Notariële Beroepsorganisatie. Een soortgelijk systeem zou ook voor advocaten kunnen worden ontwikkeld.

> 'Ook het Openbaar Ministerie is erbij gebaat dat er een oplossing komt, een communicatiekanaal komt, om vertrouwelijk te communiceren, waar wij gewoon geen zicht op hebben.'

248 Nog los van aanvullende praktische obstakels wanneer bijvoorbeeld gaandeweg een onderzoek blijkt dat er meer dan één geheimhouder is, omdat dan de gegevens van de mobiele telefoon opnieuw moeten worden ingeladen om de nieuwe filtering uit te voeren. De praktische consequentie daarvan is dat dit er (op dit moment) toe leidt dat al het eerdere onderzoek aan die telefoon opnieuw moet worden uitgevoerd.

249 Zie uitgebreider hierover par. 4.3.

6.5.2.4 Herkennen en filteren van verschoningsgerechtigde communicatie in Hansken

Wanneer het gaat om de analyse van grote digitale datasets in de opsporing, zoals e-mail- en cryptotelefooncommunicatie, wordt daarvoor veelal gebruik gemaakt van de forensische softwaretool Hansken. Om de risico's voor de vertrouwelijkheid van advocaat-cliënt-communicatie te kunnen duiden wordt in deze paragraaf uiteengezet hoe daarbij te werk wordt gegaan en welke (technische) beperkingen daarbij gelden. Het NFI heeft in Hansken speciale functies ingebouwd om digitale sporen die geheimhouderinformatie bevatten uit de datasets te filteren.[250] Er zijn twee manieren om geheimhouderinformatie uit een dataset te filteren. Allereerst kan een filtering plaatsvinden door middel van automatische matching. In overleg met rechter-commissaris en/of de advocaat van de verdachte kan voorafgaand aan de analyse een lijst met 'zoektermen' worden ingevoerd. Wanneer een van deze zoektermen in een e-mail, chatbericht, of document voorkomt, wordt het bestand gemarkeerd als geheimhouderinformatie. Enkel de onderzoeker die als medewerker geheimhouding optreedt[251] en de daarbij horende toegangsrechten heeft, kan dit bestand vervolgens inzien. Voor zaakonderzoekers zijn deze gemarkeerde bestanden niet meer toegankelijk. Voorbeelden van zoektermen die worden gebruikt om verschoningsgerechtigde informatie te identificeren zijn e-mailadressen, namen en telefoonnummers van de advocaat.[252] Hoewel de automatische matching op basis van zoektermen een logische eerste stap vormt voor het identificeren van geheimhouderstukken, kunnen er altijd geheimhouderstukken onterecht ongemarkeerd blijven (zie daarover uitgebreider hierna). Wanneer geheimhouderinformatie niet via de automatische matching uit de dataset is gefilterd, kan dit ook handmatig (tijdens de analyse van de dataset) nog gebeuren. Op het moment dat een zaakonderzoeker geheimhouderinformatie tegenkomt, kan deze dit als zodanig markeren. Het bestand is vervolgens niet meer zichtbaar voor zaakonderzoekers, en alleen nog te raadplegen door een medewerker geheimhouder.[253]

Sinds de ontwikkeling van deze dienst door het NFI is er discussie over de omgang met geheimhouderstukken en de daarmee samenhangende risico's voor de waarborging van het verschoningsrecht. In het navolgende volgt hiervan een uiteenzetting.

Beperkingen automatische matching

Wanneer binnen een dataset door middel van automatische matching actief wordt gezocht naar geheimhouderinformatie kan er discussie ontstaan over het soort zoektermen waarmee wordt gezocht. Vanuit het perspectief van het verschoningsrecht is het wenselijk om zoveel mogelijk zoektermen te gebruiken zodat de kans dat er verschoningsgerechtigde informatie in de dataset achterblijft, zo klein mogelijk is. Vanuit dit perspectief valt er wat voor te zeggen om de begrippen 'advocaat', 'cliënt', of de afkorting 'Mr.' als zoekterm in de automatische matching te includeren. Immers, het gebruik van deze

250 Voorbeelden van 'digitale sporen' die geheimhouderinformatie kunnen bevatten zijn e-mails, chatberichten, foto's en documenten.

251 Zie hierover ook par. 4.4.3.

252 Zie *Informatieblad NFI* 2023 en 'Voorlopig Beleid Uitspraak Kort Geding verschoningsrecht', (om.nl), 19 april 2022.

253 *Hansken – Informatieblad Geheimhouderinformatie NFI* 2020, p. 2-3.

woorden kan een aanwijzing zijn dat het gaat om communicatie tussen een advocaat en een cliënt. Praktisch gezien stuit dit echter op bezwaren, zo blijkt uit de interviews met het OM en het NFI. 'Mr.' is niet enkel de afkorting van 'Meester', maar daarnaast ook een veelvoorkomende lettercombinatie en het woord 'cliënt' wordt tevens als technische term in alle softwarepakketten gebruikt. Wanneer deze begrippen worden geïncludeerd in de automatische matching zal Hansken ook alle niet-vertrouwelijke documenten waarin het woord cliënt of de lettercombinatie 'Mr.' voorkomt, uit de dataset filteren, met als gevolg veel fout positieven: documenten die geen verschoningsgerechtigde informatie bevatten en onterecht als zodanig worden gemarkeerd.

Een zelfde soort discussie kan ontstaan over het filteren en markeren van 'samenhangende sporen'.[254] Vanuit verschoningsrechtperspectief kan het wenselijk zijn om samenhangende sporen automatisch ook te markeren. Dit is bijvoorbeeld het geval wanneer een e-mail van een advocaat als geheimhouderstuk is gemarkeerd. Het is dan, met het oog op het verschoningsrecht, logisch en wenselijk om ook de bijlagen van deze e-mail als zodanig te markeren. Echter, op dit moment worden de samenhangende sporen niet automatisch gemarkeerd, mede omdat het in andere gevallen, met het oog op de waarheidsvinding, juist niet wenselijk is om dit te doen. Wanneer een e-mail van een advocaat bijvoorbeeld onderdeel is van een e-maildatabase, is het onwenselijk om de hele database (de samenhangende sporen) te markeren. Dit zou immers betekenen dat alle e-mailcorrespondentie op de database wordt uitgesloten van het opsporingsonderzoek door één geheimhouderstuk.[255]

Met betrekking tot geheimhouderstukken kan zich ook nog de complicatie voordoen dat deze zich op meerdere plekken in de dataset bevinden, bijvoorbeeld doordat een bijlage op een telefoon is gedownload en daarmee (ook) wordt opgeslagen in de downloadfolder of doordat een bestand of bericht dat afkomstig is van een geheimhouder, door de ontvanger is doorgestuurd naar iemand anders. Hoewel de duplicaten (deels) dezelfde inhoud hebben, kunnen deze, bijvoorbeeld door het doorsturen, technisch zo zijn gewijzigd dat ze niet meer als hetzelfde (oorspronkelijk verschoningsgerechtigde) bestand herkenbaar zijn.[256] Wanneer dit ook aan het bestand zelf niet te zien is, bijvoorbeeld omdat het gaat om een foto of een document waaruit niet valt op te maken dat het van een geheimhouder afkomstig is, dan kan het complex zijn om vast te stellen dat het om verschoningsgerechtigde informatie gaat.[257]

Uitgrijzen i.p.v. vernietigen

Een andere discussie ziet op het markeren van geheimhouderinformatie in Hansken. Dit is niet hetzelfde als het verwijderen van geheimhouderinformatie. Door markering wordt de informatie ontoegankelijk gemaakt voor zaakonderzoekers, dit proces wordt ook wel 'uitgrijzen' genoemd, dit is niet hetzelfde als het definitief verwijderen van geheimhouderinformatie.[258] Over de praktijk van het 'uitgrijzen' in plaats

254 *Informatieblad NFI* 2023, p. 2.
255 *Informatieblad NFI* 2023, p. 12
256 Zie uitgebreider *Informatieblad NFI* 2023, p. 11-12.
257 *Informatieblad NFI* 2023, p. 11-12.
258 *Informatieblad NFI* 2023, p. 1.

van vernietigen van geheimhouderinformatie is veel te doen geweest.[259] De kern van de juridische discussie betreft de vraag of het uitgrijzen van sporen gelijkgesteld kan worden aan 'vernietigen' in de zin van art. 126aa Wetboek van Strafvordering. Indien dit niet het geval zou zijn, wordt niet voldaan aan de wettelijke vernietigingsplicht.[260]

Hoewel vanuit de ratio van het verschoningsrecht betoogd kan worden dat vernietiging van geheimhouderstukken de voorkeur verdient, is dit om technische redenen, met name bij complexe datastructuren, niet altijd mogelijk en/of wenselijk.[261] Tijdens het interview zegt de digitaal forensisch onderzoeker van het NFI daarover het volgende:

> 'Daar zitten echt wel veel technische haken en ogen aan die volgens mij zo nu en dan toch wel vergeten worden in de discussies en in uitspraken van de advocaten en rechters.'

Een voorbeeld van dergelijke technische haken en ogen is het feit dat individuele sporen die geheimhouderinformatie bevatten onderdeel kunnen uitmaken van een groter 'ondeelbaar geheel'.[262] Dit individuele spoor, bijvoorbeeld een document, kan vervolgens niet worden vernietigd zonder het grotere geheel helemaal te vernietigen. Dit heeft onder andere te maken met de complexe (en gelaagde) structuur van data. Wanneer er een e-maildatabase wordt aangetroffen bevat deze database vaak honderden e-mails, en deze e-mails bevatten op hun beurt weer verschillende bijlagen. Stel, een van deze e-mails bevat als bijlage een ZIP-bestand met daarin meerdere documenten en één van deze documenten bevat verschoningsgerechtigde informatie. Idealiter wordt alleen dit laatstgenoemde document vernietigd. Het is echter technisch niet zonder meer mogelijk om dit document met verschoningsgerechtigde informatie te vernietigen zonder het hele ZIP-bestand of zelfs de hele e-mail, inclusief alle bijlagen, te vernietigen. Dit is onwenselijk omdat in dat geval veel informatie onterecht uit het opsporingsonderzoek wordt gehouden.

Ook wanneer vernietiging van individuele sporen wel mogelijk is, is dit niet in alle gevallen wenselijk, zo blijkt uit de interviews met de medewerker(s) van het OM en het NFI. De vernietiging van sporen kan bijvoorbeeld als gevolg hebben dat bepaald forensisch onderzoek naar herkomst of authenticiteit van sporen niet meer gedaan kan worden.[263]

Bij de hiervoor geschetste afwegingen omtrent te includeren zoektermen, het wel of niet markeren van samenhangende sporen en het 'uitgrijzen' versus vernietigen, dienen overwegingen omtrent het verschoningsrecht te worden afgewogen tegen instrumentele overwegingen van het opsporingsonderzoek. Bij dergelijke afwegingen kunnen technische (on)mogelijkheden van een forensische analysetool zoals Hansken ervoor zorgen dat er bepaalde keuzes worden gemaakt ten behoeve van het opsporingsonderzoek, ten koste van de (potentieel meer volledige) filtering van verschoningsgerechtigde stukken. Met als gevolg dat er, na een automatische matching, mogelijk nog

---

259 Zie o.a. Winkels 2022; Conclusie AG Harteveld Parket bij de Hoge Raad 5 juli 2022, ECLI:NL:PHR:2022:647 en Rechtbank Oost-Brabant, 22 maart 2022, ECLI:NL:RBOBR:2022:1035 r.o. 3.2. en 4.26.

260 Parket bij de Hoge Raad 5 juli 2022, ECLI:NL:PHR:2022:647, par. 4.31.

261 Zie in dit verband o.a. *Informatieblad NFI* 2023, p. 3-4.

262 *Informatieblad NFI* 2023, p. 3.

263 *Informatieblad NFI* 2023, p. 2-3.

verschoningsgerechtigde informatie in de dataset achterblijft.[264] Deze verschoningsgerechtigde informatie moet dan door de zaakonderzoekers als zodanig worden geïdentificeerd en gemarkeerd. Dit betekent dat deze informatie in eerste instantie soms wel wordt gelezen, maar vervolgens niet mag worden gebruikt.

6.5.3 Risico's geheimhoudingsplicht en verschoningsrecht: inbreuken andere (commerciële) derden

Hoewel de angst voor potentiële inbreuken door derden, niet zijnde overheidsinstanties, minder op de voorgrond lijkt te staan in de interviews met advocaten, kan het gebruik van bepaalde extra beveiligde en/of identiteitsversluierende communicatiemiddelen ook gepaard gaan met het risico van een inbreuk door een derde partij. Met name bij cryptotelefoons wordt gewezen op het gevaar dat de aanbieders van deze telefoons zouden kunnen meelezen met de communicatie.

> 'Toen heb ik gezegd "maar hoe garandeer je mij dan dat jij niet meeleest?". Dat vond ik eigenlijk het grootste probleem. Dus de ontwikkelaars van die telefoons die kunnen natuurlijk wel meelezen want die zouden die code wel kunnen hebben. Dus toen zei ik "Ja, ga ik niet doen".'

Andere risico's voor inbreuken door derde (commerciële) partijen zijn niet zozeer verbonden aan de extra beveiliging van communicatiemiddelen, maar eerder aan het gebrek daaraan, bijvoorbeeld waar het gaat om de mogelijke toegang van providers tot (niet *end-to-end* versleutelde) e-mailcommunicatie.

6.6 Conclusie

Bij het gebruik van extra beveiligde communicatiemiddelen door advocaten kunnen verschillende knelpunten en risico's worden geïdentificeerd. Deze doen zich in het bijzonder voor bij het gebruik van cryptotelefoons, en in iets mindere mate ook bij het gebruik van (bepaalde) chatapplicaties. Dergelijke communicatiemiddelen kunnen uit oogpunt van de advocatuurlijke kernwaarden integriteit, onafhankelijkheid en de geheimhoudingsplicht problematisch zijn, en vereisen ook in het licht van de documentatieplicht van advocaten extra zorgvuldigheid. Voor wat betreft integriteit en onafhankelijkheid gaat het vooral om het potentiële risico dat advocaten onvoldoende distantie tot de cliënt kunnen bewaren en bij hun handelen (al niet onder druk) de gedrags- of strafrechtelijke grenzen uit het oog verliezen. Hierbij geldt wel dat het al dan niet ontstaan van onvoldoende distantie tot de cliënt in de eerste plaatst niet afhankelijk is van het gekozen communicatiemiddel, maar van de wijze waarop de betreffende advocaat gebruikmaakt van dit communicatiemiddel. Op basis van de bevindingen van dit onderzoek kan niet worden gesproken van een verband tussen het gebruik van een cryptotelefoon en niet-integer of niet-onafhankelijk handelen. Wel vormt, waar het gaat om

[264] Overigens kunnen er ook verschoningsgerechtigde stukken achterblijven door andere (technische) factoren. Dit kan bijvoorbeeld te maken hebben met het bestaan van (niet gemakkelijk te herkennen) duplicaten. Zie in dit kader *Informatieblad NFI* 2023, p. 2-3.

beeldvorming als onderdeel van de kernwaarde integriteit, het imago van cryptotelefoons een duidelijk risico.

Aan het gebruik van cryptotelefoons en chatapplicaties kunnen daarnaast ook risico's kleven voor de geheimhouding. In dit onderzoek zijn verschillende (praktische en technische) knelpunten geïdentificeerd die meebrengen dat het verschoningsrecht bij dergelijke communicatiemiddelen in het gedrang kan komen. Waar het gaat om het verschoningsrecht zien we echter tegelijkertijd dat ook het niet gebruiken van extra beveiliging, in ieder geval waar het gaat om e-mailcommunicatie, problematisch kan zijn.

7. Een blik over de grens: regelgeving en praktijk in andere landen

7.1 Inleiding

In dit hoofdstuk wordt stilgestaan bij de regelgeving en praktijk met betrekking tot het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in andere landen (deelvraag 4). In het vorige hoofdstuk zijn enkele knelpunten en risico's geïdentificeerd betreffende het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten. Een aantal van deze knelpunten vormt de leidraad om in dit hoofdstuk vanuit een rechtsvergelijkend perspectief in te gaan op een drietal specifieke onderwerpen. Daarbij vindt een analyse plaats van de regelgeving en/of praktijk in landen waarover voor deze onderwerpen relevante informatie bekend is geworden. Het verrichte onderzoek en de bespreking daarvan is derhalve thematisch en beperkt zich tot het schetsen van een beeld van de wijze waarop in andere landen met vergelijkbare problematiek wordt omgegaan. De bespreking concentreert zich bovendien op aspecten die in het licht van de Nederlandse knelpunten inspiratie kunnen bieden voor het denken over mogelijke oplossingsrichtingen. Waar zinvol zal dan ook steeds een verbinding worden gelegd met de vragen of knelpunten die in de Nederlandse situatie aan de orde zijn. In paragraaf 7.2 wordt gekeken naar de (strafrechtelijke) reactie in andere landen op het criminele imago en -gebruik van cryptotelefoons. In paragraaf 7.3 wordt beschreven hoe het gebruik van extra beveiliging in andere landen wordt gezien als ethische norm en als onderdeel van de geheimhoudingsplicht. In dit kader wordt tevens gekeken naar richtlijnen en handvatten voor advocaten. In paragraaf 7.4 wordt een blik geworpen op verschillende vertrouwelijke communicatiekanalen en beveiligde e-mailservices voor advocaten in andere landen. In paragraaf 7.5 volgt een korte reflectie op de bevindingen in het licht van enkele van de in de Nederlandse situatie geïdentificeerde knelpunten.

7.2 Cryptotelefoons: extra beveiliging strafbaar?

7.2.1 Cryptotelefoons, criminele activiteiten en advocaten

Het veelvuldig gebruik van cryptotelefoons binnen criminele netwerken heeft als gevolg dat deze toestellen een bepaald 'crimineel imago' hebben gekregen. Dit criminele imago wordt niet enkel binnen de opsporing, maar ook door de dekens en een deel van de respondenten expliciet benoemd als een (potentieel) goede reden om geen gebruik te maken van een dergelijk toestel. Het gebruik van een cryptotelefoon door een advocaat zou de suggestie kunnen wekken dat de advocaat betrokken is bij de criminele activiteiten van de cliënt. De verdenking jegens Inez Weski dat zij zou hebben deelgenomen aan een criminele organisatie en in dat kader gebruik zou hebben gemaakt van een cryptotelefoon, is daarvan een (Nederlands) voorbeeld.[265] Ook in België en Zweden zijn er incidenten geweest waar een strafrechtelijke verdenking is ontstaan jegens advocaten die in het bezit waren van een cryptotelefoon.

[265] Zie bijv. Haenen & Meeus 2023 en Laumans & Vugts 2023.

In 2021 zijn in het kader van de Sky-operatie twee advocaten uit Antwerpen aangehouden voor deelname aan een criminele organisatie. Beide advocaten, Jawad H. en Sahil M, zouden via een Sky ECC-toestel hebben deelgenomen aan criminele activiteiten.[266] Jawad H. werd, tezamen met de rest van de 'Vuittonbende', vervolgd en is inmiddels door de rechtbank veroordeeld tot een gevangenisstraf van achttien maanden.[267] Tegen Sahil M. heeft het OM recent vijf jaar celstraf en een boete van 30.000 euro geëist.[268] Overigens is door de verdediging van Sahil M. aangevoerd dat het onderzoek in verband met procedurele fouten nietig verklaard zou moeten worden. Politie en justitie zouden, zonder de noodzakelijke voorafgaande toestemming van de stafhouder van de balie, communicatie van Sahil M. hebben gelezen.[269] In februari 2023 is een derde advocaat uit Antwerpen opgepakt in het kader van de Sky-operatie, deze advocaat zou inmiddels onder voorwaarden vrij zijn.[270] Ook in Zweden zijn twee advocaten geschrapt vanwege hun betrokkenheid bij criminele activiteiten. De twee advocaten hebben beiden gebruik gemaakt van een EncroChat telefoon en worden beschuldigd van het lekken van informatie van de opsporingsinstanties naar criminele bendes.[271] Inmiddels zijn beide advocaten ook veroordeeld wegens betrokkenheid bij een drugsdelict (vier jaar gevangenisstraf) respectievelijk voorbereiding van moord (zes jaar gevangenisstraf).[272]

Bij al deze aanhoudingen gaat het om advocaten die een tijd hebben gecommuniceerd via een cryptotelefoon en worden beschuldigd van het deelnemen aan en/of faciliteren van criminele activiteiten (al dan niet mede door het gebruik van een cryptotelefoon). Het enkele bezitten of gebruiken van een cryptotelefoon wordt hen niet verweten, dat is immers in Nederland, België en Zweden (nog) niet verboden.

7.2.2 Strafbaarstellingen in het Verenigd Koninkrijk en Australië

Door de verschillende cryptotelefoon-operaties is duidelijk geworden dat dergelijke toestellen veel worden gebruikt binnen het criminele milieu. In een aantal landen vormt dit een aanleiding voor (het nadenken over) strafbaarstellingen in het kader van de aanpak van georganiseerde misdaad. In Nieuw-Zuid-Wales, een deelstaat van Australië, is in februari 2023 nieuwe wetgeving aangenomen gericht op aanpak van georganiseerde criminaliteit (mede) door het verbieden van een bepaalde categorie versleutelde telefoons.[273] De *Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022* voegt een nieuwe bepaling toe aan het Wetboek van Strafrecht in Nieuw-Zuid-Wales. Het gaat om

266 'Onderschepte berichten tonen hoe opgepakte advocaten zich bezighielden met criminele praktijken', *nieuwsblad.be* 12 maart 2021 en 'Advocaat mag gevangenis verlaten met enkelband na arrestatie in dossier Sky ECC', *gva.be* 21 juni 2021.

267 'Zware celstraffen voor 'Vuittonbende' na meer dan 20 drugstransporten, ook advocaat veroordeeld', *nieuwsblad.be* 10 februari 2023.

268 'Aanklager eis 5 jaar cel tegen advocaat van drugsmaffia', *nieuwsblad.be* 2 oktober 2023.

269 'Aanklager eis 5 jaar cel tegen advocaat van drugsmaffia', *nieuwsblad.be* 2 oktober 2023.

270 'Antwerpse advocaat opgepakt in Sky-onderzoek: "verhoord en vrijgelaten onder voorwaarden"', *nieuwsblad.be* 14 februari 2023.

271 'Två advokater i Stockholm avstängda pga Encrochat', *blaljus.nu* 30 juni 2021; het besluit tot schrapping (Beslut den 30 juni 2021 meddelat av Sveriges advokatsamfunds disciplinnämnd) is op te vragen bij de Zweedse balie via advokatsamfundet.se.

272 'Ex-advokaterna Güngör och Amdouni döms till fängelse', *Expressen.se* 12 juli 2022.

273 *The Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022,* (parliament.nsw.gov.au).

een verbod op *dedicated encrypted criminal communication devices* (hierna: DECCD). Een DECCD wordt omschreven als een telefoon die specifiek is ontworpen om communicatie te faciliteren tussen personen waarvan redelijkerwijs kan worden vermoed dat deze betrokken zijn bij serieuze criminele activiteiten en met als doel om deze communicatie buiten het zicht van de opsporingsautoriteiten te houden. Een DECCD kenmerkt zich door aangepaste hardware en/of software die bedoeld is om te verhinderen dat overheidsinstanties toegang kunnen krijgen tot informatie op het toestel. De wet noemt enkele voorbeelden van functionaliteiten die erop zouden kunnen duiden dat het om een DECCD gaat, waaronder de onmogelijkheid om via de server het toestel aan een individu te koppelen en de mogelijkheid om alle data in één keer te verwijderen (*wipe)*.[274]

Ook in het Verenigd Koninkrijk wordt sinds dit jaar nagedacht over de strafbaarstelling van cryptotelefoons. In januari 2023 heeft het Britse Ministerie van Binnenlandse Zaken verschillende (legislatieve) maatregelen om de aanpak van georganiseerde criminaliteit te verbeteren voorgesteld en voorgelegd ter consultatie bij andere overheidsorganen.[275] Een van de maatregelen betreft het ontwerpen van nieuwe strafbaarstellingen op het gebied van het produceren, aanbieden, leveren en/of bezitten van bepaalde artikelen die bedoeld zijn om te gebruiken in het kader van ernstige criminaliteit. In het voorstel worden *sophisticated encrypted communication devices* (hierna: SECD) omschreven als toestellen met toegang tot een versleuteld communicatieplatform, die worden gebruikt door 'serious and organised criminals to plan their illicit activities'. De toestellen worden gekenmerkt door sterke encryptie, hoge (abonnements-)kosten en complexe communicatiemethoden voor de gebruikers.[276]

Zowel de omschrijving van de DECCD als de omschrijving van de SECD sluit aan bij wat wij in dit rapport verstaan onder een cryptotelefoon. De voorstellen in Australië en het Verenigd Koninkrijk laten zien dat in andere landen het criminele imago en -gebruik van cryptotelefoons de aanleiding was voor een (potentiële) strafbaarstelling. Beide voorstellen zijn ontstaan vanuit de wens om georganiseerde misdaad tegen te gaan en vanuit de – daaraan verbonden – gedachte dat cryptotelefoons veel door criminelen worden gebruikt. De kenmerken van een SECD resulteren in het vermoeden dat deze telefoons niet voor legitieme doeleinden gebruikt worden, aldus het Britse Ministerie van Binnenlandse Zaken.[277]

> 'Just as their level of encryption makes them ideal for those engaged in serious criminality, so their price and complexity make it harder to foresee a need for anyone to use them for legitimate, legal reasons.'[278]

Tegelijkertijd blijkt uit beide voorstellen dat het enkele bezit van een cryptotelefoon, zonder een link met criminele activiteiten, geen strafbaar feit op kan leveren. De nieuwe strafbaarstelling in het Verenigd

---

274 *The Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022*, (parliament.nsw.gov.au) p. 16.

275 *Two legislative measures to improve the law enforcement response to serious and organised crime Government consultation,* (gov.uk), 24 januari 2023.

276 *Two legislative measures to improve the law enforcement response to serious and organised crime Government consultation,* (gov.uk), 24 januari 2023, p. 11.

277 *Two legislative measures to improve the law enforcement response to serious and organised crime Government consultation,* (gov.uk), 24 januari 2023, p. 11.

278 *Two legislative measures to improve the law enforcement response to serious and organised crime Government consultation,* (gov.uk), 24 januari 2023, p. 11.

Koninkrijk zou tot gevolg hebben dat het bezitten van een SECD op zichzelf een strafbaar feit oplevert, mits er redelijke gronden zijn om te vermoeden dat de SECD zal worden gebruikt in het kader van ernstige criminaliteit.[279] In Nieuw-Zuid-Wales is een persoon strafbaar wanneer deze een DECCD bezit en er daarnaast redelijke gronden zijn om te vermoeden dat de DECCD in het bezit is ten behoeve van het begaan en/of faciliteren van ernstige criminele activiteiten.[280] Het enkele bezit van een DECCD, zonder enige link met dergelijke criminaliteit, is onvoldoende. Echter, het hoeft niet bewezen te worden dat de DECCD daadwerkelijk door de verdachte is gebruikt in het kader van (het plannen van) criminele activiteiten.[281] De wet bevat een niet-limitatieve lijst van overwegingen die meegewogen kunnen worden bij het bepalen of er redelijke gronden zijn om te vermoeden dat de DECCD in het bezit is met als doel criminele activiteiten te faciliteren. Zo kan worden meegenomen of de verdachte de DECCD heeft gekocht of gekregen van een crimineel netwerk of dat de verdachte naast het bezit van een DECCD ook in het bezit is van drugs en/of wapens.[282]

7.2.3 (Potentiële) gevolgen van een strafbaarstelling voor advocaten

Hoewel beide voorstellen gericht zijn op de aanpak van georganiseerde misdaad en niet op het (legitieme) gebruik van cryptotelefoons door advocaten, is duidelijk dat de strafbaarstellingen ook gevolgen kunnen hebben voor advocaten die een cryptotelefoon gebruiken in het contact met cliënten. Dit geldt met name in Nieuw-Zuid-Wales, wanneer een advocaat een cryptotelefoon zou hebben gekregen van of via een cliënt. Immers, het krijgen van een cryptotelefoon via een crimineel netwerk betreft daar een indicatie voor crimineel gebruik.[283] Hoewel geen empirische data bekend zijn over het gebruik van dergelijke communicatiemiddelen door advocaten in Nieuw-Zuid-Wales of in het Verenigd Koninkrijk, zal de keuze om als advocaat al dan niet gebruik te maken van een cryptotelefoon mede beïnvloed worden door het (toekomstige) bestaan van een strafbaarstelling. Ook wanneer het bezit en gebruik slechts strafbaar is wanneer een relatie met crimineel handelen kan worden vastgesteld, levert dit voor advocaten immers een risico op, ook indien zij (uiteindelijk) kunnen aantonen dat daar in hun

---

279 *Two legislative measures to improve the law enforcement response to serious and organised crime Government consultation* 2023, p. 16-18. Het voorstel bevat twee verschillende opties voor een strafbaarstelling. Bij de eerste optie dient bewezen te worden dat de verdachte redelijke gronden had om te vermoeden dat de cryptotelefoon gebruikt zal worden in het kader van ernstige criminele activiteiten ('reasonable grounds to suspect'). Bij de tweede optie dient bewezen te worden dat de verdachte redelijkerwijs vermoedde ('reasonably suspects') dat de cryptotelefoon gebruikt zal worden in het kader van ernstige criminele activiteiten.

280 *The Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022*, (parliament.nsw.gov.au) p. 17. In dat geval kan een gevangenisstraf van maximaal drie jaar worden opgelegd.

281 *The Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022*, (parliament.nsw.gov.au) p. 17. Zie in dat verband: A*rt.192Q,* van het voorstel: *'Proof of particular offence not required'.*

282 *The Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022*, (parliament.nsw.gov.au) p. 17. De wet lijkt daarnaast met name procesrechtelijke gevolgen te hebben. Naast de voornoemde strafbepaling wordt een nieuw instrument geboden aan opsporingsambtenaren: *dedicated encrypted criminal communication device prohibition order* (hierna: DECCD-order). Wanneer een opsporingsambtenaar het vermoeden heeft dat iemand in het bezit is van een DECCD, kan deze een DECCD-order aanvragen bij een hogere autoriteit. Indien de DECCD-order door de hogere autoriteit is afgegeven mag een opsporingsambtenaar, zonder bevelschrift ('*warrant*'), verschillende bevoegdheden inzetten met als doel om te onderzoeken of een persoon in bezit is van een DECCD.

283 *The Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022*, (parliament.nsw.gov.au) p. 17.

geval geen sprake van was. Strafbaarstelling zou dan dus een sterk argument kunnen zijn om dergelijke toestellen als advocaat niet te gebruiken.

7.3 (Extra) beveiliging als beroepsethische plicht

Van een advocaat mag, met het oog op de waarborging van de vertrouwelijkheid, zorgvuldigheid worden verlangd bij het maken van de keuze voor een specifiek medium en het niveau van beveiliging. Het is echter, zo blijkt uit paragraaf 6.5.1, niet altijd duidelijk wat deze zorgvuldigheid vervolgens in concrete gevallen inhoudt en welke communicatiemiddelen advocaten het beste kunnen gebruiken om de vertrouwelijkheid van de communicatie te waarborgen. Het feit dat advocaten vaak niet beschikken over optimale (technische) kennis over risico's en beveiligingswaarborgen lijkt hierbij ook een rol te spelen. In dat licht kan de vraag rijzen of het mogelijk is om de beroepsgroep meer richtlijnen en handvatten te bieden voor wat betreft de verantwoordelijkheden en verplichtingen die zij hebben op basis van de geheimhoudingsplicht, in relatie tot de keuze voor een bepaald communicatiemiddel.

Een blik over de grens leert dat in ieder geval de *American Bar Association* (hierna: ABA), met name de afgelopen jaren, heeft geïnvesteerd in beroepsethische documenten en richtlijnen betreffende de verantwoordelijkheden van advocaten in relatie tot digitale communicatie met cliënten. In *The Model Rules of Professional Conduct* van de ABA worden (beroeps-)ethische regels voor advocaten opgesomd.[284] In verschillende door de ABA uitgewerkte *Ethics Opinions* wordt de inhoud van deze regels nader uitgewerkt. Hierna volgt een korte uiteenzetting van de voor dit onderzoek meest relevante (ethische) richtlijnen en documenten van de ABA met betrekking tot dit onderwerp.[285]

Uit *The Model Rules of Professional Conduct* en de verschillende *Ethics Opinions* blijkt dat van advocaten wordt verwacht dat ze 'redelijke inspanningen' (*reasonable efforts*) leveren teneinde de vertrouwelijkheid van de (digitale) communicatie met cliënt te waarborgen en te voorkomen dat een ongeautoriseerde derde toegang krijgt tot de vertrouwelijke informatie.[286] Indien vertrouwelijke informatie toch bij een derde terecht is gekomen, maar de advocaat redelijke inspanningen heeft geleverd om dit voorkomen, heeft deze zijn of haar geheimhoudingsplicht niet geschonden.[287] Of een advocaat 'redelijke inspanningen' heeft geleverd is mede afhankelijk van de gevoeligheid van de informatie, de kans dat deze informatie bij een derde terechtkomt indien er geen extra beveiligingsmaatregelen worden genomen, de kosten en moeite die gepaard gaan met het aanwenden van beveiligingsmaatregelen en de mate waarin

---

284 Model Rules of Professional Conduct', *americanbar.org*. The Model Rules of Professional Conduct zijn aangenomen door het beleidsvormende orgaan van de ABA: The House of Delegates.

285 Ook in enkele andere landen zijn (meer of minder) uitgebreide richtlijnen en/of handvatten gezien, bijvoorbeeld in het Verenigd Koninkrijk de *Email guidelines for the Bar* van de UK Bar Council (barcouncilethics.co.uk), en in Frankrijk de *Guide pratique les avocats et le règlement général sur la protection des données*, in combinatie met een 'self diagnosis tool' voor advocaten (cnb.avocat.fr). Nu de Amerikaanse richtlijnen het meest uitgebreid zijn worden deze andere landen hier niet verder besproken.

286 The Model Rules of Professional Conduct, Rule 1.6 'Duty of Confidentiality': *'(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.'*

287 The Model Rules of Professional Conduct, Rule 1.6, Comment 18; Formal Opinion 477R* May 11, 2017 Revised May 22, 2017, Securing Communication of Protected Client Information, (americanbar.org), p. 4.

de beveiligingsmaatregelen negatieve invloed (kunnen) hebben op het voeren van de juridische praktijk.[288] Deze laatste factor duidt onder andere op de gebruiks(on)vriendelijkheid van bepaalde extra beveiligingsmaatregelen. De snel opeenvolgende technologische ontwikkelingen resulteren in een verantwoordelijkheid voor advocaten om per geval te bepalen welke beveiliging redelijkerwijs moet worden aangewend. Dit betekent, aldus de Ethische Commissie van de ABA, ook dat het onder bepaalde omstandigheden niet redelijk is om als advocaat te vertrouwen op een niet-versleutelde e-mailprovider. Bovendien kunnen er omstandigheden zijn waarbij de communicatie in zijn geheel niet digitaal maar in persoon zou moeten plaatsvinden.[289]

De Ethische Commissie van de ABA maakt de inhoud van de term 'redelijke inspanningen' concreter door richtlijnen te geven betreffende de 'redelijke stappen' die advocaten zouden moeten nemen om aan hun geheimhoudingsplicht te voldoen. Van advocaten mag worden verwacht dat ze (1) het risico op een inbreuk op de vertrouwelijkheid kunnen inschatten. Dit risico is groter wanneer het gaat om meer gevoelige informatie. Daarnaast dient een advocaat (2) te begrijpen op welke wijze de (vertrouwelijke) informatie digitaal wordt overgedragen of opgeslagen en (3) te begrijpen op welke wijze de communicatie en anderszins vertrouwelijke informatie wordt beveiligd.[290] De verantwoordelijkheid voor beveiliging van digitale communicatie met de cliënt wordt neergelegd bij de advocaat. Deze dient te bepalen (4) op welke wijze de communicatie beveiligd dient te worden en dient (5) vertrouwelijke communicatie als zodanig te labelen zodat voor ongeautoriseerde derden duidelijk is dat het gaat om vertrouwelijke communicatie.[291] Tot slot zijn advocaten(kantoren) verantwoordelijk voor het vormen van beleid en het bieden van trainingen aan hun personeel om te bevorderen dat werknemers redelijke beveiligingsmethoden aanwenden in de digitale communicatie met cliënten.[292]

De ABA geeft niet enkel in *The Model Rules of Professional Conduct* en de formele *Ethics Opions* aan wat er van advocaten wordt verwacht, maar publiceert daarnaast ook veel informatieve stukken over de noodzaak van versleuteling en andere vormen van extra beveiliging in het kader van de vertrouwelijke communicatie tussen advocaat en cliënt.[293] Tot slot gebruikt de ABA blogs om uitleg en praktische tips te geven over de verschillende vormen van beveiliging.[294] Zo worden verschillende opties voor versleutelde e-mail besproken en wordt uitgelegd welke beveiligde chatapplicaties een advocaat kan gebruiken in het contact met cliënten.[295] Tot slot heeft de ABA het boek 'Encryption Made Simple for

---

288 The Model Rules of Professional Conduct, Rule 1.6, Comment 18. Formal Opinion 477R* May 11, 2017 Revised May 22, 2017, Securing Communication of Protected Client Information, (americanbar.org), p. 4.

289 Formal Opinion 477R* May 11, 2017 Revised May 22, 2017, Securing Communication of Protected Client Information, (americanbar.org), p. 5.

290 Formal Opinion 477R* May 11, 2017 Revised May 22, 2017, Securing Communication of Protected Client Information, (americanbar.org), p. 6.

291 Formal Opinion 477R* May 11, 2017 Revised May 22, 2017, Securing Communication of Protected Client Information, (americanbar.org), p. 7-8.

292 Formal Opinion 477R* May 11, 2017 Revised May 22, 2017, Securing Communication of Protected Client Information, (americanbar.org), p. 9.

293 Zie o.a. 'Encryption: Basic security you should be using now', *americanbar.org* 1 juli 2015 en 'Remember your ethical duties when it comes to encryption', *americanbar.org* oktober 2019.

294 'Encryption to protect confidentiality is easier than you think', *americanbar.org* december 2019 en 'Hot Buttons: Encrypting Communications', *americanbar.org* 18 juli 2022.

295 'Encryption to protect confidentiality is easier than you think', *americanbar.org* december 2019 en 'Hot Buttons: Encrypting Communications', *americanbar.org* 18 juli 2022.

Lawyers' uitgegeven. Dit boek bevat aanvullende informatie over de verschillende versleutelopties voor advocaten en de ethische plicht om vertrouwelijke informatie goed (door middel van encryptie) te beveiligen.[296]

7.4 Technische waarborgen voor vertrouwelijke e-mailcommunicatie

Uit de voorgaande hoofdstukken blijkt dat het onderwerp van dit onderzoek – het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten – raakt aan uiteenlopende thema's, waaronder het recht op vertrouwelijke communicatie tussen advocaat en cliënt en de waarborging van dit recht in de praktijk. Uit hoofdstuk 6 blijkt dat zich op dit punt belangrijke knelpunten voordoen, die onder meer samenhangen met het feit dat geheimhouderinformatie op dit moment via verschillende communicatielijnen het opsporingsonderzoek binnen kan komen en niet bij elke lijn automatisch 'aan de poort' wordt gefilterd. Tegen die achtergrond is gekeken naar de wijze waarop hiermee in andere landen wordt omgegaan, waarbij met name is gezocht naar (technische) instrumenten of regelingen die een mogelijke oplossing zouden kunnen bieden.

Voorbeelden van dergelijke technologische oplossingen zien we vooral waar het gaat om het gebruik van beveiligde e-mailservices. Zo leert een blik over de grens dat de Franse balie voor advocaten, de *Conseil National des Barreaux* (hierna: CNB), in 2014 een beveiligde e-mailservice voor advocaten heeft gelanceerd, de *Cloud privé des avocats*. Via deze e-mailservice kunnen advocaten die zijn ingeschreven bij de Franse balie kosteloos gebruikmaken van de domeinnaam 'avocat-conseil.fr' en daarmee beveiligd e-mailen met cliënten en andere contacten. De provider is gevestigd in Frankrijk en staat onder toezicht van de balie.[297] Omdat deze dienst in 2024 komt te vervallen zal vanaf dat moment worden overgestapt op een ander systeem, waarbij advocaten (tegen een lage prijs) beveiligd kunnen mailen met gebruikmaking van de domeinnaam 'advocat.fr'.

Ook in andere landen wordt een enigszins vergelijkbare service aangeboden of gefaciliteerd door de nationale balie. Zo biedt de *Deutsche Anwaltverein* leden een korting op TeamDrive, een online platform voor beveiligde dataopslag en e-mailcorrespondentie. Alle gegevens die met TeamDrive worden gedeeld worden automatisch *end-to-end* versleuteld en de provider is gevestigd in Duitsland.[298] De Spaanse balie, de *Consejo General de la Abogacía Española,* biedt *Correo Abogacía* aan, een beveiligde e-mailservice voor advocaten. De servers bevinden zich in de Europese Unie en de dienst biedt de mogelijkheid van versleuteling van bepaalde communicatie.[299]

296 Ries, Simek & Nelson 2016.

297 Zo blijkt uit de door de CNB aangeleverde schriftelijke reactie op de gestelde vragen. Zie ook de website van de CNB, assistance.cnb.avocat.fr. De CNB biedt ook andere instrumenten, zoals digitale platforms voor het uitwisselen van informatie voor advocaten onderling, voor communicatie tussen advocaten en de juridische instanties, en voor het indienen van stukken in lopende rechtszaken.

298 'Kommunikation und Technik', anwaltverein.de.

299 'Correo Abogacía', abogacia.es.

7.5 Reflectie op de Nederlandse situatie

Met in het achterhoofd de methodologische beperkingen die samenhangen met de omvang en insteek van dit onderdeel van het onderzoek, biedt dit hoofdstuk enkele voor de Nederlandse situatie relevante inzichten.

In de eerste plaats kan worden geconstateerd dat in enkele landen is overgegaan tot of wordt nagedacht over strafbaarstelling van het gebruik van cryptotelefoons. Op dit moment is het bezitten en gebruiken van een cryptotelefoon in Nederland niet verboden. Over de noodzaak of wenselijkheid van een eventuele strafbaarstelling kunnen in het bestek van dit onderzoek ook geen uitspraken worden gedaan. In dit verband is het goed te benoemen dat zowel in de deelstaat Nieuw-Zuid-Wales als in het Verenigd Koninkrijk kritiek is geuit op de (voorgestelde) strafbaarstelling van cryptotelefoons.[300] Wel kan iets worden gezegd over de mogelijke impact van een strafbaarstelling op het gebruik van deze communicatiemiddelen door advocaten. Ten eerste zal criminalisering van dergelijke communicatiemiddelen er naar verwachting toe leiden dat advocaten hiervan in (nog) mindere mate gebruik zullen maken. Waar in de Nederlandse context tot nog toe vooral wordt gewezen op risico's die samenhangen met het criminele imago en -gebruik van cryptotelefoons,[301] kan een door dit criminele imago en -gebruik ingevoerde strafbaarstelling een geheel nieuw en belangrijk argument opleveren voor advocaten om geen cryptotelefoon te gebruiken. Dat zal vooral gelden voor de advocaten die met de nodige aarzelingen of bedenkingen tot een dergelijke wijze van communiceren zijn overgegaan om hun cliënt ter wille te zijn. Tegelijkertijd valt, ten tweede, van een strafbepaling weinig heil te verwachten in het geval van de enkele advocaat die (al dan niet onder druk) de criminele activiteiten van de cliënt faciliteert of daaraan deelneemt.

Waar het gaat om de waarborging van de vertrouwelijkheid in het algemeen en de plichten en verantwoordelijkheden die de advocaat in dat verband heeft, leert een blik over de grens dat in ieder geval de Amerikaanse balie veel en uitgebreide richtlijnen, handvatten en praktische tips publiceert. Wanneer op dit punt een vergelijking met Nederland wordt gemaakt, lijken deze niet zozeer inhoudelijk heel anders dan het Nederlandse kader, zoals dat onder meer is neergelegd in de Voda, de Gedragsregels, de toelichting daarop en enkele door de NOvA gepubliceerde documenten.[302] Wel wordt door de ABA voorzien in veel uitgebreider en sterk op de praktijk toegespitste kaders, waarover bovendien met regelmaat wordt gepubliceerd. Nu de waarborging van de geheimhoudingsplicht tal van complexe vragen, keuzes en dilemma's kan opleveren, niet in het minst gelet op digitale uitdagingen en onzekerheden en het feit dat veel advocaten niet over optimale (technische) kennis beschikken, kan een dergelijke aanpak mogelijk van meerwaarde zijn.

---

300 Zie o.a. R. Pfefferkorn 2023. Zie voor kritiek geuit in de media o.a. 'UK proposes making the sale and possession of encrypted phones illigal', *vice.com* 8 februari 2023. In Nieuw-Zuid-Wales is er kritiek geuit door twee strafrechtadvocaten, zie 'Perrottet has passed a swag of police state laws, just prior to likely election loss', *sydneycriminallawyers.com.au* 19 oktober 2022.

301 Zie hfdst. 6.

302 Zie daarover par. 4.2.2.

Tot slot is voor de in Nederland spelende problematiek in relatie tot (niet extra beveiligde) e-mailcommunicatie relevant dat in sommige landen door balies wordt voorzien in een extra beveiligde e-mailservice, of dat het gebruik van dergelijke diensten op enigerlei wijze wordt gefaciliteerd (door deze bijvoorbeeld tegen gereduceerd tarief beschikbaar te stellen). Nu bij e-mailcommunicatie vooral het gebrek aan versleuteling of andersoortige beveiliging voor problemen kan zorgen, kunnen dergelijke initiatieven mogelijk een bijdrage leveren aan een betere waarborging van de vertrouwelijkheid van advocaat-cliënt-communicatie.

8. Conclusie en aanbevelingen

8.1 Inleiding

De Universiteit Leiden heeft in het kader van het door de NOvA opgezette Taskforce Bescherming tegen Ondermijning onderzoek gedaan naar het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen binnen de advocatuur. Het doel van dit onderzoek betreft het in kaart brengen van het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten, hun beweegredenen daarvoor en de mogelijke risico's die daarmee gepaard gaan. Daarnaast beoogt dit onderzoek kennis te vergaren over de praktijk, regelgeving en het beleid rondom extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in het buitenland. Deze doelstellingen zijn neergelegd in een tweetal centrale onderzoeksvragen:

1. *Worden of werden extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruikt door advocaten en, zo ja, welke middelen en waarom (niet)?*
2. *Hoe moet het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten worden bezien, mede in het licht van de risico's daarvan en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?*

Deze onderzoeksvragen zijn onderverdeeld in meerdere deel- en subvragen die de leidraad hebben gevormd voor de hoofdstukken 3 tot en met 7. In dit afsluitende hoofdstuk bouwen wij voort op de in die hoofdstukken neergelegde bevindingen en formuleren wij een antwoord op de centrale onderzoeksvragen. Daartoe zal allereerst een tweetal opmerkingen worden gemaakt (par. 8.2.), waarna in paragraaf 8.3 en 8.4 de beantwoording van de onderzoeksvragen plaatsvindt. Paragraaf 8.5 bevat enkele afsluitende opmerkingen en aanbevelingen.

8.2 Opmerkingen vooraf

Voor een goede duiding en interpretatie van de antwoorden op de onderzoeksvragen, is het van belang om vooraf het volgende op te merken. Zoals ook in hoofdstuk 2 is uiteengezet heeft het onderzoek bestaan uit een combinatie van verschillende onderzoeksmethoden, namelijk een combinatie van *desk research*, empirisch onderzoek en een rechtsvergelijkende inventarisatie. Ter beantwoording van de eerste onderzoeksvraag zijn advocaten geïnterviewd over de verschillende beweegredenen om wel of niet gebruik te maken van bepaalde (extra beveiligde en/of identiteitsversluierende) communicatiemiddelen. Op basis van de kwalitatieve interviewdata kunnen geen kwantitatieve uitspraken worden gedaan over het aantal advocaten dat gebruikmaakt van de verschillende soorten extra beveiligde communicatiemiddelen.[303] Bovendien is het niet mogelijk om op basis van de interviewdata uitspraken te doen over de beweegredenen van de gehele beroepsgroep om van bepaalde communicatiemiddelen

[303] Maesschalck 2016, p. 141.

wel of geen gebruik te maken. Het doen van (statistisch) generaliserende uitspraken over de beroepsgroep is dan ook niet een van de doelen van dit rapport. Waar een kwantitatieve benadering zonder meer ook interessant kan zijn voor de beantwoording van de eerste deelvraag, is het wat ons betreft ook zonder dergelijke data goed mogelijk in meer algemene zin een antwoord op de eerste onderzoeksvraag te formuleren. Volledigheidshalve zij nog opgemerkt dat een kwantitatieve onderzoeksmethodiek voor de tweede onderzoeksvraag niet aan de orde is.

Een tweede opmerking hangt samen met de gekozen steekproef en (daarmee samenhangend) de reikwijdte van het verrichte empirische onderzoek. Gelet op het onderwerp van dit onderzoek en de context daarvan – de bescherming van advocaten tegen ondermijning – ligt het voor de hand om vooral te spreken met respondenten die werkzaam zijn in de strafrechtspraktijk.[304] In totaal zijn zeventien advocaten geïnterviewd, waarvan veertien advocaten die met name strafzaken behandelen, twee advocaten met een ondernemings- en/of insolventierechtpraktijk en één advocaat die naast strafzaken ook personen-, familie- en jeugdrechtzaken behandelt. Dat brengt mee dat de bevindingen van dit onderzoek vooral een beeld geven van het gebruik van extra beveiligde communicatiemiddelen door advocaten werkzaam in de strafrechtspraktijk, hun beweegredenen daarvoor en de risico's daarvan. Hoewel enkele meer algemene bevindingen, bijvoorbeeld over het belang dat advocaten hechten aan hun geheimhoudingsplicht, ook (kunnen) gelden voor advocaten die werkzaam zijn in andere rechtsgebieden, geldt dat niet zonder meer voor andere bevindingen. Daarbij komt bovendien dat uit de voorgaande hoofdstukken blijkt dat er ook binnen de strafrechtadvocatuur grote verschillen zijn en het gebruik van bepaalde typen extra beveiligde communicatiemiddelen – in het bijzonder cryptotelefoons – vooral bij de bijstandverlening in specifieke typen strafzaken een rol speelt. Dit alles brengt mee dat voorzichtigheid geboden is bij het generaliseren van de bevindingen. De hierna opgenomen conclusies en aanbevelingen zijn dan ook niet zonder meer van toepassing op alle advocaten, werkzaam in het strafrecht of daarbuiten.

8.3 Het gebruik van extra beveiligde communicatiemiddelen en de beweegredenen daarvoor

De beantwoording van de eerste vraag (*worden of werden extra beveiligde en/of identiteitsversluierende communicatiemiddelen gebruikt door advocaten en, zo ja, welke middelen en waarom (niet)?*) is gebaseerd op de bevindingen uit de interviews met advocaten, die uitgebreid zijn beschreven in hoofdstuk 5. Het beeld dat daaruit naar voren komt is dat advocaten verschillende extra beveiligde communicatiemiddelen gebruiken. Het gebruik van chatapplicaties zoals WhatsApp, Signal en Telegram door advocaten komt geregeld voor, niet in de laatste plaats omdat het makkelijk en snel is en – ook door cliënten – veel wordt gebruikt. Daarbij wordt soms bewust gekozen voor een ander middel dan WhatApp, veelal vanwege betere privacy-waarborgen ten opzichte van derde (commerciële) partijen, en soms vanwege specifieke beveiligingsfunctionaliteiten van deze chatapplicaties. Extra beveiligde e-mailapplicaties worden in wat mindere mate gebruikt. Hoewel advocaten in hun contacten met de

[304] Zie hfdst. 2 voor een meer gedetailleerde verantwoording.

Rechtspraak in beginsel gebruik (moeten) maken van Zivver, wordt dat door velen als tamelijk gebruiksonvriendelijk en onpraktisch ervaren. E-mailcommunicatie met cliënten en anderen loopt dan ook meestal via het advocatenmailadres, zonder daarbij gebruik te maken van extra beveiliging, bijvoorbeeld in de vorm van encryptie. Slechts enkele respondenten hebben aangegeven dat zij cryptotelefoons hebben gebruikt in het contact met cliënten. Uit het onderzoek komt het beeld naar voren dat deze middelen vrijwel alleen worden of werden gebruikt door een relatief beperkte groep advocaten die geregeld bijstand verleent in grote strafzaken met betrekking tot georganiseerde (drugs)criminaliteit.[305] Het lijkt er bovendien op dat de verschillende cryptotelefoon-operaties waarbij servers zijn gehackt of in beslag zijn genomen, ervoor hebben gezorgd dat veel van de betreffende advocaten bewust de keuze maken om geen cryptotelefoon (meer) te gebruiken.[306]

De belangrijkste reden voor het gebruik van extra beveiligde communicatiemiddelen is de wens om de advocaat-cliënt-communicatie vertrouwelijk te houden. Die drijfveer zorgt ervoor dat de meeste respondenten (zeer) vertrouwelijke informatie bij voorkeur in persoon bespreken, en is mede ingegeven door een vrij breed gedeelde terughoudendheid ten aanzien van de vertrouwelijkheid van andere gebruikelijke communicatiemiddelen, waaronder de geheimhoudertelefoon. Daarbij loopt het beeld overigens wel uiteen; waar sommige respondenten een uitgesproken wantrouwen koesteren tegen de – met name strafvorderlijke – overheid, geldt dat voor anderen in veel mindere mate. Echter, ook bij deze laatste groep is er een zekere reserve ten aanzien van de werking van het systeem, al is het maar omdat in het verleden verschillende (technische) incidenten hebben plaatsgevonden.[307] De zorgen om andersoortige inbreuken op de vertrouwelijkheid, bijvoorbeeld doordat gegevens bij (commerciële) derden belanden, staan voor veel advocaten minder op de voorgrond. Daarbij speelt mee dat zij aangeven hun ICT-voorzieningen volgens de voorschriften te hebben ingericht.[308]

De wens of voorkeur van de cliënt is voor veel advocaten een belangrijke factor bij de keuze voor een bepaald communicatiemiddel. Vaak zijn zij bereid om aan die wens tegemoet te komen, mits zij dit met hun eigen opvattingen en verplichtingen kunnen verenigen. Daarbij zijn er duidelijke verschillen tussen advocaten, met name waar het gaat om het gebruik van cryptotelefoons: waar sommigen bereid zijn (of in het verleden bereid waren) mee te gaan in de behoefte van de cliënt, geven anderen aan dat zij dit middel niet willen gebruiken vanwege bijvoorbeeld het criminele imago ervan, of vanwege zorgen om het kunnen bewaren van voldoende distantie tot de cliënt. De advocaten die wel gebruik hebben gemaakt van cryptotelefoons geven aan dat (huidige en potentieel nieuwe) cliënten op enig moment enkel nog communiceerden via een cryptotelefoon. In het onderzoek is niet gebleken dat advocaten dwang, drang of druk vanuit hun cliënt of diens omgeving ervaren om bepaalde middelen te gebruiken. Wel kan er sprake zijn van een zekere commerciële druk, bijvoorbeeld wanneer een cryptotelefoon nodig is om bijstand te kunnen verlenen in bepaalde zaken, omdat de cliënt alleen nog daarmee communiceert.[309]

---

305 Zie over het gebruik van cryptotelefoons door advocaten uitgebreider par. 5.2.3.
306 Zie over de gebruikte communicatiemiddelen uitgebreider par. 5.2.
307 Zie uitgebreider par. 5.3.4.
308 Zie over waarborging van de vertrouwelijkheid als beweegreden uitgebreider par. 5.3.
309 Zie over de wens van de cliënt en eventuele druk uitgebreider par. 5.4.

De vraag of advocaten daadwerkelijk gebruikmaken van extra beveiligde communicatiemiddelen, en zo ja, welke, hangt mede af van praktische aspecten waarbij in het bijzonder de hiervoor al genoemde gebruiks(on)vriendelijkheid een rol speelt. Een andere factor is de persoon van de cliënt en diens feitelijke situatie (gedetineerd of niet, in Nederland of in het buitenland, al dan niet voldoende vaardig met digitale communicatiemiddelen).[310]

Advocaten komen bij de keuze voor de wijze van communiceren dan ook voor afwegingen en dilemma's te staan. Daarbij gaat het in de eerste plaats om het feit dat optimale geheimhouding niet altijd verenigbaar is met de praktische realiteit. Ten tweede blijkt dat de keuze voor extra beveiligde communicatiemiddelen, in ieder geval waar het gaat om het gebruik van cryptotelefoons, soms juist extra risico's voor de geheimhouding met zich brengt. Uit het onderzoek blijkt dan ook dat de uiteindelijke keuze voor een (al dan niet) extra beveiligd communicatiemiddel afhangt van veel verschillende factoren, waarbij de voordelen daarvan moeten worden afgewogen tegen de mogelijke risico's, en waarbij de wens van de cliënt, eigen opvattingen van de advocaat en de praktische realiteit een rol spelen. Van dwang, drang of druk vanuit (de omgeving van) de cliënt om dergelijke communicatiemiddelen te gebruiken is in dit onderzoek niet gebleken.

8.4 Waardering van het gebruik van extra beveiligde communicatiemiddelen in het licht van risico's en bestaande regelingen

Voor de beantwoording van de tweede deelvraag *(hoe moet het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten worden bezien, mede in het licht van de risico's daarvan en de bestaande regelingen met betrekking tot de vertrouwelijke communicatie tussen advocaten en cliënten?)* zijn de verschillende in dit onderzoek opgedane bevindingen bij elkaar gebracht. Op basis hiervan kunnen de volgende conclusies worden getrokken.

8.4.1 Legitieme zoektocht naar waarborging van de geheimhouding

Vooropgesteld moet worden dat de zoektocht naar maximale geheimhouding, gelet op het fundamentele belang van de vertrouwelijkheid van advocaat-cliënt-communicatie, op zichzelf als volstrekt legitiem en gerechtvaardigd kan worden beschouwd. Dat veel advocaten in meer of mindere mate een voorbehoud maken waar het gaat om hun vertrouwen in de waarborgen die in de Nederlandse wet- en regelgeving en praktijk zijn ingebouwd, is voorts niet onbegrijpelijk. Daarbij spelen verschillende factoren een rol. Waar het gaat om strafzaken kan in de eerste plaats worden gewezen op de inherente spanning die bestaat tussen de belangen van justitie en die van personen of groepen die zich bezighouden met criminele activiteiten. In het kader van de opsporing en vervolging van strafbare feiten kan de communicatie van- en naar deze personen immers een interessante en belangrijke bron van informatie zijn, ook wanneer die (deels) onder het verschoningsrecht valt. Dit brengt mee dat zolang het voor de strafvorderlijke

[310] Zie par. 5.5.

overheid technisch mogelijk is om kennis te nemen van vertrouwelijke communicatie, nooit helemaal uitgesloten kan worden dat dit ook gebeurt. Daarmee is niet gezegd dat die mogelijkheid betekent dat dit per definitie (structureel) gebeurt, maar het verklaart deels wel de geconstateerde terughoudendheid onder advocaten. Daarbij kan, ten tweede, worden gewezen op concrete gebeurtenissen in het (verre en minder verre) verleden die hebben laten zien dat de waarborging van het verschoningsrecht geen rustig bezit is. De ontwikkelingen van de laatste jaren rondom de Box-affaire en de aanhouding van advocaat Inez Weski, hebben het binnen de advocatuur bestaande wantrouwen tegen de strafvorderlijke overheid waar het gaat om het respecteren van het verschoningsrecht stevig aangewakkerd.[311] Dat geldt niet alleen voor advocaten die ook daarvóór al weinig vertrouwen hadden in de waarborging van het verschoningsrecht, bijvoorbeeld omdat zij zich bezighouden met bijstand in de zwaardere strafzaken rondom georganiseerde criminaliteit of terrorisme, en daarbij altijd al rekening houden met meeluisteren of -lezen door de (strafvorderlijke) overheid. Dit wantrouwen lijkt ook waarneembaar bij advocaten die juist als uitgangspunt hebben (gehad) dat de waarborging van het verschoningsrecht in beginsel op orde is, vooral zij die zich bezighouden met financieel-economische strafzaken. In zoverre kan worden gesteld dat de ontwikkelingen in de laatste jaren een (extra) voedingsbodem zijn geweest voor het zoeken naar alternatieve manieren om veilig met cliënten te communiceren. Tegen die achtergrond lijkt het raadzaam om het gebruik van minder conventionele communicatiemiddelen door advocaten niet te snel als een signaal van normoverschrijdend, niet-integer of ondermijnend handelen te beschouwen. Hetzelfde geldt voor andere waarborgen die advocaten nemen om de geheimhouding te waarborgen, zoals het schriftelijk communiceren met hun cliënt in penitentiaire inrichtingen. Voor wat betreft het gebruik van cryptotelefoons dient daarbij bovendien het gegeven dat in bepaalde typen zaken cliënten (in ieder geval in het verleden) vooral of alleen met een cryptotelefoon communiceren, als praktische realiteit onder ogen te worden gezien.

8.4.2 Extra beveiliging als risico

Tegelijkertijd is er ook nadrukkelijk een andere kant aan het gebruik van extra beveiligde communicatiemiddelen, vooral waar het gaat om het gebruik van cryptotelefoons en – in mindere mate – chatapplicaties. Daarbij kan in de eerste plaats worden geconstateerd dat de wens om communicatie af te schermen voor de strafvorderlijke overheid, ertoe kan leiden dat gebruik wordt gemaakt van communicatiediensten die minder waarborgen bieden op het gebied van vertrouwelijkheid ten opzichte van derden. Zo is met name bij cryptotelefoons niet altijd duidelijk hoe ervoor is gezorgd dat de communicatie niet voor derden (waaronder de aanbieders van deze diensten) toegankelijk is.

Ten tweede is duidelijk dat het feit dat de identiteit van gebruikers van cryptotelefoons (deels) kan worden versluierd, juist voor geheimhouders een risico kan vormen. Wanneer met dergelijke middelen gevoerde communicatie in een opsporingsonderzoek terechtkomt, is het namelijk niet altijd eenvoudig om eventuele verschoningsgerechtigde informatie te herkennen, laat staan er (op voorhand) uit te filteren. Dit geldt met name voor communicatie via een cryptotelefoon waarvan de gebruikersgegevens

311 Zie uitgebreider par. 4.4.2 en par. 5.3.2.

niet door de advocaat aan het OM zijn doorgegeven. De dataset kan in dat geval niet preventief geschoond worden op basis van de gebruikersgegevens, zodat de mogelijkheid bestaat dat de opsporingsambtenaar de betreffende communicatie, nadat hiervan al kennis is genomen, handmatig moet verwijderen. In het licht van de verschillende, succesvolle cryptotelefoon-operaties en gelet op de wijze waarop met het doorzoeken van dit soort data wordt omgegaan en de (technische) beperkingen die daarbij gelden, is er een reëel risico dat de inhoud van de communicatie tussen advocaat en zijn cliënt door opsporingsdiensten en/of justitie wordt ingezien. Hoewel er maatregelen kunnen worden getroffen waarmee dit risico mogelijk wordt verkleind – waaronder het doorgeven van de gebruikersgegevens aan het OM – blijft dit een problematisch aspect. Dat betekent dus dat het gebruik van (dit type) extra beveiligde communicatiemiddelen, paradoxaal genoeg, nadrukkelijk een risico vormt voor de waarborging van de vertrouwelijkheid van de advocaat-cliënt-communicatie.

Daarnaast zijn er risico's voor de geheimhouding waar het gaat om het gebruik van chatapplicaties zoals WhatsApp, Signal of Telegram. Hoewel de communicatie via deze applicaties door de *end-to-end* encryptie niet kan worden meegelezen c.q. afgeluisterd, kan deze wel door inbeslagname van een telefoon bij de opsporing terechtkomen. Een aantal van de geïnterviewde advocaten is in de veronderstelling dat de communicatie in dat geval automatisch of gemakkelijk als geheimhoudercommunicatie zou moeten (kunnen) worden geïdentificeerd omdat zij gebruikmaken van een chatapplicatie die gelinkt is aan hun geheimhoudernummer. Dit is echter niet het geval, in de eerste plaats omdat het OM niet beschikt over een overzicht van alle geheimhoudertelefoonnummers, zodat een voorafgaande filtering van verschoningsgerechtigde communicatie in deze gevallen alleen kan plaatsvinden wanneer de betrokkenheid en het telefoonnummer van een advocaat bij (de bij een opsporingsonderzoek betrokken medewerkers van) het OM c.q. de opsporingsdiensten bekend is. In de tweede plaats omdat een (voorafgaande) filtering op verschoningsgerechtigde informatie om verschillende redenen praktisch (en technisch) ingewikkeld of zelfs niet haalbaar is, zo wordt door het OM aangegeven. Dit heeft onder meer te maken met de onmogelijkheid om Hansken, of een andere forensische analysetool die vertrouwelijke communicatie uit een dataset kan halen, bij elke strafzaak in te zetten. Dit alles brengt mee dat filtering vaak pas zal plaatsvinden na kennisneming van de inhoud van de communicatie.[312]

Ten derde kan worden gewezen op de risico's die samenhangen met andere kernwaarden van de advocaat, in het bijzonder onafhankelijkheid en integriteit. Ook deze risico's manifesteren zich vooral bij het gebruik van cryptotelefoons en hangen voor een belangrijk deel samen met het criminele imago dat hieraan kleeft. Risico's voor de onafhankelijkheid en de integriteit kunnen zich voordoen wanneer de advocaat bij de communicatie via een cryptotelefoon onvoldoende distantie kan bewaren tot (de criminele activiteiten van) de cliënt of de criminele groepering waarvan deze deel uitmaakt. Hierbij geldt wel dat er geen direct verband bestaat tussen de wijze waarop wordt gecommuniceerd en onvoldoende distantie tussen advocaat en cliënt. Een dergelijk risico is immers niet afhankelijk van het communicatiemiddel, maar van de wijze waarop de betreffende advocaat daarvan gebruikmaakt. Hiermee kan het risico voor de onafhankelijkheid dus enigszins worden gerelativeerd. Dat geldt in mindere mate voor het risico voor de integriteit, omdat ook beeldvorming daar nadrukkelijk onderdeel

312 Zie uitgebreider par. 6.5.2.3.

van is. Met andere woorden, ook wanneer de advocaat in de communicatie via een cryptotelefoon handelt in overeenstemming met de kernwaarden en gedragsregels, brengt de beeldvorming rondom cryptotelefoons als exclusief communicatiemiddel voor criminelen mee dat het gebruik hiervan afbreuk kan doen aan het vertrouwen in (de integriteit van) de beroepsgroep. Tot slot kan in dit verband nog worden gewezen op de mogelijke risico's voor de documentatieplicht, wanneer het door bepaalde kenmerken van de extra beveiligde communicatiemiddelen lastig(er) is om belangrijke (processtrategische) afspraken met de cliënt adequaat vast te leggen. Ook hier geldt echter dat het al dan niet ontstaan van risico's omtrent de documentatieplicht in de eerste plaats afhankelijk is van het handelen van de advocaat, en niet van het gekozen communicatiemiddel.

8.4.3 Niet extra beveiligen als risico

Waar het gebruik van extra beveiligde communicatiemiddelen onder omstandigheden een risico kan vormen voor de vertrouwelijkheid, is bij – met name – communicatie via e-mail juist het uitblijven van extra beveiliging een potentieel risico. Daarbij speelt mee dat er bij e-mailcommunicatie minder waarborgen voor de vertrouwelijkheid zijn: ten opzichte van de geheimhoudertelefoon omdat er geen systeem van automatische e-mailherkenning is; ten opzichte van chatapplicaties omdat niet standaard wordt gewerkt met *end-to-end* encryptie. In zoverre is de inhoud van e-mailcommunicatie voor zowel (strafvorderlijke) overheden als andere partijen (waaronder e-mailproviders) eenvoudiger toegankelijk. Dat is anders voor extra beveiligde e-mailapplicaties, maar uit het onderzoek blijkt dat hiervan tamelijk beperkt gebruik wordt gemaakt. Dat hangt vooral samen met praktische overwegingen en gebruiks(on)vriendelijkheid. Hoewel ook bij reguliere e-mailcommunicatie bepaalde voorzorgsmaatregelen kunnen worden getroffen, bijvoorbeeld het gebruik van e-mailadressen waarin de naam van de advocaat en/of het advocatenkantoor goed herkenbaar is, elektronische handtekeningen en/of een vermelding van de vertrouwelijke aard van de communicatie in de onderwerpregel, blijft de waarborging van de vertrouwelijkheid dan in belangrijke mate afhankelijk van de vraag hoe de geldende regels worden nageleefd. Dat daarin kwetsbaarheden zitten is (inmiddels) duidelijk.[313]

8.5 Slotbeschouwing en aanbevelingen

Mede gelet op de verschillende typen extra beveiligde en/of identiteitsversluierende communicatiemiddelen en de uiteenlopende redenen voor het gebruik daarvan, kan op basis van dit onderzoek niet één eenduidige conclusie over de (on)wenselijkheid van het gebruik van deze middelen worden getrokken. Tegen de achtergrond van de in hoofdstuk 1 geschetste aanleiding voor dit onderzoek, die onder meer is gelegen in de mogelijke relatie tussen ondermijning en het gebruik van extra beveiligde communicatiemiddelen door advocaten, en het streven om advocaten tegen ondermijning te beschermen, kunnen wel de navolgende afsluitende opmerkingen worden gemaakt.

313 Zoals onder meer uit de Box-affaire is gebleken, zie daarover uitgebreider par. 4.4.3.

Uit het onderzoek komt het beeld naar voren van een beroepsgroep die zich sterk bewust is van het fundamentele belang van de vertrouwelijkheid van advocaat-cliënt-communicatie. Dat bewustzijn lijkt de afgelopen jaren versterkt door incidenten waarbij de (strafvorderlijke) overheid de regels voor waarborging van het functionele verschoningsrecht niet (voldoende) heeft nageleefd. Die incidenten hebben ook gezorgd voor een toegenomen wantrouwen van cliënten en advocaten in (de betrouwbaarheid van) opsporingsdiensten en het OM, en hebben bijgedragen aan het zoeken naar alternatieve manieren van veilig communiceren. Andersom lijkt het gebruik van cryptotelefoons door advocaten aan de zijde van de opsporing ook aanleiding te geven tot achterdocht, wat de neiging om in gehackte cryptocommunicatie kennis te nemen van vertrouwelijke communicatie zou kunnen versterken. In zoverre lijkt dan ook sprake van een zichzelf versterkende dynamiek, waarbij het wederzijds wantrouwen dus op verschillende manieren problematisch kan zijn voor de waarborging van de vertrouwelijkheid van advocaat-cliënt-communicatie. Bovendien lijkt sprake van een zekere patstelling: advocaten wijzen op de verantwoordelijkheid van het OM om het verschoningsrecht te respecteren, maar hebben tegelijkertijd weinig vertrouwen dat dit ook (voldoende) gebeurt. Dat verklaart bijvoorbeeld de terughoudendheid om (crypto)telefoonnummers te delen. Het OM daarentegen benadrukt de eigen verantwoordelijkheid van advocaten om te kiezen voor een wijze van communiceren waardoor het verschoningsrecht in het opsporingsonderzoek op eenvoudiger wijze kan worden gewaarborgd, bijvoorbeeld door het delen van gebruikte cryptotelefoonnummers. Tegen de achtergrond van een toch al zichtbare verharding in het criminele milieu, maar ook tussen professionele deelnemers aan het strafproces, kan dit een bedreiging vormen voor het goed functioneren van de (straf)rechtspleging in het algemeen. Hoewel incidenten, zowel aan de zijde van het OM als aan de zijde van de advocatuur, nooit helemaal zijn te voorkomen, draagt het werken op basis van wederzijds wantrouwen immers niet bij aan een betere waarborging van het verschoningsrecht als een van de fundamentele voorwaarden voor een goede (straf)rechtspleging.

Tegen deze achtergrond kunnen naar aanleiding van dit onderzoek drie aanbevelingen worden geformuleerd, die – gelet op de focus van dit onderzoek – vooral betrekking hebben op het gebruik van (extra beveiligde) communicatiemiddelen door advocaten. In het licht van de hiervoor gepresenteerde conclusies is het echter van belang om ook aandacht te besteden aan de rol en verantwoordelijkheden van andere actoren in de (straf)rechtspleging. De hiernavolgende aanbevelingen vloeien voort uit de beantwoording van de tweede onderzoeksvraag, die ziet op de waardering van het gebruik van extra beveiligde en/of identiteitsversluierende communicatiemiddelen door advocaten in het licht van de in kaart gebrachte risico's daarvan. De aanbevelingen hangen inhoudelijk met elkaar samen en moeten daarom in onderling verband worden gelezen.

1. Een eerste aanbeveling houdt in dat door de betrokken actoren, in het bijzonder de NOvA en het OM, actief wordt gewerkt aan het tegengaan en verminderen van de huidige polarisatie en het wantrouwen waar het gaat om het debat over de waarborging van de vertrouwelijkheid. Waar het in dit onderzoek niet gaat om het duiden of waarderen van de oorzaken van dit wantrouwen, kan wel worden gesteld dat het van belang is om te werken aan verbetering. Zoals uit het voorgaande blijkt is de sfeer van wederzijds wantrouwen, in het bijzonder waar het gaat

om een correcte omgang met het verschoningsrecht, immers niet bevorderlijk voor het goede functioneren van de (straf)rechtspleging in het algemeen, en het waarborgen van de vertrouwelijkheid in het bijzonder. Mede gelet op de verschillende rollen en verantwoordelijkheden en de daarmee gepaard gaande onderlinge afhankelijkheden is een zeker vertrouwen tussen procesdeelnemers onontbeerlijk.[314] Vanuit de zijde van de opsporing gaat het dan om het vertrouwen dat advocaten op integere wijze bijstand verlenen en daarbij het verschoningsrecht niet misbruiken, vanuit de zijde van de advocatuur gaat het om het vertrouwen dat het verschoningsrecht door de strafvorderlijke overheid wordt gerespecteerd. Het onderlinge vertrouwen tussen partijen zou kunnen worden versterkt door aan de opsporingszijde actief in te zetten op goede naleving van de regels rondom de geheimhouding. Daarnaast zou gewerkt kunnen worden aan technische oplossingen om de voorafgaande filtering op verschoningsgerechtigde informatie bij inbeslagname van (grote hoeveelheden) data te verbeteren. Maar ook lijkt winst te behalen waar het gaat om de wijze waarop positie wordt genomen. Zo kan actief worden ingezet op het creëren van een beter begrip van elkaars rol en positie en de daarbij horende moeilijkheden. Daarbij valt bijvoorbeeld te denken aan de in dit onderzoek geconstateerde praktische (on)mogelijkheden en technische moeilijkheden omtrent de filtering van verschoningsgerechtigde informatie uit bepaalde communicatielijnen aan de zijde van het OM enerzijds. Anderzijds gaat het aan de zijde van de advocatuur onder meer om de legitieme zorgen over de waarborging van de vertrouwelijkheid en de soms ingewikkelde dilemma's die daarmee gepaard gaan. Bij de keuze voor een bepaald communicatiemiddel dienen advocaten immers ook rekening te houden met verschillende praktische (bereikbaarheids)aspecten en wensen en opvattingen van cliënten. Mede met het oog op de beeldvorming als onderdeel van de integriteit kan het bijvoorbeeld geen kwaad om (meer) te benadrukken dat met extra beveiligd communiceren op zichzelf niets mis is, om enig tegenwicht te bieden tegen het beeld advocaten iets 'verdachts' doen als ze extra maatregelen treffen. Het is van belang dat de betrokken organisaties over deze onderwerpen met elkaar het gesprek (blijven) aangaan, en daarbij aandacht hebben voor de wijze en toon waarop hierover naar buiten wordt getreden. Zo kan de erkenning dat er dingen mis zijn gegaan of mis kunnen gaan, een positieve invloed hebben op de onderlinge verhoudingen.[315]

2. In het verlengde hiervan is het aan te bevelen dat door het OM, de NOvA en de Rechtspraak, in samenspraak met de wetgever, in onderling overleg wordt nagedacht over en gewerkt aan effectieve(re) waarborgen voor het verschoningsrecht wanneer het gaat om communicatie via andere middelen dan (telefonisch contact met) de geheimhoudertelefoon. Dit overleg zou zich moeten richten op de vraag wat op dit moment – met inachtneming van alle praktische ingewikkeldheden – de beste manier is om vertrouwelijke communicatie uit het opsporingsonderzoek te houden. Ook de verdeling en invulling van ieders

314 Daarbij gaat het in de huidige situatie vooral om vertrouwen tussen OM en opsporingsdiensten enerzijds en de advocatuur anderzijds, in ieder geval tot de in het gemoderniseerde Wetboek van Strafvordering voorgestane centrale rol van de RC bij de waarborging van het verschoningsrecht een feit is, zie daarover par. 4.2.3.

315 In dat opzicht zijn onlangs wellicht eerste stappen gezet met het persbericht van het OM omtrent de gang van zaken in (onder meer) de Box-affaire, zie par. 4.3.

verantwoordelijkheden zou hiervan een onderdeel moeten zijn, evenals de uitdagingen en complicaties die de (huidige en toekomstige) digitale realiteit met zich brengt. De huidige situatie, waarin geheimhouderinformatie via verschillende communicatielijnen binnenkomt en niet bij elke lijn automatisch 'aan de poort' kan worden gefilterd, lijkt immers onwenselijk voor zowel de advocatuur als voor het OM. Bij het werken aan oplossingen kan worden gedacht aan het treffen van aanvullende maatregelen binnen de opsporing, zoals het door de NOvA voorgestelde systeem van e-mailherkenning.[316] Daarnaast blijkt ook de filtering van geheimhouderinformatie uit verschillende communicatielijnen ingewikkeld, tijdrovend en soms technisch en/of praktisch niet goed mogelijk, zodat een oplossing kan zijn gelegen in het beperken van het aantal kanalen waarover vertrouwelijk kan worden gecommuniceerd. Verder kan worden gedacht aan de ontwikkeling van een (door de NOvA beheerde) vertrouwelijke communicatiestandaard. In dat kader wordt door het OM gewezen op de aanpak van andere beroepsgroepen met eenzelfde geheimhoudingsplicht, zoals het gebruik van Zorgmail door artsen en de door de Koninklijke Notariële Beroepsorganisatie aangeboden beschermde digitale omgeving voor communicatie tussen de notaris en de cliënt. In dat verband kan bijvoorbeeld worden gedacht aan het ontwikkelen en aanbieden van een beveiligd e-mailsysteem door de NOvA, zoals ook in Frankrijk en Spanje door de balies gebeurt.[317]

3. Een derde aanbeveling houdt in dat er duidelijke kaders en richtlijnen worden gecreëerd voor het gebruik van de verschillende, al dan niet extra beveiligde communicatiemiddelen door advocaten, zoals dat immers (op dit moment) een realiteit is. Uit de hiervoor gepresenteerde conclusies vloeit voort dat dit gebruik in beginsel legitiem moet worden geacht, in ieder geval wanneer dit is ingegeven door de wens om de vertrouwelijkheid te waarborgen. Dit neemt niet weg dat aan (extra beveiligde) communicatiemiddelen zowel voor- als nadelen kunnen kleven, die bovendien variëren per type communicatiemiddel en voor wat betreft het soort risico (bijvoorbeeld inbreuken door derde partijen of door overheden). Het creëren van duidelijke kaders en richtlijnen voor het gebruik van dergelijke middelen door advocaten is in dat licht wenselijk, waarbij meespeelt dat veel advocaten niet beschikken over toereikende (technische) kennis om steeds zelf een goed geïnformeerde keuze te maken. Een onderdeel van die kaders kan zijn dat advocaten er zich bij hun werkzaamheden bewust van dienen te zijn dat geen enkel communicatiemiddel uit oogpunt van vertrouwelijkheid volledig veilig is. In dat licht is het voorstelbaar dat bespreking in persoon de voorkeur verdient, zoals in dit onderzoek door veel respondenten werd aangegeven, en dat bij communicatie op andere wijze zo min mogelijk inhoudelijke c.q. gevoelige informatie wordt uitgewisseld. Tegelijkertijd brengt de praktische realiteit mee dat ook inhoudelijk overleg moet kunnen plaatsvinden met communicatiemiddelen zoals telefoon, chatapplicaties en/of e-mail. Duidelijke richtlijnen of adviezen kunnen daarbij helderheid bieden, bijvoorbeeld over de chatapplicatie(s) die het meest veilig worden geacht. Als praktisch voorbeeld kunnen de door de American Bar Association

316 *Advies Aanwijzing omgang verschoningsgerechtigd materiaal* 2023, p. 3.
317 Zie uitgebreider par. 7.4.

gepubliceerde kaders en documenten worden genoemd, waarin niet alleen het belang van goede beveiliging wordt benadrukt, maar ook praktische handvatten worden geboden.[318] Gelet op de specifieke risico's voor e-mailverkeer ligt het verder uit oogpunt van bescherming van de vertrouwelijkheid voor de hand om vaker gebruik te maken van e-mail met extra beveiligingsfunctionaliteiten. In dat kader kan ook worden gedacht aan een verplichting tot versleuteling bij (meer inhoudelijke) e-mailcommunicatie, of facilitering hiervan door middel van een specifiek e-mailplatform.[319] Aanbevelingswaardig is voorts dat advocaten handvatten krijgen aangereikt hoe zij kunnen handelen wanneer zij gebruik willen maken van minder conventionele communicatiemiddelen, waarbij in het bijzonder aan cryptotelefoons kan worden gedacht. Gelet op de potentiële risico's voor de vertrouwelijkheid en (in wat mindere mate ook) integriteit en onafhankelijkheid brengt het gebruik van deze middelen een extra zorgplicht voor de advocaat met zich mee. In het kader van die zorgplicht lijkt het in ieder geval wenselijk dat een advocaat voorafgaand aan het gebruik van een cryptotelefoon overleg voert met de deken. Om de herkenbaarheid als geheimhouder te bevorderen is verder aan te bevelen dat de advocaat gebruikmaakt van een als zodanig herkenbare *nickname*. Ten slotte kan de advocaat, om voorafgaande filtering van de verschoningsgerechtigde communicatie mogelijk te maken, er (ook) voor kiezen om het gebruikte cryptotelefoonnummer (op voorhand) met het OM te delen.

318 Zie par. 7.3.
319 Vgl. daarover par. 7.4.

Literatuur

***Advies Aanwijzing omgang verschoningsgerechtigd materiaal* 2023**
Advies Aanwijzing omgang verschoningsgerechtigd materiaal (Adviescommissie strafrecht NOvA), 9 februari 2023.

Beyens, Kennes & Tournel 2016
K. Beyens, P. Kennes & H. Tournel, 'Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview', in: T. Decorte & D. Zaitch, *Kwalitatieve Methoden en Technieken in de Criminologie,* Culemborg: Centraal Boekhuis bv 2016, p. 187-222.

De Bree & Buruma 2022
R. de Bree & Y.E.A. Buruma, 'Verschoningsrecht in het gedrang', *Adv. bl.* 2022/8, p. 94-97.

Brent & Kraska 2021
J.B. Brent & P.B. Kraska, 'In Depth Interviewing', in: J.C. Barns & D.R. Forde, *The Encyclopedia of Research Methods in Criminology and Criminal Justice,* Hoboken: Willey 2021, p. 405-411.

Boutellier, Van Steden, Eski & Boelens 2020
H. Boutellier, R. van Steden, Y. Eski & M. Boelens, 'Een einde aan ondermijning: over de opkomst en werking van een nieuwe veiligheidsstrategie', *Tijdschrift voor Veiligheid* 2020/19, p. 3-16.

Brouwer 2022
D.V.A. Brouwer, 'Naar een gesloten 'ZwaCri-balie'?', *NJB* 2022/289, p. 333-338.

***Cybersecurity Woordenboek* 2021**
Cybersecurity Woordenboek: van Cybersecurity naar Nederlands, Cyberveilig Nederland i.s.m. Cybersecurity Alliantie 2021.

Decorte 2016
T. Decorte, 'Kwalitatieve data-analyse', in: T. Decorte & D. Zaitch (red.), *Kwalitatieve methoden en technieken in de criminologie*, Culemborg: Centraal Boekhuis bv 2016, p. 463-512.

Doorenbos & Rosing 2020
D.R. Doorenbos & M.E. Rosing, 'Recht doen aan het verschoningsrecht', *TvSO* 2020/5-6, p. 217-224.

Doorenbos 2022
D.R. Doorenbos, 'E-mails en verschoningsrecht – kortsluiting bij het OM', njb.nl, 18 september 2022.

Droogleever Fortuyn 2022
S. Droogleever Fortuyn, 'OM opnieuw uit de bocht met vertrouwelijke communicatie', advocatenblad.nl, 6 april 2022.

Duò 2023
M. Duò, 'De top 14 beveiligde e-mailproviders van 2023', kinsta.nl, 22 juni 2023.

***Een maatschappelijke orde* 2006**
Een maatschappelijke orde (Commissie Van Wijmen) Bijlage brief van de minister van Justitie ter aanbieding van het rapport van de Commissie Advocatuur 'Een maatschappelijke Orde', 30.300 VI, nr. 144, 24 april 2006.

Eurojust 2021
Eurojust. *Report on Drug Trafficking – Experiences and challenges in judicial cooperation*. 2022.

Eurojust 2022
Eurojust. *Eurojust annual Report 2021: 20 years of criminal justice across borders*. 2021.

Europol & Eurojust 2019
Europol & Eurojust. *First report of the observatory function on encryption*. The Hague 2019.

Europol & Eurojust 2021
Europol & Eurojust. *Third report of the observatory function on encryption*. 2021.

Fanoy 2018
N.A.M.E.C. Fanoy, *De geheimhoudingsplicht en het verschoningsrecht van de advocaat* (diss. UvA), Antwerpen/Apeldoorn: Maklu Uitgevers 2018.

Fanoy 2019
N.A.M.E.C. Fanoy, 'Het professionele verschoningsrecht in het nieuwe wetboek', *Platform Modernisering Strafvordering* 2017.

Fanoy 2022
N.A.M.E.C. Fanoy, 'Kroniek functioneel verschoningsrecht; belangwekkende uitspraken in coronatijd', *NTS* 2022/1, p. 13-22.

Gloudemans-Voogd 2018
N. Gloudemans-Voogd, 'Nieuwe anti-afluistertelefoons voor geheimhouders', advocatenblad.nl, 12 maart 2018.

Haenen & Meeus 2023
M. Haenen & J. Meeus, 'Advocaat Inez Weski is opgepakt, verdacht van doorspelen informatie van Ridouan Taghi', *NRC* 21 april 2023.

***Hansken – Informatieblad Geheimhoudersinformatie NFI* 2020**
Hansken – Informatieblad Geheimhoudersinformatie (Nederlands Forensisch Instituut), 2020.

Heuvel, Huberts & Muller 2012
J.H.J. van den Heuvel, L.W.J.C. Huberts & E.R. Muller (red.), *Integriteit. Integriteit en integriteitsbeleid in Nederland* (Handboeken Veiligheid), Deventer: Kluwer 2012.

Hirsch Ballin & Oerlemans 2023
M.F.H. Hirsch Ballin & J.J. Oerelemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden', *DD* 2023/2, p. 18-38.

***Informatieblad NFI* 2023**
Informatieblad – Vernietigen van digitale sporen met verschoningsgerechtigde informatie (Nederlands Forensisch Instituut, 2023.

IOCTA report 2021
Internet Organised Crime Threat Assessment (IOCTA), Europol 2021.

Jansen e.a. 2023
J. Jansen e.a, *De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden* (WODC Rapport 3218), 2023.

Karssing 2006
E.D. Karssing, *Integriteit in de beroepspraktijk* (diss. Rotterdam), Assen: Koninklijke Van Gorcum 2006.

Kerr & Schneier 2018
O. S. Kerr & B. Schneier, 'Encryption Workarounds', *Georgetown Law Journal* 2018, 106(4), p. 989-1020.

Kestemont 2018
L. Kestemont, *Handbook on Legal Methodology. From Objective to Method*, Cambridge: Intersentia 2018.

Laumans & Vugts 2023
W. Laumans & P. Vugts, 'De familie van Taghi bleef Inez Weski bestoken als doorgeefluik voor berichten', *Het Parool* 29 april 2023.

Laumans & Vugts 2022
'Politie keek vijf maanden mee met versleutelde communicatie criminelen, 42 aanhoudingen', *Het Parool* 3 februari 2023.

Lewis, Zheng & Carter 2017
J. A. Lewis, D. E. Zheng & W. A. Carter, *The Effect of Encryption on Lawful Access to Communication and Data*, (Center for Strategic & International Studies), 2017.

Maesschalck 2016
J. Maesschalck, 'Methodologische kwaliteit in het kwalitatief onderzoek', in: T. Decorte & D. Zaitch, *Kwalitatieve Methoden en Technieken in de Criminologie,* Culemborg: Centraal Boekhuis bv 2016, p. 131-160.

Mannheims & Felix 2021
L. Mannheims & T. Felix, 'Verschoningsrecht', in: P.T.C. van Kampen & N. van der Laan (red.), *Handboek Verdediging*, Deventer: Wolters Kluwer 2021.

Meeus 2017
J. Meeus, 'OM vraagt advocaten gebruik van PGP-telefoon te melden', *NRC* 8 juni 2017.

Van Miltenburg, Van Straaten & Bouwmeester 2022
C. van Miltenburg, G. van Straaten & J. Bouwmeester, *Agressie, intimidatie en bedreiging bij advocaten* (I&O Research), Amsterdam 2022.

Mortelmans 2016
D. Mortelmans, 'Het kwalitatief onderzoeksdesign', in: T. Decorte & D. Zaitch, *Kwalitatieve Methoden en Technieken in de Criminologie,* Culemborg: Centraal Boekhuis bv 2016, p. 81-128.

Mos & Polman 2023a
B. Mos & J. Polman, 'OM ging ernstig in de fout tijdens onderzoek naar Inez Weski', *Financieel Dagblad* 17 juli 2023.

Mos & Polman 2023b
B. Mos & J. Polman, 'Rechters breken met geheimhoudersofficier in Weski-onderzoek', *Financieel Dagblad* 20 juli 2023.

Naef 2022
T. Naef, 'The Global Reach of the Right to Data Protection', in: T. Naef, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*. Cham: 2022, p. 19-113.

Nationaal Social Media Onderzoek 2023
Nationaal Social Media Onderzoek, Newcom Research & Consultancy 2023.

NOvA 2017
Adviescommissie Strafrecht van de NOvA, *Advies van de Nederlandse Orde van Advocaten inzake de wetsvoorstellen tot vaststelling van de boeken 1 en 2 van het Wetboek van Strafvordering*, 30 juni 2017.

Oerlemans 2021
J.J. Oerlemans, 'iOCTA-rapport 2021', jjoerlemans.com, 22 november 2021.

Oerlemans 2022a
J.J. Oerlemans, 'Oprichter van crypotelefoonaanbieder Ennetcom veroordeeld', *TBS&H* 2022/2, p. 138-142.

Oerlemans 2022b
J.J. Oerlemans, 'Overzicht cryptophone-operaties', jjoerlemans.com, 14 november 2022.

Oerlemans 2022c
J.J. Oerlemans, 'Meer duidelijkheid over de ANOM-operatie', jjoerlemans.com, 14 november 2022.

Oerlemans & Van Toor 2022
J.J. Oerlemans & D.A.G. van Toor, 'Legal Aspect of the EncroChat Operation: A Human Rights Perspective', *European Journal of Crime, Criminal Law and Criminal Justice* 2022/3-4, p. 309-328.

OM 2017
OM, *Advies van het Openbaar Ministerie (OM) bij het wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering het opsporingsonderzoek)*, 5 juli 2017.

Pfefferkorn 2023
R. Pfefferkorn, 'My comment to the UK government on its proposal to ban "bespoke" "sophisticated" encrypted phones', cyberlaw.stanford.edu, 23 februari 2023.

Pijnappels 2022
K. Pijnappels, 'Het eindeloze gevecht om het verschoningsrecht', *Adv. bl.* 2022/03, p, 18-21.

Project bijstand TK Modernisering Sv 2023
Project bijstand Tweede Kamer modernisering Wetboek van Strafvordering, *Inhoudelijke rapportage Boek 2: Het opsporingsonderzoek*, 11 september 2023.

***Rapport van de Commissie Telefonie Voor Justitiabelen* 2009**
Rapport van de Commissie Telefonie Voor Justitiabelen (Onderzoeksrapport Commissie 'Telefonie voor Justitiabelen'), bijlage bij Kamerstukken II 2019/20, 24587, 756.

Rensen 2023
F. Rensen, 'Luiden de vijf explosies van afgelopen weekend het einde in voor de app Telegram in Nederland?', *De Volkskrant* 20 september 2023.

Ries, Simek & Nelson 2016
D.G. Ries, J.W. Simek & S.D. Nelson, *Encryption Made Simple for Lawyers,* American Bar Association 2016.

Rietbroek 2018
J. Rietbroek, 'Encryptie-telefoons voor advocaten: "Ik wilde het uit de schimmige sfeer halen"', advocatie.nl, 14 maart 2018.

Royer & Van Leeuw 2022
S. Royer & R. van Leeuw, 'Cryptotelefoons, privacyvriendelijke applicaties en het vermoeden van onschuld', *TBS&H* 2022/2, p. 90-97.

SOCTA report 2021
European Union Serious and Organised Crime Threat Assessment (SOCTA), Europol 2021.

Spronken 2022
T. Spronken, 'Verschoningsrecht en 'repressieve' druk', *NJB* 2022/1188, p. 1515.

***Toezichtsrapport CTIVD* 2017**
Toezichtsrapport Over de inzet van bijzondere bevoegdheden jegens advocaten en journalisten door de AIVD en de MIVD (Rapport Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten van 7 februari 2017).

Van Toor 2022
D.A.G. van Toor, 'Het enkele gebruik van cryptophones als basis voor procesrechtelijke concepten', *TBS&H* 2022/2, p. 77-81.

Vermeulen, Soudijn & Van der Leest 2021
I. Vermeulen, M. Soudijn & W. van der Leest, 'Open heimelijke netwerken in de Nederlandstalige georganiseerde synthetische-drugscriminaliteit', *Tijdschrift voor Criminologie* 2021/2, p. 187-211.

***Vision Statement Hansken* 2021**
Vision Statement Hansken (Nederlands Forensisch Instituut), 2021.

Vugts & Laumans 2021
P. Vugts & W. Laumans, 'Politie onderschept 80 miljoen versleutelde berichten van criminelen', *Het Parool* 9 maart 2021.

Winkels 2022
J. Winkels, 'Digitale geheimhouderinformatie: vernietigen ≠ bewaren', njb.nl, 22 augustus 2022.

Soudijn & de Been 2020
M.R.J. Soudijn en W.H.J. de Been, 'Law enforcement and money laundering: Big data is coming', in: P. van Duyne e.a. (red.), *Criminal defiance in Europe and beyond*, Den Haag: Eleven 2020, p. 399-426.