Redactioneel

Het *enkele* gebruik van *cryptophones* als basis voor procesrechtelijke concepten

D.A.G. van Toor PhD LLM BSc*

1. Inleiding

Kijkers van de HBO-serie *The Wire*[1] (of andere politieseries met focus op digitale opsporing) kennen het kat-en-muisspel tussen verdachten en de politie. Het gebruik van nieuwe technologische mogelijkheden door verdachten wordt steevast gevolgd door een reactie van de autoriteiten. Zo worden in *The Wire* (en in de realiteit) *burner phones* gebruikt, nadat normale mobiele telefoons in de ban worden gedaan door de criminelen omdat de autoriteiten eenvoudig gegevens van providers kunnen vorderen. Burner phones zijn prepaid mobiele telefoons waarvoor geen gebruikersgegevens worden afgeven aan de provider (en zijn daarom bijvoorbeeld in België verboden[2]). Hierdoor lopen de autoriteiten achter de feiten aan: zodra de prepaid minuten op zijn, wordt de telefoon inclusief simkaart *geburned* (lees: weggegooid of anderszins vernietigd), terwijl de autoriteiten in de korte periode dat een persoon een burner phone gebruikt geen telefoontap *up and running* kunnen krijgen. Immers, het is bij burner phones meestal onduidelijk welk nummer door een verdachte wordt gebruikt, omdat de gebruikersgegevens van prepaid telefoons niet door providers worden vergaard. De reactie van de autoriteiten is dat zij gaan zoeken naar manieren om het nummer van een prepaid telefoon zonder tussenkomst van providers te achterhalen. Hiervoor zijn IMSI-*catchers* ingezet: dit is een *man-in-the-middle-attack*. De IMSI-catcher fungeert als telefoonpaal waarmee een mobiele telefoon contact zoekt (en telefoons hebben de automatische functie ingebouwd naar het dichtstbijzijnde, optimale netwerk te zoeken), terwijl de IMSI-catcher niets anders doet dan als tussenstation het signaal uitlezen en doorsturen naar een echte telefoonpaal. Op die manier kan het telefoonnummer dat wordt gebruikt, worden uitgelezen. Hierdoor vormt de IMSI-catcher een methode om achter de telefoonnummers van prepaid simkaarten te komen, om er volgens een telefoontap op te kunnen plaatsen.

Zoals iedereen weet die fan is van een politieserie of die enige betrokkenheid heeft met de strafrechtspleging, houdt dit kat-en-muisspel nooit op. De burner phones en de IMSI-catcher zijn zeker niet de laatste gadgets als het gaat om het geheimhouden van communicatie door criminelen en de drang van de autoriteiten om deze gesprekken te kunnen beluisteren. De laatste mode is dat criminelen veelvuldig gebruikmaken van *cryptophones* en cryptocommunicatie. Dit is, eenvoudig gezegd, niets anders dan een vorm van versleutelde communicatie (waarvoor in sommige gevallen smartphones speciaal worden geprogrammeerd zodat daarmee niets anders kan worden gedaan dan versleutelde communicatie versturen en ontvangen – dat is dan een zogenoemde cryptophone –), vergelijkbaar met populaire communicatie-applicaties zoals WhatsApp. Criminelen waanden zich hiermee veilig – waarschijnlijk mede door de marketingstrategie van aanbieders van cryptophones en cryptocommunicatie – en communiceerden, in strijd met alle geldende regels over 'gedegen' criminele aspi-

* D.A.G. van Toor PhD LLM BSc is als universitair docent verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtstaat en Rechtspleging van de Universiteit Utrecht.

1 Een must-see!

2 Wet van 1 september 2016 tot wijziging van art. 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van art. 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *BS* 7 december 2016. Zie nader de bijdrage van Royer en Deleeuw in dit nummer.

doi: 10.5553/TBSenH/229567002022008002001

raties, openlijk en zonder codetaal. Door de ontmanteling van meerdere cryptoaanbieders (bijvoorbeeld *Ennetcom*, *EncroChat* en *Sky ECC*) en het onder de vlag van de autoriteiten uitbrengen van cryptodienst *ANOM* hebben de autoriteiten een schat aan informatie bemachtigd.

Zoals altijd heeft deze instrumentele ontwikkeling echter een rechtsbeschermende keerzijde.[3] In de laatste maanden hebben veel rechtsbeschermende thema's met betrekking tot cryptocommunicatie in de wetenschap de revue gepasseerd. Zo bestaat er, door het enorm toegenomen gebruik van encryptie, wederom aandacht voor gedwongen decryptie.[4] Een ander probleem doet zich voor wanneer een cryptoaanbieder wordt ontmanteld. Op dat moment wordt namelijk niet alleen bewijs verkregen tegen een individueel persoon, maar worden tera- of misschien wel petabytes aan informatie vergaard (terwijl nog niet duidelijk is tegen welke personen verdenkingen rijzen op basis van die informatie of welke informatie als bewijs in een strafzaak kan worden gebruikt). Met andere woorden, de (belastende) informatie is voorhanden na een ontmanteling van een cryptoaanbieder, maar de verdachten zijn nog niet in beeld. De vraag rijst in hoeverre een individuele verdachte toegang dient te krijgen tot een volledige dataset of de achterliggende analysesoftware,[5] bijvoorbeeld om na te gaan hoe uit de wirwar van informatie een verdenking tegen hem is gerezen. Verder wijs ik nog op de discussie over het gebruik van cryptocommunicatie voor niet-criminele doeleinden, bijvoorbeeld als de verdachte de cryptophone ook gebruikt om te communiceren met zijn advocaat,[6] en het achterhouden van informatie met betrekking tot de ontmanteling van cryptoaanbieders door een internationaal justitieel samenwerkingsverband op basis van het internationale vertrouwensbeginsel.[7]

Ondanks alle publicaties waarnaar zojuist is verwezen (en vele andere), is de discussie over cryptodiensten in het Nederlandse strafrecht nog lang niet beëindigd. Een van de onderwerpen die tot nu toe niet de revue heeft gepasseerd, is hoe het enkele *gebruik* van een cryptophone kan of mag worden gewaardeerd, ondanks het feit dat het gebruik van zo'n smartphone legaal is. Zo kan de vraag rijzen of het gebruik van zo'n dienst voldoende is voor het aannemen van een redelijk vermoeden van schuld aan een strafbaar feit, waardoor andere opsporingsbevoegdheden kunnen worden ingezet, of zelfs voldoende kan zijn voor het aannemen van ernstige bezwaren. Daarnaast kan worden gedacht aan de discussie of het gebruik van een cryptodienst voldoende is voor het aannemen van een grond voor voorlopige hechtenis: blijkt uit het feit dat de verdachte er alles aan heeft gedaan om versleuteld te communiceren dat aangenomen kan worden dat van de verdachte recidivegevaar uitgaat? In dit redactioneel plaats ik het *enkele gebruik* van cryptodiensten in het licht van twee strafvorderlijke concepten, namelijk het redelijk vermoeden van schuld en het recidivegevaar.

2. Als bewijs voor een redelijk vermoeden van schuld aan een strafbaar feit

Een van de strafvorderlijke concepten die ik bespreek, is het verdachtebegrip, dat veelal als vereiste geldt voor veel van de Nederlandse opsporingsbevoegdheden en dwangmiddelen.[8] Artikel 27 lid 1 Sv luidt: 'Als verdachte wordt vóórdat de vervolging is aangevangen, aangemerkt degene te wiens aanzien uit feiten of omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit voortvloeit.' Centraal in de beoordeling of iemand als verdachte kan worden aangemerkt, is of uit feiten en omstandigheden een *redelijk vermoeden* van schuld aan een strafbaar feit kan worden afgeleid. Die beoordeling moet zijn gebaseerd op objectieve en concrete informatie dat een strafbaar feit heeft plaatsgevonden of dat een persoon mogelijk betrokken is bij een strafbaar feit.[9] Zo kan een anonieme tip in beginsel voldoende zijn voor een *redelijk vermoeden*,[10] bijvoorbeeld wanneer de tip concrete en verifieerbare inhoud bevat.[11] Algemene ervaringsregels op zichzelf of een algoritmische voorspelling zijn in beginsel onvoldoende voor het aannemen van datzelfde redelijk vermoeden.[12]

Het gebruik van een cryptophone als grond voor een redelijk vermoeden van schuld lijkt het meest op een algemene ervaringsregel. Die zou dan bijvoorbeeld als volgt kunnen luiden: cryptophones worden uitsluitend, of ten minste in een grote meerderheid van de gevallen, gebruikt door criminelen. Andersom: als een persoon een cryptophone gebruikt, is het, op basis van de algemene ervaringsregel over het gebruik van zulke diensten, redelijk om aan te nemen dat die persoon strafbare feiten

3 Vgl. R. Foqué & A.C. 't Hart, *Instrumentaliteit en rechtsbescherming. Grondslagen van een strafrechtelijke waardendiscussie*, Arnhem: Gouda Quint 1990.

4 D.A.G van Toor, W. Albers, C.M. Taylor Parkins-Ozephius & T. Beekhuis, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131; T. Beekhuis, C.M. Taylor Parkins-Ozephius, D.A.G. van Toor & W. Albers, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 2)', *Computerrecht* 2020/179.

5 H. Henseler, 'Het inzagerecht en de groeiende omvang van digitaal bewijs', *EeR* 2020/6; M. Galič, 'De rechten van de verdediging in omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BSb* 2021/2.

6 www.advocatenorde.nl/nieuws/advocaten-kunnen-zich-bij-om-melden-als-geheimhouder-in-versleutelde-chatdiensten, laatst geraadpleegd op 11 november 2021.

7 J.S. Boeser, 'Cybersecurity en datagedreven opsporing: stand van zaken met betrekking tot de interceptie van versleutelde cryptocommunicatie', *TBS&H* 2021, p. 351-356.

8 G.J.M. Corstens, bewerkt door M.J. Borgers & T. Kooijmans, *Het Nederlandse strafprocesrecht*, Deventer: Kluwer 2021, p. 97.

9 Corstens 2021, p. 98-99.

10 HR 11 maart 2008, ECLI:NL:HR:2008:BC1367.

11 Corstens 2021, p. 99.

12 R.A. Hoving, 'Verdacht door een algoritme. Kan predictive policing leiden tot een redelijke verdenking?', *DD* 2019/41.

doi: 10.5553/TBSenH/229567002022008002001

pleegt.[13] Nu ligt het voor de hand dat deze ervaringsregel waar is. Bij vele aanbieders van cryptodiensten dienen grote bedragen cash te worden betaald (bijvoorbeeld bij Ennetcom[14] en EncroChat[15]) om een cryptophone van die aanbieder te bemachtigen en een abonnement af te sluiten. Uit het *affidavit* dat ten grondslag lag aan *Operation Trojan Shield*[16] blijkt dat de ANOM-telefoons alleen via een ons-kent-ons-regel konden worden bemachtigd[17] en uit de analyse van de *beta*-fase blijkt dat alle telefoons door criminelen werden gebruikt.[18] Natuurlijk geldt dat laatste niet voor alle cryptoaanbieders: het lijkt erop dat ook advocaten de diensten hebben gebruikt.[19] Hoe dan ook, de grote meerderheid van de gebruikers lijken de cryptodiensten voor criminele doeleinden te gebruiken.

Het probleem bij het aannemen van een redelijk vermoeden van schuld aan een *strafbaar feit* ligt in dat laatste criterium besloten. Waar een algoritme *soortgelijke* strafbare feiten kan voorspellen,[20] is dit bij een cryptophone nauwelijks mogelijk. De zaken die zijn gebaseerd op de hacks van de eerdergenoemde aanbieders betreffen een breed palet aan delicten: vermogenscriminaliteit, gewelds- en levensdelicten en overtredingen van de Opiumwet. Hiermee lijkt het vrijwel onmogelijk om het *enkele* gebruik van een cryptophone als voldoende voor een redelijk vermoeden van schuld aan een (concreet) strafbaar feit aan te merken. Zo oordeelde de rechter-commissaris in het onderzoek Werl onlangs dat het enkele gebruik van een Sky ECC-toestel onvoldoende is 'voor een redelijk vermoeden van concrete betrokkenheid van de individuele gebruiker bij het in georganiseerd verband beramen of plegen van misdrijven in de zin van artikel 126o lid 1 Sv',[21] te weten voorlopige hechtenis-feiten die ernstige inbreuk op de rechtsorde opleveren.

De enige uitweg is de gebruiker van een cryptophone altijd als een verdachte van deelname aan een criminele organisatie te bestempelen. Dit is enigszins vergezocht, maar niet geheel onredelijk.[22] Zo hoeft de deelnemingsgedraging aan de organisatie niet nader te worden gespecificeerd en bewezen,[23] worden weinig eisen gesteld aan de 'organisatie' – namelijk een 'samenwerkingsverband, met een zekere duurzaamheid en structuur, tussen de verdachte en ten minste één andere persoon'[24] – en is het daadwerkelijk plegen van strafbare feiten ook niet noodzakelijk voor een veroordeling voor artikel 140 Sr.[25] Tevens is geen opzet vereist op concrete misdrijven begaan door de organisatie.[26] De stelling van de vervolgende autoriteit kan dan zijn dat de cryptophone wordt gebruikt om regelmatig en voor een bepaalde duur met anderen over strafbare feiten te communiceren[27] en dat is voldoende voor een verdenking van overtreding van artikel 140 Sr. Het gebruik van een kostbare cryptophone door alle leden van de organisatie – want met een cryptophone kan alleen met een andere cryptophone worden gecommuniceerd – is dan het bewijs voor de duurzaamheid en beslotenheid van de organisatie. Een verder uitgangspunt is de algemene ervaringsregel, volgend uit onder andere de onderzoeken naar EncroChat en ANOM, dat een grote meerderheid van de gebruikers de telefoon voor criminele doeleinden gebruikt, dat een cryptophone juist wordt gebruikt om contact te onderhouden met medeverdachten binnen een (criminele) organisatie, en dat de geldinvestering in cryptophones duidelijk maakt dat de organisatie een bepaalde duurzaamheid kent. Artikel 140 Sr biedt dan, vanwege de

13 Uit de in mijn artikel in dit themanummer te bespreken beschikking van het *Landgericht* Berlijn blijkt dat op de peildatum 12 juni 2020 ten minste 67,3 % van de EncroChat-gebruikers zijn cryptophone gebruikt ten behoeve van criminele doeleinden. Onduidelijk blijft in hoeverre de overige gebruikers EncroChat voor niet-criminele doeleinden gebruiken. Onder de resterende een derde van de gebruikers vallen namelijk ook inactieve gebruikers of gebruikers die niet duidelijk aan criminaliteit zijn te linken (bijv. doordat niet openlijk wordt gecommuniceerd of omdat misschien sprake is van hand-en-spandiensten waarvan de relevantie voor een strafbaar feit niet direct duidelijk is).

14 Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085.

15 www.volkskrant.nl/nieuws-achtergrond/waarom-criminelen-geen-whatsapp-gebruiken-en-meer-over-hoe-de-politie-kon-meelezen~b4c7afd5/?referrer=https%3A%2F%2Fwww.google.com%2F, laatst geraadpleegd op 29 november 2021.

16 Zie uitgebreid: C.M. Taylor Parkins-Ozephius, I.N. De Wit, D.A.G. van Toor & T. Beekhuis, 'De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel', *TBS&H* 2021, p. 322-333.

17 www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 16, laatst geraadpleegd op 29 november 2021.

18 www.documentcloud.org/documents/20799201-operation-trojan-shield-court-record, rn. 15, laatst geraadpleegd op 29 november 2021.

19 In het Advocatenblad is namelijk een oproep verschenen gericht aan advocaten die zulke diensten van gekraakte aanbieders hebben gebruikt zich te melden ten behoeve van het waarborgen van het verschoningsrecht. www.advocatenorde.nl/nieuws/advocaten-kunnen-zich-bij-ommelden-als-geheimhouder-in-versleutelde-chatdiensten, laatst geraadpleegd op 29 november 2021.

20 Zie bijvoorbeeld het algoritme dat in de podcast *Algorithm* wordt beschreven. Ook het *Sensingproject Outlet Roermond* was gebaseerd op het idee dat gelijksoortige vermogenscriminaliteit kon worden voorspeld. Zie voor een beschrijving en analyse van dat laatste project: L. Stevens, M. Hirsch Ballin, M. Galič e.a., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling', *TBS&H* 2021/, 4, p. 234-245.

21 Rb. Amsterdam 26 november 2021, ECLI:NL:RBAMS:2021:6866.

22 Vgl. EHRM 20 juli 2021, ECLI:CE:ECHR:2021:0720JUD001969918 (*Akgün t. Turkije*), par. 167. Hierin zet het EHRM de deur open om het gebruik van cryptocommunicatie-applicatie en -producten als voldoende redengevend voor het aannemen van een redelijk vermoeden van schuld te zien. Dat hangt wel samen met de karakteristieken van de applicatie of het product. Zo is de applicatie waarover *Akgün* gaat een applicatie die in gangbare portalen vrij downloadbaar was. Hierbij kan moeilijk bij voorbaat worden vastgesteld dat dit een applicatie is die criminelen gebruiken voor hun communicatie-infrastructuur. Dit is anders bij dure producten (*EncroChat*) die niet op de vrije markt beschikbaar zijn (*ANOM*). Zie nader mijn annotatie bij *Akgün* in *EHRC Updates* februari 2022.

23 F.C.W. de Graaf, 'Deelneming aan een criminele organisatie en ne bis in idem - De toepasselijkheid van het ne bis in idem-beginsel bij vervolging wegens deelneming aan een criminele organisatie na vervolging wegens een concreet misdrijf en vice versa', *NTS* 2021/04, par. 2.2.

24 HR 22 januari 2008, ECLI:NL:HR:2008:BB7134.

25 J.M. ten Voorde, 'Commentaar bij artikel 140 Sr', *T&C Strafrecht*, actueel tot 1 februari 2021.

26 HR 8 oktober 2002, *NJ* 2003/64.

27 Zoals eerder gemeld, heeft ruim twee derde van de gebruikers van EncroChat de cryptodienst voor criminele doeleinden gebruikt; gebruikte *elke* bezitter van een ANOM-toetsel het apparaat voor criminele doeleinden; en blijkt uit de metadata dat Sky ECC 'wordt gebruikt bij het plegen van ernstige strafbare feiten die een ernstige inbreuk op de rechtsorde opleverden'. (Het citaat is afkomstig uit Rb. Amsterdam 26 november 2021, ECLI:NL:RBAMS:2021:6866.)

enorme reikwijdte van die bepaling, mogelijkheden om te reageren op nog onbekende concrete handelingen. Hiermee wordt de gebruiker van een cryptophone vogelvrij: hij wordt van deelname aan een criminele organisatie verdacht op basis van het enkele gebruik van de cryptophone en daarmee bestaat een grond om die telefoon in beslag te nemen. Hierdoor kunnen vervolgens, als de telefoon met succes wordt gekraakt of ontgrendeld, de precieze rol en handelingen van de verdachte duidelijk worden.

3. Als bewijs voor een grond voor voorlopige hechtenis

Naast de bovenstaande kwestie (en daaropvolgend dat het eventuele gebruik van een cryptophone ook relevant kan zijn voor de beoordeling van andere verdenkingsmaatstaven), volgt uit de Duitse feitenrechtspraak een andere wijze van het gebruik van de cryptophone voor de beoordeling van strafprocesrechtelijke concepten. In de zaak waarin het *Amtsgericht* Flensburg moest oordelen,[28] betrof het geschilpunt of het feit dat de verdachte een cryptophone gebruikte voldoende is om recidivegevaar als grond voor voorarrest aan te nemen indien de verdachte geen strafblad heeft. In Duitsland geldt dat aan de motivering voor het recidivegevaar hoge eisen worden gesteld en dat, wanneer een eerdere veroordeling ontbreekt, het recidivegevaar alleen kan worden aangenomen indien zwaarwegende gronden aanleiding geven om een hoge waarschijnlijkheid van recidive vast te stellen (‘*sonstige schwerwiegende Gründe die Wiederholung mit hoher Wahrscheinlichkeit erwarten lassen*’).[29] De vaststelling van het recidivegevaar moet worden gebaseerd op feiten en omstandigheden waaruit blijkt dat de verdachte zo’n sterke impuls (‘*starke Neigung*’) heeft om gelijksoortige delicten te plegen wanneer hij zijn proces in vrijheid kan afwachten.

Het onderwerp van deze beschikking – het gaat namelijk om beroep tegen de voorlopige hechtenisbeschikking – is een gebruiker van EncroChat. Niet duidelijk uit de beschikking blijkt of de cryptophone van de verdachte na zijn aanhouding in beslag is genomen en vervolgens is uitgelezen – de verdachte en medeverdachte werden namelijk al geobserveerd – of dat de analyse van de EncroChat-berichten in het buitenland aanleiding hebben gegeven tot aanhouding. Hoe dan ook, de inhoud van de communicatie, die is verstuurd en ontvangen door middel van de cryptophone van de verdachte, is bekend bij de autoriteiten. Het Amtsgericht Flensburg legt echter ook het feit dat de verdachte een cryptophone heeft gebruikt, waaraan hoge kosten zijn verbonden,[30] ten grondslag aan de aanname van het recidivegevaar, omdat de aanschaf van een cryptophone een bijzonder hoge bereidheid laat zien om wederrechtelijk verkregen vermogen te vergaren. Tevens laat het gebruik van een cryptophone, waarmee contact wordt onderhouden met een crimineel netwerk – in het geval van de onderhavige verdachte zijn dat 16 contactpersonen –, zien dat de verdachte midden in de criminaliteit staat. Volgens het Amtsgericht Flensburg kan zo’n netwerk namelijk niet uit het niets worden opgebouwd of kan daaruit niet gemakkelijk worden teruggetreden.[31]

Net zoals het redelijk vermoeden van schuld, kan derhalve ten minste de recidivegrond (mede) worden gebaseerd op het enkele *gebruik* van cryptophones. Vergelijkbaar zijn de hierboven genoemde argumenten om het enkele gebruik als redengevend voor de betreffende strafprocesrechtelijke concepten te beschouwen: (1) de kosten van de aanschaf en het gebruik van zulke diensten en (2) de klaarblijkelijk gevoelde noodzaak om binnen het criminele netwerk/de criminele organisatie versleutelend te moeten communiceren, (3) maken duidelijk dat het bij het gebruik van cryptophones niet om kleinschalige of eenmalige criminaliteit gaat maar om duurzame verbanden. Daarmee lijkt het recidivegevaar, blijkens de argumentatie van het Amtsgericht Flensburg, een gegeven bij het gebruik van cryptophones.

De bovenstaande argumenten die zijn gebruikt door het Amtsgericht Flensburg lijken te voldoen aan de eisen die het EHRM stelt aan de motivering van de voorlopige hechtenis (in tegenstelling tot de afwezigheid van een gemotiveerde beslissing in *Hasselbaink*, *Zohlandt* en *Maassen*[32]). Het EHRM vereist namelijk dat ‘*the risk that the suspect, if released, would reoffend, consideration must be given to, inter alia, the nature and seriousness of the charges against a defendant, his or her criminal record, and his or her character or behaviour that would indicate that he or she presented such a risk*’.[33] Het gebruik van een cryptophone is een (duurzame) gedraging binnen een netwerk waaruit zo’n gevaar kan worden afgeleid.

4. Conclusie

Het lijkt er dus sterk op dat – ondanks dat een cryptophone een legaal goed is, dat door rechtbanken wel wordt onttrokken aan het verkeer[34] – het enkele gebruik daarvan strafvorderlijk relevant is of kan zijn. Het geeft namelijk een beeld van grote financiële mogelijkheden om communicatie geheim en versleuteld plaats te laten vinden (anders dan de zaak *Akgün* waarin het EHRM het

28 AG Flensburg, Beschl. v. 27.05.2021 – 485 Gs 527/21 131 Js 24455/20.
29 OLG Dresden, StV 2006, 534-535.
30 ‘Etwa 850,- € für 3 Monate bzw. 1.500,- € für 6 Monate gemäß den Feststellungen des Hanseatisches Oberlandesgericht in Bremen, Beschluss vom 18. Dezember 2020 - 1 Ws 166/20 -, Rn. 13’; AG Flensburg, Beschl. v. 27.05.2021 – 485 Gs 527/21 131 Js 24455/20, rn. 2.
31 AG Flensburg, Beschl. v. 27.05.2021 – 485 Gs 527/21 131 Js 24455/20, rn. 2.
32 Alle drie de uitspraken zijn van 9 februari 2021, ECLI’s (respectievelijk) ECLI:CE:ECHR:2021:0209JUD007332916; ECLI:CE:ECHR:2021:0209JUD006949116; ECLI:CE:ECHR:2021:0209JUD001098215.
33 EHRM 9 februari 2021, *NJ* 2021/94, par. 70.
34 Zie bijv. Rb. Den Haag 19 maart 2020, ECLI:NL:RBDHA:2020:2473; Rb. Noord-Nederland 29 april 2021, ECLI:NL:RBNNE:2021:1804.

doi: 10.5553/TBSenH/229567002022008002001

gebruik van de gratis applicatie *ByLock* binnen de context van de Turkse strafrechtspraktijk onvoldoende redengevend vond), een wens om versleuteld te kunnen communiceren via speciale aanbieders (en dus expliciet niet via de gangbare applicaties) en de wens om binnen een gesloten netwerk versleuteld te communiceren. Dit zijn relevante aspecten van het enkele gebruik van een cryptophone voor de invulling van strafvorderlijke concepten.

doi: 10.5553/TBSenH/229567002022008002001