MASTER'S THESIS

De chatapplicatie als heimelijk opsporingsmiddel

Een innovatief opsporingsmiddel of een ongerechtvaardigde inbreuk op het recht op privacy?

van Det, V.M.

Award date:
2022

Awarding institution:
Department of Public Law

De chatapplicatie als heimelijk opsporingsmiddel

Een innovatief opsporingsmiddel of een ongerechtvaardigde inbreuk op het recht op privacy?

Naam	:	V.M. van Det
Studentennummer	:	851245203
Begeleider	:	mr. J.W. Mensink
Examinator	:	mr. dr. M.F. Attinger
Instituut	:	Open Universiteit
Aantal woorden	:	15.051
Inleverdatum	:	13 juni 2022

Inhoudsopgave

1 Inleiding en probleemstelling

1.1 Aanleiding

Sinds enkele jaren is het gebruik van *high-end* encryptietelefoons binnen het criminele milieu een veel gezien verschijnsel.[1] Met deze encryptietelefoons kunnen criminelen versleutelde elektronische communicatieberichten naar elkaar sturen. Een te verzenden bericht wordt met behulp van een (chat)applicatie (hierna: (chat)app) op de *smartphone* van de verzender door een digitaal protocol versleuteld (veelal *end-to-end* encryptie (hierna: E2EE)) en door dezelfde chatapp op de telefoon van de ontvanger met behulp van datzelfde protocol ontsleuteld. Tijdens de verzendfase kunnen derden het bericht niet meelezen.

Het ontwikkelen van chatapps en het inrichten van servers om de communicatieberichten te versturen, vraagt specifieke ICT-kennis. Kennis die veel mensen vaak ontberen. ICT-bedrijven nemen deze zorg uit handen. Ook *mainstream* chatapps als WhatsApp, Telegram of Signal verzorgen versleutelde communicatie volgens het E2EE-principe. Het criminele milieu bleef terughoudend in het gebruik van *mainstream* chatapps, omdat gevreesd werd dat opsporingsinstanties de samenwerking met de moederbedrijven van deze chatapps zochten.[2] Enkele ICT-bedrijven zijn in dit gat gesprongen. Daar ligt ook de reden waarom criminele encryptietelefoons als *high-end* communicatiemiddelen worden beschouwd. Deze ICT-bedrijven ontwikkelen zelf chatapps en besturingsprogramma's met encryptiebeveiliging om die vervolgens binnen het criminele circuit, en onttrokken aan het zicht van de publieke massa, te exploiteren. Het beheer van de servers waarover de berichten worden verstuurd ligt ook bij deze ICT-bedrijven. Door het opzetten van dergelijke communicatienetwerken ontzorgen en faciliteren deze ICT-bedrijven criminelen om anoniem, onbespied en onbevangen te kunnen communiceren over hun activiteiten. Het ontwikkelen, aanbieden en verhandelen van encryptietelefoons is in beginsel legitiem.[3]

1.2 Het Anom-netwerk

In 2018 rekruteerde de Amerikaanse Federal Bureau of Investigations (hierna: FBI) een spijtoptant die zijn medewerking verleende bij de ontwikkeling van een chatapp met encryptiebeveiliging.[4] Vervolgens exploiteerde de FBI de chatapp onder de naam 'Anom' binnen criminele netwerken met het doel om informatie van en over criminelen en hun activiteiten te vergaren.[5] Het Anom-netwerk werd een wereldwijd communicatienetwerk voor, onder andere Nederlandse, criminelen.[6] De criminele netwerken verkeerden in de veronderstelling dat zij buiten het zicht van opsporingsinstanties vrijelijk over hun

[1] Boeser, *TBS&H* 2021, nr. 5, p. 352.
[2] Stol & Strikwerda 2017, p. 282-283. Van der Sloot, *NJB* 2014, Afl. 17, p. 1173.
[3] Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 170. Aansluitend stelt de rechtbank wel dat het anders ligt 'wanneer die telefoons uitsluitend of in overwegende mate worden gebruikt door lieden wier doel het bij dat gebruik is om de nasporing van door hen gepleegde of nog te plegen misdrijven te verijdelen en een dergelijk doel binnen de organisatie bekend was.'
[4] *Affidavit* 2021, p. 6, voetnoot 3.
[5] De FBI startte een politieoperatie onder de naam *Operation Trojan Shield*. ´FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown´, justice.gov 8 juni 2021. *Affidavit* 2021, p. 6-7.
[6] Boere, *ad.nl* 8 juni 2021.

criminele activiteiten konden communiceren. In werkelijkheid kon de FBI zowel de *content* als de metadata ontsleutelen.[7] Op deze wijze werden meer dan 27 miljoen verstuurde berichten inzichtelijk gemaakt.[8] Op basis van deze data konden opsporingspartners strafrechtelijke onderzoeken instellen.

1.3 Nederland en de juridische implicaties

De versleuteling van elektronische gegevens vormt voor de Nederlandse politie in toenemende mate een probleem bij de opsporing van strafbare feiten.[9] De politie kan versleutelde communicatie nauwelijks tot niet inzichtelijk maken.[10] Het feit dat Nederlandse criminelen veelal gebruik maken van encryptietelefoons voor hun (internationale) communicatie, zou de heimelijke inzet van beveiligde chatapps, zoals gebruikt door de FBI, vanuit strafrechtelijk oogpunt ook voor de Nederlandse politie een interessant en innovatief opsporingsmiddel kunnen maken. Een dergelijk opsporingsmiddel zou een verregaand inzicht kunnen geven in organisatiestructuren en handelswijzen binnen het Nederlandse criminele milieu. Daarnaast biedt het de mogelijkheid om snel en gericht te interveniëren in levensbedreigende situaties en bewijs te vergaren voor lopende of nog te starten opsporingsonderzoeken.[11]

Uit bovenstaande valt af te leiden dat het doel van de exploitatie van de beveiligde chatapp gelegen is in het creëren van een mogelijkheid om alle verzonden data van alle gebruikers van de chatapp te vergaren. Het opsporingsmiddel zou daarmee ook data van onschuldige gebruikers van de chatapp kunnen vergaren. Het (heimelijk) vergaren van privécommunicatie tussen personen door de politie kan een inbreuk van het recht op eerbiediging van de privacy opleveren.[12] Onder andere art. 8 van het Europees Verdrag van de Rechten van de Mens en de fundamentele vrijheden (hierna: EVRM) beschermt grondrechtelijk het recht op privacy.[13] Het artikel laat de wetgever ruimte om een inbreuk op dit recht te maken. Wil de Nederlandse politie een dergelijke inbreuk maken, dan dient het boven beschreven opsporingsmiddel op basis van het legaliteitsbeginsel haar grondslag te vinden in een Nederlandse wet.

De algemene opsporingsbevoegdheid voor de politie is neergelegd in art. 3 Politiewet 2012 (hierna: Polw).[14] Specifieke opsporingsbevoegdheden zijn onder meer vervat in het Wetboek van Strafvordering (hierna Sv).[15] Er lijkt, op het eerste gezicht, geen specifieke regeling te bestaan die voor de politie de

[7] *Affidavit* 2021, p. 7.
[8] '800 criminals arrested in biggest ever law enforcement operation against encrypted communication', europol.europa.eu 8 juni 2021.
[9] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 7.
[10] Oerlemans, *JV* 2012, nr. 3, p. 28-29.
[11] In de Encrochat-zaak deed zich soortgelijke mogelijkheden voor. Zie hiervoor Deiters, *Politievakblad Blauw*, nr. 03, p. 12-16.
[12] EHRM 02 augustus 1984, ECLI:NL:XX:1984:AB8061, *NJ* 1988, 534, m.nt. J.V. van Dijk, par. 64 (*Malone/ Verenigd Koninkrijk*); Eskens, *Computerrecht* 2015/85, nr. 3, p. 126.
[13] Het EHRM gebruikt in haar Verdragstekst het meeromvattende woord 'privéleven'. Omdat dit onderzoek zich op een specifieker onderdeel van het ruime begrip 'privéleven' richt, namelijk de 'privacy', heeft het gebruik begrip 'privacy' de voorkeur boven het gebruik van het begrip 'privéleven'. Dit onderscheid wordt in hoofdstuk 3 nader toegelicht.
[14] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 13.
[15] Ook in bijzondere wetten kunnen opsporingsbevoegdheden voor opsporingsinstanties neergelegd zijn. Zie bijvoorbeeld Titel III 'Van de opsporing' in de Wet op de economische delicten.

bevoegdheid schept om een beveiligde chatapp als heimelijk strafvorderlijk opsporingsmiddel in te zetten met de vergaring van (bulk)data als doel.

1.4 Onderzoeksvraag

Bovenstaande leidt dan ook tot de volgende centrale onderzoeksvraag:
'In hoeverre biedt het Nederlandse strafprocesrecht een grondslag voor de vergaring van (bulk)data door de inzet van beveiligde chatapplicaties als heimelijk opsporingsmiddel en hoe verhoudt dit opsporingsmiddel zich tot het recht op eerbiediging van de privacy zoals gewaarborgd in artikel 8 EVRM?'

De onderzoeksvraag is opgedeeld in drie deelvragen:

1. Hoe ziet de vergaring en ontsleuteling van data via beveiligde chatapps eruit en welke data, waaronder bulkdata, worden met een bericht meegezonden?
2. Op basis van welke vereisten mag de nationale wetgever een inbreuk maken op het recht op privacy zoals gewaarborgd in art. 8 EVRM?
3. In hoeverre biedt het nationaal strafprocesrecht een strafvorderlijke bevoegdheid die als grondslag kan dienen voor de inzet van het beschreven opsporingsmiddel?

Het doel van het onderzoek is te toetsen of het beschreven opsporingsmiddel ter vergaring van bulkdata naar de huidige stand van het recht kan en mag worden ingezet door de politie in een Nederlandse strafzaak. De verwerking van de vergaarde data is een opvolgend proces. In verband met de omvang richt dit onderzoek zich alleen op de vergaring van (bulk)data. De opslag, analyse en verwerking van deze data valt buiten het bestek van dit onderzoek.

1.5 Gehanteerde onderzoeksmethode en leeswijzer

Om tot het antwoord op de deelvragen en de onderzoeksvraag te komen is literatuuronderzoek verricht. Hierbij is gebruik gemaakt van handboeken, verzamelboeken, publicaties in tijdschriften, dissertaties, kamerstukken, rapporten, jurisprudentie en bronnen op het internet. In hoofdstuk twee wordt eerst kort inzicht gegeven in de functie en de werking van chatapps met encryptiebeveiliging. Verder besteedt dit hoofdstuk aandacht aan de verschillende soorten data die met versleutelde communicatieberichten worden meegezonden. Hoofdstuk drie gaat in op art. 8 EVRM. Eerst wordt de reikwijdte van het begrip 'privacy' beschreven. Aansluitend wordt onderzocht aan welke criteria een verdragsstaat moet voldoen, wil zij een inbreuk op het recht op eerbiediging van de privacy kunnen maken. Het recent verschenen *Big Brother Watch*-arrest van het EHRM stelt een aantal uitgangspunten onder welke omstandigheden verdragsstaten bulkdata mogen vergaren ten behoeve van de opsporing.[16] Hoofdstuk vier gaat in op de nationale wetgeving. Hierin wordt onderzocht welke bijzondere opsporingsbevoegdheid als grondslag kan dienen voor de inzet van dit opsporingsmiddel. In hoofdstuk vijf worden de bevindingen uit de voorgaande hoofdstukken met elkaar in verbinding gebracht. Hierbij wordt het opsporingsmiddel, de

[16] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*).

grondslag voor deze nationale bevoegdheid en art. 8 EVRM aan elkaar getoetst. In hoofdstuk zes wordt de conclusie op de hoofdvraag beantwoord. Afsluitend worden twee aanbevelingen beschreven.

2 Encryptietelefoons en door encryptie beveiligde chatapplicaties

2.1 Inleiding

Nagenoeg iedere *smartphone*-gebruiker heeft wel één of meerdere chatapps op zijn telefoon geïnstalleerd.[17] De ontwikkeling en inrichting van een chatapp en de achterliggende ICT-infrastructuur is een ingewikkelde onderneming. Het vraagt van de ontwikkelaars specialistische kennis op het gebied van ICT. Iedere ontwikkelaar van chatapps geeft daarbij een eigen invulling aan de ontwikkeling, vormgeving, beveiliging en infrastructuur van zijn app.[18] Een chatapp is min of meer een gesloten systeem doordat de verstuurde berichten via de servers van de ontwikkelaars/ aanbieders verlopen.[19] In de basis kan alleen via de chatapps van dezelfde ontwikkelaar worden gecommuniceerd.[20] Met de chatapps die speciaal voor het criminele milieu zijn ontwikkeld is dat niet anders.[21] Het gaat het bestek van dit onderzoek te buiten om de gedetailleerde werking van chatapps te beschrijven. Voor het later te bespreken juridisch kader is het wel van belang op hoofdlijnen enig inzicht in de werking van chatapps en encryptietelefoons te geven. Daarnaast wordt aan het begrip bulkdata betekenis gegeven en beschreven welke soorten gegevens kunnen worden verzameld.

2.2 De werking

In maart 2018 rekruteerde de FBI een zogenaamde *Confidential Human Source* (hierna: *CHS*). [22] Deze *CHS* was bezig met de ontwikkeling van de volgende generatie versleutelde communicatieproducten.[23] De *CHS* stelde dit product, 'Anom' genaamd, ter beschikking aan de FBI. Met dit product in de hand startte de FBI in samenwerking met internationale opsporingspartners een dekmanteloperatie onder de naam *Operation Trojan Shield*.[24] Het product Anom bestond uit twee onderdelen: (1) de encryptietelefoon met (2) daarop geïnstalleerd de chatapp.[25]

2.2.1 De encryptietelefoon

Om chatberichten te kunnen verzenden is in eerste instantie een *smartphone* nodig. Aanbieders van *high-end* encryptietelefoons maken gebruik van diverse merken telefoons. Anom gebruikte voornamelijk

[17] Op peildatum 12 februari 2020 werd een aantal van 2 miljard gebruikers van de chatapp WhatsApp gemeten. Zie ´Twee miljard gebruikers - De wereld privé met elkaar verbinden', blog.whatsapp.com 6 januari 2022. Op 13 januari 2020 werden 500 miljoen gebruikers van de chatapp Telegram geregistreerd. 'Telegram bereikt 500 miljoen gebruikers na commotie rond WhatsApp', *nu.nl* 13 januari 2021. In januari 2021 werd een aantal van 40 miljoen Signal-gebruikers geregistreerd. Zie Curry, *buisinessofapps.com* 11 januari 2022.
[18] De vergelijking kan worden getroffen met verbrandingsmotoren van auto's. In de basis werken nagenoeg alle verbrandingsmotoren op dezelfde manier. Echter, ieder automerk brengt zijn specificaties aan de motor aan waardoor deze specificaties merktyperend worden.
[19] Een ontwikkelaar van een app is niet altijd ook de aanbieder van een app. Een ontwikkelaar kan bijvoorbeeld een app bouwen in opdracht van een aanbieder, die de app vervolgens exploiteert.
[20] Ontwikkelaars kunnen binnen de app wel mogelijkheden tot delen bieden via bijvoorbeeld een 'delen via' functie.
[21] *Affidavit* 2021, p. 4, voetnoot 1.
[22] Deze rekrutering viel samen met het uit de lucht halen van het veel gebruikte encryptienetwerk Phantom Secure en de aanhouding van diens directeur Vincent Ramos door de FBI. 'International Criminal Communication Service Dismantled', fbi.gov 16 maart 2018.
[23] *Affidavit* 2021, p. 6.
[24] *Operation Trojan Shield* liep van 7 oktober 2019 tot en met 7 juni 2021. *Affidavit* 2021, p. 7 en 9.
[25] Ook de aanbieders Ennetcom, EncroChat, en Sky ECC verkochten encryptietelefoons en de beveiligde chatapp als een twee-eenheid. De ene is doorgaans niet verkrijgbaar zonder de andere. Voor Ennetcom: Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 53; Schermer & Oerlemans, *Computerrecht* 2020/3, p. 6-7. Voor EncroChat: Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2. Voor Sky ECC: *Computerrecht* 2022/41, p. 78.

toestellen van het merk Google Pixel.[26] EncroChat werd geïnstalleerd op telefoons van het merk BQ Aquarius, en Sky ECC op iPhones, Google Pixels, BlackBerry's en Nokia's.[27] Veelal passen chatapp-ontwikkelaars de besturingssystemen en hardware van de *smartphones* aan. Zo maakten Anom-encryptietelefoons gebruik van het onbekende besturingssysteem ArcaneOS.[28] Voor deze aanpassingen zijn enkele redenen te noemen. In de eerste plaats zorgen deze aanpassingen ervoor dat toepassingen op de telefoon die tot identificering van de gebruiker kunnen leiden, worden uitgeschakeld.[29] In de tweede plaats verkleint het de kans op ontdekking van de chatapp zelf door opsporingsinstanties.[30] Als derde reden geldt de compatibiliteit van de ontwikkelde chatapp met het besturingssysteem.[31]

2.2.2 De chatapplicatie

Het tweede onderdeel van het product is de chatapp zelf. De chatapp verstuurt haar data via een achterliggende ICT-structuur van servers. De chatapp en de daarachterliggende ICT-infrastructuur van de ontwikkelaar en/ of aanbieder zijn onlosmakelijk met elkaar verbonden.

Een chatapp is een softwareprogramma dat onder andere op *smartphones* kan worden geïnstalleerd. Met een chatapp kunnen gebruikers onderling met elkaar 'chatten'.[32] Gebruikers van de Anom-chatapp konden alleen communiceren met hun gesprekspartners als deze ook in het bezit waren van de Anom-chatapp. Om de chatapp te kunnen gebruiken beschikte iedere gebruiker over een uniek, identificerend gebruikersaccount. Bij Anom bestond het unieke, identificerende gebruikersaccount uit een '*Jabber Identification*' (hierna: JID). De JID werd door de chatapp-aanbieder aangemaakt en aan de gebruiker toegewezen. In de JID konden Anom-gebruikers hun eigen gebruikersnamen aanmaken.[33] Gebruikersnamen betreffen namen die zichtbaar worden in het chatvenster van de ontvanger. Anom-gebruikers konden zelf een contactenlijst samenstellen en aanpassen.[34] Het toevoegen van een persoon aan een contactenlijst gebeurde door de onderlinge uitwisseling van de JID's.[35]

Na invoer van de tekst en selectie van de ontvanger kan de gebruiker het chatbericht verzenden. Afhankelijk van het ontwerp van de chatapp kunnen naast tekstberichten ook andere media als afbeeldingen, spraakberichten en video's worden meegezonden. Via het mobiele internet belandt het

[26] Cox, v*ice.com* 8 juni 2021a.
[27] Voor EncroChat: Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2. Voor Sky ECC: *Computerrecht* 2022/41, p. 78.
[28] Cox, *vice.com* 8 juli 2021.
[29] Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 194. Deze *smartphones* zijn vaak zo gemodificeerd dat alle functies zijn verwijderd of uitgeschakeld die tot identificatie kunnen leiden. Dan kan worden gedacht aan het (fysiek) verwijderen of uitschakelen van bluetooth, de gps, de camera en de microfoon.
[30] Cox, *vice.com* 8 juli 2021. Ook EncroChat maakte gebruik van een verborgen laag om de chatapp te maskeren. Frediani, *valigiablu.it* 12 juli 2020.
[31] Met name besturingssystemen die hun oorsprong in open source software vinden, zoals bijvoorbeeld Android en Ubuntu Touch, bieden goede mogelijkheden tot aanpassingen in het besturingssysteem. Zie hiervoor 'Android Open Source Project', source.android.com 11 februari 2022; ubuntu-touch.io 11 februari 2022.
[32] To chat is een Engels werkwoord en betekent 'praten', 'babbelen' en 'kletsen'.
[33] *Affidavit* 2021, p. 7.
[34] *Affidavit* 2021, p. 7.
[35] Van deze werkwijze was in ieder geval in de EncroChat-zaak sprake. Niets wijst er op dat bij Anom een andere werkwijze voor het uitwisseling van JID's werd gehanteerd. Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2. In tegenstelling tot Anom maken de *mainstream* chatapps in grote mate gebruik van synchronisatie met de reeds ingevoerde 'gewone' contactenlijst die bijvoorbeeld wordt gebruikt voor het opslaan van telefoonnummers.

bericht in de servers van de chatapp-aanbieder. Hier koppelt het netwerk van servers de unieke, identificerende gebruikersaccounts van de verzender en de gewenste ontvanger aan elkaar. De server verzendt het bericht naar de ontvanger.

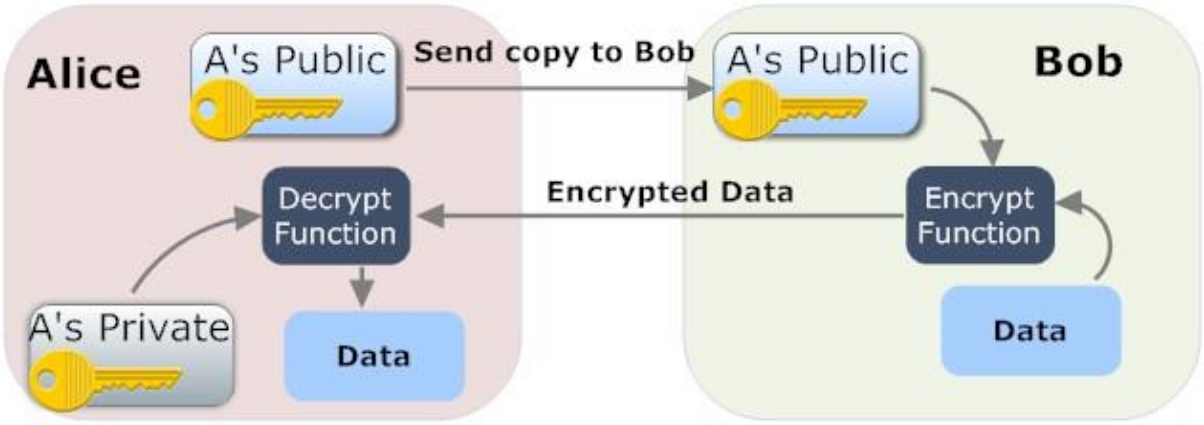
2.2.3 Dienstverlening

Encryptietelefoons worden vaak in combinatie met een abonnement geleverd.[36] Het abonnement is doorgaans gericht op een vorm van dienstverlening. Deze dienstverlening bestaat voornamelijk uit het beheer van de encryptietelefoon en de chatapp.[37] De beheerder kan (op afstand) profielen of beperkingen instellen, updates verzenden enzovoort.[38] Maar het gaat verder. Een veel gebruikte functie op encryptietelefoons is de zogenaamde '*wipe*'-functie. Met een druk op een knop of het versturen van een code verzoekt de gebruiker de beheerder alle data op de telefoon onherstelbaar te wissen (*'wipen*').[39] Van deze functie wordt gebruik gemaakt als de encryptietelefoon in verkeerde handen valt. Een andere service die vaak door aanbieders wordt geleverd, is een aangepast retentiebeleid. Dit betreft een instelling waarmee berichten op de encryptietelefoon automatisch na een bepaalde tijd van de telefoon worden gewist.[40]

2.3 End-to-end encryptie (E2EE)

De beveiliging van informatie geldt als belangrijk onderdeel van de versterking van digitale weerbaarheid en veiligheid en de bescherming van het maatschappelijk verkeer.[41] De beveiliging van informatie gebeurt ook in chatapps. De meeste chatapps, zowel de *mainstream* als die speciaal ontworpen voor crimineel gebruik, maken gebruik van zogenaamde E2EE om communicatiedata te beveiligen.[42] Encryptie is het proces waarbij informatie wordt getransformeerd in een veilig format zodat derden niet ongevraagd kennis van de informatie kunnen nemen.[43] Met E2EE wordt een zichtbaar tekstbericht ('*plain text*') met behulp van asymmetrische encryptie al in de chatapp van de verzender versleuteld en om gezet in gecodeerde tekst ('*cipher text')*.[44] Pas in de chatapp van de ontvanger wordt *cipher text* terug ontsleuteld naar *plain text*.[45] Bij deze wijze van versleuteling zijn ´sleutels´ nodig.[46] Bij asymmetrische encryptie maakt de chatapp van de ontvanger twee sleutels aan: een *public key* en een *private key*. De *private key* wordt gebruikt om *plain text* te versleutelen. De *public key* wordt naar de ontvanger gestuurd en gebruikt om de *cipher text* te ontsleutelen.[47]

[36] Criminelen betalen honderden, zo niet duizenden euro´s, al dan niet met een aanvullende abonnementsdienst, voor een encryptietelefoon.
[37] Dit wordt ook wel 'Mobile Device Management' genoemd.
[38] Frediani, *valigiablu.it* 12 juli 2020; Cox, *vice.com* 8 juni 2021b.
[39] Cox, *vice.com* 8 juli 2021; Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 198.
[40] Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 198. Gangbaar is een retentie van 24 tot 48 uur.
[41] Boeser, *TBS&H* 2021, nr. 5, p. 352.
[42] Europol & Eurojust 2019, p. 19; Thompson, *policeprofessional.com* 13 november 2018; 'Info over end-to-end versleuteling', faq.whatsapp.com 18 februari 2022.
[43] Katz & Lindell 2021, p. 2; Europol & Eurojust 2019, p. 10.
[44] *Report of the Manhattan District Attorney's Office on smartphone encryption and public safety* 2015, p. 2.
[45] Europol & Eurojust 2019, p. 19.
[46] Katz & Lindell 2021, p. 2.
[47] Katz & Lindell 2021, p. 401.



Bron: dzone.com[48]

Asymmetrische encryptie geeft een grote mate van beveiliging aan de data en maakt het voor opsporingsinstanties nagenoeg onmogelijk om onderschepte *cipher text* te ontcijferen. Het Anom-netwerk was zo ontworpen dat elk bericht dat werd verzonden vanaf een Anom-encryptietelefoon met encryptie werd beveiligd.[49] Een kopie van het (versleutelde) bericht werd heimelijk naar servers van de FBI verzonden.[50] De Anom-chatapp voegde bij de verzending van het bericht geautomatiseerd heimelijk een *master key* toe waarmee de FBI het bericht kon ontsleutelen.[51]

2.4 Bulkdata

Zowel *Operation Trojan Shield* als de EncroChat-zaak laten zien dat opsporingsinstanties alle data van alle gebruikers, die via de beveiligde chatapps werden verzonden, vergaarden.[52] Er lijkt sprake te zijn van het vergaren van 'bulkdata'. Maar wat zijn bulkdata precies? De rechtbank van Amsterdam oordeelde dat het begrip 'bulkdata' niet duidelijk is omschreven, maar wel dat 'er een grens ligt tussen het min of meer afgebakend opslaan en analyseren van bepaalde data, en het ongedifferentieerd opslaan, opvragen of doorzoeken van grote hoeveelheden data.'[53] Het Wetboek van Strafvordering kent geen definitie van de term bulkdata. Wel geeft de wet in art. 80quinquies Wetboek van Strafrecht (hierna: Sr) een definitie van het begrip gegevens: 'iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken'. Gegevens kunnen zodoende bestaan uit (lees)tekens, signalen en symbolen, maar omvatten ook tekens die een instructie vormen voor een machine of een instrument.[54] Alle data die van en naar de encryptietelefoon en de beveiligde chatapps worden verzonden, moeten

[48] 'A gentle introduction to asymmetric encryption and SSL certificates', dzone.com 18 februari 2022.
[49] *Affidavit* 2021, p. 7.
[50] *Affidavit* 2021, p. 7. Voor *Operation Trojan Shield* werd door de FBI gebruik gemaakt van een '*third country*' om de communicatie van buiten Amerikaans grondgebied te vergaren. Onduidelijk is waarom berichten die werden verzonden met Anom-encryptietelefoons zich binnen Amerikaans grondgebied bevonden niet door de FBI werden vergaard. Volgens Taylor Parkins-Ozephius e.a. zou dit kunnen liggen aan het feit dat voor de vergaring van communicatie binnen het Amerikaans grondgebied geen vereiste *search warrant* aan de FBI was afgegeven. Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 325, voetnoot 38.
[51] *Affidavit* 2021, p. 6-7.
[52] *Affidavit* 2021, p. 7; Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.
[53] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.6.
[54] *Kamerstukken II* 1991/92, 21551, nr. 11, p. 3-4.

worden aangemerkt als gegevens. Het maakt hierbij geen verschil of deze data zien op de inhoud van een communicatiebericht, een verkeersgegeven of een instructie tot het *wipen* van de encryptietelefoon.

De Evaluatiecommissie Wiv 2017 geeft in haar evaluatieverslag wel een definitie van het begrip ´bulkdata´.[55] De Wiv 2017 voorziet in regelgeving voor de Nederlandse inlichtingen- en veiligheidsdiensten. Vanuit hun taakstelling houden inlichtingen- en veiligheidsdiensten zich niet bezig met de opsporing van strafbare feiten. De evaluatiecommissie omschrijft bulkdata als ´een omvangrijke verzameling van gegevens waarvan het merendeel betrekking heeft op personen en/of organisaties die niet in onderzoek zijn van de diensten en dit ook nooit zullen worden.´[56] Ook het EHRM definieerde bulkdata in vergelijkbare bewoording.[57] Het begrip bulkdata richt zich op de aard en omvang van de data. De aard van de data heeft binnen dit begrip betrekking op persoonsgegevens.[58] Persoonsgegevens betreffen 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon'.[59] Met behulp van apparatuur, applicaties, instrumenten en protocollen, zoals IP-adressen, identificatiecookies of andere identificatoren kunnen natuurlijke personen worden gekoppeld aan online-identificatoren. Op basis van (een cluster van) identificatoren kunnen natuurlijke personen worden herkend.[60] Uit vorengaande moet de conclusie worden getrokken dat de politie bij de vergaring van bulkdata zeer mogelijk (persoons)gegevens verwerft van personen die in eerste instantie niet interessant lijken.

Naar aanleiding van het in deze paragraaf beschrevene en binnen de context van dit onderzoek, definieer ik het begrip 'bulkdata' als: een massa aan gegevens die, individueel of in samenhang, kunnen leiden tot de herkenbaarheid en/of identificatie van natuurlijke personen, onafhankelijk of van deze personen enige betrokkenheid bij een strafbaar feit blijkt.

2.5 Gegevensverzameling

Telecomaanbieders verzorgen het onderling transport van verschillende soorten (versleutelde) data van de encryptietelefoon van en naar de servers van de aanbieders van de encryptietelefoons. Hierbij moet onderscheid worden gemaakt tussen enerzijds data die zien op de inhoud van communicatie en

[55] *Rapport Commissie Jones-Bos* 2020. Dit rapport evalueert de Wet op de inlichtingen- en veiligheidsdiensten. Inlichtingen- en veiligheidsdiensten hebben in tegenstelling tot het strafrecht verregaande bevoegdheden tot vergaring van bulkdata.
[56] *Rapport Commissie Jones-Bos* 2020, p. 39.
[57] Meer specifiek: 'These communications will belong to a large number of individuals, many of whom will be of no interest whatsoever to the intelligence services.', zie hiervoor EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 326 (*Big Brother Watch e.a./Verenigd Koninkrijk*); EHRM 25 mei 2021, appl. nr. 35252/08, par. 240 (*Centrum för Rättviva/ Zweden*).
[58] *Rapport Commissie Jones-Bos* 2020, p. 39.
[59] Art. 4 lid 1 Verordening (EU) 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 (algemene verordening gegevensbescherming) (hierna: Verordening (EU) 2016/679).
[60] Overweging 30 Verordening (EU) 2016/679. De Verordening is niet van toepassing op rechtspersonen. Zie overweging 14 Verordening (EU) 2016/679.

anderzijds de verkeersgegevens. Bij inhoudelijke communicatie kan worden gedacht aan de inhoud van telefoongesprekken, sms-berichten en chatberichten. Daarnaast verzendt een encryptietelefoon ook verkeers- en locatiegegevens. Verkeersgegevens zijn 'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.'[61] Locatiegegevens zijn 'gegevens die worden verwerkt in een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven.'[62] De combinatie van verkeers- en locatiegegevens wordt ook wel metadata genoemd. Telecomaanbieders hebben de verplichting bepaalde verkeers- en locatiegegevens op te slaan en tijdelijk te bewaren voor overheidsinstanties.[63] Deze verplichting tot opslag vloeit voort uit de Telecommunicatiewet (hierna: Tw) en betreft een implementatie van Richtlijn 2006/24/EG.[64] In het geval van mobiele telefonie moeten de telecomaanbieder in ieder geval vastleggen: telefoonnummer van beller en ontvanger, naam en adresgegevens van de geregistreerde gebruikers, datum en tijdstip aanvang en einde verbinding, de gebruikte telefoondienst, het IMSI- en IMEI-nummer en locatieaanduidingen van gebruikte telefoonmasten.[65] Voor mobiel internet dienen als belangrijkste gegevens nog de datum en tijdstip van de log-in en log-off van een internetsessie, samen met het IP-adres en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker te worden vastgelegd.[66] Juist die gebruikersidentificatie kan bij encryptietelefoons tot problemen bij de opsporing van strafbare feiten leiden. Aan de hand van een gebruikersidentificatie kan de politie betrekkelijk eenvoudiger een mogelijke gebruiker van een telefoontoestel identificeren.[67] Aanbieders van EncroChat boden hun toestellen aan in combinatie met simkaarten die alleen data kunnen versturen.[68] Dit kunnen zogenaamde prepaid simkaarten betreffen van zowel Nederlandse als buitenlandse telecomaanbieders. Prepaid simkaarten kunnen in Nederland anoniem gekocht en gebruikt worden.[69] Het gebruik van prepaid of buitenlandse simkaarten leidt tot de mogelijkheid dat de gebruiker van de encryptietelefoon in meer of mindere mate anoniem gebruik kan maken van het Nederlandse telecomnetwerk.[70] Immers, bij de ingebruikname van een prepaid simkaart is de gebruiker niet verplicht zijn persoonsgegevens bij de telecomaanbieder vast te leggen.

Naast de telecomaanbieders verzamelen ook de aanbieders van chatapps data. Deze data zijn nodig om de communicatie tussen de gebruikers tot stand te brengen en te houden. *Mainstream* chatapps

[61] Art. 11.1 onder b Tw.
[62] Art.11.1 onder d Tw.
[63] Art. 13.2a lid 3 Tw: Bewaartermijn gegevens in verband met mobiele telefonie: twaalf maanden. Bewaartermijn gegevens in verband met internettoegang, e-mail over het internet en internettelefonie: zes maanden.
[64] Voluit: 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.
[65] Onderdeel A van de bijlage behorende bij art. 13.2a Tw. Een IMSI-nummer is een uniek nummers dat gekoppeld is aan een simkaart. Het nummer identificeert het abonnement waarmee personen bellen of internetten. Een IMEI-nummer is een uniek nummer dat gekoppeld is aan een telefoon. Het nummer identificeert de telefoon.
[66] Onderdeel B van de bijlage behorende bij art. 13.2a Tw.
[67] Dit kan bijvoorbeeld op grond van art. 126na Sv.
[68] Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2. Deze simkaarten hadden een wereldwijde dekking waardoor de toestellen met chatapp ook aan buitenlandse afnemers geleverd konden worden.
[69] *Kamerstukken II* 2018/19, 29279, nr. 534.
[70] Uitgaande van de situatie dat de encryptietelefoon zich op dat moment in Nederland bevindt. Betreft de simkaart er een van een buitenlandse telecomaanbieder, zal alsnog gebruik worden gemaakt van het Nederlandse netwerk. Dit wordt 'roaming' genoemd.

slaan onder andere gegevens op over het gebruikersaccount, waaronder het gekoppelde telefoonnummer, profielnaam en profielfoto, een lijst met contactpersonen, apparaat- en verbindingsgegevens, locatiegegevens en gegevens die anderen over de gebruiker verstrekken.[71] Welke data de FBI precies van de Anom-gebruikers vergaarden wordt uit de beschikbare stukken niet helemaal duidelijk. Uit de *affidavit* wordt wel duidelijk dat metadata werden verkregen.[72] In ieder geval vergaarde de FBI de inhoud van berichten, locatiegegevens, datum en tijdstip van verzending en/ of ontvangst van een bericht, evenals de *master keys* om de berichten te ontsleutelen. De FBI hield ook een lijst bij van de JID's en corresponderende gebruikersnamen.[73] Deze gegevens zijn onder andere nodig voor de identificatie van Anom-gebruikers. Als laatste zal het niet vreemd zijn als de FBI ook beschikte over het IMEI- en IMSI-nummer die aan elke Anom-encryptietelefoon gekoppeld waren.[74] Deze nummers zijn nodig om verbinding te maken met de netwerken van telecomproviders.[75]

2.6 Tussenconclusie

In dit hoofdstuk is het antwoord op de eerste deelvraag beschreven: Hoe ziet de vergaring en ontsleuteling van data via beveiligde chatapps eruit en welke data, waaronder bulkdata, worden met een bericht meegezonden? De FBI ontwikkelde een chatapp en geëxploiteerde deze binnen het criminele milieu. Chatapplicaties worden gebruikt om berichten aan anderen te kunnen sturen. Chatberichten worden versleuteld met behulp van E2EE. Hierdoor kunnen alleen de verzender en de ontvanger kennis nemen van de inhoud van het bericht. Door het meesturen van een *master key* met de berichten kon de FBI de inhoud van alle berichten van alle gebruikers van de chatapplicatie ontsleutelen en inzien. Met de berichten werd ook metadata meegestuurd. Metadata is informatie over communicatie. Analyse van metadata kan tot identificering van de gebruiker van de chatapp leiden. De vergaring van alle data van alle gebruikers (bulkdata) door overheidsinstanties kunnen de privacy raken.

[71] Zie voor WhatsApp: 'Privacybeleid van WhatsApp', whatsapp.com (bijgewerkt 4 januari 2021). Zie voor Telegram: 'Telegram Privacy Policy', telegram.org (bijgewerkt 14 augustus 2018).
[72] *Affidavit* 2021, p. 22; Cox, *vice.com* 4 januari 2022.
[73] *Affidavit* 2021, p. 7.
[74] In de EncroChat-zaak werden ook de IMEI-nummers van encryptietelefoongebruikers via de chatapp-server vergaard. Zie hiervoor Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.
[75] Van de Pol, *crimesite.nl* 10 februari 2021.

3 Het Europees Verdrag van de Rechten van de Mens (EVRM)

3.1 Inleiding

In het vorige hoofdstuk zijn de werking en inrichting van beveiligde chatapps als opsporingsmiddel beschreven. (Bulk)data kunnen privacygevoelige gegevens bevatten. De bescherming van privacy is een grondrecht dat onder andere door art. 8 EVRM wordt beschermd.[76] Art. 8 EVRM laat de wetgever wel ruimte om een inbreuk op het recht op privacy te maken. Dit hoofdstuk beschrijft de voorwaarden waaraan de nationale wetgever moet voldoen om een inbreuk op het recht op privacy van burgers door de politie mogelijk te maken. Interceptie van communicatie behelst meerdere fasen en de jurisprudentie en literatuur hieromtrent is uitgebreid.[77] Omwille van de omvang van dit onderzoek wordt alleen de fase van vergaring van (bulk)data aan het EVRM getoetst.

3.2 Artikel 8 EVRM

Ter bescherming van de rechten van de mens is in het EVRM een aantal algemene grondrechten gecodificeerd. Met de vastlegging van deze grondrechten wil het EVRM garanderen dat de deelnemende staten zich actief onthouden van het plegen van inbreuken op deze grondrechten (negatieve verplichtingen) en de effectieve uitoefening van deze rechten bevorderen (positieve verplichtingen).[78] Nederland is partij bij het EVRM.[79] Art. 1 EVRM vereist van Nederland dat zij de rechten die in het EVRM zijn vastgelegd garandeert. Nederland heeft dit geborgd in de Grondwet (hierna: Gw). In art. 93 Gw is gesteld dat een ieder verbindende verdragsbepalingen bindende kracht hebben. Art. 8 EVRM betreft voor Nederland een ieder verbindende bepaling in de zin van art. 93 Gw.[80] Op grond van art. 94 Gw moet de Nederlandse rechter nationaal geldende wettelijke bepalingen buiten toepassing laten indien deze in strijd zijn met het EVRM. De Nederlandse rechter streeft ernaar nationale bepalingen zoveel mogelijk in het licht van het EVRM uit te leggen.[81]

Eén van die grondrechten betreft het recht op eerbiediging van het privé-, familie- en gezinsleven. Dit recht is vastgelegd in art. 8 lid 1 EVRM: ‘Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.’ Met deze bepaling beoogt het EHRM een ieder bescherming te bieden tegen misbruik van recht en een willekeurige inmenging door overheidsinstanties in het persoonlijke leven.[82] Met ‘een ieder’ richt art. 8 lid 1 EVRM zich op natuurlijke

[76] De bescherming van het recht op privacy wordt tevens beschermd in art. 10 Grondwet, art. 17 Internationaal Verdrag inzake burgerrechten en politieke rechten en art. 7 Handvest van de grondrechten van de Europese Unie. In verband met de omvang en afbakening van dit onderzoek zullen deze artikelen hooguit zijdelings worden besproken.
[77] Zo omvat interceptie niet alleen de vergaring van data maar ook op de opslag, analyse en deling met derden. Zie hiervoor onder andere Eskens, *Computerrecht* 2015/85, nr. 3; EHRM 29 juni 2006, appl. nr. 54943/00 (*Weber en Saravia/ Duitsland*); EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[78] Gerards 2011, p. 97.
[79] *Trb.* 1951, 154.
[80] Hielkema & Krabbe 2004, p. 14-15.
[81] Nieuwenhuis 2017, p. 49.
[82] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 323; Krabbe 2004, p. 138; EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, *NJ* 1993, 400, m.nt. E.J. Dommering, par. 31 (*Niemietz/ Duitsland*); EHRM 27 oktober 1994, appl. nr. 18535/91, par. 31 (*Kroon/ Nederland*); EHRM 29 juni 2006, appl. nr. 54943/00, par. 78, 106 (*Weber en Saravia/ Duitsland*); EHRM 22 februari 2018, appl. nr. 588/13, par. 43 (*Libert/ Frankrijk*). In Niemietz noemt het EHRM deze twee waarborgen ‘*the essential object and purpose of Article 8*’. Zie hiervoor par. 31 van het genoemde arrest.

personen.[83] Het begrip 'privéleven' moet volgens het EHRM breed en niet uitputtend worden geïnterpreteerd.[84] Zo omvat het recht op een privéleven onder andere het recht op lichamelijke en psychische integriteit,[85] zelfbeschikking,[86] de eigen identiteit, [87] het eigen portret [88] maar ook het recht op het ontwikkelen van relaties met anderen.[89] Interactie tussen personen kan daarmee onder het bereik van het begrip 'privéleven' vallen.[90] Daarbij moet wel worden vermeld dat de rechten elkaar onderling kunnen overlappen. Het EHRM bepaalde dat de interceptie van telefooncommunicatie zowel een inbreuk op het recht op respect voor een privéleven als het recht op respect voor correspondentie opleverde.[91] Het EHRM benoemt in haar uitspaken dan ook vaak dat op beide rechten een inbreuk is gemaakt. In verband met de context en de omvang van dit onderzoek zal alleen het recht op respect voor een privéleven worden onderzocht. Indien nodig wordt alleen het sterk verwante recht op respect voor correspondentie hooguit zijdelings besproken. Tevens beperkt dit onderzoek zich tot de negatieve verplichting van de Verdragsstaat. Dit omdat de politie met de opsporingsmethodiek een inbreuk op het recht op privacy kan maken en zich daar in de basis van heeft te onthouden.

Een begrip dat het EHRM veelvuldig in één adem met het begrip 'privéleven' (*private life*) gebruikt is 'privacy'. Hoewel het EHRM in haar jurisprudentie geen vaste definitie van het begrip privacy geeft, lijkt er onderscheid te kunnen worden gemaakt. In een *toolkit* stelt de Raad van Europa dat 'privéleven' breder is dan 'privacy'. Privacy richt zich meer op het recht op vertrouwelijkheid en beslotenheid.[92] In de *joint partly concurring opinion* in *Big Brother Watch e.a.* stellen drie EHRM-rechters dat *'[t]he mere feeling that one is constantly being observed and evaluated by others can have serious effects on one's mental and physical well-being. It makes individuals internalise too much of their social behaviour, so that they feel guilty or ashamed because of any feelings or thoughts, desires or practices that they would not want to express publicly.*'[93] Hierin kan worden gelezen dat mensen hun gedrag aanpassen omdat zij zich bespied voelen. Dit bespieden omvat mijns inziens de registratie van waarneembare (*observed*) sociaal gedrag (zoals observeren en (af)luisteren), maar ook het vastleggen van gegevens in registratiesystemen waardoor analyse (*evaluated*) van dat gedrag kan plaatsvinden. Dit laatste noemen

[83] Krabbe 2004, p. 137. Slechts bij uitzondering genieten rechtspersonen rechtsbescherming onder dit artikel. Zie hiervoor onder andere EHRM 16 april 2002, ECLI:NL:XX:2002:AE4682, *NJ* 2003, 452, m.nt. E.J. Dommering, par. 44-45 (*Sté Colas Est/ Frankrijk*).
[84] EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, *NJ* 1993, 400, m.nt. E.J. Dommering, par. 29 (*Niemietz/ Duitsland*); EHRM 16 februari 2000, appl. nr. 27798/95, par. 65 (*Amann/ Zwitserland*); EHRM 25 september 2001, appl. nr. 44787/98, par. 56 (*P.G. en J.H./ Verenigd Koninkrijk*); EHRM 29 april 2002, appl. nr. 2346/02, par. 61 (*Pretty/ Verenigd Koninkrijk*); EHRM 28 januari 2003, app. nr. 44647/98, par. 57 (*Peck/ Verenigd Koninkrijk*).
[85] EHRM 26 maart 1985, appl. nr. 8978/80, par. 22 (*X en Y/ Nederland*).
[86] EHRM 20 januari 2011, appl. nr. 31322/07, par. 51 (*Haas/ Zwitserland*).
[87] EHRM 7 februari 2002, appl. nr. 53176/99, par. 53 (*Mikulic/ Kroatië*).
[88] EHRM 24 juni 2004, appl. nr. 59320/00, par. 50 (*Von Hannover/ Duitsland*).
[89] EHRM 16 februari 2000, appl. nr. 27798/95, par. 65 (*Amann/ Zwitserland*); EHRM 29 april 2002, appl. nr. 2346/02, par. 61 (*Pretty/ Verenigd Koninkrijk*).
[90] EHRM 25 september 2001, appl. nr. 44787/98, par. 56 (*P.G. en J.H./ Verenigd Koninkrijk*).
[91] EHRM 6 september 1978, appl. nr. 5029/71, par. 41 (*Klass e.a./ Duitsland*); EHRM 02 augustus 1984, ECLI:NL:XX:1984:AB8061, *NJ* 1988, 534, m.nt. J.V. van Dijk, par. 64 (*Malone/ Verenigd Koninkrijk*); EHRM 25 juni 1997, appl. nr. 20605/92, par. 44 (*Halford/ Verenigd Koninkrijk*).
[92] Meer precies: 'rights to confidentiality and seclusion'. 'Right to respect for private and family life', https://www.coe.int/en/web/echr-toolkit/le-droit-au-respect-de-la-vie-privee-et-familiale 8 maart 2022.
[93] Join partly concurring opinion of judges Lemmens, Vehabovic en Bosnjak, par. 5 bij EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*).

Keulen & Knigge 'informationele privacy'.[94] Ten behoeve van de eenduidigheid hanteert dit onderzoek zoveel mogelijk het begrip privacy.

3.3 Reikwijdte recht op privacy

Hierboven werd het recht op privacy besproken. Nu moet eerst worden onderzocht of de verzonden chatgesprekken en metadata via een chatapplicatie binnen het beschermingsbereik van het recht op privacy vallen. Het EVRM is in 1950 opgesteld in het licht van de toenmalige technische mogelijkheden. Toch vindt ook het gebruik van de moderne communicatiemogelijkheden bescherming binnen art. 8 EVRM. Dit is mogelijk doordat de bepalingen in het EVRM betrekkelijk open zijn geformuleerd.[95] Dit geeft veel ruimte voor interpretatie.[96] Voor het eerst in *Tyrer* bepaalde het EHRM dat het EVRM moet worden gezien als '*a living instrument which […] must be interpreted in the light of present-day conditions.*'[97] Met een open formulering en de dynamische, evolutieve uitleg van normen kan het EHRM omgaan met hedendaagse vraagstukken.[98]

Om in vertrouwelijkheid en beslotenheid uiting te kunnen geven aan gedrag en gedachten, is vrijheid van vertrouwelijke communicatie nodig. Telefoneren is één van de mogelijkheden tot vertrouwelijke communicatie. In diverse uitspraken bevestigt het EHRM dat telefoneren onder de bescherming van het recht op privacy valt. In *Klass* stelde het EHRM dat geheim overheidstoezicht op telefoongesprekken de vrijheid van communicatie tussen gebruikers van de post- en telecommunicatiediensten aantast. Het vormt daarmee een inmenging van een overheidsinstantie in de uitoefening van het recht op eerbiediging van het privé- en gezinsleven en op correspondentie.[99] In *Huvig* en *Kruslin* hield het EHRM deze lijn vast door te bepalen dat elke wijze van interceptie van telefoongesprekken een ernstige inmenging in het privéleven vormt.[100] In *Roman Zakharov* bracht het EHRM communicatie gevoerd middels een mobiele telefoon ook onder het beschermingsbereik van art. 8 EVRM.[101] Met de komst van de *smartphone* kwam ook de technische mogelijkheid om vanaf de telefoon e-mail- en chatberichten te versturen en internet te raadplegen. In *Copland* bevestigde het EHRM wederom dat telefonie onder het beschermingsbereik van het recht op privéleven valt, maar vulde dit recht aan door de verzending van (persoonlijke) e-mailberichten en internetgebruik eveneens onder dit recht te laten vallen.[102] In *Barbulescu* bepaalde het EHRM dat het gebruik van een instant messaging service een vorm van communicatie is die individuen de mogelijkheid biedt een sociaal privéleven te leiden, en daarmee onder het recht op privacy valt.[103]

---

[94] Keulen & Knigge 2020, p. 92. Meer precies omschrijven zij informationele privacy als '[h]et verzamelen, documenteren en gebruiken van persoonlijke gegevens[…].'
[95] Hielkema & Krabbe 2004, p. 19-20.
[96] Hielkema & Krabbe 2004, p. 20.
[97] EHRM 25 april 1978, appl. nr. 5856/72, par. 31 (*Tyrer/ Verenigd Koninkrijk*); Gerards 2011, p. 35; Oerlemans 2017, p. 80.
[98] Gerards 2011, p. 35; Oerlemans 2017, p. 80; EHRM 16 april 2002, ECLI:NL:XX:2002:AE4682, *NJ* 2003, 452, m.nt. E.J. Dommering, par. 45 (*Sté Colas Est/ Frankrijk*).
[99] EHRM 6 september 1978, appl. nr. 5029/71, par. 41 (*Klass e.a./ Duitsland*).
[100] EHRM 24 april 1990, appl. nr. 11105/84, par. 32 (*Huvig/ Frankrijk*); EHRM 24 april 1990, appl. nr. 11801/85, par. 33 (*Kruslin/ Frankrijk*).
[101] EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, *Computerrecht* 2016/86, m.nt. S.J. Eskens, par. 173 (*Roman Zakharov/ Rusland*).
[102] EHRM 3 april 2007, appl. nr. 62617/00, par. 41 (*Copland/ Verenigd Koninkrijk*). Zie ook EHRM 1 juli 2007, appl. nr. 58243/00, par. 56 (*Liberty e.a./ Verenigd Koninkrijk*); EHRM 24 april 2018, appl. nr. 62357/14, par. 104 (*Benedik/ Slovenië*).
[103] EHRM 5 september 2017, appl. nr. 61496/08, par. 74, 141 (*Barbulescu/ Roemenië*).

Jurisprudentie rondom metadata kent een soortgelijke ontwikkeling. In *Malone* werd bepaald dat het tijdstip en duur van het telefoongesprek, en de gebelde telefoonnummers onder de bescherming van art. 8 EVRM vallen.[104] In respectievelijk *P.G. en J.H.* en *Ben Faiza* bepaalde het EHRM dat de verkrijging van metadata van (mobiele) telefoons door de politie een inmenging op het recht op privéleven en correspondentie was.[105] In *Big Brother Watch e.a.* erkende het EHRM dat een groot deel van het leven tegenwoordig in het digitale domein plaatsvindt en deze verplaatsing een aanzienlijk grotere hoeveelheid elektronische communicatie van een andere aard en kwaliteit genereert dan tien jaar geleden.[106] Tegenwoordig worden inhoudelijke data omgeven door stukken metadata. Hoewel metadata versleuteld kunnen zijn, kan het persoonlijke informatie onthullen.[107] Het EHRM erkent verder dat de (bulk)vergaring van metadata niet minder indringend is dan inhoudelijke *content*.[108] Hiermee kent het EHRM aan metadata dezelfde beschermingsgraad toe als aan inhoudelijke *content*.

Omdat in de jurisprudentie van het EHRM niet specifiek wordt gesproken over de bescherming van het verzenden van berichten en metadata via chatapps, zal art. 8 EVRM als een *living instrument* moeten worden uitgelegd naar *present-day conditions.* Het lijkt erop dat het EHRM de vertrouwelijkheid en beslotenheid van communicatie wil beschermen tegen inmenging van overheidsinstanties en in mindere mate de wijze waarop de communicatie plaatsvindt. Uit de jurisprudentie blijkt dat het EHRM persoonlijke (mobiele) telefoongesprekken, e-mailberichten, instant-messaging berichten en metadata onder het beschermingsbereik van het recht op privacy heeft gebracht. Door een dynamische en evolutieve benadering van het EVRM-recht kan het mijns inziens tot geen andere conclusie leiden dat de verzending van inhoudelijke chatberichten en de bijbehorende metadata via een chatapplicatie vanaf een *smartphone* binnen de beschermingssfeer van art. 8 lid 1 EVRM valt.

3.4 Beperkingsvoorwaarden art. 8 lid 2 EVRM

Het door het EVRM beschermde recht op privacy is niet absoluut.[109] Art. 8 lid 2 EVRM voorziet in een aantal beperkingsvoorwaarden waarmee de politie een inbreuk op het recht op privacy kan maken: ‘Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen’. Om te beoordelen of de politie binnen de reikwijdte van haar bevoegdheid is gebleven, beoordeelt het EHRM een voorgelegde casus op basis van een aantal vaste vragen.

[104] EHRM 02 augustus 1984, ECLI:NL:XX:1984:AB8061, *NJ* 1988, 534, m.nt. J.V. van Dijk, par. 83-84 (*Malone/ Verenigd Koninkrijk*).
[105] EHRM 25 september 2001, appl. nr. 44787/98, par. 42 (*P.G. en J.H./ Verenigd Koninkrijk*); EHRM 8 februari 2018, appl. nr. 31446/12, par. 66-68 (*Ben Faiza/ Frankrijk*).
[106] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 341 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[107] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 342 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[108] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 363 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[109] Gerards 2011, p. 97.

3.4.1 Toetsing inbreuk op art. 8 lid 2 EVRM

Eerst dient onderzocht te worden of de vergaring van (bulk)data door de inzet van beveiligde chatapplicaties door de politie een inbreuk op het recht op privacy maakt. Gerards stelt dat de jurisprudentie nauwelijks eisen stelt aan de omvang, aard en ernst van de inbreuk en daarmee geen duidelijk kader geeft dat bepaalt wanneer er sprake is van een inbreuk op een grondrecht.[110] Zodra een individueel belang binnen het beschermingsbereik van het EVRM valt, neemt het EHRM een inbreuk van het grondrecht snel aan.[111] In *Leander* werd de opslag van privacy-gerelateerde gegevens van individuen door de politie als een inbreuk op het recht op privacy beoordeeld.[112] In *Big Brother Watch e.a.* stelde het EHRM dat bulkinterceptie van data door inlichtingen- en veiligheidsdiensten binnen het beschermingsbereik van art. 8 EVRM valt.[113] Deze uitspraak is ook van toepassing op politieonderzoeken.[114] Het EHRM spreekt onder andere over de inzet van bulkinterceptie voor de bestrijding van '*serious crimes*'. Hiermee wordt mijns inziens de weg vrij gemaakt voor de inzet van bulkinterceptie door de politie. Het EHRM beoordeelt primair het middel, niet de instantie die het middel inzet.[115] Het EHRM ziet bulkinterceptie als een gradueel proces waarbij de mate van de inbreuk vergoot naar gelang het proces vordert.[116] Het EHRM onderscheidt vier fasen: (i) de vergaring en initiële opslag van de data, (ii) de toepassing van specifieke selectiecriteria op de verkregen data, (iii) analyse van de geselecteerde data en (iv) de opslag en gebruik van het eindproduct.[117] Op elke fase is art. 8 EVRM van toepassing, hoewel het EHRM bij de eerste fase nog niet wil spreken van een significante inbreuk op het recht op privacy.[118]

3.4.2. Legaliteitsvereisten

Een overheidsinstantie mag onder voorwaarden het recht op privacy beperken. De eerste beperkingsvoorwaarde is die van de legaliteit: de inperking van het recht op privacy is alleen mogelijk als er enige nationale wettelijke regeling aan ten grondslag ligt die op de beperking is gericht.[119] Het materiële recht, het ongeschreven recht alsook gepubliceerde strafvorderlijke richtlijnen en algemene rechtsbeginselen vallen onder het begripsbereik ´wet´.[120] Bepalend is de uitleg die een nationale rechter aan het recht geeft.[121] Het EHRM stelt sinds *Malone* enkele kwaliteitseisen aan de wet, om deze zodoende in overeenstemming met de '*rule of law*' te brengen.[122] In het verlengde van *Malone* onderscheidt Taylor Parkins-Ozephius e.a. vier vereisten in de *rule of law*-gedachte: de wet moet (i)

---

[110] Gerards 2011, p. 99-100.
[111] Gerards 2011, p. 99.
[112] EHRM 26 maart 1987, appl. nr. 9248/81, par. 48 (*Leander/ Zweden*).
[113] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 330 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[114] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 345 (*Big Brother Watch e.a./Verenigd Koninkrijk*). Zie ook Eskens, Van Daalen & Van Eijk 2016, p. 12.
[115] Eskens, Van Daalen & Van Eijk 2016, p. 12.
[116] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 325 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[117] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 325 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[118] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 330 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[119] Gerards 2011, p. 115; EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema, par. 47-48 (*Sunday Times/ Verenigd Koninkrijk*).
[120] Nieuwenhuis 2017, p. 112; Corstens/Borgers & Kooijmans 2021, p. 36, 42-43; EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema, par. 49 (*Sunday Times/ Verenigd Koninkrijk*); EHRM 24 april 1990, appl. nr. 11801/85, par. 28-29 (*Kruslin/ Frankrijk*).
[121] Krabbe 2004, p. 162-163.
[122] EHRM 02 augustus 1984, ECLI:NL:XX:1984:AB8061, *NJ* 1988, 534, m.nt. J.V. van Dijk, par. 67 (*Malone/ Verenigd Koninkrijk*). Zie omtrent de *rule of* law verder de alinea 'Rechtmatigheid overheidsoptreden'.

toegankelijk en (ii) voorzienbaar zijn, (iii) voorzien in waarborgen tegen willekeurig gedrag en (iv) rechtmatig overheidsoptreden bieden op basis van de bepaling.[123]

Toegankelijkheid

De toegankelijkheid vereist dat de burger het geldende recht moet kunnen (laten) nazoeken.[124] Voldoende is dat de wettelijke bepaling op enige wijze is gepubliceerd. Echter, publicatie is niet altijd vereist. Ook ongepubliceerde regelgeving waar bij bestendig gebruik alleen in bijzondere gevallen van wordt afgeweken, dient als vaste praktijk en voldoet aan het toegankelijkheidsvereiste.[125] De richtlijn moet wel direct beschikbaar zijn voor de burger.[126] Van de burger die door het opsporingsmiddel wordt getroffen, mag enige inspanningsverplichting worden verwacht om te achterhalen of diens recht op privacy wordt geschonden.[127]

Voorzienbaarheid

De voorzienbaarheid eist dat de nationale regeling zo precies is omschreven dat de burger kan inschatten wanneer de uitoefening van zijn grondrecht door een overheidsinstantie wordt beperkt.[128] Zo kan de burger zijn gedrag op de wettelijke bepaling afstemmen.[129] Niet is vereist dat alle regelingen rigide en met absolute zekerheid zijn geformuleerd.[130] Het gebruik van min of meer vage bewoordingen en open formuleringen bieden de mogelijkheid dat regelgeving zich aan veranderde omstandigheden kan aanpassen.[131] Het EHRM verlangt wel dat vage normen en open formuleringen nader worden ingevuld door nationale jurisprudentie om aan het vereiste van voorzienbaarheid te voldoen.[132] Of een regelgeving voorzienbaar is hangt in belangrijke mate af van de inbreuk die het maakt op het recht op privacy. Hoe groter de inbreuk, hoe preciezer de formulering van de regeling moet zijn.[133] Tappen en andere vormen van telefoonintercepte vormen een serieuze inbreuk op de privacy en vereisen duidelijke, gedetailleerde wetgeving.[134] Zeker nu de beschikbare technologie steeds geavanceerder wordt en misbruik en willekeur van de opsporingsbevoegdheid op de loer liggen.[135]

---

[123] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 324. In *Malone* wordt voor de kwaliteit van de wet vereist dat deze voldoende toegankelijk (*adequately accessible*) en voorzienbaar (*foreseeability*) is. EHRM 02 augustus 1984, ECLI:NL:XX:1984:AB8061, *NJ* 1988, 534, m.nt. J.V. van Dijk, par. 66-67 (*Malone/ Verenigd Koninkrijk*).
[124] EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema, par. 49 (*Sunday Times/ Verenigd Koninkrijk*).
[125] Krabbe 2004, p. 164. Zie ook EHRM 28 maart 1990, appl. nr. 10890/84, par. 68 (*Groppera Radio AG e.a./ Zwitserland*).
[126] EHRM 25 september 2001, appl. nr. 44787/98, par. 37 (*P.G. en J.H./ Verenigd Koninkrijk*).
[127] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 324; Gerards 2011, p. 123. Keulen & Knigge 2020, p. 97. In deze mag van een professional een grotere inspanningsverplichting worden verwacht dan van een leek. Zie hiervoor onder andere EHRM 16 juni 2016, appl. nr. 49176/11, par. 55 (*Versini-Campinchi en Crasnianski/ Frankrijk*).
[128] EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema, par. 49 (*Sunday Times/ Verenigd Koninkrijk*).
[129] EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema, par. 49 (*Sunday Times/ Verenigd Koninkrijk*); Nieuwenhuis 2017, p. 112.
[130] EHRM 25 maart 1983, appl. nr. 5947/72, par. 88 (*Silver/ Verenigd Koninkrijk*); EHRM 9 oktober 2003, appl. nr. 48321, par. 107 (*Slivenko/ Letland*).
[131] EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema, par. 49 (*Sunday Times/ Verenigd Koninkrijk*).
[132] EHRM 25 maart 1983, appl. nr. 5947/72, par. 88 (*Silver/ Verenigd Koninkrijk*).
[133] EHRM 25 september 2001, appl. nr. 44787/98, par. 62 (*P.G. en J.H./ Verenigd Koninkrijk*).
[134] EHRM 24 april 1990, appl. nr. 11105/84, par. 32 (*Huvig/ Frankrijk*); EHRM 24 april 1990, appl. nr. 11801/85, par. 33 (*Kruslin/ Frankrijk*).
[135] EHRM 24 april 1990, appl. nr. 11105/84, par. 32 (*Huvig/ Frankrijk*); EHRM 24 april 1990, appl. nr. 11801/85, par. 33 (*Kruslin/ Frankrijk*); EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, *Computerrecht* 2016/86, m.nt. S.J. Eskens, par. 229 (*Roman Zakharov/ Rusland*). EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 333 (*Big Brother Watch e.a./Verenigd Koninkrijk*).

Waarborgen

Het zou de opsporing niet ten goede komen als de inzet van geheime interceptie, waartoe de vergaring van (bulk) data hoort, vooraf bij de verdachte bekend wordt zodat deze zijn gedrag daar op kan afstemmen.[136] Hier heeft het EHRM oog voor gehad. De politie moet een bevoegdheid tot heimelijke interceptie kunnen (blijven) inzetten. Heimelijke interceptie vergroot de kans op misbruik en willekeur van de bevoegdheid.[137] Vooraf aan en tijdens de heimelijke inzet van de interceptiebevoegdheid kan de geïntercepteerde niet opkomen tegen een inbreuk op zijn grondrecht. Om de burger in die fasen toch bescherming tegen misbruik en willekeur te bieden, heeft het EHRM in *Big Brother Watch e.a.* minimumwaarborgen geformuleerd. Bij de heimelijke vergaring van (bulk)data moeten de waarborgen voorzien in:

(i) gronden waarop bulkinterceptie kan worden geautoriseerd;
(ii) de omstandigheden waarin de communicatie van een individu kan worden verzameld;
(iii) de procedures en modaliteiten voor toezicht door een onafhankelijke autoriteit op de naleving van deze waarborgen en de bevoegdheden van die autoriteit als het gaat om het adresseren van onrechtmatig handelen.[138]

Deze minimumwaarborgen zijn een aanscherping van de eerder in *Weber en Saravia* opgestelde minimumwaarborgen die de nationale wetgever in acht moet nemen bij het opstellen van interceptiebevoegdheden: (i) de soort overtredingen die aanleiding kunnen zijn voor inzet interceptiebevoegdheid, (ii) de categorieën personen waarop de interceptiebevoegdheid kan worden ingezet en (iii) afbakening tijdsduur inzet interceptiebevoegdheid.[139] De aanscherping in *Big Brother Watch e.a.* richt zich voornamelijk op *end-to-end safeguards* bij het graduele proces van vergaring van (bulk)data.[140] Van iedere chatapp-gebruiker worden data vergaard en opgeslagen. Pas in fase iii in het gradueel proces komen (gegevens van) specifieke personen steeds meer in zicht en wordt de inbreuk op de privacy groter.[141] Om misbruik en willekeur te voorkomen eist het EHRM dat de toepassing van elke fase van het graduele proces onderworpen is aan een beoordeling op noodzakelijkheid en proportionaliteit door een nationale, onafhankelijke instantie.[142]

---

[136] Eskens, *Computerrecht* 2015/85, nr. 3, p. 129.
[137] EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, *Computerrecht* 2016/86, m.nt. S.J. Eskens, par. 229 (*Roman Zakharov/ Rusland*); EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 333 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[138] De overige waarborgen betreffen (iv) de procedure die moet worden gevolgd voor autorisatie, (v) de procedures die gelden voor het selecteren, onderzoeken en gebruiken van verzameld materiaal; (vi) de voorzorgsmaatregelen die zijn genomen als het gaat om het doorgeven van materiaal aan andere partijen; (vii) de beperkingen op de bewaarduur, de wijze van bewaren van verzameld materiaal en de omstandigheden waarin dergelijk materiaal moet worden verwijderd en vernietigd, (viii) de procedures voor onafhankelijk onderzoek ex post facto naar de naleving van deze waarborgen en de bevoegdheden voor het bevoegde orgaan als het gaat om het onderzoeken van eventueel onrechtmatig handelen. EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 361 (*Big Brother Watch e.a./Verenigd Koninkrijk*). Zie ook Hagens & Oerlemans, par. 11, *ehrc-updates.nl* 22 maart 2022.
[139] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 361 (*Big Brother Watch e.a./Verenigd Koninkrijk*); EHRM 29 juni 2006, appl. nr. 54943/00, par. 95 (*Weber en Saravia/ Duitsland*). Deze overige waarborgen betreffen achtereenvolgens (iv) voorschriften ten aanzien van de inzage, opslag en verwerking vergaarde data, (v) voorschriften ten aanzien van het delen van gegevens met andere instanties en (vi) voorschriften ten aanzien van vernietiging van vergaarde data vernietigd.
[140] Zie met betrekking tot dit gradueel proces par. 3.4.1. van dit onderzoek.
[141] Hagens & Oerlemans, par. 14, *ehrc-updates.nl* 22 maart 2022.
[142] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 263-264 (*Big Brother Watch e.a./Verenigd Koninkrijk*).

Rechtmatigheid overheidsoptreden

De *rule of law* impliceert dat een inbreuk door overheidsinstanties op het recht op privacy onderworpen moet zijn aan een effectieve controle.[143] Hierin ligt *the essential object and purpose* van art. 8 lid 1 EVRM verscholen: het bieden van bescherming tegen misbruik van recht en een willekeurige inmenging door de politie.[144] Ook de overheid moet zich aan haar eigen regels houden, wil zij bij een burger een inbreuk maken op het recht op privacy.[145]

3.4.3 Doelcriteria

Om een inbreuk op het recht op privacy te kunnen maken, moet de maatregel de in art. 8 lid 2 EVRM limitatief genoemde legitieme doelen dienen: de nationale en openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. De criteria zijn ruim geformuleerd.[146] Dit heeft tot gevolg dat een overheidsmaatregel redelijk makkelijk onder één van de criteria is te brengen.[147] Doorgaans neemt het Hof zonder al te veel moeite aan dat een overheidsmaatregel één van de legitieme doelen dient.[148] Het EHRM schaart niet-vrijheidsbenemende strafvorderlijke maatregelen onder het doelcriterium 'voorkoming van wanordelijkheden en strafbare feiten'.[149]

3.4.4 Noodzakelijkheidsvereisten

Als laatste toetst het EHRM of de gemaakte inbreuk op het recht op privacy noodzakelijk is in een democratische samenleving. Om te bepalen of een inbreuk op het recht op privacy noodzakelijk is, moeten de belangen van de Verdragsstaat tegen die van de klager worden afgewogen (*fair balance*).[150] 'Noodzaak' houdt het midden tussen enerzijds 'onmisbaar' en 'essentieel' en anderzijds 'nuttig' en 'bevorderlijk'.[151] Noodzaak impliceert het bestaan van een dringende maatschappelijke behoefte (*pressing social need*), waarbij de inmenging in verhouding moet staan tot het legitieme doel dat de Verdragsstaat nastreeft (proportionaliteitstoets).[152] Uit de dringende maatschappelijke behoefte moet voortvloeien dat de redenen die zijn aangevoerd om de inbreuk te rechtvaardigen *relevant and sufficient* zijn in relatie tot het nagestreefde legitieme doel.[153] Verder voert het EHRM een subsidiariteitstoets uit.[154] Met deze subsidiariteitstoets onderzoekt het EHRM of een minder ingrijpend middel beschikbaar is waarmee hetzelfde doel kan worden bereikt. Omdat de nationale wetgever van een Verdragsstaat

[143] EHRM 25 maart 1983, appl. nr. 5947/72, par. 90 (*Silver/ Verenigd Koninkrijk*).
[144] EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, *NJ* 1993, 400, m.nt. E.J. Dommering, par. 31 (*Niemietz/ Duitsland*).
[145] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 325.
[146] Krabbe 2004, p. 176; Gerards 2011, p. 133; Nieuwenhuis 2017, p. 115.
[147] Gerards 2011, p. 133.
[148] Gerards 2011, p. 123.
[149] Krabbe 2004, 176.
[150] Nieuwenhuis 2017, p. 116; Krabbe 2004, p.177; Gerards 2011, p. 158.
[151] Nieuwenhuis begrensde dit vereiste als volgt: 'De inmenging dient met andere woorden meer dan louter wenselijk of redelijk te zijn, maar hoeft niet onmisbaar in strikte zin te zijn.' Zie hiervoor Nieuwenhuis, *NTM/NJCM-bull*. 2014/2, p. 21.
[152] EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, m.nt. E.A. Alkema, par. 59, 62 (*Sunday Times/ Verenigd Koninkrijk*). EHRM 25 maart 1983, appl. nr. 5947/72, par. 97 (*Silver/ Verenigd Koninkrijk*). Nieuwenhuis stelt dat uit de dringende maatschappelijke behoefte kan voortvloeien dat de inmenging van een staat urgentie moet hebben. Mijns inziens wordt de urgentie al omvat met het woord 'dringend'. Zie hiervoor Nieuwenhuis, *NTM/NJCM-bull*. 2014/2, p. 14.
[153] Keulen & Knigge 2020, p. 95; EHRM 22 oktober 1981, appl. nr. 7525/76, par. 51-54 (*Dudgeon/ Verenigd Koninkrijk*); EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, m.nt. E.A. Alkema, par. 62 (*Sunday Times/ Verenigd Koninkrijk*).
[154] Gerards 2011, p. 152.

het beste zelf de noodzakelijkheid van een beperking op EVRM-grondrecht in het eigen rechtsstelsel kan bepalen, kent het EHRM Verdragsstaten enige beoordelingsruimte toe (*margin of appreciation*).[155] Hoe groot de beoordelingsruimte van een Verdragsstaat is, hangt af van de consensus die onder de Verdragsstaten bestaat over de noodzakelijkheid van de beperking.[156] Heeft een Verdragsstaat een grote beoordelingsruimte, dan toetst het EHRM de noodzakelijkheid van de beperking minder kritisch dan wanneer een Verdragsstaat een kleine beoordelingsruimte heeft.[157] Als laatste beoordeelt het EHRM in steeds grotere mate of de wetgever van een Verdragsstaat de grondrechtbeperkende maatregel zorgvuldig heeft voorbereid en voorzien van waarborgen waarmee misbruik van de bevoegdheid en willekeur van de inmenging kan worden voorkomen.[158]

3.5 Tussenconclusie

In dit hoofdstuk is het antwoord op de tweede deelvraag beschreven: Op basis van welke vereisten mag de nationale wetgever een inbreuk maken op het recht op privacy zoals gewaarborgd in art. 8 EVRM? Het gebruik van een chatapp ter vergaring van (bulk)data als opsporingsmiddel kan een inbreuk op het recht op privacy van de geïntercepteerde opleveren. Om misbruik van de bevoegdheid en willekeurige inmenging door overheidsinstanties te voorkomen, wordt het recht op privacy beschermd door art. 8 lid 1 EVRM. Eerst is onderzocht of de chatdata, zowel de inhoudelijke *content* als de metadata, onder het beschermingsbereik van het recht op privacy vallen. Het recht op privacy is niet absoluut. Lid 2 van dit artikel somt de beperkingsvoorwaarden op waardoor overheidsinstanties een inbreuk op het recht op privacy mogen maken. De eerste voorwaarde is dat er sprake moet zijn van een inbreuk op het recht op privacy. Blijkt dat het geval te zijn, dan vereist het EHRM dat de bevoegdheid aan legaliteitsvereisten voldoet, waarbij de toegankelijkheid, voorzienbaarheid, waarborgen en rechtmatigheid van het overheidsoptreden van de wettelijke grondslag van de bevoegdheid van belang zijn. De volgende voorwaarde is dat de opsporingsbevoegdheid één van de in lid 2 genoemde doelcriteria dient. Het EHRM neemt doorgaans snel aan dat een bevoegdheid één van de doelcriteria dient. De belangrijkste voorwaarde betreft die van de noodzakelijkheidsvereisten. Een wetgever moet toetsen of de inbreuk die een bevoegdheid op het recht op privacy van de geïntercepteerde maakt, in redelijk evenwicht staat met het maatschappelijk belang dat de inbreuk dient. Van belang hierbij is dat de inbreuk een dingende maatschappelijke behoefte vervult en het lichtste middel wordt gebruikt om het doel te bereiken. Hierbij wordt de wetgever wel enige beoordelingsruimte gelaten.

[155] Gerards 2011, p. 183.
[156] EHRM 10 april 2007, ECLI:NL:XX:2007:BA6787, par. 77 (*Evans/ Verenigd Koninkrijk*).
[157] Gerards 2011, p. 143.
[158] Gerards 2011, p. 169.

4 Nationale opsporingsbevoegdheden

4.1 Inleiding

Het vorige hoofdstuk beschrijft mede dat de inperking van het recht op privacy alleen is toegestaan indien er enige nationale wettelijke regeling aan ten grondslag ligt. Hoe groter de inbreuk, hoe preciezer de formulering van de regeling moet zijn. Net als art. 8 EVRM kent het Nederlandse Wetboek van Strafvordering een legaliteitsbeginsel. Art. 1 Sv stelt dat strafvordering alleen plaats heeft op de wijze bij de wet voorzien. Het doel van dit artikel is om burgers rechtszekerheid te bieden.[159] Dit artikel biedt burgers bescherming tegen willekeurige vervolging en bestraffing door overheidsinstanties, en dwingt overheidsinstanties zich aan de voorgeschreven wet te houden.[160] Voor de vergaring van (bulk)data lijkt op het eerste gezicht geen specifieke strafvorderlijke bevoegdheid te bestaan. Dit hoofdstuk onderzoekt het bestaan van een wettelijke bevoegdheid waarmee (bulk)data met behulp van een chatapplicatie door de politie mogen worden vergaard. In verband met de context en de omvang van dit onderzoek wordt alleen de fase van vergaring van (bulk)data onderzocht op het bestaan van een nationale strafvorderlijke bevoegdheid.

4.2 Algemene opsporingsbevoegdheid op grond van de Politiewet

Eerst wordt onderzocht of er een algemene opsporingsbevoegdheid bestaat die als grondslag voor het opsporingsmiddel kan dienen. In art. 3 Polw is de algemene taakstelling van de politie geformuleerd.[161] Eén van die taken betreft de strafrechtelijke handhaving van de rechtsorde.[162] Onder strafrechtelijke handhaving verstaat de wetgever 'de daadwerkelijke voorkoming, de opsporing, de beëindiging, […] van strafbare feiten […]'.[163] Op grond van deze strafrechtelijke handhavingstaak is de politie bevoegd opsporingshandelingen te verrichten.[164] Uit art. 3 Polw vloeit een impliciete bevoegdheid voort voor de inzet van niet-specifiek in de wet beschreven opsporingsmiddelen.[165] Om een opsporingsbevoegdheid op grond van art. 3 Polw uit te kunnen oefenen, mag deze slechts een beperkte inbreuk op het recht op privacy maken en een te verwaarlozen risico voor de integriteit en beheersbaarheid van de opsporing vormen.[166] De vraag wanneer er sprake is van een meer dan beperkte inbreuk op de privacy is casuïstisch, maar het EHRM hanteert als leidend beginsel de stelselmatigheid van de inzet van een opsporingsmiddel.[167] Zo is de toepassing van de observatiebevoegdheid pas stelselmatig indien de observatie 'een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands

[159] Corstens/Borgers & Kooijmans 2021, p. 23.
[160] Keulen & Knigge 2020, p. 23.
[161] Art. 3 Politiewet (Polw) voluit: 'De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'
[162] Art. 3 juncto art. 12 Polw.
[163] Toen nog art. 2 Polw. *Kamerstukken II* 1985/86, 19535, nr. 3, p. 6. Met de invoering van de nieuwe Politiewet in 2012 is deze taakstelling ongewijzigd gebleven. *Kamerstukken II* 2006/07, 30880, nr. 3, p. 45-46, 49.
[164] Art. 141 en 142 Sv juncto art. 3 juncto art. 12 Polw.
[165] Keulen & Knigge 2020, p. 305-306.
[166] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249, m.nt. T.M. Schalken, r.o. 6.4.2-6.4.5; HR 1 juli 2014, ECLI:NL:HR:2014:1562, r.o.3.5.2; HR 1 juli 2014, ECLI:NL:HR:2014:1563, r.o. 2.4. Zie ook Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 326; Borgers, *DD* 2015/15, p. 143.
[167] Borgers, *DD* 2015/15, p. 146.

leven'.[168] Daarbij hangt de stelselmatigheid af van de duur, de plaats, de intensiteit of frequentie van de observatie en het gebruik van een technisch hulpmiddel.[169] In *Big Brother Watch e.a.* wilde het EHRM bij de vergaring en initiële opslag van (bulk)data nog niet spreken van een significante inbreuk op het recht op privacy, maar wel dat art. 8 EVRM van toepassing was.[170] Oerlemans noemt de vergaring van bulkdata 'bulkinterceptie'.[171] Oerlemans stelt dat de interceptie van communicatie een serieuze inbreuk op het recht op privacy maakt en dat dergelijke bevoegdheden altijd met voldoende precisie in de wet dienen te worden omschreven.[172] Met behulp van de chatapp worden inhoudelijke data en metadata vergaard. De rechtbank van Amsterdam overwoog dat deze data een min of meer volledig beeld van iemands privéleven kunnen weergeven.[173] Zo bezien biedt art. 3 Polw geen toereikende grondslag voor het opsporingsmiddel. De bevoegdheid om het opsporingsmiddel in te mogen zetten, dient dus te worden gebaseerd op een specifieke regeling uit het Wetboek van Strafvordering.

4.3 Bijzondere opsporingsbevoegdheden

Pas sinds 2000 kent het Nederlandse Wetboek van Strafvordering een regeling die specifiek en nauwkeurig met waarborgen omklede opsporingsbevoegdheden beschrijft, waarmee inbreuk op het recht op privacy van burgers mag worden gemaakt.[174] Aanleiding hiervoor was de IRT-affaire en het daaropvolgend onderzoek door de parlementaire enquêtecommissie.[175] Naar aanleiding van haar onderzoek kwam de parlementaire enquêtecommissie tot de conclusie dat de toepassing van bijzondere opsporingsbevoegdheden een wettelijke basis behoeft. Deze conclusie leidde tot de invoering van de Wet bijzondere opsporingsbevoegdheden (hierna: Wet BOB).

Door de intrede van het digitale tijdperk heeft veel criminaliteit tegenwoordig enig raakvlak met de digitale wereld. Denk alleen al aan het gebruik van chatapps als communicatiemiddel. Nu worden opsporingsmiddelen met een digitale component veelal ingelezen in de reeds bestaande bevoegdheden en dat zou ten koste kunnen gaan van de voorzienbaarheid van de wet voor burgers.[176] Schermer stelt de vraag of er sprake is van een nieuwe (digitale) IRT-affaire nu de politie opsporingsmiddelen gebruikt die eigenlijk niet voldoende specifiek in het Wetboek van Strafvordering zijn beschreven.[177] Schermer concludeerde dat een verheldering en modernisering van het juridisch kader voor de online opsporing op zijn plaats was.[178] De gedachtegang van Schermer kan ik begrijpen. Hoewel digitale toepassingen nu ingelezen worden in de reeds bestaande bevoegdheden, voorzien deze bevoegdheden wel in diverse toetsingsmomenten, al dan niet door een onafhankelijke rechter-commissaris (hierna:R-C). Daarmee is het belang van de door de bevoegdheid getroffen burger in de basis beschermd. Wel ben ik van mening dat BOB-bevoegdheden techniek-neutraler kunnen worden geformuleerd zodat ook

[168] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27. Art. 126g Sv.
[169] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 27.
[170] Zie paragraaf 5.2.1, alinea 'waarborgen' van dit onderzoek.
[171] Oerlemans 2020, p. 6.
[172] Oerlemans 2017, p. 79-80. Zie ook Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.4, 3.6.
[173] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.4.
[174] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 9-11.
[175] *Eindrapport Commissie-Van Traa 1996*.
[176] Schermer, *webwereld.nl* 14 maart 2012.
[177] Schermer, *webwereld.nl* 14 maart 2012.
[178] Schermer, *webwereld.nl* 14 maart 2012.

toekomstige ontwikkelingen beter onder bestaande bevoegdheden gebracht kunnen worden. Zo wordt voorkomen dat een te rigide wetgeving ontstaat die bij elke ontwikkeling uitgebreid wordt. In die lijn ben ik het met Schermer eens dat het belang van het vastleggen van grenzen van de toepassing van een bevoegdheid prevaleert boven het opstellen van nieuwe bevoegdheden.[179] Inmiddels is de wetgever een moderniseringstraject van het Wetboek van Strafvordering gestart.[180] De hierna in dit onderzoek te bespreken bijzondere opsporingsbevoegdheden zijn naar aard, inhoud en strekking nagenoeg onveranderd gebleven in het concept-Wetboek van Strafvordering. Om deze reden zal het moderniseringstraject hier onbesproken blijven.

De huidige Wet BOB biedt drie grondslagen voor bijzondere opsporingsbevoegdheden. Titel IVa biedt bijzondere bevoegdheden tot opsporing (‘klassieke opsporing’), Titel V biedt bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband (‘vroegsporing’) en Titel Vb biedt bijzondere opsporingsbevoegdheden tot opsporing van terroristische misdrijven. Titel Vb wordt hier verder onbesproken gelaten. De in Titels IVa en V beschreven bevoegdheden lijken zeer sterk op elkaar. Het voornaamste verschil zit in het gebruikte verdenkingscriterium. In geval van Titel IVa dient er sprake te zijn van een op grond van art. 27 Sv gefundeerde concrete verdenking van een strafbaar feit.[181] Waar Titel IVa spreekt van een ‘verdenking van een strafbaar feit’ en een meer reactieve functie heeft, beoogt Titel V een proactieve opsporing te bewerkstelligen. Titel V richt zich op de aanpak van criminele organisaties waartegen ‘een redelijk vermoeden bestaat dat ofwel een misdrijf is gepleegd (Titel IVa) ofwel dat in georganiseerd verband voorlopige-hechtenismisdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren.’[182] Titel V spreekt doorgaans over een ‘persoon die deelneemt of waarvan naar feiten en omstandigheden een redelijk vermoeden voortvloeit’. Deze persoon wordt dan nog niet concreet verdacht van een strafbaar feit. De georganiseerde criminaliteit onderscheidt zich van de traditionele criminaliteit doordat op stelselmatige wijze misdrijven worden gepleegd die veelal verborgen blijven of nog moeten plaatsvinden.[183] Titel V richt zich op het crimineel samenwerkingsverband, inclusief haar organisatoren en alle daarbij betrokken personen, en in mindere mate op een bepaald persoon jegens wie een concrete verdenking bestaat.[184] De vergaring van (bulk)data via een chatapp heeft een proactieve opsporing als uitgangspunt, waarbij het doel is zicht te krijgen op criminele organisaties en haar (toekomstige) criminele activiteiten ter verzameling van bewijsmateriaal. Het verkrijgen van een informatiepositie mag geen doel op zich zijn.[185] Verdachten kunnen met dit bewijsmateriaal worden vervolgd voor gepleegde strafbare feiten en deelname aan een criminele organisatie.[186] Titel V lijkt derhalve de meest aangewezen grondslag voor dit opsporingsmiddel.

[179] Schermer, *webwereld.nl* 14 maart 2012.
[180] Ambtelijke versie juli 2020 Memorie van Toelichting Wetboek van Strafvordering, p. 9, rijksoverheid.nl 1 april 2022.
[181] Krommendijk, Terpstra & Van Kempen 2009, p. 9.
[182] Krommendijk, Terpstra & Van Kempen 2009, p. 111, gebaseerd op art. 126o lid 1 Sv.
[183] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 4; Corstens/Borgers & Kooijmans 2021, p. 293
[184] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.6. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 23. Corstens/Borgers & Kooijmans 2021, p. 292.
[185] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 3.
[186] Deelname aan een criminele organisatie is als zelfstandig strafbaar feit opgenomen in art. 140 van het Wetboek van Strafrecht: ‘Deelneming aan een organisatie die tot oogmerk heeft het plegen van misdrijven, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.’

Het Wetboek van Strafvordering kent twee vormen van gegevens: opgeslagen en stromende gegevens. Opgeslagen gegevens zijn gegevens die in een geautomatiseerd werk vastliggen.[187] Stromende gegevens betreffen gegevens die in een proces van verwerking of overdracht zijn tussen geautomatiseerde werken.[188] Doordat de chatapp communicatie tussen twee personen uitwisselt (stromende gegevens tussen geautomatiseerde werken), kan gebruik worden gemaakt van de opsporingsbevoegdheden 'opnemen van vertrouwelijke communicatie' (art. 126s Sv) en 'opnemen telecommunicatie' (art. 126t Sv).[189] Beide bevoegdheden zullen als eerst worden besproken, voordat de overige bevoegdheden 126o tot en met 126qa Sv op toepasselijkheid, zijnde de rechtmatige verkrijging van (bulk)data ten behoeve van de strafvordering, worden onderzocht. De bevoegdheden die zien op het verkrijgen van opgeslagen gegevens (art. 126u tot en met art. 126ui Sv) blijven onbesproken.

4.3.1. Opnemen vertrouwelijke communicatie

Art. 126s Sv regelt het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (hierna: OVC): 'In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie (hierna: OvJ), indien het onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onderdelen b, c en d, met een technisch hulpmiddel vertrouwelijke communicatie opneemt waaraan een persoon deelneemt […].'

Onder vertrouwelijke communicatie wordt elke vorm van niet in het openbaar geuite uitgewisselde berichten, waaronder gesprekken, geschreven woorden of verzonden signalen, tussen twee of meer personen verstaan.[190] De wetgever heeft voor deze bevoegdheid de vorm van communicatie bewust technologie-onafhankelijk gehouden, zodat geanticipeerd kan worden op toekomstige ontwikkelingen.[191] De bevoegdheid maakt het zodoende mogelijk om heimelijk communicatie op het internet op te nemen met behulp van een technisch hulpmiddel.[192] Het geautomatiseerd werk, bijvoorbeeld een computer of een *smartphone*, dient op een netwerk te zijn aangesloten.[193] Er moet sprake zijn van stromende gegevens, waarbij de gegevens vanaf het geautomatiseerd werk van de verzender wordt overgebracht naar een ontvanger.[194] Opgeslagen gegevens op een *standalone* computer vallen niet onder de reikwijdte van dit artikel.[195] Voor de toepassing van de bevoegdheid is van belang dat in ieder geval of de ontvanger of de verzender betrokken is bij het beramen of plegen van misdrijven in crimineel verband. Of de communicatiepartner van de persoon nu een geautomatiseerd werk in de vorm van een computer of een ander persoon is, is voor toepassing van dit

[187] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 18. Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Zie art. 80sexies Wetboek van Strafrecht.
[188] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 18-19. Met de komst van cloudcomputing is dit onderscheid in de praktijk echter diffuus geworden.
[189] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 18, 23.
[190] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 36. Naar analogie kunnen e-mails, sms-berichten en berichten verstuurd via sociale sites ook als vertrouwelijke communicatie worden aangemerkt. Zie hiervoor *Kamerstukken II* 2015/16, 34372, nr. 3, p. 23.
[191] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35; Corstens/Borgers & Kooijmans 2021, p. 509.
[192] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 36.
[193] Koops & Oerlemans 2019, p. 170.
[194] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 36.
[195] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35-36.

artikel niet van belang.[196] Voor OVC vanaf een geautomatiseerd werk mag gebruik worden gemaakt van een softwarepakket als technisch middel.[197] De software wordt in het geautomatiseerd werk geïnstalleerd. Oerlemans stelt dat de software fysiek op het geautomatiseerd werk moet worden geïnstalleerd omdat er (toentertijd) geen juridische basis bestond voor het op afstand binnendringen van een geautomatiseerd werk.[198] Inmiddels is met de zogenaamde 'hackbevoegdheid' van art. 126uba Sv deze mogelijkheid wel geschapen en kan de hackbevoegdheid worden ingezet ter uitvoering van een bevel tot OVC.[199] De software biedt de politie de mogelijkheid om de communicatiedata direct te vergaren, voordat versleuteling of nadat ontsleuteling van de communicatie plaatsvindt.[200] In dergelijke software kan ook een toepassing worden verwerkt waarmee gebruikte wachtwoorden en decryptiesleutels vanaf geautomatiseerd werken worden vergaard. Met deze decryptiesleutels kan de politie vervolgens communicatie ontsleutelen. Art. 126s Sv herbergt de impliciete bevoegdheid tot het ontsleutelen van opgenomen communicatie.[201] Om te voorkomen dat opsporingsinstanties met lichtzinnigheid deze bevoegdheid toepassen, heeft de wetgever met het vereiste dat het onderzoek de inzet van de bevoegdheid 'dringend vordert', een subsidiariteitstoets ingebouwd. Alvorens men overweegt om gebruik te maken van de OVC-bevoegdheid van art. 126s Sv, moet eerst de toepasselijkheid van de lichtere tapbevoegdheid van art. 126t Sv worden onderzocht.[202]

4.3.2. Opnemen telecommunicatie

Art. 126t Sv betreft het opnemen van telecommunicatie met behulp van een technisch middel (hierna: tappen): 'In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst in de zin van artikel 138g, […], wordt opgenomen.' Hoewel de wetgever tappen een minder zware bevoegdheid vindt, doet het qua aard, inhoud, voorwaarden en waarborgen nauwelijks onder aan de OVC-bevoegdheid. De wetgever acht de tapbevoegdheid een minder zware bevoegdheid omdat de OVC-bevoegdheid meer in de directe omgeving van de betrokken persoon wordt toegepast.[203] Een telefoon- of internettap vergaart beperkter data, hetgeen een minder grote inbreuk op de privacy zou maken. Het grootste verschil met OVC is dat het tappen plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst. Art. 138g Sv definieert een aanbieder van een communicatiedienst als 'de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk […].' Art. 138g Sv is van toepassing op zowel openbare netwerken (zoals KPN, T-Mobile, internetproviders

[196] Koops & Oerlemans 2019, p. 168.
[197] Oerlemans, *JV* 2012, nr. 3, p. 36. Een voorbeeld hiervan is de inzet van een keylogger. Met een keylogger kunnen toetsaanslagen en screenshots van gebruikte computerprogramma's in een geautomatiseerd werk worden vastgelegd en verzonden Zie voor de toepassing van een keylogger: Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4620, par. 9.
[198] Oerlemans, *JV* 2012, nr. 3, p. 36-37; *Kamerstukken II* 2015/16, 34372, nr. 3, p. 13.
[199] Art. 126uba lid 1 onder b Sv.
[200] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 327. Zie ook *Kamerstukken II* 2015/16, 34372, nr. 3, p. 9-10.
[201] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35.
[202] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 37; Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 331.
[203] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 37.

en websitebeheerders) als besloten netwerken (waaronder interne netwerken van bedrijven en instellingen).[204]

Van belang is dat de aanbieder van de communicatiedienst zijn diensten 'in de uitoefening van een beroep of bedrijf' aanbiedt. In de Ennetcom-zaak merkte de rechtbank de exploitant van een chatapp aan als een aanbieder van een communicatiedienst in de zin van art. 138g Sv.[205] Art. 138g Sv richt zich namelijk ook op 'aanbieders die gebruik maken van deze netwerken om hun diensten aan te bieden.'[206] Met 'deze netwerken' bedoelt de wetgever de aanbieders van openbare telecommunicatienetwerken en -diensten, waaronder internettoegang.[207] Het aftappen van de communicatie kan met en zonder medewerking van de aanbieder van de communicatiedienst plaatsvinden.[208] Aanbieders van openbare telecommunicatienetwerken en -diensten zijn verplicht te voorzien in faciliteiten om stromende gegevens te kunnen tappen, en medewerking te verlenen aan een tapbevel.[209] In de praktijk betekent dit dat deze aanbieders de stromende gegevens doorzenden naar servers van de politie.[210] Van de overige aanbieders van communicatiediensten kan alleen de medewerking worden verlangd.[211] Het aftappen van een aanbieder van een netwerk zonder diens medewerking kan bijvoorbeeld geschieden door, al dan niet op afstand, het netwerk van de aanbieder binnen te dringen.[212] Uit onderzoek 26Rockdale 2, ontstaan uit de Encrochat-zaak, bleek dat de hackbevoegdheid van art. 126uba Sv als steunbevoegdheid diende voor de inzet van een tapbevoegdheid in de zin van art. 126t Sv.[213] Hoewel dit verder niet uit de uitspraak blijkt, lijkt mijns inziens de ratio van de rechter er in te liggen dat de verdachte rechtspersoon Encrochat is aangemerkt als een aanbieder van een communicatiedienst. Vergelijkbaar met de Ennetcom-zaak faciliteerde en exploiteerde Encrochat een chatapp waarmee versleutelde communicatie kon worden verstuurd.

Tappen richt zich op alle vormen van communicatie. Naast telefoongesprekken mogen ook internet, e-mail, chatverkeer en webcambeelden worden getapt.[214] Zoals eerder beschreven wordt chatverkeer in steeds grotere mate versleuteld. In dat geval zal de politie alleen versleutelde data ontvangen waaruit geen inhoud kan worden afgeleid. Op grond van art. 126t lid 6 Sv kan de OvJ van degene van wie dit redelijkerwijs kan worden verlangd en daartoe in staat is, vorderen dat deze persoon de communicatiedata ontsleutelt.[215] Dit betreft versleutelingen die de aanbieder zelf aan de communicatiedata heeft aangebracht.[216] Een dergelijke vordering kan niet aan de verdachte worden gericht en vereist een schriftelijke machtiging van de R-C.[217] Vaak is het niet mogelijk om de versleutelde data te ontsleutelen. Dit kan liggen in de complexiteit van de versleuteling, het feit dat versleuteling van

[204] Corstens/Borgers & Kooijmans 2021, p. 513. Koops & Oerlemans 2019, p. 159.
[205] Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 57.
[206] *Kamerstukken II* 2004/05, 26671, nr. 7, p. 26; Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086, r.o. 54
[207] *Kamerstukken II* 2004/05, 26671, nr. 7, p. 26.
[208] *Kamerstukken II* 2004/05, 26671, nr. 7, p. 41.
[209] Art. 13.1 en 13.2 Tw; ook art. 126t lid 3 Sv
[210] Zie voor een uitgebreide beschrijving van dit proces: Koops & Oerlemans 2019, p. 162.
[211] Art. 126t lid 4 Sv; Koops & Oerlemans 2019, p. 162, 166; Corstens/Borgers & Kooijmans 2021, p. 519.
[212] Bijvoorbeeld gebaseerd op de bevoegdheid van art. 126uba lid 1 onder b Sv.
[213] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.5.
[214] Koops & Oerlemans 2019, p. 159.
[215] Koops & Oerlemans 2019, p. 162.
[216] Koops & Oerlemans 2019, p. 162.
[217] Art. 126t lid 7 en 8 Sv.

de data al plaatsvindt voordat deze worden verzonden (zoals in het geval van E2EE) of de omstandigheid dat de aanbieder van de communicatiedienst in het buitenland is gevestigd, waardoor Nederland geen rechtsmacht over de aanbieder heeft.[218] De wetgever acht in dergelijke gevallen de inzet van de tapbevoegdheid dan ook niet effectief.[219]

4.3.3. Overige bijzondere opsporingsbevoegdheden

Over de inzet van de bijzondere opsporingsbevoegdheden stelselmatige observatie en inwinning (respectievelijk art. 126o en 126qa Sv), en de inkijkoperatie (art. 126r Sv) als bevoegdheid tot het verkrijgen van stromende gegevens is de wetgever kort en duidelijk. De inzet van deze bevoegdheden is niet gericht op de toegang tot stromende gegevens die langs elektronische weg worden verzonden.[220]

Art. 126o Sv regelt de bevoegdheid tot stelselmatige observatie. Observeren betreft 'het direct, fysiek heimelijk gadeslaan en heimelijk volgen van een persoon of een object, al of niet met gebruikmaking van hulpmiddelen.'[221] Het hulpmiddel mag geen vertrouwelijke communicatie opnemen, hetgeen bij de vergaring van (bulk)data wel het geval is.[222]

De bevoegdheid tot stelselmatige inwinning van informatie (art. 126qa Sv) onderscheidt zich van de stelselmatige observatie doordat een opsporingsambtenaar heimelijk en actief interfereert in het (online) leven van de betrokken persoon met als doel informatie over die persoon te krijgen.[223] De opsporingsambtenaar zal zich op een zodanige wijze in de directe omgeving van de verdachte of de betrokkene ophouden dat hij daardoor met personen contacten onderhoudt uit diens directe omgeving.[224]

Bij een infiltratiebevoegdheid (art. 126p Sv) participeert een *undercover* opsporingsambtenaar in een crimineel samenwerkingsverband om zodoende zicht te krijgen op activiteiten en werkwijzen van dat crimineel samenwerkingsverband.[225] Een van de methodieken van infiltratie is het opzetten van dekmantelbedrijven (hierna: *frontstores*). Een *frontstore* is een (legaal) dekmantelbedrijf dat ten behoeve van een criminele organisatie wordt opgezet en geëxploiteerd, waarmee facilitaire ondersteuning aan de criminele organisatie wordt aangeboden.[226] Echter, hiermee lijkt de vergaring van stromende gegevens via de chatapp nog niet juridisch gelegitimeerd. In art. 126p. Sv is namelijk niet uitdrukkelijk opgenomen of uitgesloten dat (vertrouwelijke) communicatie met een technisch hulpmiddel mag worden vergaard, hoewel specifieke normering van strafvorderlijke bevoegdheden wel het uitgangspunt van de wetgever is. Zo'n uitsluiting is wel specifiek opgenomen in art. 126o lid 3 Sv. In de Hansa Market-zaak bracht de rechtbank de heimelijke overname van een handelswebsite op het

[218] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 8.
[219] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 8.
[220] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 13.
[221] *Eindrapport Commissie-Van Traa 1996*, p. 173.
[222] Art. 126o lid 3 Sv.
[223] Stol & Strikwerda, *Tijdschrift voor Veiligheid* 2018 (17), p. 14.
[224] Aanwijzing Opsporingsbevoegdheden, par. 2.6, wetten.overheid.nl, laatst geraadpleegd 5 mei 2022.
[225] Aanwijzing Opsporingsbevoegdheden, par. 2.9, wetten.overheid.nl, laatst geraadpleegd 5 mei 2022. Oerlemans, *Computerrecht* 2019/178, p. 345; *Kamerstukken II* 1995/96, 24072, nr. 10/11, p. 229.
[226] Art. 1 onder b Regeling financieel beheer van met infiltratie en store-fronts gegenereerde ontvangsten.

darkweb door de politie onder de infiltratiebevoegdheid van art. 126h Sv. Hansa Market was een online marktplaats, gericht op de verkoop van strafbare goederen. De overname van Hansa Market door de politie had als doel wachtwoorden, berichten en orderinformatie onversleuteld af te vangen teneinde verdachten te identificeren en illegale goederen in beslag te nemen. Het onderzoeksteam fungeerde daarbij als beheerder van Hansa Market.[227] In zijn annotatie bij dit vonnis stelt Oerlemans, mijns inziens terecht, dat de rechtbank wel heel summier de goedkeuring van de infiltratiebevoegdheid onderbouwde.[228] Oerlemans suggereert dat er mogelijk andere ondersteunende bevoegdheden zijn toegepast.[229] Mijns inziens zou dit met hetgeen hierboven is beschreven over specifieke regelgeving, juist zijn. De gedachtegang van Taylor Parkins-Ozephius e.a. volgend kan de infiltratiebevoegdheid mijns inziens alleen dienen om de chatapp binnen het criminele milieu te verspreiden en de politie als beheerder van de chatapp op te laten treden.[230]

Dit laatste uitgangspunt is ook te verdedigen ten aanzien van de lichtere variant op de infiltratiebevoegdheid, de bevoegdheid tot pseudokoop en -dienstverlening (art. 126q Sv). Met deze bevoegdheid koopt een *undercover* opsporingsambtenaar goederen of gegevens van of verleent hij een dienst aan een persoon binnen een crimineel samenwerkingsverband teneinde bewijs tegen de organisatie te vergaren. De bevoegdheid tot pseudodienstverlening heeft in beginsel een eenmalig karakter.[231] Indien pseudodienstverlening binnen een crimineel samenwerkingsverband een frequenter karakter krijgt, dient de infiltratiebevoegdheid te worden toegepast.[232] Bij de pseudokoop en -dienstverlening mag de opsporingsambtenaar de persoon niet tot andere strafbare feiten brengen dan waarop diens opzet reeds tevoren was gericht, ook het 'Tallon-criterium' genoemd.[233] Pseudoverkoop van illegale producten is wettelijk niet toegestaan, omdat daarmee de toetsing van het Tallon-criterium moeilijk controleerbaar is.[234] Jurisprudentie laat echter wel een kleine opening voor pseudoverkoop van legale producten.[235] Encryptietelefoons met chatapps zijn niet verboden. Maar weer, deze bevoegdheid geeft hooguit een legitimatie voor de verspreiding van het opsporingsmiddel.[236]

4.4 Besluit technisch hulpmiddel strafvordering

Met name de artikelen 126o, 126s en 126t Sv spreken over de toepassing van technische hulpmiddelen. Op grond van art. 126ee Sv is de toepassing van technische hulpmiddelen genormeerd. De normering is nader uitgewerkt in het Besluit technische hulpmiddelen strafvordering (hierna: het Besluit). Dit besluit dient het uitgangspunt dat de middels een technisch hulpmiddel vastgelegde gegevens betrouwbaar,

[227] Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, r.o. 4.3.
[228] Oerlemans, *Computerrecht* 2019/178, p. 345.
[229] Oerlemans, *Computerrecht* 2019/178, p. 345.
[230] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 326. Zie over beheer: par. 2.2.3 van dit onderzoek.
[231] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 33.
[232] De infiltratiebevoegdheid herbergt een impliciete bevoegdheid tot pseudodienstverlening. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 33.
[233] Art. 126p lid 3 Sv; HR 04 december 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980, 356, m.nt. Th.W. van Veen.
[234] Keulen & Knigge 2020, p. 366.
[235] Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, p. 326 met verwijzing naar de arresten HR 5 maart 2019, ECLI:NL:HR:2019:298 en HR 20 december 2011, ECLI:NL:HR:2011:BP0199.
[236] Zie hiervoor verder Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5, par. 4.2.

toetsbaar (herleidbaar) en niet-manipuleerbaar zijn.[237] Met de komst van de Wet computercriminaliteit III werd het gebruik van software als technisch hulpmiddel in het Besluit gecodificeerd.[238] Hoewel de Wet computercriminaliteit III voornamelijk geschreven lijkt te zijn op de toepassing van hacksoftware, zijn de beschreven waarborgen ook gericht op software dat als technisch hulpmiddel ter vergaring van vertrouwelijke communicatie dient.[239] Volgens de minister valt het gebruik van '*spyware*' aan te merken als een technisch hulpmiddel bij de OVC-bevoegdheid, waarop 126ee Sv van toepassing is.[240] Voorwaarde is wel dat de software fysiek op het geautomatiseerd werk wordt geïnstalleerd.[241] Het Besluit vereist als eerste dat de opslag, verstrekking, plaatsing, controle en verwijdering van een technisch hulpmiddel geschiedt door aangewezen en deskundige opsporingsambtenaren.[242] Ten tweede geeft het Besluit technische eisen waaraan de software moet voldoen, de beveiligingseisen voor het transport van signalen, de controle op het technische hulpmiddel en de verwijdering ervan.[243] Indien het softwarematige technisch hulpmiddel vergaarde vertrouwelijke communicatie naar een politieserver verzendt, dient dit transport beveiligd te zijn. Dit kan door de data te versleutelen.[244] Als laatste dient het technisch middel te zijn gekeurd.[245] Het Besluit geeft regels ten aanzien van technische eisen, keuringsprotocollen en de registratie van keuringsrapporten.

4.5 Tussenconclusie

In dit hoofdstuk is het antwoord op de derde deelvraag beschreven: In hoeverre biedt het nationaal strafprocesrecht een strafvorderlijke bevoegdheid die als grondslag kan dienen voor de inzet van het beschreven opsporingsmiddel? Wil de politie (bulk)data vergaren middels een chatapp, dan dient dit opsporingsmiddel te steunen op een opsporingsbevoegdheid. De algemeen taakstellende bevoegdheid van art. 3 Polw is niet toereikend. Op grond van dit artikel mag slechts een beperkte inbreuk op het recht op privacy van de burger worden gemaakt. Met de vergaring van (bulk)data is daar geen sprake van. Dit middel maakt juist een vergaande inbreuk op het recht op privacy en dient zodoende te steunen op een specifieke opsporingsbevoegdheid uit het Wetboek van Strafvordering. Gezien het feit dat het opsporingsmiddel als doel heeft de georganiseerde criminaliteit te bestrijden, ligt het voor de hand de strafvorderlijke bevoegdheden van Titel V toe te passen. Art. 126s Sv schept de bevoegdheid tot OVC. Met deze bevoegdheid kan de politie vertrouwelijke communicatie tussen personen opnemen die in beslotenheid worden geuit. De wetgever heeft de vorm van communicatie technologie-onafhankelijk gehouden. Hierdoor is het mogelijk om stromende gegevens, zoals chatberichten, te vergaren. De

[237] Nota van toelichting bij Besluit technische hulpmiddelen strafvordering, p. 9 (*Stb.* 2006, 524); HR 12 juli 2011, ECLI:NL:HR:2011:BP4650, r.o. 4.2.
[238] Voluit: Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III).
[239] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 109. Zie de tweede alinea van de paragraaf 'Artikel 126ee' waarin de wetgever spreekt over: 'Aanvullend op de normen voor de camera en de richtmicrofoon zullen regels worden vastgelegd voor de opslag, plaatsing, verstrekking en verwijdering van de softwareapplicatie die kan worden gebruikt voor onderzoek in een geautomatiseerd werk en de technische eisen voor de softwareapplicatie.' Met name het gebruik van het woord 'kan' geeft mijns inziens ruimte voor een bredere toepassing van het besluit dan alleen op de hackbevoegdheid. Zie ook: Oerlemans, *Computerrecht* 2017/103, p. 178-179; Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, r.o. 5.3.
[240] *Aanhangsel Handelingen II* 2014/15, nr. 202.
[241] Oerlemans, *JV* 2012, nr. 3, p. 36-37; *Kamerstukken II* 2015/16, 34372, nr. 3, p. 13.
[242] Art. 5 tot en met 9 Besluit technische hulpmiddelen strafvordering; *Kamerstukken II* 2015/16, 34372, nr. 3 p. 30.
[243] Art. 9 tot en met 17 Besluit technische hulpmiddelen strafvordering; *Kamerstukken II* 2015/16, 34372, nr. 3 p. 31.
[244] Nota van toelichting bij Besluit technische hulpmiddelen strafvordering, p. 24 (*Stb.* 2006, 524).
[245] Art. 18 en 19 Besluit technische hulpmiddelen strafvordering.

chatapp als opsporingsmiddel betreft een softwarepakket (een technisch middel) dat op een geautomatiseerd werk, in casu de telefoon, wordt geïnstalleerd. De chatapp verzendt de communicatiedata, voorzien van een decryptiesleutel, naar de servers van de politie. Na de ontsleuteling kan de politie beschikken over de inhoud van de communicatie en metadata. Zeer vergelijkbaar is de opsporingsbevoegdheid tappen. Daarbij wordt met behulp van een aanbieder van een communicatiedienst telecommunicatie onderschept. Infiltratie kan als ondersteunende bevoegdheden dienen om een *frontstore* op te zetten ter verspreiding van de encryptietelefoons met chatapps en beheer van het chatapp-systeem. Nu dringt de vraag op of (een *frontstore* van) de politie als een aanbieder van een communicatiedienst moet worden aangemerkt. In dat geval lijkt namelijk de tapbevoegdheid van art. 126t Sv de meeste passende bevoegdheid bij dit opsporingsmiddel. Met de exploitatie van de chatapp verzorgt de politie een communicatiedienst. Een aanbieder van een communicatiedienst is een natuurlijk of rechtspersoon die handelt in de uitoefening van zijn bedrijf of beroep. Ik meen dat de politie niet handelt in de uitoefening van een beroep of bedrijf maar deze hoogstens gebruikt als dekmantel ten behoeve van de opsporing van strafbare feiten. Daarnaast is het maar de vraag of de politie kan voldoen aan de uit art. 126t lid 6 Sv voortvloeiende ontsleutelplicht indien de chatapp gebruik maakt van E2EE. Ik meen dan ook dat art. 126s Sv de juiste bevoegdheid is om (bulk)data te vergaren middels een chatapp ten behoeve van de strafvordering.

5 Toetsing

5.1 Inleiding

In de vorengaande hoofdstukken is achtereenvolgend uiteen gezet hoe een beveiligde chatapp werkt en wat moet worden verstaan onder het begrip (bulk)data (hoofdstuk 2), aan welke criteria van art. 8 EVRM een overheidsinstantie moet voldoen om een gerechtvaardigde inbreuk te kunnen maken op iemands recht op privacy (hoofdstuk 3) en welke nationale bevoegdheid ten grondslag ligt aan de inzet van een beveiligde chatapp ter vergaring van (bulk)data ten behoeve van de strafvordering (hoofdstuk 4). In dit hoofdstuk zal de vergaring van (bulk)data middels een chatapp op basis van de OVC-bevoegdheid, en de daarin opgenomen waarborgen tegen misbruik en willekeurige inmenging van de bevoegdheid door overheidsinstanties, worden getoetst aan de criteria van art. 8 EVRM.

5.2 Toetsing van de bevoegdheid aan de voorwaarden van art. 8 lid 2 EVRM

In paragraaf 3.3 is beargumenteerd dat een dynamische en evolutieve benadering van het EVRM-recht tot de conclusie leidt dat de verzending van inhoudelijke berichten en de bijbehorende metadata via een chatapp vanaf een *smartphone* binnen de beschermingssfeer van art. 8 lid 1 EVRM valt. Nu dient getoetst te worden of de vergaring van (bulk)data door de inzet van beveiligde chatapps op grond van de OVC-bevoegdheid een inbreuk maakt op het recht op privacy van de geïntercepteerde. De opslag van privacy-gerelateerde gegevens van individuen door de politie merkt het EHRM aan als een inbreuk op het recht op privacy.[246] Als het EHRM in *Big Brother Watch e.a.* daarbij de vergaring van bulkdata aanmerkt als een inbreuk op het recht op privacy, is het mijns inziens evident dat de vergaring van (bulk)data door de politie met behulp van een chatapp eveneens een inbreuk op het recht op privacy vormt. Immers, van iedere gebruiker van de chatapp worden zowel de inhoudelijke *content* als de metadata vergaard. Dergelijke data geven de politie uiteindelijk, individueel geanalyseerd maar zeker gecombineerd, een min of meer volledig beeld van iemands persoonlijke leven, waarvan niet kan worden gezegd dat deze persoon in vertrouwelijkheid en beslotenheid uiting heeft kunnen geven aan gedrag en gedachten. Nu blijkt dat de politie met het opsporingsmiddel privacygevoelige data vergaart en deze vergaring een inbreuk op het recht op privacy van burgers maakt, moet het opsporingsmiddel worden getoetst aan de beperkingsvoorwaarden van art. 8 lid 2 EVRM.

5.2.1. Legaliteitsvereisten

Toegankelijkheid

Het uitgangspunt van het toegankelijkheidsvereiste is dat de burger het geldig recht moet kunnen (laten) nazoeken. De OVC-bevoegdheid van art. 126s Sv is opgenomen in het Wetboek van Strafvordering. De regeling is gepubliceerd in het Staatsblad.[247] Met deze publicatie is de relevante regeling met betrekking tot de OVC-bevoegdheid beschikbaar en voldoende toegankelijk voor de burger.

[246] EHRM 26 maart 1987, appl. nr. 9248/81, par. 48 (*Leander/ Zweden*).
[247] *Stb.* 1999, 245.

Voorzienbaarheid

In het geval van de opsporing van strafbare feiten is het niet wenselijk dat de geïntercepteerde weet dat zijn vertrouwelijke communicatie wordt opgenomen. De inzet van de OVC-bevoegdheid dient dan ook heimelijk te gebeuren. Zoals uit het vorige hoofdstuk bleek, is de wettelijke OVC-bevoegdheid tamelijk ruim omschreven en de toepassing van OVC op velerlei manieren mogelijk. Dat maakt dat de voorzienbaarheid van de bevoegdheid voor een potentieel geïntercepteerde beperkt is. Aan het vereiste van voorzienbaarheid is zodoende niet voldaan. Om tegenwicht te bieden aan de beperkte voorzienbaarheid, dient de OVC-bevoegdheid omkleed te zijn met voldoende waarborgen die misbruik en willekeur van de bevoegdheid tegengaan.

Waarborgen

Om de burger te beschermen tegen misbruik en willekeur van de OVC-bevoegdheid door de politie, heeft de wetgever waarborgen in het wetsartikel van art. 126s Sv opgenomen. Deze waarborgen worden getoetst langs de kaders die het EHRM heeft gecreëerd in de arresten *Weber en Saravia* en *Big Brother Watch e.a.* Op basis van *Big Brother Watch e.a.* schrijven Hagens en Oerlemans dat de eerste twee minimumwaarborgen uit *Weber en Saravia* (soort overtreding en categorie mensen) niet onverkort toepasbaar zijn op bulkinterceptie.[248] Dit is gelegen in het feit dat in *Big Brother Watch e.a.* ongerichte bulkinterceptie werd ingezet door inlichtingen- en veiligheidsdiensten. Daar was geen sprake van verdachten of een redelijke verdenking. Er zijn twee argumenten aan te dragen waarom de waarborgen uit *Weber en Saravia*, die zien op de fase van vergaring van (bulk)data, wel moeten worden meegenomen bij de toetsing van het opsporingsmiddel aan art. 8 EVRM. Het eerste argument is dat *Weber en Saravia* uitgaat van gerichte interceptie van verdachten waarbij sprake is van een redelijke verdenking.[249] Eerder is al gesteld dat al het bepaalde in *Big Brother Watch e.a.* ook van toepassing is op de opsporingspraktijk. De vergaring van (bulk)data door chatapps vindt plaats in het kader van de strafvordering. Art. 126s Sv vereist een redelijk vermoeden van betrokkenheid bij het plegen van misdrijven in georganiseerd verband. Een tweede argument vloeit voort uit een recente uitspraak van de rechtbank van Amsterdam in de 26Rockdale 2-zaak. Deze rechtbank oordeelde dat bij de vergaring van en onderzoek aan alle Encrochat-data 'geen sprake is geweest van 'bulkdata' in de zin van ongedifferentieerde dataverzameling' maar van 'een afgebakende groep, namelijk de gebruikers van Encrochat, en om een concrete verdenking, namelijk dat Encrochat werd gebruikt, geheel of in overwegende mate, door deelnemers aan georganiseerde criminaliteit.'[250] Mijns inziens zijn de twee minimumwaarborgen uit *Weber en Saravia* zodoende wel van toepassing bij de vergaring van (bulk)data door de politie.[251] Het vormt zelfs een scherpere afbakening van de *end-to-end safeguards*. De waarborgen uit *Weber en Saravia* zullen dan ook ter toetsing worden meegenomen.

[248] Hagens & Oerlemans, par. 12, *ehrc-updates.nl* 22 maart 2022. Zie ook EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 348 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[249] Hagens & Oerlemans, par. 13-14, *ehrc-updates.nl* 22 maart 2022.
[250] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.6.
[251] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 348 (*Big Brother Watch e.a./Verenigd Koninkrijk*).

De vraag die hier nog opgeworpen dient te worden, is in welke mate de vergaring van (bulk)data inbreuk maakt op het recht op privacy van een burger. Het antwoord op deze vraag is van belang om te bepalen in welke mate waarborgen dienen te kleven aan de OVC-bevoegdheid voor de vergaring van bulkdata. Ik meen dat de inbreuk op het recht op privacy gering is. Zoals al uit *Big Brother Watch e.a.* bleek, bestaat het proces rondom bulkinterceptie uit vier fasen.[252] Over fase i (de vergaring en initiële opslag) zegt het EHRM slechts dat de data in bulk worden vergaard en dat deze data van een grote groep individuen afkomstig zijn. Een groot deel van deze groep individuen is voor de opsporingsinstantie oninteressant. Sommige communicatie die waarschijnlijk niet van belang is, kan in dit stadium worden weggefilterd.[253] Bij fase i wil het EHRM nog niet spreken van een significante inbreuk op het recht op privacy, hoewel ook op deze fase de bescherming van art. 8 EVRM van toepassing is.[254] Zowel Schermer en Oerlemans als Galiç delen deze zienswijze. Zij stellen in vergelijkbare bewoordingen dat bij bulkdata de privacy-inbreuk juist groter is in de fase van kennisname en analyse van de data.[255] De chatapp past geautomatiseerd het E2EE-proces toe. Dit betekent dat de inhoud van de datapakketten vanaf het moment van verzending tot aan het moment van ontsleuteling voor niemand inzichtelijk is, ook niet voor opsporingsambtenaren. Na ontsleuteling vindt de toepassing van selectiecriteria plaats. Pas tijdens het toepassen van (sterke) selectiecriteria, zoals een e-mailadres of complexe zoekopdrachten, (fase ii) begint het onderzoek zich op individuen te richten.[256] Feitelijk wordt in de vergaringsfase niet inhoudelijk kennis genomen van de inhoud van het *content* of metadata. Zo bezien is het begrijpelijk dat Galiç stelt dat de EHRM-toets voor wat betreft de bescherming van het recht op privacy zich richt op fase ii tot en met fase iv.[257]

De eerste *Weber en Saravia*-waarborg vereist dat de bevoegdheid aangeeft welke soorten overtredingen aanleiding kunnen geven voor inzet van de interceptiebevoegdheid. Uit de wetsomschrijving van art. 126s Sv juncto art. 126o lid 1 Sv kan het OVC-bevel worden afgegeven indien ‘uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren.’ Art. 67 lid 1 Sv benoemt de zogenaamde voorlopige hechtenis-feiten. Voorlopige hechtenis-feiten zijn alle misdrijven waarop een wettelijke gevangenisstraf staat van vier jaar of meer en de in het artikel met name genoemde feiten. Onder een ernstige inbreuk op de rechtsorde verstaat de wetgever misdrijven die de rechtsorde ernstig schokken door hun gewelddadige karakter of door hun omvang en gevolgen voor de samenleving.[258] Daarbij kan worden gedacht aan moord, drugs-, wapen- en mensenhandel en ernstige milieudelicten. Ook minder ernstige misdrijven kunnen een ernstige inbreuk maken op de rechtsorde, doordat zij in combinatie met andere

[252] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 325 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[253] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 326 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[254] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 330 (*Big Brother Watch e.a./Verenigd Koninkrijk*); EHRM 26 maart 1987, appl. nr. 9248/81, par. 48 (*Leander/ Zweden*).
[255] Schermer & Oerlemans, *TBS&H* 2022, nr. 2, p. 89. Galiç, *TBS&H* 2022, nr. 2, p. 131.
[256] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 327, 353 (*Big Brother Watch e.a./Verenigd Koninkrijk*). Zie ook Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.6, alinea ‘Bulkdata?’.
[257] Galiç, *TBS&H* 2022, nr. 2, p. 133.
[258] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 24-25.

misdrijven worden gepleegd.[259] Een voorbeeld hiervan is ambtelijke corruptie ter inklaring van een container met drugs. Het zinsdeel 'uit feiten en omstandigheden een redelijk vermoeden voortvloeit […]' sluit aan bij de criteria van art. 27 Sv.[260] Dit artikel stelt dat op basis van feiten of omstandigheden een redelijk vermoeden voort moet vloeien dat een crimineel verband zich schuldig maakt aan het plegen van misdrijven. Het vermoeden moet objectief redelijk en enigszins stevig zijn.[261]

De tweede *Weber en Saravia*-waarborg betreft het benoemen van de categorieën personen waarop de interceptiebevoegdheid kan worden ingezet. Doordat art. 126s Sv in Titel V is geplaatst, is de bevoegdheid toepasbaar op een ruime groep personen die in georganiseerd verband criminele activiteiten (gaan) plegen. Bij een georganiseerd verband kan sprake zijn van een min of meer vast verband, maar ook van wisselende verbanden.[262] De gedachtegang van de rechtbank in 26Rockdale 2 volgend, is de toepassing van de OVC-bevoegdheid op een afgebakende groep, namelijk de gebruikers van de chatapp, die in het geval van een concrete verdenking, namelijk dat de chatapp werd gebruikt, geheel of in overwegende mate door deelnemers aan georganiseerde criminaliteit, geen bezwaar.[263]

De derde *Weber en Saravia*-waarborg vereist dat wetsomschrijving voorziet in een afbakening van de tijdsduur voor de inzet van de interceptiebevoegdheid. De geldigheid van het OVC-bevel heeft een duur van maximaal vier weken, dat telkens met de duur van vier weken kan worden verlengd.[264] Elke verlenging, aanvulling of wijziging van het OVC-bevel behoeft een machtiging van de R-C.[265] Art. 126s lid 3 onder a-f Sv vermeldt de vereisten waaraan het schriftelijk bevel moet voldoen.

Zoals eerder al beschreven volgt uit *Big Brother Watch e.a.* een aantal minimumwaarborgen die zich richten op geheime vergaring van (bulk)data:

(i) gronden waarop bulkinterceptie kan worden geautoriseerd;
(ii) de omstandigheden waarin de communicatie van een individu kan worden verzameld;
(iii) de procedures en modaliteiten voor toezicht door een onafhankelijke autoriteit op de naleving van deze waarborgen en de bevoegdheden van die autoriteit als het gaat om het adresseren van onrechtmatig handelen.

De eerste twee *end-to-end safeguards* vloeien voort uit de reeds besproken *Weber en Saravia*-waarborgen. In hun analyse van *Big Brother Watch e.a.* beschrijven Hagens en Oerlemans de *end-to-end-safeguards* als volgt:

(i) Een onafhankelijke instantie, niet per se een rechter, beoordeelt de interceptie op noodzakelijkheid en proportionaliteit.
(ii) Ieder stadium van het interceptieproces, inclusief de initiële toestemming, verlengingen en wijze van interceptie, staat onder toezicht van een onafhankelijke autoriteit. Dit toezicht moet voldoende

[259] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 24-25.
[260] Krommendijk, Terpstra & Van Kempen 2009, p. 111.
[261] Krommendijk, Terpstra & Van Kempen 2009, p. 111.
[262] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 24.
[263] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.6.
[264] Art. 126s lid 5 Sv.
[265] Art. 126s lid 6 Sv.

robuust zijn om te bewerkstelligen dat de inbreuk op het recht op privacy beperkt blijft tot wat noodzakelijk is in een democratische samenleving.

(iii) Er moet een effectief rechtsmiddel beschikbaar zijn dat de geïntercepteerde kan inroepen.[266]

Uit deze analyse blijkt dat elk stadium (voorbereidende fase inzet OVC, feitelijke vergaring van en onderzoek aan data, en beëindiging van bevel OVC) onder toezicht van een onafhankelijke autoriteit dient te staan. De interpretatie door de rechtbank van Amsterdam van het begrip bulkdata kan leiden tot het gevolg dat de kring van te onderzoeken personen breder is dan alleen degenen ten aanzien van wie een redelijk vermoeden van schuld bestaat.[267] Om de rechten van iedere geïntercepteerde te beschermen kan een R-C een centrale rol innemen.

Hoewel de vergaring van (bulk)data middels een chatapp een geringe inbreuk op het recht op privacy van een burger maakt, vereist art. 126s Sv dat de OvJ een bevel afgeeft. Hiervoor behoeft deze een schriftelijke machtiging van een R-C, die alle onderdelen van het bevel dekt.[268] De R-C toetst of met de afgifte van het OVC-bevel aan alle wettelijke voorwaarden en de beginselen van een behoorlijke procesorde wordt voldaan.[269] Met het vereiste van een machtiging beoogt de wetgever een onafhankelijke rechterlijke toetsing te bewerkstelligen voordat een dergelijk zware opsporingsbevoegdheid wordt ingezet.[270] In de Encrochat-zaak zijn de politie en het OM uiterst behoedzaam omgegaan met de verkrijging van een machtiging van de R-C.[271] Zo beschreef de politie in een proces-verbaal uitvoerig de aanleiding en het doel van het onderzoek, de verdenkingen tegen de betrokken personen, waaronder de anonieme Encrochat-gebruikers, en een lijst met strafrechtelijke onderzoeken waarin het bedrijf Encrochat of haar gebruikers naar voren kwamen. Op basis van dit proces-verbaal machtigde de R-C de OvJ voor een OVC-bevel. De R-C voorzag de initiële machtiging van waarborgen om de privacyschending zoveel mogelijk in te kaderen en zogenaamde '*fishing expeditions*' te voorkomen.[272] Deze kaders met waarborgen richtten zich onder andere op de personen van wie en waarover data ontvangen zouden worden en het feit dat het delen van data met andere strafrechtelijke onderzoeken alleen na toestemming van de R-C mocht.[273] Na de vergaring en initiële opslag van de data mocht alleen op basis van onderzoeksgerelateerde zoektermen (selectiecriteria) de data worden doorzocht. Met de toepassing van selectiecriteria ging het onderzoek over naar fase ii van de bulkinterceptie. De opbrengst van de zoektermen diende eerst aan een R-C te worden voorgelegd, alvorens deze opbrengst ter beschikking van een opsporingsonderzoek werd gesteld.[274] Met de toepassing van zoektermen werd een schifting gemaakt tussen buikbare en niet-bruikbare data. Een

[266] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 263-264 (*Big Brother Watch e.a./Verenigd Koninkrijk*); Hagens & Oerlemans, par. 13-14, *ehrc-updates.nl* 22 maart 2022.
[267] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.6.
[268] Art. 126s lid 4 Sv.
[269] Corstens/Borgers & Kooijmans 2021, p. 511.
[270] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 15.
[271] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.2. In deze zaak draaide het om de vergaring van grote hoeveelheden versleutelde communicatiedata die tussen criminelen via een chatapp van het bedrijf Encrochat werden verzonden. Samenvattend kan worden gesteld een samenwerkingsverband tussen de Franse en Nederlandse politie resulteerde in de inzet de combinatiebevoegdheid van art. 126uba lid 1 onder b juncto art. 126t Sv ter vergaring van versleutelde data, die werden verzonden via een chatapp. De servers van het bedrijf Encrochat bevonden zich in Frankrijk. Dat de vergaringsbevoegdheid werd gegrond op art. 126t Sv heeft er mijns inziens mee te maken dat het bedrijf Encrochat vermoedelijk werd aangemerkt als een aanbieder van een communicatiedienst.
[272] Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243, r.o. 3.2, alinea 'De machtiging van de rechter-commissaris'.
[273] Rb. Rotterdam 15 juli 2021, ECLI:NL:RBROT:2021:6853, r.o. 3.
[274] Schermer & Oerlemans, *TBS&H* 2022, nr. 2, p. 84.

dergelijke schifting verkleint ook aanzienlijk de kans dat vergaarde data van personen, die niet betrokken zijn bij een crimineel verband, worden ingezien.

Hagens en Oerlemans stellen dat er een effectief rechtsmiddel beschikbaar moet zijn, dat de geïntercepteerde kan inroepen, om de rechtmatigheid van de interceptie of de verenigbaarheid met het EVRM te kunnen aanvechten.[275] In beginsel kan de verdachte, wiens data is onderschept, de rechtmatigheid of verenigbaarheid van het opsporingsmiddel aanvechten tijdens de strafzaak bij de rechter. De wetenschap dat een opsporingsmiddel tegen de verdachte is ingezet kan de verdachte uit het opgestelde procesdossier halen.[276] Indien het oordeel van de rechter de verdachte niet welgevallig is, kan deze beroep en cassatie aantekenen. Geïntercepteerden die geen procesdossier ontvangen dienen door de OvJ genotificeerd te worden.[277] Een dergelijke mededeling kan de OvJ achterwege laten indien dit redelijkerwijs niet mogelijk is. Dit is het geval indien een onderzoek in een andere strafzaak of bij een onderzoek tegen meerdere verdachten pas deels is afgerond.[278] Deze geïntercepteerden hebben de mogelijkheid eerst een klacht in te dienen bij de politie of daaropvolgend bij de Nationale Ombudsman.[279]

Indien alleen de fase van vergaring van de (bulk)data middels een chatapp in ogenschouw wordt genomen, zijn mijns inziens met de toetsing door de R-C en diens afgifte van de machtiging, al dan niet voorzien van voorwaarden, toetsings- en toezichtmomenten ingebouwd door een onafhankelijke instantie. Met het rechterlijke toezicht van de R-C op het vergaringsproces en de mogelijkheid van een onafhankelijke toetsing van het opsporingsmiddel achteraf worden de belangen van de (potentieel) geïntercepteerde op het recht op privacy voldoende bewaakt. De waarborgen van art. 126s Sv voldoen aan de criteria van het EHRM.

Rechtmatigheid overheidsoptreden

Als waarborg achteraf kan de rechter op grond van art. 359a Sv een verzuim tijdens de toepassing van een opsporingsbevoegdheid sanctioneren. Aan het vereiste van rechtmatig overheidsoptreden is zodoende voldaan.

5.2.2. Doelcriteria

Om een inbreuk op het recht op privacy van een burger te kunnen maken, dient de bevoegdheid een legitiem doel van art. 8 lid 2 EVRM te dienen. De inzet van de chatapp ter vergaring van (bulk)data betreft een strafvorderlijke maatregel en richt zich op de opsporing van reeds gepleegde of toekomstige strafbare feiten, die ernstig van karakter zijn en gepleegd worden in georganiseerd verband. Het EHRM

[275] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 263-264 (*Big Brother Watch e.a./Verenigd Koninkrijk*); Hagens & Oerlemans, par. 13-14, *ehrc-updates.nl* 22 maart 2022.
[276] Art. 126aa Sv. Het OM is verantwoordelijk voor het opstellen van het procesdossier. Art. 149a Sv juncto art. 2 lid 1 Besluit processtukken in strafzaken.
[277] Art. 126bb Sv.
[278] *Kamerstukken II* 2015/16, 34372, nr. 3, p. 39-40.
[279] Voor de politie: Art. 9.1 lid 1 juncto art. 9.20 lid 1 juncto 9.18 Algemene wet bestuursrecht. Voor de Nationale Ombudsman: Art. 9.18 lid 1 Algemene wet bestuursrecht juncto art. 1a lid 1 onder c Wet Nationale ombudsman.

schaart niet-vrijheidsbenemende strafvorderlijke maatregelen onder het doelcriterium ‘voorkoming van wanordelijkheden en strafbare feiten’. Aan dit vereiste is voldaan.

5.2.3. Noodzakelijkheidsvereisten

Als laatste toetst het EHRM of de gemaakte inbreuk op het recht op privacy noodzakelijk is in een democratische samenleving. Daarbij dient te worden opgemerkt dat het EHRM de toepassing van een opsporingsmiddel in het concrete geval toetst. Dat betekent dat het EHRM rekening houdt met de omstandigheden van het geval om te bepalen of de privacy-inbreukmakende maatregel van de overheid in verhouding staat tot het nagestreefde legitieme doel.[280] Het EHRM kent de Verdragsstaten enige beoordelingsruimte toe bij het bepalen van de noodzakelijkheid van de beperking van het EVRM-grondrecht. Bij de keuze van het opsporingsmiddel ter bestrijding van de georganiseerde criminaliteit en de daaraan gerelateerde ernstigere delicten geniet de Verdragsstaat een ruimere beoordelingsvrijheid dan bij de bestrijding van lichtere delicten.[281] Ook de vergaring van bulkdata valt binnen de beoordelingsruimte.[282] Om te bepalen of een inbreuk op het recht op privacy noodzakelijk is, moeten de belangen van de Verdragsstaat tegen die van de klager worden afgewogen. Er moet sprake zijn van een dringende maatschappelijke behoefte waarbij de redenen die zijn aangevoerd om de inbreuk te rechtvaardigen *relevant and sufficient* zijn in relatie tot het nagestreefde legitieme doel. Het opsporingsmiddel heeft tot doel om zware, georganiseerde criminaliteit te bestrijden. Nederland is een internationaal knooppunt in de drugshandel.[283] In deze wereld woedt reeds enkele jaren een machtsstrijd waarbij, al dan niet onschuldige, burgers worden gemarteld of geliquideerd. Daarnaast wordt met de drugshandel grof (zwart) geld verdiend en witgewassen, wapens verhandeld en ambtenaren gecorrumpeerd. Dit tast direct de veiligheid van en het vertrouwen in de democratische samenleving aan. Een effectieve opsporing van criminelen en vroegsporing van zware criminaliteit vervullen dan ook een dringende maatschappelijke behoefte.

Wordt er naar de subsidiariteit van het opsporingsmiddel gekeken, dan lijkt de vraag of een minder ingrijpend middel beschikbaar is waarmee hetzelfde doel kan worden bereikt, zichzelf deels te beantwoorden. In art. 126s Sv is reeds de toets van dringende noodzakelijkheid opgenomen waarmee eerst moet worden onderzocht of de toepassing van de tapbevoegdheid meer gepast is. De tapbevoegdheid lijkt hier niet goed toepasbaar. De chatcommunicatie wordt vanuit de chatapp middels E2EE beveiligd en versleuteld verzonden. De interceptie van deze data resulteert dan in vergaarde onontsleutelbare data waar de politie geen onderzoek aan kan plegen. Daarnaast onderschept de telecomprovider, waar het tapbevel aan afgegeven is, geen data indien de telefoon gebruikt maakt van draadloze verbindingen zoals (openbare) wifi, hotspots van derden of VPN-servers. Het is vrijwel ondoenlijk en onwenselijk om alle mogelijke draadloze verbindingen waar een persoon gebruik van

[280] Oerlemans 2017, p. 76.
[281] EHRM 4 december 2008, ECLI:NL:XX:2008:BH1813, par. 105 (*S. en Marper/ Verenigd Koninkrijk*); EHRM 8 juli 2014, appl. nr. 3910/13, par. 58 (*M.P.E.V. e.a./ Zwitserland*); EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 274 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[282] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, par. 275, 340 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[283] ‘Nederland is een knooppunt voor cocaïnehandel en daar lijkt weinig aan te doen’, *nos.nl* 15 december 2019. In vergelijkbare woorden zie: Dirksen, Van der Leest & Vermeulen, *Tijdschrift voor Criminologie* 2021 (63) 2, p. 133.

maakt te tappen.[284] Bij georganiseerde criminaliteit kan sprake zijn van een vast verband en wisselende verbanden.[285] Met het opsporingsmiddel op grond van de OVC-bevoegdheid kan juist snel worden geanticipeerd op wisselende verbanden omdat elke nieuw uitgegeven encryptietelefoon automatisch onder het werkingsbereik van het reeds lopende OVC-bevel kan worden gebracht. In het geval van een tapbevoegdheid zal telkens opnieuw een met redenen omschreven tapbevel moeten worden afgegeven. Ook zou gedacht kunnen worden dat de hackbevoegdheid van art.126uba Sv een geschikt middel is om (bulk)data te vergaren. Ten aanzien van deze bevoegdheid dient te worden gezegd dat het 'slechts' als steunbevoegdheid kan bijdragen aan de uitvoering van de OVC-bevoegdheid.[286] Voor de feitelijke vergaring van de (bulk)data is nog steeds de OVC-bevoegdheid nodig. Het staat de wetgever niet voor ogen om ten behoeve van interceptiebevoegdheden wetgeving op te stellen die tot verzwakking van digitale systemen leidt. Zodoende wordt namelijk ook de (achter)deur opengezet voor kwaadwillenden.[287] De wetgever accepteert daarmee bewust het risico dat criminelen gebruik maken van beveiligde digitale systemen en dat de opsporing van strafbare feiten ernstig kan worden belemmerd.[288] Het EHRM beoordeelt in steeds grotere mate of de wetgever van een Verdragsstaat de grondrechtbeperkende maatregel zorgvuldig heeft voorbereid en voorzien van waarborgen. Deze waarborgen zijn reeds in paragraaf 5.2.1 beschreven. Het volstaat hier te benoemen dat voor de feitelijke vergaring van de (bulk)data via de chatapp voldoende waarborgen zijn geïmplementeerd om misbruik van de bevoegdheid en willekeur van de inmenging te voorkomen. Aan de vereisten van noodzakelijkheid is voldaan.

5.3 Tussenconclusie

Dit hoofdstuk toetste de OVC-bevoegdheid van art. 126s Sv ter vergaring van (bulk)data met behulp van een chatapp aan de beperkingsvoorwaarden van art. 8 lid 2 EVRM. Met de vergaring van (bulk)data via de opsporingsmethode wordt een inbreuk gemaakt op het recht op privacy van de gebruiker van de chatapp. De grondslag voor de datavergaring berust op de OVC-bevoegdheid van art. 126s Sv. Doordat deze wettelijke bepaling in het Wetboek van Strafvordering is opgenomen, is het toegankelijk. Door de ruime wettelijke beschrijving, beperkte jurisprudentie en heimelijkheid van de opsporingsmethode, is het voor de geïntercepteerde niet voldoende voorzienbaar wanneer hij subject van de OVC-bevoegdheid is. Hierdoor kan de geïntercepteerde tijdens de interceptiefase niet in rechte opkomen tegen misbruik en willekeur van de bevoegdheid door de politie. Om hier voldoende tegenwicht aan te bieden, dient de OVC-bevoegdheid met voldoende waarborgen omgeven te zijn. Deze waarborgen worden bewaakt door de R-C. Elk OVC-bevel behoeft zijn machtiging. Na notificatie van de inzet van de OVC-bevoegdheid kan de geïntercepteerde wel in recht opkomen tegen de inzet van het opsporingsmiddel tegen hem. Wordt het belang van de geïntercepteerde, zijnde zijn recht op privacy, afgewogen tegen het belang van de staat, zijnde de bestrijding van de ernstige criminaliteit ter bescherming van de

[284] Oerlemans, *JV* 2012, nr. 3, p. 30-31; *Kamerstukken II* 2015/16, 26643, nr. 383, p. 10. De onwenselijkheid vloeit voort uit het feit dat ook alle data van onschuldige burgers die op geen enkele wijze betrokken zijn bij criminele activiteiten toch worden onderschept.
[285] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 24.
[286] Art. 126uba lid 1 onder b Sv.
[287] *Kamerstukken II* 2015/16, 26643, nr. 383, p. 4-5.
[288] *Kamerstukken II* 2015/16, 26643, nr. 383, p. 3.

democratische samenleving, dan kom ik tot de conclusie dat het belang van de staat prevaleert boven die van de geïntercepteerde. Met de vergaring van (bulk)data via een chatapp op grond van de OVC-bevoegdheid heeft de politie een heimelijke opsporingsmethode in handen die het criminele milieu kan ontwrichten en waarmee zicht kan worden verkregen op toekomstige of reeds gepleegde ernstige (levens)delicten. Een dergelijk brede en diepe informatiepositie kan niet op een andere wijze worden bereikt. Dit belang weegt zwaarder dan de zeer beperkte inbreuk op het recht op privacy, die de geïntercepteerde moet dulden in de fase van vergaring van de (bulk)data.

6 Conclusie en aanbevelingen

6.1 Conclusie

Het doel van dit onderzoek is om tot een antwoord te komen op de centrale hoofdvraag:
'In hoeverre biedt het Nederlandse strafprocesrecht een grondslag voor de vergaring van (bulk)data door de inzet van beveiligde chatapplicaties als heimelijk opsporingsmiddel en hoe verhoudt dit opsporingsmiddel zich tot het recht op eerbiediging van de privacy zoals gewaarborgd in artikel 8 EVRM?'
Om tot dit antwoord te komen zijn drie deelvragen geformuleerd die zien op de beantwoording van de hoofdvraag:

1. Hoe ziet de vergaring en ontsleuteling van data via beveiligde chatapps eruit en welke data, waaronder bulkdata, worden met een bericht meegezonden?
2. Op basis van welke vereisten mag de nationale wetgever een inbreuk maken op het recht op privacy zoals gewaarborgd in art. 8 EVRM?
3. In hoeverre biedt het nationaal strafprocesrecht een strafvorderlijke bevoegdheid die als grondslag kan dienen voor de inzet van het beschreven opsporingsmiddel?

De chatapp als opsporingsmiddel betreft een op een *smartphone* geïnstalleerd softwarepakket waarmee de politie van alle chatapp-gebruikers zowel de inhoudelijke berichten als de metadata in bulk kan vergaren. De vergaarde data vallen onder het beschermingsbereik van art. 8 EVRM. Lid 2 van dit artikel somt de beperkingsvoorwaarden op waaronder overheidsinstanties een inbreuk op het recht op privacy mogen maken. De eerste voorwaarde is dat er sprake moet zijn van een inbreuk op het recht op privacy. Hoewel de feitelijke vergaring van chatdata een beperkte inbreuk op het recht op privacy maakt, geven dergelijke data de politie uiteindelijk een min of meer volledig beeld van iemands persoonlijke leven. Als tweede voorwaarde vereist het EHRM dat de bevoegdheid aan legaliteitsvereisten voldoet, waarbij de toegankelijkheid, voorzienbaarheid, waarborgen en rechtmatigheid van het overheidsoptreden van de wettelijke basis van de bevoegdheid van belang zijn. De grondslag voor de toepassing van het opsporingsmiddel kan worden gevonden in art. 126s Sv. Art. 126s Sv schept de bevoegdheid tot OVC. Met deze bevoegdheid kan de politie vertrouwelijke communicatie tussen personen opnemen die in beslotenheid worden geuit. Hierdoor is het mogelijk om stromende gegevens, zoals chatberichten, te vergaren. Doordat deze wettelijke bepaling in het Wetboek van Strafvordering is opgenomen, is het toegankelijk. Door de ruime wettelijke beschrijving, beperkte jurisprudentie en heimelijkheid van de opsporingsmethode, is de bevoegdheid voor de geïntercepteerde niet voldoende voorzienbaar. Om hieraan voldoende tegenwicht aan te bieden, is de OVC-bevoegdheid omkleed met waarborgen. Eén van die waarborgen betreft de omstandigheid dat een OVC-bevel pas mag worden afgeven na een machtiging door een R-C. De derde voorwaarde is dat de opsporingsbevoegdheid één van de in lid 2 genoemde doelcriteria dient. Het gebruik van het opsporingsmiddel richt zich op het doelcriterium ´voorkoming van wanordelijkheden en strafbare feiten'. De laatste voorwaarde betreft die van de noodzakelijkheidsvereisten. Een wetgever moet toetsen of de inbreuk, die een bevoegdheid op het recht op privacy van de geïntercepteerde maakt, in redelijk

evenwicht staat met het maatschappelijk belang dat de inbreuk moet dienen. Met de vergaring van (bulk)data via een chatapp op grond van de OVC-bevoegdheid heeft de politie een heimelijke opsporingsmethode in handen die het criminele milieu kan ontwrichten en waarmee zicht kan worden verkregen op toekomstige of reeds gepleegde ernstige (levens)delicten. Dit belang weegt zwaarder dan de zeer beperkte inbreuk op het recht op privacy die de geïntercepteerde moet dulden in de fase van (bulk)datavergaring. Gezien het bovenstaande kom ik tot de conclusie dat vergaring van (bulk)data door de inzet van beveiligde chatapplicaties als heimelijk opsporingsmiddel in overeenstemming is met de vereisten van het recht op eerbiediging van de privacy zoals gewaarborgd in art. 8 EVRM.

6.2 Aanbevelingen

Op basis van dit onderzoek worden de volgende aanbevelingen gedaan.

De eerste aanbeveling richt zich op de interceptieduur van art. 126s Sv. Aan de vergaring van bulkdata kunnen verschillende bevoegdheden ten grondslag liggen met elk hun eigen geldigheidsduur van het bevel. Zo geeft de infiltratiebevoegdheid geen vastomlijnde geldigheidsduur en de tap- en OVC-bevoegdheid een maximale geldigheidsduur van vier weken. Ook in het gemoderniseerde Wetboek van Strafvordering blijft de geldigheidsduur van de OVC-bevoegdheid onveranderd.[289] Bij elke verlenging van het OVC-bevel moet de OvJ het dringend onderzoeksbelang van de OVC-bevoegdheid aantonen. Daarbij loopt hij het risico dat de R-C de vordering voor de machtiging afwijst en het lopende OVC-bevel stopt. De vraag is of een dergelijk risico wenselijk is. De aard van het opsporingsmiddel vereist een voorzienbare lange opstart- en interceptietijd waarbij de inbreuk op de privacy voor de geïntercepteerde zeer gering is in de fase van feitelijke (bulk)datavergaring.[290] Pas vanaf fase ii wordt een grotere inbreuk op het recht op privacy gemaakt.[291] Alles in ogenschouw genomen adviseer ik de wetgever om in een aanvullend besluit de interceptietermijn voor de feitelijke vergaring van bulkdata op grond van art. 126s Sv te verruimen naar ten hoogste drie maanden. De aanbevolen termijn komt overeen met de termijn die ten grondslag ligt aan de observatiebevoegdheid.[292] Om het recht op privacy van de geïntercepteerde in de opvolgende fase te beschermen, zou de wetgever in hetzelfde besluit kunnen opnemen dat elke volgende fase tenminste een aparte machtiging van de R-C behoeft.

De tweede aanbeveling richt zich op de notificatieverplichting van art. 126bb Sv. Het ligt in de verbeelding dat bij de vergaring van (bulk)data met een chatapp een groot deel van de gebruikers niet zal worden geïdentificeerd. De notificatieverplichting noopt het OM iedere geïntercepteerde, ook de personen die uiteindelijk niet worden vervolgd, schriftelijk te informeren over de toepassing van een

[289] Art. 2.8.16 Ambtelijke versie juli 2020 wetsvoorstel Wetboek van Strafvordering (Boek 2) (*Kamerstukken II* 2021/22, 29279), p. 108, rijksoverheid.nl 5 mei 2022.
[290] Voor dergelijke omstandigheden had de wetgever bij de infiltratiebevoegdheid wel oog. Binnen deze bevoegdheid mag de OvJ binnen het redelijke een termijn voor het bevel bepalen, omdat de aard van het middel dit verlangd Hierbij dient wel opgemerkt te worden dat een infiltratietraject onder toezicht van de Centrale Toetsingscommissie staat, en het college van procureurs-generaal met de termijn van het bevel moet instemmen. Zie hiervoor: Aanwijzing Opsporingsbevoegdheden, par. 2,9, wetten.overheid.nl, laatst geraadpleegd 5 mei 2022; Blom, in: *T&C Strafvordering*, art. 126p Sv, aant. 7b, navigator.nl, actueel tot en met 1 januari 2022.
[291] Schermer & Oerlemans, *TBS&H* 2022, nr. 2, p. 84.
[292] Art. 126o lid 5 juncto art. 126g lid 4 Sv.

opsporingsbevoegdheid.[293] Pas als een dergelijke mededeling niet mogelijk is, mag deze achterwege blijven. Zo'n omstandigheid kan liggen in het feit dat de gebruiker van de chatapp niet individualiseerbaar is of verdere persoonsgegevens niet te achterhalen.[294] Niet-individualiseerbare personen, bijvoorbeeld die in groepsverband optreden, hoeven niet als betrokkenen in de zin van art. 126bb Sv te worden aangemerkt.[295] Uit de wet blijkt niets van een inspanningsverplichting voor de OvJ tot het achterhalen van de identiteit van geïntercepteerden. Daarmee kan het recht op informatie en de mogelijkheid tot toetsing door de geïntercepteerde worden ontnomen. De wetgever laat de notificatieverplichting nagenoeg ongewijzigd in het gemoderniseerde Wetboek van Strafvordering.[296] Het enige substantiële verschil met het huidige wetsartikel 126bb Sv is de weglating van het woord 'schriftelijk'.[297] Deze weglating geeft naar mijn mening de mogelijkheid geïntercepteerden op andere manieren te informeren, die beter aansluiten bij de huidige gedigitaliseerde maatschappij. Bij het ontmantelen van Hansa Market en Ennetcom verspreidde de politie via het communicatiemiddel een (laatste) bericht dat het medium door de politie offline was gehaald.[298] In een dergelijk bericht kan ook enige vorm van notificatie worden verwerkt. Gezien bovenstaande adviseer ik de wetgever dan ook in haar wetgeving een inspanningsverplichting jegens de OvJ op te nemen waarin deze al het mogelijke in het werk stelt om de geïntercepteerde te identificeren en, al dan niet via digitale weg, te notificeren.

[293] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 85.
[294] Aanwijzing Opsporingsbevoegdheden, par. 5.4, wetten.overheid.nl, laatst geraadpleegd 5 mei 2022.
[295] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 85.
[296] Concept Memorie van toelichting nieuwe Wetboek van Strafvordering (ambtelijke versie juli 2020) (*Kamerstukken II* 2021/22, 29279), p. 488, rijksoverheid.nl 5 mei 2022.
[297] Art 2.8.2 Ambtelijke versie juli 2020 wetsvoorstel Wetboek van Strafvordering (Boek 2) (*Kamerstukken II* 2021/22, 29279), p. 108, rijksoverheid.nl 5 mei 2022.
[298] Voor Hansa Market zie 'Ondergrondse Hansa Market overgenomen en neergehaald', om.nl 20 juli 2017. Voor Ennetcom zie: 'Politie onderschept miljoenen berichten criminelen', rtlnieuws.nl 9 maart 2017. In het geval van Ennetcom bevatte het bericht tevens een uitnodiging aan wettelijk verschoningsgerechtigden opgenomen zich te melden.

Literatuurlijst

***Affidavit* 2021**

Affidavit in support of application for search warrant, https://www.justice.gov/usao-sdca/press-release/file/1402426/download.

Blom, in: *T&C Strafvordering*

T. Blom, commentaar op art. 126p Sv, in: C.P.M. Cleiren, M.J.M. Verpalen & J.H. Crijns (red.) *Tekst & Commentaar Strafvordering*, navigator.nl, actueel tot en met 1 januari 2022.

Boere, *ad.nl* 8 juni 2021

R. Boere, '49 arrestaties in Nederland bij unieke internationale politieactie tegen drugsmaffia', *ad.nl* 8 juni 2021.

Boeser, *TBS&H* 2021, nr. 5

J.S. Boeser, 'Cybersecurity en 'datagedreven' opsporing: stand van zaken met betrekking tot de interceptie van versleutelde cryptocommunicatie', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2021, nr 5, p. 351-356.

Borgers, *DD* 2015/15

M.J. Borgers, 'Normering van 'lichte' opsporingshandelingen', *Delikt en Delinkwent* 2015/15, nr. 3 p. 143-155.

***Computerrecht* 2022/41**

'(Iets) meer duidelijkheid over Sky ECC-operatie', *Computerrecht* 2022/41, afl. 1, p. 78-79.

Corstens/Borgers & Kooijmans 2021

M.J. Borgers & T. Kooijmans, *G.M.J. Corstens. Het Nederlands strafprocesrecht,* Deventer: Wolters Kluwer 2021.

Cox, *vice.com* 8 juni 2021a

J. Cox, 'Trojan Shield: How the FBI secretly ran a phone network for criminals', *vice.com* 8 juni 2021.

Cox, *vice.com* 8 juni 2021b

J. Cox, 'DOJ Charges Criminal 'Influencers' Who Worked for FBI's Honeypot Phone Company', *vice.com* 8 juni 2021.

Cox, *vice* 8 juli 2021

J. Cox, 'We Got the Phone the FBI Secretly Sold to Criminals', *vice.com* 8 juli 2021.

Cox, *vice.com* 4 januari 2022

J. Cox, 'FBI's Backdoored Anom Phones Secretly Harvested GPS Data Around the World', *vice.com* 4 januari 2022.

Curry, *buisinessofapps.com* 11 januari 2022

D. Curry, ´Signal Revenue & Usage Statistics (2022)´, *buisinessofapps.com* 11 januari 2022.

Deiters, *Politievakblad Blauw*, nr. 03

E. Deiters, 'De Encrochatzaak: Live meelezen met crimineel Nederland', *Politievakblad Blauw* 2020, nr. 03, p. 12-16.

Dirksen, Van der Leest & Vermeulen, *Tijdschrift voor Criminologie* 2021 (63) 2

V. Dirksen, W. van der Leest & I. Vermeulen, 'Netwerken van netwerken in transit. De doorvoer van cocaïne via Nederland', *Tijdschrift voor Criminologie* (63) 2, p. 129-145.

Eindrapport Commissie-Van Traa 1996

Inzicht in opsporing. Eindrapport parlementaire enquêtecommissie opsporingsmethoden, bijlage bij *Kamerstukken II* 1995/96, 24072, nr. 10-11.

Eskens, *Computerrecht* 2015/85, nr. 3

S.J. Eskens, 'Ongerichte interceptie, of het verwerven van bulkcommunicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden', *Computerrecht* 2015/85, nr. 3, p. 125-131.

Eskens, Van Daalen & Van Eijk 2016

S.J. Eskens, O.L. van Daalen & N.A.N.M. van Eijk, *Geheime surveillance en opsporing. Richtsnoeren voor de inrichting van wetgeving*, Amsterdam: IViR 2016.

Europol & Eurojust 2019

Europol & Eurojust, '*First report of the observatory function of encryption'*, Den Haag: 2019.

Frediani, *valigiablu.it* 12 juli 2020

C. Frediani, 'Dalle indagini hi-tech al mercato dei criptofonini: retroscena della maxiretata Encrochat contro la criminalità', *valigiablu.it* 12 juli 2020.

Galiç, *TBS&H* 2022, nr. 2

M. Galic, 'Bulkbevoegdheden en strafrechtelijk onderzoek. Lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2022, nr. 2, p. 130-137.

Gerards 2011

J. Gerards, *EVRM. Algemene beginselen, studenteneditie*, Den Haag: Sdu Uitgevers 2011.

Hagens & Oerlemans, *erhcr-updates* 22 maart.

M. Hagens & J.J. Oerlemans, annotatie bij EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *erhcr-updates.nl* 22 maart.

Hielkema & Krabbe 2004

J. Hielkema & H.G.M. Krabbe, 'Algemene opmerkingen', in: A.E. Harteveld e.a. (red.) *Het EVRM en het Nederlandse strafprocesrecht*, Deventer: Kluwer Deventer 2004, p. 11-32.

Katz & Lindell 2021

J. Katz & Y. Lindell, '*Introduction to modern cryptography. Third edition´*, Boca Raton: CRC Press 2021.

Keulen & Knigge 2020

B.F. Keulen & G. Knigge, *Strafprocesrecht*, Deventer: Wolters Kluwer, 2020.

Koops & Oerlemans 2019

B.J. Koops & J.J. Oerlemans, 'Formeel strafrecht en ICT', in: B.J. Koops & J.J. Oerlemans (red.) *Strafrecht en ICT, Monografieën recht en informatietechnologie*, Den Haag: Sdu 2019, p. 117-208.

Krabbe 2004

H.G.M. Krabbe, 'Artikel 8. De eerbiediging van het privéleven', in: A.E. Harteveld e.a. (red.) *Het EVRM en het Nederlandse strafprocesrecht*, Deventer: Kluwer 2004, p. 137-183.

Krommendijk, Terpstra & Van Kempen 2009

M. Krommendijk, J. Terpstra & P.H. van Kempen, *De Wet BOB: Titels IVa en V in de praktijk. Besluitvorming over bijzondere opsporingsbevoegdheden in de aanpak van georganiseerde criminaliteit*, Den Haag: Boom Juridische Uitgevers 2009.

Nieuwenhuis, *NTM/NJCM-bull.* 2014/2

A.J. Nieuwenhuis, 'Pressing social need; Op zoek naar het dringende karakter van de maatschappelijke behoefte', *NTM/NJCM-bull.* 2014/2, p. 7-23.

Nieuwenhuis 2017

A.J. Nieuwenhuis, 'Beperkingen in grondrechten', in: A.J. Nieuwenhuis, M. den Heijer & A.W. Hins (red.), *Hoofdstukken grondrechten*, Nijmegen: Ars Aequi Libri, 2017, p. 103-142.

Oerlemans, *JV* 2012, nr. 3

J.J. Oerlemans, 'Mogelijkheden en beperkingen van de internettap', *Justitiële Verkenningen* 2012, nr. 3, p. 20-39.

Oerlemans 2017

J.J. Oerlemans, *Investigating Cybercrime* (diss. Tilburg), Amsterdam: Amsterdam University Press 2017.

Oerlemans, *Computerrecht* 2017/103

J.J. Oerlemans, annotatie bij Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, afl. 3, p. 169-180.

Oerlemans, *Computerrecht* 2019/178

J.J. Oerlemans, annotatie bij Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, afl. 5, p. 338-346.

Oerlemans 2020

J.J. Oerlemans, *Grenzen stellen aan datahonger. De bescherming van de nationale veiligheid in een democratische rechtsstaat* (oratie Utrecht), Utrecht 2020.

Van de Pol, *crimesite.nl* 10 februari 2021

W. van de Pol, 'EncroChat: de reconstructie van de hack (UPDATE), *crimesite.nl* 10 februari 2021.

***Rapport Commissie Jones-Bos* 2020**

Rapport van de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017, bijlage bij *Kamerstukken II* 2020/21, 34588, nr. 88.

Schermer, *webwereld.nl* 14 maart 2012

B. Schermer, 'Digitale IRT-affaire of nieuwe opsporing?', *webwereld.nl* 14 maart 2012.

Schermer & Oerlemans, *Computerrecht* 2020/3

B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3, afl. 1, p. 14-21.

Schermer & Oerlemans, *TBS&H* 2022, nr. 2

B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2022, nr. 2, p. 82-89.

Van der Sloot, *NJB* 2014, afl. 17

B. van der Sloot, 'Privacy in het post NSA-tijdperk. Tijd voor een fundamentele voorziening?', *Nederlandse Juristenblad* 2014, afl. 17, p. 1172-1179.

Stol & Strikwerda 2017

W. Stol & L. Strikwerda, *Strafrechtspleging in een digitale samenleving*, Den Haag: Boom Juridisch 2017.

Stol & Strikwerda, *Tijdschrift voor Veiligheid* 2018, (17)

W. Stol & L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek.', *Tijdschrift voor Veiligheid* 2018 (17), nr. 1-2, p. 8-22.

Taylor Parkins-Ozephius e.a., *TBS&H* 2021, nr. 5

C.M. Taylor Parkins-Ozephius e.a., 'De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2021, nr. 5, p. 322-333.

Thompson, *policeprofessional.com* 13 november 2018

T. Thompson, 'Dutch police admit accessing criminal chats by intercepting encryption server´, *policeprofessional.com* 13 november 2018.

(Overige) internetbronnen

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

'A gentle introduction to asymmetric encryption and SSL certificates', dzone.com 18 februari 2022.

'Android Open Source Project', source.android.com 11 februari 2022.

´FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown´, justice.gov 8 juni 2021.

'Info over end-to-end versleuteling', faq.whatsapp.com 18 februari 2022.

'International Criminal Communication Service Dismantled', fbi.gov 16 maart 2018.

'Nederland is een knooppunt voor cocaïnehandel en daar lijkt weinig aan te doen', *nos.nl* 15 december 2019.

'Ondergrondse Hansa Market overgenomen en neergehaald', om.nl 20 juli 2017.

'Politie onderschept miljoenen berichten criminelen', rtlnieuws.nl 27 april 2018.

'Privacybeleid van WhatsApp', whatsapp.com (bijgewerkt 4 januari 2021).

'Report of the Manhattan District Attorney's Office on smartphone encryption and public safety 2015', https://cyber.harvard.edu/pubrelease/don't-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf.

'Right to respect for private and family life', https://www.coe.int/en/web/echr-toolkit/le-droit-au-respect-de-la-vie-privee-et-familiale 8 maart 2022.

‘Telegram bereikt 500 miljoen gebruikers na commotie rond WhatsApp’, nu.nl 13 januari 2021.
‘Telegram Privacy Policy’, telegram.org, par. 3.3.1 (bijgewerkt 14 augustus 2018).
‘Twee miljard gebruikers - De wereld privé met elkaar verbinden’, blog.whatsapp.com 6 januari 2022.
ubuntu-touch.io 11 februari 2022.

Jurisprudentielijst

Europees Hof voor de Rechten van de Mens

EHRM 25 april 1978, appl. nr. 5856/72 (*Tyrer/ Verenigd Koninkrijk*).

EHRM 6 september 1978, appl. nr. 5029/71 (*Klass e.a./ Duitsland*).

EHRM 26 april 1979, ECLI:NL:XX:1979:AC6568, *NJ* 1980, 146, m.nt. E.A. Alkema (*Sunday Times/ Verenigd Koninkrijk*).

EHRM 22 oktober 1981, appl. nr. 7525/76 (*Dudgeon/ Verenigd Koninkrijk*).

EHRM 25 maart 1983, appl. nr. 5947/72 (*Silver/ Verenigd Koninkrijk*).

EHRM 02 augustus 1984, ECLI:NL:XX:1984:AB8061, *NJ* 1988, 534, m.nt. J.V. van Dijk (*Malone/ Verenigd Koninkrijk*).

EHRM 26 maart 1985, appl. nr. 8978/80 (*X en Y/ Nederland*).

EHRM 26 maart 1987, appl. nr. 9248/81 (*Leander/ Zweden*).

EHRM 28 maart 1990, appl. nr. 10890/84 (*Groppera Radio AG e.a./ Zwitserland*).

EHRM 24 april 1990, appl. nr. 11105/84 (*Huvig/ Frankrijk*).

EHRM 24 april 1990, appl. nr. 11801/85 (*Kruslin/ Frankrijk*).

EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800, *NJ* 1993, 400, m.nt. E.J. Dommering (*Niemietz/ Duitsland*).

EHRM 27 oktober 1994, appl. nr. 18535/91 (*Kroon/ Nederland*).

EHRM 25 juni 1997, appl. nr. 20605/92 (*Halford/ Verenigd Koninkrijk*).

EHRM 16 februari 2000, appl. nr. 27798/95 (*Amann/ Zwitserland*).

EHRM 25 september 2001, appl. nr. 44787/98 (*P.G. en J.H./ Verenigd Koninkrijk*).

EHRM 7 februari 2002, appl. nr. 53176/99 (*Mikulic/ Kroatië*).

EHRM 16 april 2002, ECLI:NL:XX:2002:AE4682, *NJ* 2003, 452, m.nt. E.J. Dommering (*Sté Colas Est/ Frankrijk*).

EHRM 29 april 2002, appl. nr. 2346/02 (*Pretty/ Verenigd Koninkrijk*).

EHRM 28 januari 2003, app. nr. 44647/98 (*Peck/ Verenigd Koninkrijk*).

EHRM 9 oktober 2003, appl. nr. 48321 (*Slivenko/ Letland*).

EHRM 24 juni 2004, appl. nr. 59320/00 (*Von Hannover/ Duitsland*).

EHRM 29 juni 2006, appl. nr. 54943/00 (*Weber en Saravia/ Duitsland*).

EHRM 3 april 2007, appl. nr. 62617/00 (*Copland/ Verenigd Koninkrijk*).

EHRM 10 april 2007, ECLI:NL:XX:2007:BA6787 (*Evans/ Verenigd Koninkrijk*).

EHRM 1 juli 2007, appl. nr. 58243/00 (*Liberty e.a./ Verenigd Koninkrijk*).

EHRM 4 december 2008, ECLI:NL:XX:2008:BH1813 (*S. en Marper/ Verenigd Koninkrijk*).

EHRM 20 januari 2011, appl. nr. 31322/07 (*Haas/ Zwitserland*).

EHRM 8 juli 2014, appl. nr. 3910/13 (*M.P.E.V. e.a./ Zwitserland*).

EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306, *Computerrecht* 2016/86, m.nt. S.J. Eskens (*Roman Zakharov/ Rusland*).

EHRM 16 juni 2016, appl. nr. 49176/11 (*Versini-Campinchi en Crasnianski/ Frankrijk*).

EHRM 5 september 2017, appl. nr. 61496/08 (*Barbulescu/ Roemenië*).

EHRM 8 februari 2018, appl. nr. 31446/12 (*Ben Faiza/ Frankrijk*).
EHRM 22 februari 2018, appl. nr. 588/13 (*Libert/ Frankrijk*).
EHRM 24 april 2018, appl. nr. 62357/14 (*Benedik/ Slovenië*).
EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
EHRM 25 mei 2021, appl. nr. 35252/08 (*Centrum för Rättviva/ Zweden*).

Hoge Raad
HR 04 december 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980, 356, m.nt. Th.W. van Veen.
HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249, m.nt. T.M. Schalken.
HR 12 juli 2011, ECLI:NL:HR:2011:BP4650.
HR 20 december 2011, ECLI:NL:HR:2011:BP0199.
HR 1 juli 2014, ECLI:NL:HR:2014:1562.
HR 1 juli 2014, ECLI:NL:HR:2014:1563.
HR 5 maart 2019, ECLI:NL:HR:2019:298.

Gerechtshof
Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4620.

Rechtbank
Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627.
Rb. Rotterdam 03 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, m.nt. J.J. Oerlemans.
Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113.
Rb. Rotterdam 15 juli 2021, ECLI:NL:RBROT:2021:6853.
Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9086.
Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1243.