Hacken als opsporingsbevoegdheid in het licht van artikel 8 lid 2 EVRM: de zoektocht naar een *'fair balance'* tussen opsporing en privacy

Masterscriptie Straf(proces)recht
Faculteit der Rechtsgeleerdheid, Radboud Universiteit Nijmegen

Naam:	**Y.J.G.H.L. (Yannick) Straus**
Studentnummer:	**0842974**
Begeleider:	**mr. M.G.J.M. van der Staak**
Tweede lezer:	**prof. mr. P.H.P.H.M.C. van Kempen**
Verdedigd op:	**9 december 2013**

Inhoudsopgave

Lijst van gebruikte afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMvB	Algemene Maatregel van Bestuur
aant.	aantekening
BKA	*Bundeskriminalamt*
BVerfG	*Bundesverfassungsgericht*
CCV	Cybercrimeverdrag
CTC	Centrale Toetsingscommissie
EHRC	European Human Rights Cases
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden
Gw	Grondwet voor het Koninkrijk der Nederlanden
ICT	Informatie- en communicatietechnologie
IM	*Instant messaging*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
KLPD	Korps Landelijke Politiediensten
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
m.nt.	met noot
MvT	Memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III
NIST	*National Institute of Standards and Technology*
NJ	Nederlandse Jurisprudentie
NJB	Nederlands Juristenblad
NJCM	Nederlands Juristen Comité voor de Mensenrechten
NSA	*National Security Agency*
OM	Openbaar Ministerie
RIPA	*Regulation of Investigatory Powers Act 2000*
SOCTA	*Serious and Organised Crime Threat Assessment*
Sr	Wetboek van Strafrecht
Stb.	Staatsblad
Sv	Wetboek van Strafvordering
TILT	*Tilburg Institute for Law, Technology, and Society*
Tor	The Onion Router
Trb.	Tractatenblad
VoIP	*Voice-over Internet Protocol* (internettelefonie)
VPN	*Virtual Private Network*
Wbp	Wet bescherming persoonsgegevens
Wet BOB	Wet bijzondere opsporingsbevoegdheden
Wet RO	Wet op de rechterlijke organisatie
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002

WLAN	*Wireless local area network*
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Hoofdstuk 1: Inleiding

§ 1. Achtergrond

De opkomst van de personal computer in de jaren ’80, het internet vanaf de jaren ’90 en de smartphones en tablets in het nieuwe millennium hebben voor de samenleving een nieuwe wereld aan mogelijkheden geopend, waarvan de voordelen voor iedereen binnen die samenleving duidelijk zijn. Helaas komen de ontwikkelingen echter niet enkel ten goede aan degenen die via sociale media de contacten met hun familie en vrienden onderhouden, graag online winkelen of zich tegoed doen aan de vele informatieve en entertainment websites die het internet rijk is. De ‘donkere’ kant van de samenleving wil eveneens zijn voordeel doen met de nieuwe mogelijkheden. Cybercriminaliteit en kinderporno zijn dankzij de technologische ontwikkelingen in opkomst, maar ook ‘klassieke’ criminaliteit maakt steeds meer gebruik van de mogelijkheden van de hedendaagse technologie om activiteiten te ondersteunen.

Tegenover de technologische ontwikkelingen in de criminaliteit staat de vraag welke methoden de Nederlandse opsporingsdiensten hiertegen in kunnen zetten. Al lange tijd bestaan er bevoegdheden tot het doorzoeken van een plaats (mede) om computergegevens vast te leggen (tegenwoordig vastgelegd in artikel 125i Sv),[1] om vanaf een computer op de doorzochte plaats onderzoek te doen in een elders aanwezig geautomatiseerd werk (‘netwerkzoeking’, artikel 125j Sv),[2] en om telecommunicatie zoals e-mailverkeer af te tappen (artikel 126m Sv).[3] Er gaan echter ook al jaren stemmen op om geheel nieuwe opsporingsbevoegdheden te creëren naar aanleiding van de technologische ontwikkelingen en de gevaren die cybercriminaliteit en kinderporno voor de samenleving vormen.[4] De mogelijkheid van een opsporingsbevoegdheid tot het ‘op elektronische wijze binnendringen’ van geautomatiseerde werken is al sinds het begin van deze eeuw onderwerp van discussie.[5] Dit heeft uiteindelijk op 2 mei 2013 geleid tot een conceptwetsvoorstel ‘Computercriminaliteit III’, waarin wordt voorgesteld om met artikel 125ja een ‘hackbevoegdheid’ aan het Wetboek van Strafvordering toe te voegen.[6] Naar verwachting zal het wetsvoorstel in 2014 in de Tweede Kamer worden behandeld.[7]

In de discussie omtrent de toelaatbaarheid van een hackbevoegdheid speelt de inbreuk van een dergelijke opsporingsbevoegdheid op de privacy van burgers een grote rol. Burgers vertrouwen immers een grote hoeveelheid vertrouwelijke en persoonlijke informatie en

[1] Wet van 16 juli 2005, *Stb.* 2005, 390 (Wet bevoegdheden vorderen gegevens), in werking getreden op 1 januari 2006. Vgl. over de plaats van computergegevens in de strafvordering reeds *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 11.
[2] Wet van 23 december 1992, *Stb*. 1993, 33 (Wet Computercriminaliteit), in werking getreden op 1 maart 1993.
[3] Wet van 27 mei 1999, *Stb*. 1999, 245 (Wet Bijzondere opsporingsbevoegdheden), in werking getreden op 1 februari 2000.
[4] Zie o.a. *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 2 – 3, *Aanhangsel Handelingen II* 2010/11, nr. 201015331, *Aanhangsel Handelingen II* 2011/12, nr. 2012Z02969 en *Kamerstukken II* 2012/13, 28 684, nr. 363, p. 8.
[5] Zie reeds Boek 2000, p. 589 – 593, Oerlemans 2011, p. 888 – 908, Koning 2012, p. 46 – 52 en voorts de parlementaire stukken *supra* noot 4.
[6] <http://www.internetconsultatie.nl/computercriminaliteit>.
[7] Zie ‘Aanpak van meer grote, internationale cybercrime-zaken’, *Veiligheid en Justitie Bulletin* 17 september 2013.

communicatie toe aan hun computers, smartphones en tablets.[8] De vraag is dan ook of de inbreuk van een hackbevoegdheid op de privacy van burgers toelaatbaar is, met het oog enerzijds op de ernst van de inbreuk en anderzijds op de belangen die op het spel staan, of dat deze inbreuk (anders dan bijvoorbeeld de reeds bestaande bevoegdheden tot aftappen van telecommunicatie of tot stelselmatige observatie) net iets te ver gaat. Het antwoord op deze vraag dient te worden gezocht in artikel 8 EVRM, de grondslag op Europees niveau voor het recht op bescherming van de persoonlijke levenssfeer. Dit artikel hanteert in lid 1 als uitgangspunt dat inbreuken op de persoonlijke levenssfeer van burgers niet toegestaan zijn. In artikel 8 lid 2 EVRM worden echter de drie cumulatieve voorwaarden geformuleerd waaronder een inbreuk toch toelaatbaar kan zijn: de inbreuk moet zijn voorzien bij wet, met de inbreuk moet een legitiem doel worden nagestreefd, en de inbreuk moet noodzakelijk zijn in een democratische samenleving. Deze minimalistisch geformuleerde voorwaarden zijn door het EHRM nader uitgewerkt in zijn jurisprudentie. Mede vanwege de rechtstreekse doorwerking van artikel 8 EVRM in de Nederlandse rechtsorde komt bij de totstandkoming van opsporingsbevoegdheden aan dit artikel een doorslaggevend belang toe bij de vraag of de beperking op het recht op bescherming van de persoonlijke levenssfeer gerechtvaardigd is.[9] De focus ligt hierbij met name op het derde vereiste, inhoudende dat de bevoegdheid 'noodzakelijk' moet zijn in een democratische samenleving: houdt de nieuwe opsporingsbevoegdheid voldoende rekening met de privacy van de Nederlandse burgers?[10]

§ 2. Probleemstelling en deelvragen

Met dit onderzoek wil ik nagaan of, en zo ja onder welke voorwaarden, een hackbevoegdheid in Nederland 'noodzakelijk' is in de zin van artikel 8 lid 2 EVRM. Hiermee wil ik duidelijkheid geven omtrent de juridische toelaatbaarheid van een hackbevoegdheid. Een grondige juridische analyse is des te meer van belang gezien de controverse die het idee van 'hacken door de politie' oproept.[11]

De basis voor dit onderzoek wordt gevormd door de volgende probleemstelling:
Wat zijn de mogelijkheden voor de invoering van een wettelijke bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk in Nederland, met inachtneming van het vereiste 'noodzakelijk in een democratische samenleving' als vastgelegd in artikel 8 lid 2 EVRM?

De deelvragen die uit deze probleemstelling voortkomen zijn als volgt:
1) Op welke wijze valt de inbreuk van een wettelijke bevoegdheid tot het binnendringen in een geautomatiseerd werk binnen de reikwijdte van artikel 8 lid 2 EVRM?
2) Heeft de opsporing een 'dringend belang' bij de invoering van een wettelijke bevoegdheid tot het binnendringen in een geautomatiseerd werk?

[8] Zie hierover bijvoorbeeld Oerlemans 2011, p. 898 en Koning 2012, p. 48.
[9] Zie bijvoorbeeld *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 9 – 12 en *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 4 – 6. Zie tevens Buruma 2001, p. 13. Ook de memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III (hierna: MvT) hanteert artikel 8 lid 2 EVRM als toetsingsmaatstaf voor de vraag of het recht op privacy voldoende wordt gerespecteerd, zie MvT, p. 38.
[10] Zie de bronnen *supra* noot 9 en tevens o.a. Oerlemans 2011, p. 903 – 908 en Koops e.a. 2012, p. 47.
[11] Zie o.a. Jacobs 2012, p. 2761 – 2764; <https://www.bof.nl/2013/05/02/opstelten-grijpt-overhaast-naar-hackbevoegdheid/>; Engelfriet 2013. Ook de onthullingen medio 2013 omtrent de praktijken van de NSA dragen bij aan de controverse.

3) Wat is het belang van de Nederlandse burgers bij bescherming van hun recht op privacy?
4) Hoe kan een redelijke verhouding worden gerealiseerd tussen het belang van de opsporing bij de invoering van een wettelijke bevoegdheid tot het binnendringen in een geautomatiseerd werk enerzijds en het belang van de burgers bij bescherming van hun recht op privacy anderzijds?

De vraag of een hackbevoegdheid in Nederland kan worden beschouwd als 'noodzakelijk in een democratische samenleving' ziet op de fundamentele toelaatbaarheid van een hackbevoegdheid in Nederland. Om die reden is dit mijns inziens de belangrijkste toets binnen artikel 8 lid 2 EVRM, in ieder geval als het gaat om de invoering van nieuwe strafvorderlijke bevoegdheden, hetgeen ook blijkt uit de rol die het noodzakelijkheidsvereiste in wetsgeschiedenis, literatuur en jurisprudentie toebedeeld krijgt.[12] Over de twee andere vereisten die artikel 8 lid 2 EVRM noemt voor rechtvaardiging van een inbreuk op de persoonlijke levenssfeer, overweeg ik kort het volgende omtrent hun afwezigheid in dit onderzoek en hun verhouding tot de noodzakelijkheidstoets.

De legitieme doelen die ter rechtvaardiging van een inbreuk op artikel 8 EVRM kunnen worden aangevoerd zijn limitatief opgesomd in lid 2. Het legitieme doel levert in de regel geen problemen op in de rechtspraak van het EHRM: wanneer een staat een of meer van de in artikel 8 lid 2 EVRM genoemde, zeer algemeen geformuleerde doelen aanvoert en het enigszins te billijken is dat de inbreuk met dit doel te maken heeft, is aan dit vereiste reeds voldaan.[13] Wat betreft een hackbevoegdheid voor opsporingsambtenaren is zeer wel te billijken dat deze de aangevoerde doelen van bescherming van de openbare veiligheid en de voorkoming en vervolging van strafbare feiten nastreeft, waardoor reeds is voldaan aan het vereiste van een legitiem doel.[14] De nadere invulling van dit doel komt in de rechtspraak aan bod in het kader van de noodzakelijkheidstoets, bij de vraag hoe de inbreuk zich tot dit legitieme doel verhoudt. In zoverre heeft het vereiste van een legitiem doel dan ook geen zelfstandige betekenis. Hoewel ik in dit onderzoek zal pleiten voor een strengere toetsing aan artikel 8 lid 2 EVRM door de nationale wetgever dan de toetsing die het EHRM doorgaans uitvoert, is het mijns inziens evenwel weinig zinvol om een strengere, zelfstandige toets van het legitieme doel uit te voeren. Voor deze toets zijn geen verdere maatstaven te vinden buiten de limitatieve, ruim geformuleerde en in de rechtspraak niet nader uitgewerkte opsomming van doelen in artikel 8 lid 2 EVRM; bovendien komt aan het legitieme doel ook naar mijn mening pas echt betekenis toe wanneer dit in de noodzakelijkheidstoets wordt afgezet tegen de inbreuk die dit doel moet dienen.

[12] Zie de bronnen *supra* noot 9 en 10 en voorts Gerards 2011, p. 140. Zie ook EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 46 – 59 en EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 101 – 125.
[13] Zie o.a. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 44 – 46; EHRM 26 maart 1987, nr. 9248/81 (*Leander/Sweden*), § 49; EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 100.
[14] Deze doelen worden concreet aangevoerd in de memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III. Zie MvT, p. 39.

Het legaliteitsvereiste vormt daarentegen wel een belangrijk zelfstandig criterium binnen de toets of een inbreuk op artikel 8 EVRM gerechtvaardigd is.[15] Het EHRM ziet in het legaliteitsvereiste het criterium van de toegankelijkheid van de regelgeving en het vereiste dat de betreffende regels voldoende duidelijk zijn geformuleerd zodat ze voldoende voorzienbaar zijn voor de burgers.[16] Benadrukt zij dat het Hof de term '*law'* niet beperkt tot wetgeving in formele zin.[17] In dit onderzoek zal ik het legaliteitsvereiste niet apart behandelen. Hoewel het een belangrijk vereiste is in het kader van de toelaatbaarheid van een hackbevoegdheid, heb ik in het kader van de omvang van het onderzoek keuzes moeten maken en is het mijns inziens op dit moment belangrijker (en wetenschappelijk interessanter) om de noodzakelijkheid van een hackbevoegdheid te onderzoeken en te bespreken. Immers, pas wanneer duidelijk is aan welke vereisten de bevoegdheid moet voldoen om te kwalificeren als 'noodzakelijk in een democratische samenleving' is het zinvol om te onderzoeken op welke wijze de bevoegdheid en de bijbehorende voorwaarden moeten worden vastgelegd.
Desondanks is er wel enige overlapping mogelijk tussen het noodzakelijkheidsvereiste en het legaliteitsvereiste van artikel 8 lid 2 EVRM. Wanneer hiervan binnen dit onderzoek sprake is, zal ik dit aanstippen en het verschil benadrukken tussen het noodzakelijkheidsaspect en het legaliteitsaspect van het betreffende vraagstuk.

§ 3. Terminologie en begrippen

'Hackbevoegdheid'

In dit onderzoek zal ik doorgaans spreken van een 'hackbevoegdheid', soms van een 'bevoegdheid tot het binnendringen in een geautomatiseerd werk'. Voor een meer officiële definitie verwijs ik naar het conceptwetsvoorstel Computercriminaliteit III: 'een bevoegdheid voor opsporingsambtenaren om, onder strikte voorwaarden, een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten.'[18]

Geautomatiseerd werk

Een 'geautomatiseerd werk' is volgens artikel 80sexies Sr 'een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.' Praktisch gezien dienen onder 'geautomatiseerd werk' te worden verstaan computers (desktop pc's, laptops, tablets), netwerken van computers en geautomatiseerde inrichtingen voor telecommunicatie, zoals telefoon en telefax.[19]

Binnendringen

Voor de term 'binnendringen' in de bevoegdheid tot het binnendringen in een geautomatiseerd werk kan aansluiting worden gezocht bij de feitelijke handelingen die artikel 138ab Sr aanmerkt als 'binnendringen' in een geautomatiseerd werk: binnendringen door het

[15] Zie o.a. EHRM 2 augustus 1984, nr. 8691/79 (*Malone/United Kingdom*), § 66 – 80; EHRM 1 juli 2008, nr. 58243/00 (*Liberty and Others/United Kingdom*), § 59 – 70.
[16] Zie o.a. EHRM 25 maart 1983, nr. 5947/72 (*Silver and Others/United Kingdom*), § 87 – 88.
[17] Zie o.a. EHRM 26 april 1979, nr. 6538/74 (*Sunday Times/United Kingdom*), § 47.
[18] MvT, p. 5. Zie ook Boek 2000, p. 589 en Koning 2012, p. 46.
[19] Zie *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 5 – 6, en voorts *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 5 en p. 31.

doorbreken van een beveiliging, een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.[20] De memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III noemt niet limitatief enkele specifieke technieken: ten eerste het via internet zenden van een elektronisch bericht aan de betrokkene, met als doel de betrokkene software te laten installeren die het geautomatiseerde werk opent voor de plaatsing van een 'bug' of 'keylogger', en ten tweede het binnendringen van een geautomatiseerd werk door middel van een gebruikersnaam en wachtwoord die middels het tappen van communicatie of door 'social engineering' zijn verkregen van de verdachte of iemand in zijn nabije omgeving.[21] Oerlemans noemt ook nog het benutten van een kwetsbaarheid in een ICT-systeem of het uitproberen van een groot aantal wachtwoordvariaties totdat toegang wordt verschaft tot het geautomatiseerde werk.[22]

Opsporing van strafbare feiten

Artikel 8 lid 2 EVRM vereist voor een gerechtvaardigde inbreuk op het recht op bescherming van de persoonlijke levenssfeer dat die inbreuk in redelijke verhouding staat tot het nagestreefde legitieme doel.[23] Dit onderzoek zal zich richten op hacken als *opsporings*bevoegdheid, oftewel het binnendringen in een geautomatiseerd werk ten behoeve van de opsporing van strafbare feiten. Dit is een legitiem doel naar de maatstaven van artikel 8 lid 2 EVRM.[24] Tevens vormt dit het voornaamste onderdeel van de met het conceptwetsvoorstel Computercriminaliteit III nagestreefde legitieme doelen, zijnde de bescherming van de openbare veiligheid en de voorkoming en vervolging van strafbare feiten.[25] In dit onderzoek worden, in aansluiting op de opsporingsdefinitie van artikel 132a Sv, derhalve alleen die bevoegdheden tot het binnendringen in een geautomatiseerd werk behandeld die zien op het vergaren van informatie aan de hand waarvan strafvorderlijke beslissingen kunnen worden genomen.[26] De toelaatbaarheid van een hackbevoegdheid voor de uitvoering van verdere strafvorderlijke handelingen is een apart vraagstuk.[27]

§ 4. Opbouw van het onderzoek

De opbouw van het onderzoek is afhankelijk van de maatstaven van artikel 8 lid 2 EVRM en de wijze waarop deze moeten worden toegepast. Om die reden zal ik in hoofdstuk 2 allereerst de vraag beantwoorden op welke wijze de inbreuk van een hackbevoegdheid onder de reikwijdte van artikel 8 EVRM valt. Vervolgens zal ik in paragrafen 3 en 4 aangeven hoe het onderzoek op basis van de maatstaven van artikel 8 lid 2 is opgebouwd.

---

[20] Zie ook MvT, p. 13.
[21] MvT, p. 25 – 26.
[22] Oerlemans 2011, p. 889.
[23] Zie bijvoorbeeld EHRM 25 maart 1983, nr. 5947/72 (*Silver and Others/United Kingdom*), § 97 onder c.
[24] Zie bijvoorbeeld EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 147, waarin de Britse opsporingsbevoegdheden vastgelegd in de RIPA door het EHRM worden beoordeeld als (onder andere) het legitieme doel van voorkoming van strafbare feiten nastrevend.
[25] MvT, p. 39.
[26] Zie ook Corstens 2011, p. 244 – 245.
[27] Hierbij kan worden gedacht aan de ontoegankelijkmaking van gegevens (het voorgestelde artikel 125ja lid 1 aanhef en onder c Sv), maar bijvoorbeeld ook aan 'terughacken' om handhavend op te treden tegen bepaalde vormen van cybercriminaliteit, zoals botnets.

Hoofdstuk 2: De toetsing aan artikel 8 lid 2 EVRM

§ 1. Inleiding

In dit hoofdstuk komt in paragraaf 2 de (deel)vraag aan bod hoe de inbreuk van een hackbevoegdheid binnen de reikwijdte van artikel 8 EVRM kan worden ingepast. Met de vaststelling hiervan kan vervolgens in paragrafen 3 en 4 de nadere opbouw van het onderzoek worden uiteengezet. Tevens biedt deze vaststelling een aanknopingspunt voor de beoordeling van het belang van de privacy van burgers in hoofdstuk 6 door vast te stellen welke specifieke belangen van burgers worden geraakt.

§ 2. Op welke wijze valt de inbreuk van een hackbevoegdheid onder artikel 8 EVRM?

Er lijkt geen discussie over mogelijk dat het binnendringen in een geautomatiseerd werk een ernstige inbreuk op de privacy van burgers maakt.[28] Het EHRM heeft evenwel nog geen uitspraken gedaan over de vraag of het op elektronische wijze binnendringen in een geautomatiseerd werk als een inbreuk op het recht op bescherming van de persoonlijke levenssfeer moet worden beschouwd die valt onder de reikwijdte van artikel 8 EVRM.[29] Evenmin is het geautomatiseerde werk op zichzelf in de jurisprudentie van het EHRM gekwalificeerd als een dimensie van het privéleven in de zin van artikel 8 EVRM.[30] Een zelfstandig oordeel omtrent de plaats van een hackbevoegdheid binnen artikel 8 EVRM is derhalve noodzakelijk alvorens de toelaatbaarheid van de bevoegdheid op basis van de maatstaven van deze bepaling te onderzoeken.

Als startpunt kan wel aansluiting worden gezocht bij de bestaande rechtspraak van het EHRM. Voor zover de toepassing van een hackbevoegdheid plaatsvindt met het oog op het onderscheppen van communicatie, geldt dat zowel telecommunicatie als vertrouwelijke communicatie (vgl. artikel 126m Sv respectievelijk 126l Sv) door het Hof onder het recht op privéleven in de zin van artikel 8 EVRM wordt geplaatst.[31] Voor zover de toepassing van een hackbevoegdheid plaatsvindt met het oog op het verzamelen en opslaan van op geautomatiseerde werken opgeslagen gegevens, kan aansluiting worden gezocht bij de bescherming van privégegevens in de rechtspraak van het EHRM: ook de verzameling en opslag van deze gegevens wordt door het EHRM in beginsel gezien als een inbreuk op artikel 8 EVRM.[32] Eenzelfde aansluiting bij bestaande rechtspraak kan worden gezocht voor zover het gaat om de toepassing van een hackbevoegdheid met het oog op stelselmatige observatie: ook gegevens omtrent de bewegingen en verblijfplaatsen van een persoon worden beschermd

[28] Zie ook reeds Boek 2000, p. 592.
[29] Aldus ook Koning 2012, p. 48.
[30] Aldus ook Groothuis & De Jong 2010, p. 280.
[31] Wat betreft telecommunicatie zie m.n. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 41; EHRM 2 augustus 1984, nr. 8691/79 (*Malone/United Kingdom*), § 64; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 77; EHRM 1 juli 2008, nr. 58243/00 (*Liberty and Others/United Kingdom*), § 56. Wat betreft overige (vertrouwelijke) communicatie zie m.n. EHRM 12 mei 2000, nr. 35394/97 (*Khan/United Kingdom*), § 23 – 25.
[32] Zie o.a. EHRM 26 maart 1987, nr. 9248/81 (*Leander/Sweden*), § 48 en EHRM 6 juni 2006, nr. 62332/00 (*Segerstedt-Wiberg and Others/Sweden*), § 71 – 73.

door artikel 8 EVRM, mits deze gegevens op stelselmatige wijze worden verzameld en vastgelegd (vgl. artikel 126g Sv).[33]

Het privéleven dat tegenwoordig middels geautomatiseerde werken plaatsvindt vertoont veel overeenkomsten met het privéleven dat traditioneel binnen de eigen woning plaatsvindt. Dit geldt met betrekking tot de grote hoeveelheden gegevens die door burgers op geautomatiseerde werken worden opgeslagen en de privacygevoeligheid van deze gegevens, maar ook met betrekking tot de mogelijkheden die geautomatiseerde werken aan anderen die daarop zijn binnengedrongen bieden om van de huiselijke activiteiten kennis te nemen.[34] Aan de privacygevoeligheid en de omvang van in de woning opgeslagen gegevens en de privacygevoeligheid van activiteiten die binnen de woning plaatsvinden ontleent de woning traditioneel ook zijn bijzondere, absolute bescherming als locatie waar de burger 'onbevangen zichzelf kan zijn'.[35] In dat licht bezien zou voor de bescherming van het algehele privéleven dat met gebruik van geautomatiseerde werken plaatsvindt mogelijk aansluiting kunnen worden gezocht bij het huisrecht, waarbij het geautomatiseerde werk onder de categorie 'woning' zou worden geplaatst met de daarbij horende absolute bescherming. Deze optie is door het Duitse hoogste gerechtshof, het *Bundesverfassungsgericht*, reeds uitdrukkelijk afgewezen en de literatuur heeft zich hierbij aangesloten.[36] Het EHRM zelf heeft echter over deze kwestie nog geen uitspraken gedaan. Het kwalificeert een woning in beginsel als '*the place, the physically defined area, where private and family life develops*'.[37] Het Hof hanteert een vrij ruime interpretatie van dit begrip 'woning', waaronder het bijvoorbeeld ook zakelijke locaties brengt, en het eist ook geen fysiek binnentreden om een inbreuk op het huisrecht aan te nemen.[38] Desondanks lijkt het mij ook voor het EHRM een te grote stap om geautomatiseerde werken rechtstreeks onder het begrip 'woning' te brengen. Dat tegenwoordig via geautomatiseerde werken '*private and family life*' zich ontwikkelt is heel goed te verdedigen, maar een geautomatiseerd werk kan mijns inziens niet als een '*physically defined area*' worden beschouwd. Een geautomatiseerd werk is weliswaar een fysiek apparaat, maar het privéleven middels dit apparaat vindt plaats in een digitale omgeving, en staat in zoverre los van de fysieke wereld waarop de bescherming van een woning of bedrijfspand is gericht.[39] Het lijkt mij dan ook waarschijnlijker dat, als het EHRM een absolute bescherming wil bieden aan geautomatiseerde werken, het hiervoor een specifiek recht zal ontwikkelen. Ik kom hier verderop in deze paragraaf nog op terug.

[33] Zie o.a. EHRM 28 januari 2003, nr. 44647/98 (*Peck/United Kingdom*), § 59 en EHRM 2 september 2010, nr. 35623/05 (*Uzun/Germany*), § 43 – 53.
[34] Zie ook Dommering 2000, p. 181; Groothuis & De Jong 2010, p. 279.
[35] Zie ook Koops, Van Schooten & Prinsen 2004, p. 13.
[36] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 191 – 195; Groothuis & De Jong 2010, p. 282; Koning 2012, p. 52.
[37] EHRM 2 november 2006, nr. 59909/00 (*Giacomelli/Italy*), § 76.
[38] Zie EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Germany*), § 29 – 33 respectievelijk EHRM 2 november 2006, nr. 59909/00 (*Giacomelli/Italy*), § 76.
[39] Zie ook Koning 2012, p. 52. Vgl. voorts (weliswaar niet in een EHRM-verdragsstaat maar met een vergelijkbare beschouwing van het op een fysieke plaats gerichte huisrecht) Supreme Court of Canada 7 november 2013, *R. v. Vu*, 2013 SCC 60, § 44.

Gezien hetgeen ik heb besproken in de voorgaande alinea's kan voor de bescherming onder artikel 8 EVRM van op geautomatiseerde werken opgeslagen gegevens en via geautomatiseerde werken verstuurde communicatie, aansluiting worden gezocht bij de bestaande rechtspraak van het EHRM inzake de algemene bescherming van gegevens en (tele-) communicatie, met uitzondering van een rechtstreekse aansluiting bij het huisrecht. De roep om een specifieke en concrete bescherming van gegevens die op geautomatiseerde werken worden opgeslagen en via geautomatiseerde werken worden verstuurd is echter sterk aanwezig en heeft geleid tot de formulering van een recht op integriteit van computersystemen en de vertrouwelijkheid van de daarop opgeslagen gegevens en de daarmee verstuurde communicatie.[40] Het recht op integriteit en vertrouwelijkheid van ICT-systemen is aanvankelijk ontwikkeld in het 'Online-Durchsuchung'-arrest van het *Bundesverfassungsgericht*.[41] Het BVerfG oordeelde dat uit de betekenis van het gebruik van informatietechnische systemen voor de persoonlijke ontwikkeling van burgers, en uit de gevaren voor de persoonlijkheid die in verband staan met dit gebruik, een noodzaak tot grondrechtelijke bescherming volgt.[42] Volgens het BVerfG is de burger er op aangewezen 'dat de staat, met het oog op de ongehinderde persoonlijkheidsontplooiing, de gerechtvaardigde verwachtingen wat betreft de integriteit en vertrouwelijkheid van [informatietechnische] systemen respecteert.'[43] De literatuur heeft zich bij deze formulering en deze achterliggende gedachte van het recht op integriteit en vertrouwelijkheid van ICT-systemen aangesloten.[44]

In (onder andere) het arrest *Peck/United Kingdom* heeft het EHRM aangegeven dat de identiteit en persoonlijke ontwikkeling onder de bescherming van artikel 8 EVRM vallen. Op basis hiervan kan het recht op integriteit en vertrouwelijkheid van ICT-systemen, dat blijkens de overwegingen van het BVerfG immers strekt tot bescherming van dezelfde belangen, mijns inziens eveneens onder artikel 8 EVRM worden gebracht.[45] In dit onderzoek zal ik dan ook uitgaan van het recht op integriteit en vertrouwelijkheid van ICT-systemen als het grondrecht waarop met een hackbevoegdheid inbreuk wordt gemaakt, en op basis daarvan invulling geven aan de maatstaven van artikel 8 EVRM.

Hoe het EHRM geautomatiseerde werken en de daarop opgeslagen gegevens en de daarmee verstuurde communicatie daadwerkelijk onder artikel 8 EVRM plaatst, is momenteel zeer moeilijk in te schatten. Het recht op integriteit en vertrouwelijkheid van ICT-systemen zoals dat in literatuur en rechtspraak vooralsnog is geformuleerd, is echter een zeer redelijk uitgangspunt dat naar mijn verwachting in ieder geval qua strekking overeen zal komen met de bescherming die het EHRM voor de op geautomatiseerde werken opgeslagen gegevens en daarmee verstuurde communicatie zal formuleren, met name omdat het recht de door artikel 8

[40] Zie Groothuis & De Jong 2010, p. 282; Oerlemans 2011, p. 888 – 908; MvT p. 38 – 39.
[41] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07.
[42] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 181.
[43] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 181.
[44] Zie o.a. Steenbruggen 2008, p. 232 – 235; De Hert, De Vries & Gutwirth 2009, p. 200 – 211; Groothuis & De Jong 2010, p. 282; Oerlemans 2011, p. 888 – 908; MvT p. 38 – 39.
[45] EHRM 28 januari 2003, nr. 44647/98 (*Peck/United Kingdom*), § 57.

EVRM beschermde belangen beoogt te beschermen. In beginsel zal elke formulering door het EHRM naar mijn verwachting ook dezelfde strekking hebben, namelijk de bescherming van gegevens die op geautomatiseerde werken zijn opgeslagen en daarmee worden verstuurd.

Op dat uitgangspunt bestaat één uitzondering, namelijk de situatie waarin het EHRM een nieuw recht ontwikkelt dat strekt tot absolute bescherming van geautomatiseerde werken, een mogelijkheid die ik reeds heb aangevoerd. Deze mogelijkheid is noch in literatuur noch in enige rechtspraak concreet aan bod gekomen.[46] Evenwel biedt de formulering van het recht op integriteit en vertrouwelijkheid van ICT-systemen mijns inziens wel de ruimte voor deze opvatting, en kan specifiek het recht op integriteit van ICT-systemen naar analogie van het huisrecht worden geïnterpreteerd.[47] Een dergelijke interpretatie zou ook gerechtvaardigd zijn gezien de vergelijkbare mate van privacygevoeligheid van de gegevens die worden of werden opgeslagen in een woning en de gegevens die worden opgeslagen op harde schijven, zoals reeds besproken. Tegelijkertijd wordt hiermee het huisrecht zelf niet opgerekt buiten de reikwijdte die het mijns inziens binnen artikel 8 EVRM heeft. Waar dit in dit onderzoek relevant is, zal ik de analoge interpretatie van het recht op integriteit van ICT-systemen aan het huisrecht dan ook betrekken in mijn overwegingen omtrent de toelaatbaarheid van een hackbevoegdheid in het licht van het noodzakelijkheidsvereiste van artikel 8 lid 2 EVRM.

Een hackbevoegdheid maakt inbreuk op het recht op integriteit en vertrouwelijkheid van ICT-systemen en valt op die manier binnen de reikwijdte van artikel 8 EVRM. Dit uitgangspunt leidt tot de verdere opzet van het onderzoek als uiteengezet in paragraaf 3.

§ 3. De toetsing aan artikel 8 lid 2 EVRM

De voorwaarden die voor het vereiste 'noodzakelijk in een democratische samenleving' in de zin van artikel 8 lid 2 EVRM moeten worden vervuld zijn door het EHRM uiteengezet in de vorm van een standaardtoets in het arrest *Silver and Others/United Kingdom*.[48] De belangrijkste voorwaarde die het Hof formuleert is dat de inbreuk op het betreffende grondrecht moet aansluiten op een '*pressing social need*' en in verhouding moet staan tot het legitieme doel dat wordt nagestreefd.[49] Dit criterium omvat de maatstaven van proportionaliteit en subsidiariteit en is een specifieke uitwerking van het criterium van de '*fair balance'* die als een rode draad door het EVRM loopt.[50] In essentie bestaat de noodzakelijkheidstoets dan ook uit een zoektocht naar een '*fair balance*', een redelijke verhouding, tussen de in het geding zijnde belangen.[51]

[46] Deze optie wordt wel voorzichtig geopperd door De Hert, De Vries & Gutwirth 2009, p. 207. Zie ook Koning 2012, p. 52, waarin de rechtstreekse toepassing van het huisrecht op geautomatiseerde werken wordt afgewezen maar een analoge interpretatie wel mogelijk lijkt te worden geacht.
[47] Zie ook De Hert, De Vries & Gutwirth 2009, p. 207.
[48] Overigens geldt dezelfde toets ook voor beperkingen op de grondrechten vastgelegd in de artikelen 9, 10 en 11 EVRM; zie Jacobs, White & Ovey 2010, p. 325.
[49] Zie EHRM 25 maart 1983, nr. 5947/72 (*Silver and Others/United Kingdom*), § 97.
[50] EHRM 7 juli 1989, nr. 14038/88 (*Soering/United Kingdom*), § 89.
[51] Vgl. Gerards 2011, p. 140.

In dit onderzoek staat derhalve centraal de zoektocht naar een *fair balance* tussen de belangen die in het geding zijn, te weten het belang van de opsporing bij het toevoegen van een hackbevoegdheid ten behoeve van de opsporing van strafbare feiten enerzijds, tegenover het belang van de burgers bij hun recht op privéleven als vastgelegd in artikel 8 EVRM anderzijds. Deze *fair balance* wordt ingevuld aan de hand van het specifieke criterium dat sprake moet zijn van een *pressing social need* en de inbreuk op het recht op privéleven in redelijke verhouding moet staan tot het belang van de opsporing van strafbare feiten.

In deze zoektocht zal ik allereerst nagaan wat het belang van de opsporing is bij de invoering van een hackbevoegdheid: is er sprake van een 'dringend belang', oftewel een *pressing social need?* Dit belang zal, op basis van de rechtspraak van het EHRM, worden beoordeeld aan de hand van drie factoren:

(1) De maatschappelijke omstandigheden die door de nationale overheid worden aangevoerd als grondslag voor een grondrechtbeperkende maatregel;[52]
(2) De beschikbaarheid van maatregelen die de aangevoerde problemen kunnen oplossen met een minder zware inbreuk op het grondrecht in kwestie: de toets van de '*less restrictive alternatives*' oftewel de subsidiariteitstoets;[53]
(3) De grondrechtbeperkende maatregel moet een effectieve bijdrage (kunnen) leveren aan het oplossen van de aangevoerde problemen: de relevantietoets.[54]

De genoemde factoren komen aan bod in respectievelijk hoofdstuk 3, hoofdstuk 4 en hoofdstuk 5. In hoofdstuk 5 zal ik tevens een conclusie geven of er sprake is van een 'dringend belang' van de opsporing bij de invoering van een hackbevoegdheid.

Tegenover het dringende belang van de opsporing staat het belang van de privacy van burgers: hoe zwaar weegt de inbreuk die met een hackbevoegdheid op de privacy wordt gemaakt? Dit belang zal in hoofdstuk 6, eveneens op basis van de rechtspraak van het EHRM, worden beoordeeld aan de hand van de volgende twee factoren:

(1) De aard en het gewicht van het grondrecht;[55]
(2) De aard en de ernst van de inbreuk op het grondrecht.[56]

In hoofdstuk 7 zal op basis van alle voorgaande factoren worden nagegaan of er sprake is van een *fair balance* tussen het belang van de opsporing en het belang van de waarborging van het recht op privacy. Hierbij komt zowel de vraag aan bod of de hackbevoegdheid in abstracto in redelijke verhouding staat tot de inbreuk op de privacy, met inachtneming van de *pressing social need*, als de vraag naar de inkleding van de bevoegdheid om de *pressing social need* en de redelijke verhouding ook in concrete gevallen te garanderen.

[52] Zie o.a. EHRM 26 april 1979, nr. 6538/74 (*Sunday Times/United Kingdom*), § 63 – 64 en EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 48.
[53] Zie o.a. Arai-Takahashi 2002, p. 88; Gerards 2011, p. 152 – 154; Vande Lanotte 2005, p. 145 – 146. Zie tevens EHRM 28 januari 2003, nr. 44647/98 (*Peck/United Kingdom*), § 80.
[54] Zie EHRM 7 december 1976, nr. 5493/72 (*Handyside/United Kingdom*), § 50 en Gerards 2011, p. 156.
[55] Zie o.a. EHRM 27 mei 2004, nr. 66746/01 (*Connors/United Kingdom*), § 82; EHRM 4 december 2008, nrs. 30562/04 en 30566/04 *(S & Marper/United Kingdom*), § 102.
[56] Zie o.a. EHRM 27 mei 2004, nr. 66746/01 (*Connors/United Kingdom*), § 86; EHRM 4 december 2008, nrs. 30562/04 en 30566/04 *(S & Marper/United Kingdom*), § 102.

In hoofdstuk 8 zal ik ten slotte de hoofdvraag beantwoorden en enkele overwegingen wijden aan het traject van de totstandkoming en evaluatie van het voorgestelde artikel 125ja Sv.

§ 4. De rol van de '*margin of appreciation*'

Benadrukt zij dat ik de toets van artikel 8 lid 2 EVRM indringend uitvoer, dat wil zeggen aan alle maatstaven (zoals uiteengezet in paragraaf 3) en aan de hand van de meest strenge interpretatie van deze maatstaven. Dit staat in contrast met de toetsing die het EHRM uitvoert bij de beoordeling van de noodzakelijkheid van heimelijke bevoegdheden. Bij deze toetsing laat het Hof staten een ruime *margin of appreciation* (beoordelingsruimte) in de beoordeling of een bepaalde bevoegdheid noodzakelijk moet worden geacht in de betreffende staat. Het Hof volstaat ermee de maatschappelijke omstandigheden te benoemen ten aanzien waarvan handelen nodig is, en hanteert dan als uitgangspunt dat dit betekent dat er voldoende grond is voor het bestaan van de heimelijke bevoegdheid in kwestie, waarna het zich enkel nog richt op een indringende toetsing van de waarborgen.[57]

De vraag dringt zich op waarom de noodzakelijkheid van een hackbevoegdheid indringend moet worden getoetst als het EHRM zelf naar verwachting hoogstens een algemene beoordeling zal uitvoeren. Het antwoord hierop ligt besloten in de grondslag voor de *margin of appreciation*. Het EHRM heeft deze *margin* ontwikkeld omdat het zichzelf als subsidiair beschouwt ten opzichte van de nationale instanties en omdat het de nationale autoriteiten beter in staat acht om te beoordelen of een beperking op een grondrecht in hun staat noodzakelijk is.[58] Het Hof beperkt zich tot een toezichthoudende taak.[59] Dit is mijns inziens een goed te verdedigen houding, echter is het hierbij wel van belang om te benadrukken dat het Hof zich zo opstelt juist omdat het de nationale autoriteiten van de betreffende staat de taak stelt om alle relevante belangen in het licht van de nationale omstandigheden af te wegen, en op basis hiervan tot een beslissing te komen omtrent de noodzakelijkheid van een wettelijke regeling.[60] Dit houdt met name in dat een indringende beoordeling door de nationale wetgever is vereist van alle elementen van de noodzakelijkheidstoets. Een andere opstelling zou betekenen dat de grondrechten van burgers niet voldoende gewaarborgd worden. Om die reden voer ik ook in dit onderzoek de indringende toetsing uit.

[57] Zie o.a. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 48 – 50; EHRM 26 maart 1987, nr. 9248/81 (*Leander/Sweden*), § 59 – 60 en EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 104 – 106.
[58] Zie EHRM 7 december 1976, nr. 5493/72 (*Handyside/United Kingdom*), § 48.
[59] Zie voor een recente benadrukking hiervan EHRM 1 maart 2010, nr. 46113/99 (*Demopoulos and Others/Turkey*), § 69. Zie ook Gerards 2011, p. 186.
[60] Zie EHRM 7 december 1976, nr. 5493/72 (*Handyside/United Kingdom*), § 48: '*The Convention leaves to each Contracting State, in the first place, the task of securing the rights and liberties it enshrines*'. Zie ook Schokkenbroek 1996, p. 204 – 205.

Hoofdstuk 3: Het dringende belang van de opsporing: manifestatie van technologische ontwikkelingen in de opsporing

§ 1. Inleiding

Het dringende belang van de opsporing bij de invoering van een hackbevoegdheid is concreet aangevoerd in de memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III. Hierin wordt gesteld dat er in de huidige opsporingspraktijk sprake is van belemmering van opsporingsonderzoeken door bepaalde technologische ontwikkelingen, te weten de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken, de opkomst van cloud computing en het gebruik van anonimiseringstechnieken op internet.[61] In dit hoofdstuk zal per genoemde technologische ontwikkeling worden beoordeeld hoe deze zich manifesteert in de opsporingspraktijk: welke complicaties veroorzaken de verschijnselen voor de opsporing en hoe vaak komen ze voor in opsporingsonderzoeken? Aan de hand van de uitkomst van deze beoordeling kan in hoofdstuk 4 respectievelijk hoofdstuk 5 worden nagegaan of er subsidiaire alternatieven voorhanden zijn om de problemen op te lossen en of een hackbevoegdheid een effectieve oplossing biedt voor deze problemen.

§ 2. Versleuteling van elektronische gegevens

Bij versleuteling (encryptie) worden leesbare data omgevormd in onleesbaar materiaal door middel van een wiskundig algoritme. Met de sleutel (vaak een lange reeks van cijfers en letters) kunnen de data weer leesbaar worden gemaakt (decryptie).[62] Versleuteling doet zich voor in de vorm van versleuteling van gegevens bij het opslaan hiervan en van versleuteling van communicatieverkeer, dat wil zeggen van gegevens die op enige wijze getransporteerd worden.[63] Versleuteling dient om te voorkomen dat anderen dan degenen bij wie de sleutel bekend is van de inhoud van de gegevens kennis kunnen nemen: in versleutelde vorm zijn gegevens immers onbegrijpelijk voor derden.[64]

Versleuteling van opgeslagen gegevens

De techniek van versleuteling van opgeslagen gegevens is in de loop der jaren steeds wijdverspreider toegepast en steeds eenvoudiger toepasbaar geworden. Burgers kunnen tegenwoordig gebruik maken van op internet verspreide programma's om gegevens te versleutelen. Het voornaamste voorbeeld van de verlaagde drempel voor versleuteling van gegevens is het aanbod aan gratis open-source encryptieprogramma's, zoals bijvoorbeeld *TrueCrypt*, die van internet kunnen worden gedownload op dezelfde manier als pakweg het

[61] Zie MvT, p. 6 – 10. Het gebruik van anonimiseringstechnieken wordt in de memorie van toelichting slechts kort aangestipt, binnen de behandeling van de ontwikkeling van versleuteling. Desondanks wordt er wel expliciet aan gerefereerd als argument voor de behoefte aan de voorgestelde bevoegdheid tot het binnendringen in een geautomatiseerd werk, en is in de literatuur en de praktijk eveneens het probleem van anonimiteit op internet geconstateerd; zie Van den Eshof e.a. 2002, p. 21 – 33; Oerlemans 2011, p. 904; Oerlemans 2012, p. 32.
[62] Zie Oerlemans 2011, p. 904. Zie tevens Wiemans 2004, p. 165.
[63] Wiemans 2004, p. 168 – 169.
[64] Wiemans 2004, p. 168.

gratis tekstverwerkingsprogramma *OpenOffice* of een webbrowser.[65] Het toegenomen gemak waarmee opgeslagen gegevens kunnen worden versleuteld manifesteert zich ook in de opsporing. Waar Koops voorheen nog constateerde dat versleuteling praktisch gezien enkel werd toegepast door enkele (georganiseerde of computerdeskundige) criminelen, is encryptie anno 2012 volgens dezelfde auteur een beduidend vaker voorkomend probleem in de opsporing.[66] Wel lijkt de toename van het aantal gevallen van encryptie van opgeslagen gegevens vooralsnog grotendeels beperkt te blijven tot kinderpornonetwerken.[67] Voor andere criminaliteit geldt vooralsnog dat versleuteling van opgeslagen gegevens nog niet vaak voorkomt, maar dat het mede vanwege de eenvoud alleszins denkbaar is dat deze vorm van encryptie zich op korte termijn verder zal verspreiden.[68]

Versleuteling van internetcommunicatie

In het kader van versleuteling van internetcommunicatie kan een onderverdeling worden gemaakt in de versleuteling van e-mailverkeer, internettelefonie, berichten via social media, en *instant messaging* (IM) berichten via internetcommunicatiediensten. Ook versleuteling van internetcommunicatie is tegenwoordig vrij eenvoudig, en vergt vaak niet eens actief handelen van de gebruiker van de communicatiedienst. Voor de encryptie van e-mailverkeer is de plug-in *Pretty Good Privacy* beschikbaar, een programma dat vergelijkbaar is met *TrueCrypt* voor versleuteling van opgeslagen gegevens.[69] Tevens wordt de versleuteling van e-mailberichten door in ieder geval de grootste (gratis) webmailaanbieders gefaciliteerd. Gmail versleutelt standaard de e-mailberichten die via haar *client* worden verstuurd, terwijl Microsoft Outlook en Yahoo! de optie van versleuteling aanbieden.[70] Voice-over Internet Protocol (VoIP) verkeer, oftewel internettelefonie, wordt altijd versleuteld door de aanbieders van de VoIP-diensten.[71] Berichten die via social media worden verstuurd zijn in beginsel versleuteld; Twitter, Facebook en Google+ zijn standaard van versleuteling voorzien.[72] Wat betreft de IM programma's is Whatsapp momenteel de grootste en daarmee de meest relevante.[73] Ook berichten via Whatsapp zijn standaard versleuteld.[74]

In de afgelopen jaren is de toepassing van 'internettaps' op basis van de bevoegdheid tot aftappen van telecommunicatie ex artikel 126m Sv sterk toegenomen. In 2010, het eerste jaar waarover het aantal internettaps bekend is gemaakt, werd 1.704 keer een bevel gegeven tot een internettap; in 2011 was dit aantal 3.331 en in 2012 16.676.[75] Het aantal internettaps stijgt

[65] Zie <http://www.truecrypt.org/>. Opgemerkt zij dat het gebruiken van encryptieprogramma's op zichzelf niet illegaal is.
[66] Koops 2012, p. 37. Zie tevens Koops 2007, p. 148.
[67] Koops 2012, p. 38. Zie ook Europol 2013, p. 29.
[68] Aldus ook Koops 2012, p. 40.
[69] <http://www.openpgp.org/>.
[70] Zie voor Gmail <http://gmailblog.blogspot.nl/2010/01/default-https-access-for-gmail.html>; voor Yahoo! zie <http://www.nbcnews.com/technology/yahoo-mail-enables-encryption-battles-security-flaw-1B7911843>.
[71] Koops 2012, p. 38; Odinot e.a. 2012, p. 53.
[72] De websites van Twitter, Facebook en Google+ zijn alle voorzien van een *Secure Sockets Layer* (SSL), waarmee de data die via die websites verstuurd wordt versleuteld is. Deze versleuteling is als gebruiker te zien doordat de URL begint met 'https://' in plaats van 'http://'.
[73] Whatsapp heeft momenteel ca. 350 miljoen gebruikers, zie *infra* noot 81.
[74] <http://www.whatsapp.com/faq/general/21864047>.
[75] *Kamerstukken II* 2011/12, 33 240 VI, nr. 1, p. 54 en *Kamerstukken II* 2012/13, 30 517, nr. 26. Bij de hoge cijfers over 2012 zij opgemerkt dat taps op een smartphone twee keer geteld worden: één op spraak en één op het datakanaal.

beduidend sneller dan het aantal telefoontaps en internettaps maken dan ook een steeds groter deel uit van het totale aantal taps dat op basis van artikel 126m Sv wordt bevolen. Dat het aantal internettaps in de toekomst zal blijven stijgen staat evenzeer buiten kijf.[76] Deze ontwikkeling is in lijn met de toenemende afhankelijkheid van burgers van communicatie via internet.[77] Het belang van e-mailverkeer in de dagelijkse communicatie van burgers is evident. Het gebruik van VoIP is de afgelopen jaren aanzienlijk toegenomen, en deze stijgende lijn zal zich naar verwachting door blijven zetten totdat (vrijwel) alle telefoonverkeer via VoIP zal worden gevoerd.[78] VoIP-aanbieder Skype heeft wereldwijd reeds ruim 300 miljoen gebruikers en concurrent Viber 200 miljoen.[79] Sociale media zijn inmiddels een gevestigd fenomeen: in Nederland maken miljoenen burgers gebruik van Facebook en Google+.[80] Tot slot worden ook programma's als Whatsapp steeds belangrijker: op termijn zullen zij naar verwachting de traditionele sms verdringen als standaard communicatiemiddel per mobiele telefoon.[81]

Met de wijdverspreide toepassing van versleuteling van internetcommunicatie en het toenemende belang van internettaps om communicatie te kunnen onderscheppen komt het probleem van encryptie van telecommunicatie steeds vaker voor in opsporingsonderzoeken.[82]

§ 3. Gebruik van draadloze netwerken

Het 'draadloos internet' (in dit onderzoek beperkt tot WLAN-verbindingen) is in de huidige samenleving niet meer weg te denken. Om te begrijpen welke gevolgen het gebruik van draadloze netwerken heeft voor de opsporing, is een korte uitleg van de technische implicaties van verbinding met deze netwerken van belang.

De technische gevolgen van de verbinding van een geautomatiseerd werk met een draadloos netwerk zijn in beginsel dezelfde als die van elke andere verbinding met het internet. Het geautomatiseerde werk krijgt een IP-adres toegewezen. Dit is een uniek nummer waarmee het geautomatiseerde werk binnen het internet kan worden geïdentificeerd.[83] Een buitenstaander kan aan de hand van een IP-adres de locatie van het bijbehorende geautomatiseerde werk vaststellen; welke gebruiker bij het betreffende IP-adres hoort is in beginsel bekend bij de ISP.[84] Het IP-adres van een geautomatiseerd werk is ook van belang voor het plaatsen van een internettap: de tap wordt geplaatst 'op' het IP-adres waarmee het geautomatiseerde werk met

[76] Zie *Aanhangsel Handelingen II* 2009/10, nrs. 2010Z04067 en 2010Z04074 (antwoorden Kamervragen van de leden Peters en Gerkens over de explosieve toename van internet- en VoIP-taps op 8 april 2010), p. 4.
[77] Zie Oerlemans 2012, p. 22.
[78] Zie Odinot e.a. 2012, p. 155; Eijpe & Van Essen 2007, p. 15.
[79] <http://www.microsoft.com/investor/EarningsAndFinancials/Earnings/Kpi/fy13/q3/Detail.aspx>; <http://www.guardian.co.uk/technology/2013/may/07/viber-skype-desktop-service>.
[80] Zie het rapport 'Social Media in Nederland 2013', te raadplegen via <http://www.slideshare.net/newcomresearch/social-media-in-nederland-2013-smo13-newcom-actuele-cijfers>.
[81] Zie <http://www.guardian.co.uk/technology/shortcuts/2012/dec/04/whatsapp-new-text-messaging>. Whatsapp heeft al 350 miljoen gebruikers, concurrent ChatOn 100 miljoen (doch vooralsnog vooral buiten Europa); zie <http://www.nu.nl/tech/3608352/whatsapp-heeft-350-miljoen-gebruikers.html> respectievelijk <global.samsungtomorrow.com/?p=28713>.
[82] Zie Koops 2012, p. 38.
[83] Kindt & Van der Hof 2009, p. 44.
[84] Zie Oerlemans 2011, p. 904 respectievelijk Kindt & Van der Hof 2009, p. 45.

andere geautomatiseerde werken communiceert, en alleen de internetcommunicatie die vanaf dat IP-adres wordt gevoerd komt over de tap.[85] Wanneer een verdachte gebruik maakt van meerdere draadloze netwerken krijgt hij bij elk netwerk een nieuw IP-adres toegewezen en hij voert dan via het IP-adres dat hij op dat moment heeft zijn internetcommunicatie. Op die manier wordt zijn internetcommunicatie verspreid over meerdere verschillende IP-adressen en dekt een internettap niet meer de volledige lading.[86]

Toegangspunten voor draadloze internetverbinding zijn tegenwoordig in groten getale beschikbaar in Nederland en velen maken hiervan gebruik voor gegevensverkeer in de vorm van internetbezoek en internetcommunicatie.[87] Verspreid over het hele land bevinden zich Wi-Fi 'hotspots' in onder andere horecagelegenheden, hotels, tankstations, treinstations en treinen. De netwerken van deze hotspots zijn over het algemeen vrij toegankelijk of de toegang tot het netwerk kan eenvoudig worden verkregen.[88] Een internetgebruiker heeft gedurende de dag dan ook via vele verschillende toegangspunten de mogelijkheid om verbinding te maken met het internet.[89] Bovendien hoeft een internetgebruiker niet eens zijn laptop bij zich te hebben voor draadloos internet: hij kan ook met zijn smartphone of tablet via draadloze netwerken gegevens ontvangen en versturen, hetgeen (zeker wat betreft de smartphone) het daadwerkelijke gebruik van meerdere draadloze netwerken aanzienlijk vereenvoudigt. Het gegevensverkeer van veel internetgebruikers zal op die manier verspreid worden over meerdere verschillende IP-adressen.[90] Elke burger met een laptop, smartphone of tablet kan eenvoudig verbinding maken met verschillende draadloze netwerken.

Er zijn geen concrete cijfers bekend omtrent de frequentie in opsporingsonderzoeken van het verschijnsel van de verspreiding van het gegevensverkeer van verdachten over meerdere verschillende IP-adressen. Draadloze netwerken en de apparaten om daarmee 'on the go' verbinding te maken zijn tegenwoordig echter dusdanig wijdverspreid en eenvoudig toegankelijk dat de verwachting gerechtvaardigd is dat verspreiding van gegevensverkeer over meerdere draadloze netwerken en daarmee over verschillende IP-adressen ook steeds vaker voorkomt en zal voorkomen in opsporingsonderzoeken.

§ 4. Cloud computing

Cloud computing is volgens het *National Institute of Standards and Technology* (NIST) '*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and*

[85] Zie Oerlemans 2012, p. 21. Zie Postel 1980 voor een technische uiteenzetting van de functie en werking van IP-adressen.
[86] Zie ook Oerlemans 2012, p. 30.
[87] Als internetbezoek heeft te gelden het bezoeken van websites en het downloaden van bestanden. Wat betreft internetcommunicatie kan hieronder worden verstaan de vierdeling die in paragraaf 2 is gemaakt: e-mailverkeer, VoIP, sociale media en IM programma's.
[88] De ontwikkeling is duidelijk wanneer de huidige situatie wordt vergeleken met die in 2002, toen Van den Eshof e.a. bij de behandeling van draadloze communicatie in opsporingsonderzoeken nog stelden dat draadloze netwerken 'veelal binnen bedrijven gebruikt [worden] als alternatief voor een fysiek bedrijfsLAN. Dit zijn geen publiek toegankelijke netwerken en daarom in het kader van deze inventarisatie niet wezenlijk van belang', Van den Eshof e.a. 2002, p. 57.
[89] Vgl. Oerlemans 2012, p. 30.
[90] Inmiddels bezit meer dan 60% van de Nederlanders een smartphone en één op de drie huishoudens heeft een tablet, zie <http://www.marketingfacts.nl/berichten/1-op-de-3-huishoudens-bezit-een-tablet>.

services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'[91] Uit deze definitie blijken meteen enkele van de grote voordelen van cloud computing: het *on-demand* karakter van de dienstverlening, de toename van opslagcapaciteit en rekenkracht dankzij efficiënt gebruik van servercapaciteit en de mogelijkheid om op eender welke locatie via de cloud toegang te krijgen tot de gewenste gegevens.[92] De kenmerken '*on-demand self-service*' (diensten op verzoek) en '*resource pooling*' (gedeelde bronnen onafhankelijk van locatie) zijn voor dit onderzoek de meest interessante vanwege hun gevolgen in opsporingsonderzoeken.[93]

On-demand self service biedt gebruikers van clouddiensten de mogelijkheid om eenzijdig (dat wil zeggen, zonder menselijke tussenkomst) de diensten in en uit te schakelen wanneer zij daar behoefte aan hebben.[94] Gevolg van dit kenmerk van flexibiliteit is een verschuiving van de verwerking van gegevens van de harde schijf van de gebruiker naar servers op afstand.[95] De gegevens staan immers alléén ter beschikking van de gebruiker wanneer deze daar behoefte aan heeft en daartoe verbinding maakt met de clouddienst. Hierdoor zijn de gegevens die in de cloud worden opgeslagen voor opsporingsambtenaren alleen zichtbaar op de harde schijf van het geautomatiseerde werk van de gebruiker wanneer er een verbinding openstaat met de clouddienst en de gegevens (tijdelijk) op de harde schijf worden verwerkt.[96]

Het kenmerk *resource pooling* houdt in (voor zover hier relevant) dat dataopslag en rekencapaciteit op dynamische wijze worden verdeeld en herverdeeld over de beschikbare cloudservers.[97] In de praktijk houdt dit in dat bij elkaar horende gegevens worden versnipperd over meerdere servers die zich vaak in verschillende landen bevinden, en dat zelfs de cloudaanbieder mogelijk niet de exacte locatie van de gegevens kan vaststellen.[98] Deze versnippering leidt tot het verschijnsel van '*loss of location*': het idee van één locatie waar bepaalde gegevens worden opgeslagen is niet meer werkbaar wanneer de betreffende data worden verwerkt middels cloud computing.[99]

Cloud computing lijkt in opsporingsonderzoeken vooralsnog, behoudens webmaildiensten als Gmail, niet frequent voor te komen, noch in Nederland noch in het buitenland.[100] Cloud computing in de vorm van opslagdiensten is nog een relatief recent verschijnsel.[101] De *Gartner Hype Cycle* van 2012 laat evenwel zien dat cloud computing reeds binnen enkele jaren een vaste en langdurige positie binnen de maatschappij zal verwerven.[102] De voordelen

[91] Mell & Grance 2011, p. 2.
[92] Zie ook Mell & Grance 2011, p. 2; Ferreira Pires 2011, p. 105 – 106.
[93] Voor de Nederlandse vertalingen zie Ferreira Pires 2011, p. 105.
[94] Mell & Grance 2011, p. 2.
[95] Zie Koops e.a. 2012, p. 47.
[96] Zie ook Koops e.a. 2012, p. 47, inclusief de reactie van Susan Brenner.
[97] Mell & Grance 2011, p. 2 ('[…] *with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.*').
[98] Koops e.a. 2012, p. 14; Spoenle 2010, p. 4 – 5.
[99] Spoenle 2010, p. 5.
[100] Koops e.a. 2012, p. 20 – 22.
[101] Microsoft SkyDrive is beschikbaar sinds 2007, Dropbox sinds 2008, iCloud sinds 2011 en Google Drive sinds 2012.
[102] Zie de afbeelding op <http://www.wired.com/beyond_the_beyond/2012/10/gartner-hype-cycle-2012/>; het bijbehorende persbericht is te raadplegen op <http://www.gartner.com/newsroom/id/2124315>.

van cloud computing zoals eerder aangestipt maken dit mijns inziens ook vrijwel onvermijdelijk. Uiteraard kunnen ook criminelen hiermee hun voordeel doen: denk aan de mogelijkheden van de toegenomen opslagcapaciteit voor kinderpornokringen en de grotere rekencapaciteit voor cybercriminelen. De logische conclusie is dat cloud computing in de komende jaren ook steeds frequenter in opsporingsonderzoeken zal opduiken.[103]

§ 5. Toepassing van anonimiseringstechnieken

Anonimiteit op internet houdt in dat voorkomen wordt dat persoonlijke informatie over een internetgebruiker wordt verspreid.[104] De voor dit onderzoek meest interessante anonimiseringstechnieken zijn er op gericht de identiteit van de gebruiker van het geautomatiseerde werk verborgen te houden middels het afschermen van het IP-adres, het voornaamste identificerende kenmerk op het internet. Afscherming kan worden bereikt door middel van een *anonymous proxy*, een VPN-dienst of het Tor-netwerk.[105] Een *anonymous proxy* is een server die verstuurde data ontdoet van het versturende IP-adres en vervolgens een eigen IP-adres opgeeft als afzender. Data verstuurd vanaf andere geautomatiseerde werken worden dan door de proxy op dat IP-adres ontvangen en doorgestuurd naar de internetgebruiker.[106] De internetgebruiker kan niet op basis van het IP-adres van de proxy worden geïdentificeerd. VPN-diensten verbergen op vergelijkbare wijze het IP-adres van gebruikers door het eigen IP-adres in de plaats te stellen.[107] Het Tor-netwerk (The Onion Router) ten slotte is een netwerk van door vrijwilligers aangeboden servers verspreid over de hele wereld, waarbinnen communicatie versleuteld wordt gerouteerd. Door gebruik van het Tor-netwerk communiceren internetgebruikers via een willekeurig IP-adres en bovendien verloopt de communicatie over verschillende punten binnen het netwerk. Hierdoor is zowel de bron als de bestemming van de communicatie moeilijk te achterhalen en blijft de internetgebruiker verborgen achter het doolhof van het Tor-netwerk.[108]

Anonimiteit is voor internetgebruikers met name wenselijk ten opzichte van derden die bevoegd (ISP's, opsporingsdiensten in bepaalde gevallen) of onbevoegd (hackers, spyware) kennis kunnen nemen van het gegevensverkeer van een bepaalde gebruiker en aan de hand van het IP-adres dit gegevensverkeer tot de betreffende gebruiker zouden kunnen herleiden. Hoewel anonimisering net als de eerder behandelde technologische mogelijkheden niet noodzakelijk met kwade bedoelingen hoeft te worden toegepast, maken criminelen ook zeker dankbaar gebruik van anonimiseringstechnieken om hun identiteit op internet verborgen te houden en het gebruik van dergelijke technieken komt met enige frequentie voor in opsporingsonderzoeken naar cybercrime.[109] Anonimiseringstechnieken, bijvoorbeeld het gebruik van het Tor-netwerk, worden ook op grote schaal ingezet bij de verspreiding van

[103] Ook Europol voorspelt in haar in maart 2013 gepubliceerde *Serious and Organised Crime Threat Assessment* (SOCTA) dat het toenemende gebruik van cloud computing zich in de komende vier jaar zal manifesteren in de opsporing; zie Europol 2013, p. 15 – 16.
[104] Zie Van den Eshof e.a. 2002, p. 21.
[105] Zie Van den Eshof e.a. 2002, p. 27; Oerlemans 2010, p. 54; Oerlemans 2012, p. 32.
[106] Van den Eshof e.a. 2002, p. 27.
[107] <http://vpnservice.nl/>.
[108] Koops e.a. 2012, p. 16. Zie tevens de uitgebreide uitleg op <https://www.torproject.org/about/overview.html.en>.
[109] Zie o.a. Van den Eshof e.a. 2002, p. 21; *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 2 – 3.

kinderporno en de kwestie van anonimiteit komt dan ook eveneens in het kader van de opsporing van kinderporno veelvuldig aan bod.[110] Volgens het recente SOCTA rapport van Europol zal het gebruik van anonimiseringstechnieken in het kader van cybercriminaliteit in het algemeen, en kinderporno in het bijzonder, de komende vier jaar nog verder toenemen.[111]

In de memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III wordt ook nog aandacht besteed aan de mogelijkheid dat de verdachte vaststelling van zijn locatie voorkomt door zijn smartphone (en naar mag worden aangenomen ook bijvoorbeeld een tablet) af te schermen voor de opsporingsdiensten.[112] Hierbij wordt enkel ingegaan op gebruik van een GPS-jammer, maar als geautomatiseerd werk met internetverbinding heeft een smartphone ook een IP-adres dat afgeschermd kan worden, waarmee eveneens de locatie wordt verhuld. Over deze mogelijkheden van anonimisering is geen onderzoek beschikbaar en onduidelijk is hoe frequent dit verschijnsel zich voordoet in opsporingsonderzoeken.

§ 6. Conclusie

De technologische ontwikkelingen die in dit hoofdstuk zijn behandeld leveren alle nieuwe complicaties op voor de opsporing van strafbare feiten. Met name de versleuteling van gegevens en de toepassing van anonimiseringstechnieken worden inmiddels al vele jaren door criminelen ingezet en komen frequent en steeds vaker voor in opsporingsonderzoeken, met name ten aanzien van cybercriminaliteit en kinderporno. Cloud computing doet zich nog niet in significante mate in opsporingsonderzoeken voor, maar het lijkt onvermijdelijk dat dit op relatief korte termijn alsnog zal gebeuren. Omtrent het gebruik van draadloze netwerken in het kader van strafbare feiten zijn geen concrete gegevens bekend, en dit verschijnsel lijkt qua frequentie in opsporingsonderzoeken de minst significante van de in dit hoofdstuk behandelde. Evenwel is de mogelijkheid voor criminelen om van draadloze netwerken gebruik te maken tegenwoordig dusdanig eenvoudig dat het reëel is om aan te nemen dat dit verschijnsel zich ook in opsporingsonderzoeken zal manifesteren.

Gezien het bovenstaande zijn de praktische problemen van de in dit hoofdstuk behandelde technologische ontwikkelingen voor de opsporing voldoende significant om nader te onderzoeken of de opsporing een ‘dringend’ belang heeft bij de invoering van een hackbevoegdheid om deze problemen op te lossen.

[110] Zie bijvoorbeeld Lünneman e.a. 2006, p. 165; Oerlemans 2010, p. 65; *Kamerstukken II* 2012/13, 28 684, nr. 363, p. 2. Zie tevens *Aanhangsel Handelingen II* 2011/12, nr. 2012Z02969, p. 2 – 3, waarin de minister schat dat er via het Tor-netwerk honderdduizenden kinderpornografische afbeeldingen en video’s zijn of worden verspreid. Zie tot slot ook het verslag van het OM over het gebruik van anonieme websites binnen het Tor-netwerk voor de verspreiding van kinderporno op <http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/>.
[111] Zie Europol 2013, p. 15 en p. 29.
[112] Zie MvT, p. 20.

Hoofdstuk 4: Het dringende belang van de opsporing: subsidiariteit van een hackbevoegdheid

§ 1. Inleiding

De opsporing kan geen dringend belang hebben bij de invoering van een hackbevoegdheid als de in hoofdstuk 3 geconstateerde problemen voor de opsporing kunnen worden opgelost met behulp van opsporingsbevoegdheden die een minder zware inbreuk maken op de persoonlijke levenssfeer, oftewel als er *less restrictive alternatives* zijn. De hackbevoegdheid doorstaat dan immers niet de subsidiariteitstoets als aangestipt in paragraaf 3 van hoofdstuk 2 en kan dan niet noodzakelijk worden geacht in de zin van artikel 8 lid 2 EVRM. Om de subsidiariteit te beoordelen, wordt in dit hoofdstuk als maatstaf genomen of er alternatieve opsporingsbevoegdheden bestaan die de beoogde resultaten van de hackbevoegdheid kunnen bereiken, te weten het vergaren van de relevante informatie voor het opsporingsonderzoek ondanks de verschijnselen van versleuteling, draadloze netwerken, cloud computing en anonimiseringstechnieken. Of en in hoeverre de hackbevoegdheid zelf deze resultaten daadwerkelijk kan bereiken komt in hoofdstuk 5 nader aan bod.

In dit hoofdstuk zal, voor zover de aangedragen bevoegdheden worden vergeleken met een hackbevoegdheid, worden uitgegaan van de in het conceptwetsvoorstel Computercriminaliteit III voorgestelde modaliteiten van de bevoegdheid tot het binnendringen in een geautomatiseerd werk ten behoeve van het verrichten van opsporingshandelingen. Deze modaliteiten zijn het binnendringen in een geautomatiseerd werk met het oog op het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker (het voorgestelde artikel 125ja lid 1 aanhef en onder a Sv); met het oog op het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn of worden verwerkt (onder b); met het oog op het opnemen van vertrouwelijke communicatie of het aftappen van telecommunicatie (onder d); en met het oog op stelselmatige observatie (onder e).

§ 2. Subsidiaire alternatieven bij versleuteling

§ 2.1. Versleuteling van opgeslagen gegevens

Om versleutelde opgeslagen gegevens weer bruikbaar te maken als informatie ten behoeve van het opsporingsonderzoek moeten de gegevens weer begrijpelijk worden gemaakt voor mensen. Het ‘kraken’ van de versleuteling middels de pure rekenkracht van computersystemen is praktisch onmogelijk wanneer de verdachte een degelijk cryptosysteem gebruikt.[113] Praktisch gezien is de sleutel nodig om versleutelde bestanden weer toegankelijk en bruikbaar te kunnen maken als informatie ten behoeve van de opsporing.[114] Hiervoor bestaat de bevoegdheid tot het geven van een decryptiebevel.

[113] Zie Koops 2007, p. 157 – 158; zie voorts Wiemans 2004, p. 167 – 168.
[114] Door cloud computing kan de rekencapaciteit van computers enorm toenemen, maar de tijd die nodig is om encryptie te kraken zal nog steeds te lang zijn om als standaardpraktijk in opsporingsonderzoeken werkbaar te zijn; zie Koops 2012, p. 40.

Artikel 125k lid 3 Sv biedt de bevoegdheid tot het geven van een bevel aan een ander dan de verdachte tot het overhandigen van een sleutel aan opsporingsdiensten of tot het rechtstreeks ontsleutelen van bepaalde gegevens om deze vervolgens aan de opsporingsdiensten over te dragen. De bevoegdheid mag worden toegepast in geval van een doorzoeking ter vastlegging van gegevens ex artikel 125i Sv of een netwerkzoeking ex artikel 125j Sv. Omdat de bevoegdheid tot het geven van een decryptiebevel derhalve niet heimelijk kan worden uitgeoefend, is de inbreuk op de persoonlijke levenssfeer geringer dan het geval is bij het heimelijk binnendringen in een geautomatiseerd werk om gegevens over te nemen.
De effectiviteit van het decryptiebevel blijkt in de praktijk echter beperkt. De voornaamste reden hiervoor is dat het decryptiebevel niet tot de verdachte mag worden gericht, terwijl deze doorgaans de enige zal zijn die kennis heeft van de sleutel tot versleutelde opgeslagen gegevens: dit is immers juist het doel van encryptie.[115] Het decryptiebevel is in zijn huidige vorm praktisch gezien dan ook niet in staat om consequent een oplossing te bieden voor het probleem van versleuteling en vormt derhalve geen subsidiair alternatief voor een hackbevoegdheid.

In het conceptwetsvoorstel Computercriminaliteit III wordt de bevoegdheid voorgesteld tot het geven van een decryptiebevel aan de verdachte.[116] Momenteel is nog onzeker of deze bevoegdheid daadwerkelijk zal worden ingevoerd, maar hoe dan ook is het, mede vanwege de discussie die al vele jaren over een dergelijke bevoegdheid wordt gevoerd, als alternatief voor een hackbevoegdheid het overwegen waard.[117] Net als het decryptiebevel jegens een ander dan de verdachte, maakt een decryptiebevel gericht aan de verdachte een geringere inbreuk op de persoonlijke levenssfeer dan een hackbevoegdheid. In theorie lost de mogelijkheid om een decryptiebevel aan de verdachte te richten ook het door Koops geconstateerde probleem op: immers wordt het bevel dan gericht aan degene die daadwerkelijk de sleutel kent. Praktisch gezien is het echter maar de vraag of een decryptiebevel aan verdachten daadwerkelijk effect zal sorteren. De ontwikkeling van versleutelingstechnieken heeft geleid tot het probleem van de ‘aannemelijke ontkenbaarheid’ van de aanwezigheid van gegevens op een harde schijf. Met de huidige encryptieprogramma’s is het mogelijk om gegevens op een harde schijf te verbergen in verschillende lagen ‘cryptocontainers’. Deze containers zien er voor de opsporingsdiensten uit als lege schijfruimte, waardoor zij niet kunnen aantonen dat er versleutelde gegevens op de harde schijf staan.[118] In zo’n geval kan in beginsel geen decryptiebevel worden gegeven.

Tevens is het zeer twijfelachtig of verdachten überhaupt in significante mate gehoor zullen geven aan een decryptiebevel. Om medewerking te bewerkstelligen wordt in het conceptwetsvoorstel Computercriminaliteit III artikel 184b Sr voorgesteld, dat met een gevangenisstraf van maximaal drie jaar een hoge strafdreiging stelt op het opzettelijk niet

[115] Koops 2000, p. 17.
[116] Conceptwetsvoorstel Computercriminaliteit III, p. 5. Zie MvT, p. 3 – 4.
[117] Zie reeds *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 25 – 26. Zie verder over deze discussie onder andere Koops 2012, p. 67 – 74.
[118] Zie Koops 2012, p. 42 – 43.

voldoen aan een bevel tot ontsleuteling.[119] Een decryptiebevel ex het voorgestelde artikel 125k lid 4 Sv kan echter alleen worden gericht aan verdachten van het maken van een beroep of gewoonte van kinderporno en verdachten van terrorisme. Op deze typen delicten staan beduidend hogere gevangenisstraffen dan drie jaar en dergelijke delicten worden doorgaans gepleegd door zware, berekenende criminelen, die een afweging zullen maken tussen de straf op het hoofddelict en de straf voor het niet voldoen aan een decryptiebevel.[120] De beperkte bekende buitenlandse resultaten laten ook geen positief beeld zien.[121] Justitie en politie in Nederland zijn sceptisch over de meerwaarde van een decryptiebevel aan verdachten in opsporingsonderzoeken.[122] Het verwachte rendement van een bevoegdheid tot het geven van een decryptiebevel aan verdachten is te laag om te kunnen spreken van een consequente oplossing voor het probleem van versleuteling en een subsidiair alternatief voor een hackbevoegdheid.

Een korte beschouwing verdient nog de optie van het verhogen van de voorgestelde strafdreiging op het niet voldoen aan een decryptiebevel. Wellicht kan hiermee wel de medewerking van verdachten worden bevorderd en zou zo met een lichtere inbreuk op de persoonlijke levenssfeer kennis kunnen worden genomen van de inhoud van versleutelde gegevens, maar een verhoging van de strafdreiging zal naar alle waarschijnlijkheid in strijd komen met het nemo-teneturbeginsel vervat in artikel 6 EVRM.[123] Niet alleen levert het inruilen van de ene grondrechtschending voor de andere rechtsstatelijke bezwaren op (een dergelijke ruil lijkt mij immers niet de bedoeling van de subsidiariteitsmaatstaf van artikel 8 lid 2 EVRM), maar tevens zal een decryptiebevel met verzwaarde strafdreiging door het EHRM (en mogelijk reeds door de Nederlandse rechters) ontoelaatbaar worden geacht wegens strijd met artikel 6 EVRM. Een decryptiebevel met verzwaarde strafdreiging kan om die reden überhaupt niet aan een verdachte worden gegeven, althans het bewijs dat daarmee wordt verkregen mag niet in het strafproces worden gebruikt. Om die reden is de bevoegdheid tot het geven van een decryptiebevel aan de verdachte ook met een hogere strafdreiging praktisch gezien geen subsidiair alternatief voor een hackbevoegdheid.

§ 2.2. Versleuteling van internetcommunicatie

Aftappen van telecommunicatie met ontsleutelbevel

Artikel 126m lid 6 tot en met 8 Sv biedt de bevoegdheid tot het geven van een ontsleutelbevel in het kader van het aftappen van telecommunicatie, aan een ieder van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van bepaalde opgenomen communicatie. De vraag of dit decryptiebevel praktisch gezien wél effect kan sorteren is echter niet relevant: het aftappen van telecommunicatie op een internetverbinding maakt namelijk niet minder inbreuk dan het ‘aftappen op het apparaat’ zoals voorgesteld in

[119] Vergelijk dit met het strafmaximum van drie maanden ex artikel 184 Sr dat geldt voor het niet voldoen aan een decryptiebevel gericht aan anderen dan de verdachte.
[120] Zie Koops 2012, p. 143 – 144. Andere overwegingen, zoals het beschermen van handlangers, contacten en bronnen kunnen eventueel ook nog een rol spelen in de afweging.
[121] Zie Koops 2012, p. 104 – 106 over de resultaten uit het Verenigd Koninkrijk.
[122] Zo volgt uit interviews met vertegenwoordigers van het OM en het KLPD, zie Koops 2012, p. 134 – 135.
[123] Zie ook Koops 2012, p. 151 – 152. Niet uit te sluiten valt dat de strafmaat van het voorgestelde artikel 125k lid 4 Sv zelfs reeds in strijd is met het nemo-teneturbeginsel.

artikel 125ja lid 1 onder d Sv. Immers wordt in beide gevallen dezelfde communicatie afgetapt en wordt niet kennis genomen van (bijvoorbeeld) de inhoud van de harde schijf van het geautomatiseerde werk. De klassieke toepassing van de aftapbevoegdheid ex artikel 126m Sv is mijns inziens niet minder inbreukmakend dan het 'aftappen op het apparaat' en vormt derhalve geen subsidiaire optie ten opzichte van een hackbevoegdheid.

Vorderen inhoudelijke opgeslagen gegevens
Artikel 126ng lid 2 Sv biedt de mogelijkheid om kennis te nemen van de inhoud van internetcommunicatie middels het vorderen van opgeslagen inhoudelijke gegevens, oftewel communicatieberichten van gebruikers die bij aanbieders van communicatiediensten zijn opgeslagen. Voor zover de berichten versleuteld worden opgeslagen dienen deze door de aanbieder onversleuteld aan de opsporingsautoriteiten te worden verstrekt.[124] Het vorderen van gegevens maakt naar de aard een minder zware inbreuk op de persoonlijke levenssfeer dan een hackbevoegdheid.[125] De vordering kan worden ingesteld tegen 'aanbieders van een communicatiedienst' in de zin van artikel 126la Sv, oftewel ISP's en aanbieders van webmail-, VoIP, social media- en IM-diensten.[126] E-mailberichten die bij webmailaanbieders zijn opgeslagen en privéberichten die via social media zijn verstuurd kunnen op basis van artikel 126ng lid 2 Sv bij aanbieders van deze diensten worden gevorderd.[127] In de praktijk zijn vorderingen op basis van dit artikel ook reeds ingesteld bij deze aanbieders.[128] Wat betreft VoIP-diensten zal een vordering ex artikel 126ng lid 2 Sv praktisch gezien een beperkte strekking hebben. Skype slaat bijvoorbeeld alleen *instant messages*, voicemailberichten en videoberichten op.[129] *Real time* telefoon- of videogesprekken worden niet opgeslagen en kunnen dus ook niet worden gevorderd. Whatsapp slaat helemaal geen berichten op van de gebruikers van haar dienst: wanneer een bericht bij de ontvanger is aangekomen, verdwijnt het van de server van Whatsapp.[130]

De aanbieders van internetcommunicatiediensten die in Nederland het meest gebruikt worden (zie paragraaf 2 van hoofdstuk 3) zijn echter in het buitenland gevestigd. Tegen deze aanbieders kan artikel 126ng lid 2 Sv vanwege het soevereiniteitsbeginsel niet worden ingezet. Wanneer een buitenlandse aanbieder gevestigd is in een staat die partij is bij het Cybercrimeverdrag, is het wel mogelijk om op basis van artikel 32 onder b CCV een

[124] Dit ligt reeds besloten in artikel 126ng lid 2 Sv, maar kan nog eens expliciet worden bevolen ex artikel 126nh Sv.
[125] Vgl. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.
[126] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 26 en T. Blom, aant. 2 op artikel 126la Sv, in: C.P.M. Cleiren & M.J.M. Verpalen (red.), *Tekst en Commentaar Strafvordering* 2011. De aanbieders van de internetcommunicatiediensten die geen ISP zijn, zijn rechtspersonen die gegevens verwerken of opslaan ten behoeve van de gebruikers van een telecommunicatiedienst, en vallen derhalve in de 'derde categorie' van artikel 126la Sv, na de aanbieders van openbare telecommunicatienetwerken of –diensten en de aanbieders van gesloten telecommunicatienetwerken of –diensten.
[127] Zie Oerlemans 2012, p. 33.
[128] Zie de statistieken van het voormalige politiekorps Limburg-Zuid over de periode 2009 – 2011: <https://www.bof.nl/live/wp-content/uploads/20120217-bevragingen-sociale-netwerken.pdf>.
[129] Zie de *Privacy Policy* van Skype, punt 12, op <http://www.skype.com/en/legal/privacy/>.
[130] Zie de *Privacy Notice* binnen de *Terms of Service* van Whatsapp op <http://www.whatsapp.com/legal/>. Berichten worden slechts op de server van Whatsapp opgeslagen zolang ze niet bij de ontvanger zijn aangekomen, maar dit duurt in beginsel niet lang genoeg om een vordering in te kunnen stellen. De situatie dat een bericht dertig dagen op de server blijft staan omdat het niet is aangekomen bij de ontvanger is te marginaal om in dit kader een rol te spelen.

rechtstreeks verzoek in te stellen tot verstrekking van opgeslagen inhoudelijke berichten.[131] Dit is over het algemeen een optie, aangezien de meeste aanbieders zijn gevestigd in de Verenigde Staten, dat partij is bij het Cybercrimeverdrag (belangrijke uitzondering hierop is Skype: ondanks de overname door Microsoft is nog steeds het recht van Luxemburg van toepassing, terwijl Luxemburg het Cybercrimeverdrag niet heeft geratificeerd). Het is aannemelijk dat aanbieders van internetcommunicatiediensten gerechtigd zijn in de zin van artikel 32 onder b CCV om de opgeslagen gegevens te verstrekken. In hun *privacy policy* wordt immers aangegeven dat onder andere de inhoud van privéberichten kan worden opgeslagen en verstrekt aan derden in bepaalde gevallen, waaronder verzoeken van officiële autoriteiten.[132] Hierdoor kan de handelingsbevoegdheid over de gegevens worden afgeleid uit de overeenkomst die is afgesloten met de gebruiker van de communicatiedienst.[133] In theorie is toepassing van artikel 32 CCV dan ook een reële optie om opgeslagen inhoudelijke berichten te verkrijgen van buitenlandse aanbieders van internetcommunicatiediensten.

Door de Nederlandse autoriteiten (behoudens een enkele uitzondering zoals politiekorps Limburg-Zuid) worden statistieken over vorderingen bij sociale-netwerkdiensten vooralsnog standvastig stilgehouden.[134] In hun *transparency reports* publiceren Microsoft en Google tegenwoordig wel hoeveel vorderingen of verzoeken gedurende een bepaalde periode van opsporingsdiensten worden ontvangen, uitgesplitst naar land.[135] In deze rapporten worden echter alle soorten verzoeken samengenomen en wordt niet gespecificeerd hoeveel verzoeken gericht waren op het verkrijgen van opgeslagen inhoudelijke gegevens, waardoor de percentages weinig betekenis hebben.[136] Uit de praktijk valt vooralsnog derhalve moeilijk op te maken wat verwacht kan worden van rechtstreekse verzoeken aan buitenlandse internetcommunicatieaanbieders om opgeslagen inhoudelijke gegevens. Oerlemans lijkt gematigd positief over de mogelijkheid om deze gegevens te verkrijgen, al zal dit zeker niet altijd succes opleveren en tevens gepaard gaan met enige vertraging ten opzichte van het *real time* aftappen van telecommunicatie.[137]

Indien het rechtstreekse verzoek aan de aanbieder van internetcommunicatie geen resultaat oplevert, is een rechtshulpverzoek aan de staat van vestiging mogelijk. Opnieuw ontbreken

---

[131] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2004, 290. Per november 2013 hebben 40 staten het verdrag geratificeerd, zie <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

[132] Zie bijvoorbeeld de *Data Use Policy* van Facebook op <https://www.facebook.com/about/privacy/your-info> en de *privacy policy* van Skype, punt 3, op <http://www.skype.com/en/legal/privacy/#disclosureOfInformation>.

[133] Zie ook *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 26.

[134] Zie *Aanhangsel Handelingen II* 2011/12, nr. 2011Z23302 (antwoord op Kamervragen van het lid El Fassed over online privacy op 7 februari 2012). Zie voorts *Aanhangsel Handelingen II* 2011/12, nr. 2012Z11858 (antwoord op Kamervragen van het lid El Fassed over online privacy op 25 juli 2012) voor de meest recente bevestiging van dit standpunt. Zie echter ook de statistieken bekendgemaakt door politiekorps Limburg-Zuid *supra* noot 128.

[135] Het '*2012 Law Enforcement Requests Report*' van Microsoft (inclusief statistieken van Skype) is beschikbaar via <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>. Het *transparency report* van Google is beschikbaar via <http://www.google.com/transparencyreport/>.

[136] Voor de volledigheid: in totaal leidde 2,2% van de verzoeken aan Microsoft tot een *disclosure of content*, terwijl de twee verzoeken aan Skype niet tot *disclosure of content* leidden. Google voldeed in de periode januari tot en met juni 2012 in 76% van de gevallen aan Nederlandse verzoeken.

[137] Oerlemans 2012, p. 34.

statistieken, maar is de verwachting gerechtvaardigd dat niet alle rechtshulpverzoeken zullen worden ingewilligd en hoe dan ook neemt deze route extra tijd in beslag.[138]

De onzekere en waarschijnlijk beperkte kans van slagen van een rechtstreeks verzoek of rechtshulpverzoek om inhoudelijke opgeslagen gegevens te verstrekken, in combinatie met de vertraging die deze routes met zich meebrengen, leidt tot de conclusie dat zij waarschijnlijk geen subsidiair alternatief voor een hackbevoegdheid kunnen vormen wegens een (verwacht) gebrek aan consequente resultaten.

Kennisnemen van de inhoud van communicatie middels het vorderen van opgeslagen inhoudelijke gegevens is technisch gezien helemaal niet mogelijk ten aanzien van versleutelde internettelefonie of IM-diensten als Whatsapp. Naar de aard zullen deze vormen van (versleutelde) communicatie rechtstreeks en *real time* moeten worden afgetapt en/of opgenomen.[139] Dit kan door toepassing van de bevoegdheden ex artikel 126m en 126l Sv of door het binnendringen in een geautomatiseerd werk om op het apparaat af te tappen of op te nemen. Reeds is overwogen dat het binnendringen in een geautomatiseerd werk met het oog op het aftappen van telecommunicatie niet méér inbreuk maakt op de persoonlijke levenssfeer dan de huidige toepassing van artikel 126m Sv, en eenzelfde overweging geldt ten aanzien van het binnendringen in een geautomatiseerd werk met het oog op het opnemen van vertrouwelijke communicatie ex artikel 126l Sv. Immers wordt met het op afstand digitaal installeren van een keylogger of aanzetten van een microfoon kennis genomen van dezelfde communicatie als wanneer deze functies fysiek worden verricht. In beginsel maken de twee bevoegdheden een vergelijkbare inbreuk op de persoonlijke levenssfeer, waardoor de een niet subsidiair is ten opzichte van de ander.[140]

§ 3. Subsidiaire alternatieven bij gebruik van draadloze netwerken

De verschillende IP-adressen van het geautomatiseerde werk van een verdachte kunnen worden achterhaald door het instellen van een vordering tot het verstrekken van verkeersgegevens en/of gebruikersgegevens ex artikel 126n respectievelijk 126na Sv, jegens de verschillende ISP's van de draadloze netwerken. Deze bevoegdheden maken naar hun aard een geringere inbreuk op de persoonlijke levenssfeer dan hacken.[141] Het vorderen van de IP-adressen bij elke verbinding met een nieuw draadloos netwerk bij verschillende ISP's is echter erg omslachtig en levert vertraging op in het opsporingsonderzoek; bovendien zal niet altijd het tijdstip van gebruik van het netwerk door de verdachte bekend zijn, waardoor opsporingsambtenaren grote hoeveelheden IP-adressen moeten doorziften om het juiste geautomatiseerde werk te vinden. Wanneer het (vervolgens) de bedoeling is om de telecommunicatie van de verdachte af te tappen geldt tevens dat het plaatsen van internettaps op alle IP-adressen die de verdachte benut praktisch onmogelijk is en dus geen consequente

[138] Oerlemans 2012, p. 33.
[139] Zie de uitleg over Skype en Whatsapp *supra* noot 129 en 130.
[140] Het opnemen van vertrouwelijke communicatie via het binnendringen in een geautomatiseerd werk moet dan wel beperkt blijven tot de communicatie via VoIP of IM-diensten; zie hierover nader paragraaf 3.1 van hoofdstuk 5.
[141] Zo blijkt uit de voorwaarden voor toepassing: de gegevens mogen worden gevorderd door elke opsporingsambtenaar bij verdenking van elk misdrijf.

oplossing vormt voor het probleem van de verspreiding van gegevensverkeer over meerdere IP-adressen (nog los van de eerder getrokken conclusie dat het aftappen van telecommunicatie op een internetverbinding geen minder zware inbreuk maakt op de privacy dan het 'aftappen op het apparaat').[142] Tot slot is ook het als onderdeel van de verkeersgegevens vorderen van de *metadata* (te weten gegevens omtrent wanneer naar welke IP-adressen is gecommuniceerd, voor hoe lang, etc.) praktisch gezien te omslachtig en levert het te veel vertraging op in het opsporingsonderzoek, aangezien deze *metadata* voor alle IP-adressen apart moeten worden verzameld.

Gezien het bovenstaande zijn er geen subsidiaire alternatieven voor de bevoegdheid tot het binnendringen in een geautomatiseerd werk wanneer de verdachte zijn internetcommunicatie middels het gebruik van draadloze netwerken over meerdere IP-adressen verspreidt.

§ 4. Subsidiaire alternatieven bij cloud computing

Vorderen en verzoeken van gegevens

Voor het vergaren van gegevens uit de cloud kunnen de bestaande bevoegdheden tot het vorderen van gegevens (artikelen 126n, 126na en 126nc tot en met 126ng Sv) worden gericht tot cloudaanbieders. Wanneer het gaat om het verkrijgen van gegevens maken deze bevoegdheden de minst zware inbreuk op de persoonlijke levenssfeer.[143] Toepassing van deze bevoegdheden kent echter enkele complicaties. Allereerst behelst het probleem van de onzichtbaarheid van gegevens ook het probleem dat bij opsporingsdiensten niet bekend is of de verdachte gebruik maakt van clouddiensten en zo ja van welke aanbieder(s). Met name wanneer een verdachte zijn cloudgebruik verspreidt over meerdere aanbieders en/of zijn cloudgebruik goed verbergt (bijvoorbeeld door geen bekende diensten te gebruiken en alle sporen van eerder cloudgebruik te wissen) blijven de opsporingsambtenaren in het ongewisse over de cloudaanbieder tot welke ze de vordering moeten richten. Dit zal alleen anders zijn wanneer de verdachte op het moment van een doorzoeking ex artikel 125i Sv openstaande verbindingen heeft (met de juiste clouddiensten) en deze niet tijdig kan uitschakelen. Dit zal in de praktijk waarschijnlijk meer afhangen van geluk dan wijsheid.[144]

Wanneer de cloudaanbieder wel bekend is geldt de beperking dat een aanzienlijk deel van de cloudaanbieders zich in het buitenland bevindt en dus vanwege het soevereiniteitsbeginsel niet op basis van Nederlandse strafvorderlijke bevoegdheden kunnen worden verplicht om gegevens te verstrekken. Op basis van artikel 32 onder b CCV kan wel een rechtstreeks verzoek worden ingesteld wanneer de cloudaanbieder zich in een van de verdragsstaten bevindt.[145] Wanneer de betreffende aanbieder geen gehoor geeft aan een rechtstreeks verzoek of zich niet in een verdragsstaat bevindt, dient een rechtshulpverzoek aan de staat van vestiging te worden gericht. Staten die zijn aangesloten bij het Cybercrimeverdrag zullen hier

[142] Zie ook Odinot e.a. 2012, p. 157 – 158; Oerlemans 2012, p. 30 – 31.
[143] Vgl. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12. Met inachtneming van de technologische opbouw van een cloud computing netwerk (zie paragraaf 4 van hoofdstuk 3) is het geven van een bevel tot uitlevering van een voorwerp dat gegevens behelst ter inbeslagneming ex artikelen 96a en 105 Sv, ten aanzien van cloudaanbieders geen reële optie.
[144] Zie Koops e.a. 2012, p. 40.
[145] Zie ook Koops e.a. 2012, p. 41.

waarschijnlijk in de regel gehoor aan geven.[146] Veel niet-verdragsstaten en/of staten waarmee Nederland geen (goede) rechtshulprelatie heeft zullen echter minder welwillend staan tegenover een dergelijk verzoek.[147] Dergelijke staten zijn daarmee een geschikte en populaire locatie voor cloudaanbieders in de vorm van *bulletproof hosting providers*. Deze providers zijn vaak gericht op het faciliteren van (cyber)criminele activiteiten en werken niet mee aan verzoeken om verstrekking van gegevens.[148] Wanneer criminelen hun activiteiten bij deze aanbieders onderbrengen zal het verkrijgen van gegevens via een verzoek praktisch onmogelijk zijn: de aanbieder zelf zal niet meewerken en de staat van vestiging (waarschijnlijk) evenmin.

De conclusie is dat rechtstreekse verzoeken of rechtshulpverzoeken hoogstens een reële kans van slagen kunnen hebben wanneer de cloudaanbieder is gevestigd in een CCV-verdragsstaat. Nederlandse opsporingsdiensten hebben met dergelijke verzoeken redelijk positieve resultaten behaald, maar met de belangrijke kanttekening dat enkel nog om webmail is verzocht.[149] De prognose omtrent de kans van slagen van verzoeken om in de cloud opgeslagen gegevens is niet positief, óók niet wanneer het gaat om cloudaanbieders die in CCV-staten zijn gevestigd.[150] De mogelijkheden om middels het vorderen of verzoeken van in de cloud opgeslagen gegevens consequent een oplossing te bieden voor de door cloud computing veroorzaakte problemen zijn derhalve te beperkt om te spreken van een subsidiair alternatief voor een hackbevoegdheid.

Doorzoeking ter vastlegging van gegevens

De doorzoeking ter vastlegging van gegevens is geen heimelijke opsporingsbevoegdheid en maakt derhalve een minder zware inbreuk op de privacy dan het heimelijk binnendringen in een geautomatiseerd werk. In aansluiting op hetgeen eerder werd opgemerkt heeft de doorzoeking echter nog slechts beperkte waarde wanneer een verdachte gebruik maakt van cloud computing: gegevens die door de verdachte in de cloud worden opgeslagen, kunnen op basis van artikel 125i Sv enkel worden vastgelegd indien deze zich op het moment van doorzoeking op de harde schijf van het geautomatiseerde werk bevinden.[151] Hoewel er mogelijkheden bestaan om de doorzoeking ex artikel 125i Sv ten aanzien van cloud computing effectiever te maken, bijvoorbeeld door in de opleiding aandacht te besteden aan het belang van het behoud van openstaande verbindingen met de cloud, moet deze bevoegdheid vanwege de afhankelijkheid van de factor toeval bij het aantreffen van openstaande verbindingen niet in staat worden geacht om consequent een oplossing te bieden voor de door cloud computing veroorzaakte problemen en deze bevoegdheid vormt dan ook geen subsidiair alternatief voor een hackbevoegdheid.[152]

[146] Zie Koops e.a. 2012, p. 39 – 40.
[147] Zie Koops e.a. 2012, p. 40 – 41.
[148] Zie Koops e.a. 2012, p. 40; MvT p. 10. Verdere literatuur over *bulletproof hosting providers* is (nog) erg schaars.
[149] Zie Koops e.a. 2012, p. 39.
[150] Zo werkt Google volgens het OM niet mee aan verzoeken om in Google Docs opgeslagen documenten, volgens Google omdat de data zo is opgeslagen dat ze niet mee kúnnen werken; zie Koops e.a. 2012, p. 40.
[151] Vgl. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11.
[152] Zie Koops e.a. 2012, p. 40.

Netwerkzoeking

Wanneer de doorzoeking op basis van artikel 125i Sv geen succes oplevert, zoals hierboven omschreven, bestaat nog de mogelijkheid om de bevoegdheid tot netwerkzoeking ex artikel 125j Sv toe te passen om onderzoek te doen naar gegevens op 'elders aanwezige geautomatiseerde werken'.[153] Evenals de doorzoeking ter vastlegging van gegevens is dit geen heimelijke opsporingsbevoegdheid en geldt het dus als minder inbreukmakend dan het heimelijk binnendringen in een geautomatiseerd werk. Toepassing van deze bevoegdheid kan in beginsel leiden tot verkrijging van dezelfde gegevens als door middel van het binnendringen in geautomatiseerde werken: met beide bevoegdheden kan technisch gezien toegang worden verkregen tot harde schijven en cloudservers en de daar door de verdachte verwerkte of opgeslagen gegevens. De memorie van toelichting noemt als bezwaar de omstandigheid dat de verdachte door de netwerkzoeking op de hoogte raakt van het onderzoek, hetgeen strijdig kan zijn met het belang van het onderzoek.[154] Dit argument snijdt hout: in bepaalde gevallen kan de noodzaak bestaan om in de opsporing heimelijk te werk te gaan, zo kan onder andere worden afgeleid uit het bestaan van de heimelijke opsporingsbevoegdheden in het Wetboek van Strafvordering. Om die reden kan de bevoegdheid tot netwerkzoeking niet in zijn algemeenheid als subsidiair alternatief gelden voor een hackbevoegdheid bij het vergaren van gegevens die in de cloud zijn opgeslagen.

Onderscheppen van gegevensverkeer

Een interessant laatste alternatief is het toepassen van de bevoegdheid tot het aftappen van telecommunicatie ex artikel 126m Sv om data te onderscheppen terwijl het 'onderweg' is naar de cloud om daar opgeslagen te worden.[155] In beginsel komen op die wijze opgeslagen gegevens over de internettap. Hiermee worden de geconstateerde problemen van onzichtbaarheid en '*loss of location*' omzeild. Toepassing van de bevoegdheid ex artikel 126m Sv op deze wijze maakt in zijn algemeenheid een minder zware inbreuk op de persoonlijke levenssfeer dan het binnendringen op een harde schijf. Alleen van die gegevens die gedurende de looptijd van het bevel in de cloud worden opgeslagen of daaruit worden opgehaald wordt kennis genomen; van reeds in de cloud of op de harde schijf opgeslagen gegevens niet. Het onderscheppen van gegevens die naar de cloud worden verstuurd wordt echter belemmerd door de mogelijkheid om deze gegevens te versleutelen.[156] In dat geval zijn de onderschepte gegevens niet begrijpelijk en ontsleuteling is zonder hackbevoegdheid doorgaans niet mogelijk (zie paragraaf 2). Om die reden zijn de mogelijkheden voor toepassing van artikel 126m Sv om gegevens te onderscheppen die naar de cloud worden verstuurd te beperkt om als subsidiair alternatief voor een hackbevoegdheid te gelden.

[153] De gebruiker van het geautomatiseerde werk zal immers in beginsel toestemming hebben van de cloudaanbieder om zich toegang te verschaffen tot deze gegevens, waarmee aan het vereiste van het tweede lid van artikel 125j Sv is voldaan.
[154] MvT, p. 10.
[155] Zie Koops e.a. 2012, p. 41 – 42. De bevoegdheid ex artikel 126m Sv ziet immers op 'gegevensverkeer', waaronder ook valt het downloaden of opslaan van gegevens; zie ook *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 80.
[156] Zie Koops e.a. 2012, p. 45 – 46.

§ 5. Subsidiaire alternatieven bij anonimiteit

Aftappen van telecommunicatie

In beginsel bestaat de mogelijkheid om de communicatie die via een vals IP-adres (van bijvoorbeeld een *anonymous proxy* of VPN-dienst) wordt verstuurd en op dat adres wordt ontvangen af te tappen met toepassing van de bevoegdheid ex artikel 126m Sv en zo uit de communicatie trachten af te leiden wat de werkelijke identiteit en/of locatie van het geautomatiseerde werk en eventueel de verdachte is. De frequente combinatie van anonimiteit en versleuteling zorgt er echter voor dat het aftappen van telecommunicatie doorgaans geen informatie zal opleveren omtrent de identiteit of locatie: versleuteling maakt de inhoud van de communicatie onbegrijpelijk, door anonimiseringstechnieken leveren de bijbehorende verkeersgegevens (*metadata*) daarnaast ook niet het juiste IP-adres op.[157] Bovendien is mijns inziens het aftappen van telecommunicatie ex artikel 126m Sv op zichzelf niet minder inbreukmakend dan het binnendringen in een geautomatiseerd werk enkel ter vaststelling van de identiteit of locatie van een verdachte of een geautomatiseerd werk: met de vaststelling van de identiteit of locatie wordt immers niet van méér informatie omtrent het privéleven kennis genomen dan bij het aftappen van telecommunicatie. Deze optie geldt dan ook niet als subsidiair alternatief voor een hackbevoegdheid.

Vorderen en verzoeken van gegevens (IP-adres)

Op basis van artikel 126n of 126na Sv kan bij een ISP een vordering tot verstrekking van gebruikersgegevens (waaronder een IP-adres) worden ingesteld, om op basis daarvan de identiteit of locatie van een verdachte of een geautomatiseerd werk vast te stellen. Het vorderen van gegevens is de bevoegdheid die de minste inbreuk op de persoonlijke levenssfeer maakt wanneer het gaat om het vergaren van gegevens.[158] Een dergelijke vordering loopt echter tegen de belemmering op dat een ISP geen gebruikersgegevens heeft bij het valse adres en dus geen informatie kan geven over de gebruiker van dat adres. Een andere optie zou zijn om de betreffende gegevens te vorderen bij de anonimiseringsdienst die het IP-adres van de verdachte afschermt. Op basis van artikel 126nc Sv kan bij Nederlandse diensten een vordering tot verstrekking van identificerende gegevens van een gebruiker, waaronder het IP-adres van zijn geautomatiseerde werk, worden ingesteld.[159] Een rechtstreeks verzoek tot verstrekking van identificerende gegevens kan tevens worden ingesteld bij buitenlandse aanbieders van anonimiseringsdiensten op basis van artikel 32 onder b CCV, mits de aanbieder is gevestigd in een verdragsstaat.[160] De kans van slagen van een vordering of een rechtstreeks verzoek valt echter te betwijfelen. Naar verwachting zal de kans vrij klein zijn dat het IP-adres van de gezochte gebruiker bij de betreffende aanbieder is opgeslagen en dus überhaupt kan worden verstrekt; dit geldt zowel ten aanzien van Nederlandse als buitenlandse aanbieders.[161] Een buitenlandse aanbieder heeft daarnaast geen verplichting tot

[157] Hierbij speelt mee dat personen die anonimiseringstechnieken toepassen doorgaans ook gebruik maken van versleuteling.
[158] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.
[159] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7. Het IP-adres wordt niet expliciet genoemd maar moet, gezien hetgeen in paragraaf 3 van hoofdstuk 3 is overwogen, worden beschouwd als een identificerend gegeven, net als een huisadres.
[160] Artikel 32 onder b CCV spreekt van opgeslagen 'computergegevens'; de definitie van artikel 1 sub b CCV laat voldoende ruimte om hieronder ook IP-adressen te scharen.
[161] Zie wat betreft VPN-diensten de resultaten van een (niet-wetenschappelijke) survey uit 2011: <http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/>.

verstrekking van gegevens en moet hiermee zelf instemmen. Een aanzienlijk deel van de aanbieders die wel gebruikersgegevens bewaren zullen deze naar verwachting niet op vrijwillige basis verstrekken.[162] Tot slot valt te betwijfelen of de buitenlandse aanbieders 'gerechtigd' zijn in de zin van artikel 32 onder b CCV om de gegevens te verstrekken.[163]
Wanneer de aanbieders niet meewerken, kan een rechtshulpverzoek worden ingesteld bij de staat die rechtsmacht heeft over de aanbieder in kwestie. Echter valt niet in zijn algemeenheid te zeggen dat een rechtshulpverzoek een grote kans van slagen zal hebben. Staten die zijn aangesloten bij het Cybercrimeverdrag zullen hier meestal (maar niet altijd) wel gehoor aan geven; bij niet-verdragsstaten zal die kans kleiner zijn.[164] Het grootste bezwaar is evenwel ook bij een rechtshulpverzoek dat de gevorderde informatie veelal niet zal zijn opgeslagen bij de betreffende aanbieder en dus überhaupt niet kan worden verstrekt.[165]
Wat betreft het Tor-netwerk geldt een aparte situatie. Het netwerk wordt geheel gerund door vrijwillige particulieren en het verkeer binnen dit netwerk is onzichtbaar totdat het bij de *exit relay* naar buiten komt.[166] Ook de beheerders van de *exit relays* zijn vrijwillige particulieren die in beginsel geen gebruikersgegevens registreren.[167] Noch een rechtstreeks verzoek noch een vordering via een rechtshulpverzoek zal dan ook effect sorteren.
Gezien het bovenstaande kan het vorderen van gebruikersgegevens of identificerende gegevens niet consequent een oplossing bieden voor het probleem van anonimiteit en de betreffende bevoegdheden vormen derhalve geen subsidiair alternatief voor een hackbevoegdheid.

Observatie, infiltratie, inwinnen van informatie
Voor het vaststellen van de locatie en/of identiteit van een geautomatiseerd werk en/of een verdachte die wordt verborgen door anonimiseringstechnieken, zou ook gedacht kunnen worden aan stelselmatige observatie, infiltratie en het stelselmatig inwinnen van informatie. Mijns inziens maken deze bevoegdheden echter niet minder inbreuk op het recht op privéleven dan het binnendringen in een geautomatiseerd werk ten behoeve van de bepaling van de identiteit en locatie van het geautomatiseerde werk en de gebruiker. Met toepassing van de bevoegdheid tot observatie ex artikel 126g Sv kan immers een 'min of meer volledig beeld van bepaalde aspecten van iemands leven [worden] verkregen'.[168] Bij toepassing van infiltratie op basis van artikel 126h Sv en het stelselmatig inwinnen van informatie ex artikel 126j Sv kan eveneens de persoonlijke levenssfeer van betrokkenen in het geding komen.[169] Toepassing van een van deze bevoegdheden kan een breder beeld geven van de persoonlijke levenssfeer van de betrokkene(n) dan de enkele vaststelling van de locatie en/of identiteit van

[162] Zie bijvoorbeeld de reacties van de VPN-diensten in het genoemde onderzoek *supra* noot 161. Wat betreft de anonieme proxyservers geeft een deel in de *privacy policy* aan wel gegevens te verstrekken in geval van bijvoorbeeld misbruik en geeft het andere deel aan geen persoonlijke informatie te bewaren en/of geen persoonlijke informatie aan derden te verstrekken.
[163] Vgl. *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 25 – 26. Anonimiseringsdiensten staan in een wat andere verhouding tot de persoonlijke informatie van hun gebruikers dan communicatieaanbieders.
[164] Vgl. Koops e.a. 2012, p. 39 – 40.
[165] Zie opnieuw het onderzoek *supra* noot 161. Alle VPN-diensten respecteren een rechterlijk bevel tot verstrekking van gebruikersgegevens, maar kunnen hier alleen daadwerkelijk gevolg aan geven als die gegevens ook (nog) opgeslagen zijn.
[166] Zie ook het schema op <https://www.torproject.org/about/overview.html.en>.
[167] Zie <https://www.torproject.org/eff/tor-legal-faq.html.en>.
[168] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26.
[169] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 30 respectievelijk *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 34.

het geautomatiseerde werk en/of de verdachte. Hiermee kunnen zij in ieder geval niet in de regel worden beschouwd als subsidiaire alternatieven ten opzichte van een hackbevoegdheid.

Voor de bevoegdheid tot het bepalen van de identiteit en/of locatie van een smartphone middels een softwareapplicatie om stelselmatige observatie mogelijk te maken, kan een alternatief worden gezocht in de reeds bestaande technische hulpmiddelen voor stelselmatige observatie als vastgelegd in lid 3 van artikel 126g Sv. Zolang de hackbevoegdheid echter enkel ziet op het verrichten van een locatiebepaling maakt het geen zwaardere inbreuk op de persoonlijke levenssfeer dan de bestaande bevoegdheid om technische hulpmiddelen toe te passen. De enkele vaststelling van de locatie van een persoon is op zichzelf geen stelselmatige observatie, en wordt derhalve niet beschouwd als een (ernstige) inbreuk op de persoonlijke levenssfeer.[170] De stelselmatige observatie ex artikel 126g Sv die vervolgens na de locatiebepaling kan worden toegepast maakt dezelfde inbreuk als elke stelselmatige observatie; dat van tevoren is binnengedrongen op de smartphone van de geobserveerde verandert op zichzelf niets aan de mate van inbreuk. Wel is het mogelijk dat bijvoorbeeld het activeren van de GPS ertoe leidt dat de bewegingen van de verdachte dusdanig nauwkeurig kunnen worden gevolgd dat wel sprake is van stelselmatige observatie.[171] Nog steeds is de inbreuk in dat geval echter niet zwaarder dan enige andere toepassingswijze van stelselmatige observatie; met bijvoorbeeld IMSI catchers, die op basis van artikel 126g lid 3 Sv kunnen worden ingezet, kunnen de bewegingen ook nauwkeurig worden gevolgd.

§ 6. Conclusie

Praktisch gezien zijn er geen alternatieve opsporingsbevoegdheden beschikbaar die met een minder zware inbreuk op de persoonlijke levenssfeer consequent de geconstateerde complicaties in de opsporing kunnen doorbreken of omzeilen. Om vast te kunnen stellen of de opsporing daarom ook een dringend belang heeft bij de invoering van een bevoegdheid tot het binnendringen in een geautomatiseerd werk, rest nog de vraag of een hackbevoegdheid daadwerkelijk geschikt en effectief is om de geconstateerde problematiek het hoofd te bieden: de toets van het relevantiecriterium, uit te voeren in het volgende hoofdstuk.

Een belangrijke kanttekening bij de subsidiariteit van de hackbevoegdheid is dat de algemene subsidiariteit met het oog op artikel 8 lid 2 EVRM niet betekent dat toepassing in concreto van deze opsporingsbevoegdheid automatisch voldoet aan het subsidiariteitsvereiste. Bij elke toepassing van de hackbevoegdheid moet worden afgewogen of toepassing van een of meer van de in dit hoofdstuk uiteengezette alternatieven in het concrete geval wél dezelfde resultaten kan bereiken als het binnendringen in een geautomatiseerd werk. Dit zal in beginsel in ieder geval zo zijn wanneer zich in een opsporingsonderzoek niet een van de verschijnselen van versleuteling, gebruik van draadloze netwerken, cloud computing en anonimiseringstechnieken voordoet. Aan dit punt zal in hoofdstuk 7 nog enig belang toekomen.

[170] Vgl. *Kamerstukken I* 1998/99, 25 403 en 23 251, nr. 119b, p. 1.
[171] Zie MvT, p. 20.

Hoofdstuk 5: Het dringende belang van de opsporing: relevantie van een hackbevoegdheid

§ 1. Inleiding

De opsporing kan geen dringend belang hebben bij de invoering van een hackbevoegdheid als deze bevoegdheid geen effectieve bijdrage levert aan de oplossing van de in hoofdstuk 3 geconstateerde problemen voor de opsporing. De hackbevoegdheid doorstaat dan immers niet de relevantietoets als genoemd in paragraaf 3 van hoofdstuk 2 en kan dan niet noodzakelijk worden geacht in de zin van artikel 8 lid 2 EVRM. In dit hoofdstuk zal wederom het in het conceptwetsvoorstel Computercriminaliteit III voorgestelde artikel 125ja Sv als uitgangspunt worden genomen, om een concrete basis te bieden voor toetsing van de relevantie van een hackbevoegdheid.

Benadrukt zij dat in het kader van het relevantiecriterium niet voldoende is dat een hackbevoegdheid een bijdrage levert aan de opsporing van strafbare feiten in het algemeen. Dát een hackbevoegdheid dit doel kan bereiken zal niet tot veel discussie leiden, maar daarmee is mijns inziens slechts nog voldaan aan het '*legitimate aim*' vereiste van artikel 8 lid 2 EVRM. De toets aan het relevantiecriterium is strenger en meer specifiek: om deze toets te doorstaan moet de voorgestelde bevoegdheid tot het binnendringen in een geautomatiseerd werk effectief zijn en een bijdrage leveren aan de oplossing van de specifieke problemen veroorzaakt in de opsporing door versleuteling, gebruik van draadloze netwerken, cloud computing en anonimiseringstechnieken.[172] Het EHRM voert deze toets zelden zo indringend uit als hierboven geformuleerd, en laat deze in het kader van heimelijke opsporingsbevoegdheden vanwege de *margin of appreciation* zelfs helemaal achterwege. De taakverdeling die het EHRM stelt, zoals besproken in paragraaf 4 van hoofdstuk 2, vereist echter dat op nationaal niveau wel op de meest indringende wijze wordt getoetst. Enkel als aan deze indringende toetsing is voldaan, is er sprake van relevantie van een hackbevoegdheid in de zin van artikel 8 lid 2 EVRM en is er sprake van een dringend belang van de opsporing bij de invoering van een hackbevoegdheid.

Aangezien de hackbevoegdheid in Nederland nog moet worden ingevoerd zijn er nog geen resultaten van deze bevoegdheid beschikbaar die kunnen bevestigen wat de daadwerkelijke relevantie van een hackbevoegdheid is in de praktijk van de opsporing. De AIVD en de MIVD beschikken op grond van artikel 24 van de Wiv 2002 weliswaar over een bevoegdheid om te hacken, maar de resultaten van toepassing hiervan zijn niet publiekelijk bekend.[173] Ook uit het buitenland zijn vrijwel geen resultaten bekend. In Duitsland bestaat wel een

[172] Zie Vande Lanotte 2005, p. 142 voor het subtiele maar belangrijke verschil tussen de legitieme doel-toets en de toets aan het relevantiecriterium. Zie ook Arai-Takahashi 2002, p. 87 en Van Dijk e.a. 2006, p. 341, die weliswaar stellen dat de relevantietoets in het algemeen geen problemen oplevert gezien het nauwe verband met de voorafgaande legitieme doel-toets, maar hiermee impliceren dat dit vooral wordt veroorzaakt door de wijze van toetsing van het Hof en niet zozeer doordat de twee vereisten daadwerkelijk dezelfde maatstaf hanteren.

[173] Overigens zouden die resultaten niet één op één bruikbaar zijn in het beoordelen van de relevantie van hacken als opsporingsbevoegdheid, aangezien de bevoegdheid van de AIVD en de MIVD niet ten behoeve van de opsporing van strafbare feiten bestaat.

hackbevoegdheid voor het *Bundeskriminalamt*, maar de weinige bekende cijfers daaromtrent zijn zo algemeen dat hieruit geen zinvolle conclusie omtrent de bijdrage van een hackbevoegdheid in opsporingsonderzoeken kan worden getrokken.[174] Van het Verenigd Koninkrijk is enkel bekend dat door politie wordt gehackt, de resultaten zijn echter niet voorhanden.[175] Van Frankrijk en de Verenigde Staten zijn helemaal geen gegevens beschikbaar omtrent hacken door opsporingsambtenaren, al bestaat de bevoegdheid hiertoe in beide staten wel.[176] Vooralsnog zijn er dan ook nagenoeg geen resultaten om als aanknopingspunt te dienen voor de relevantie van een hackbevoegdheid in de praktijk en moeten conclusies hieromtrent worden gebaseerd op prognoses.

§ 2. Effectiviteit

Alvorens in de volgende paragrafen over te gaan tot de beoordeling van de bijdrage die een hackbevoegdheid kan leveren bij de oplossing van de specifieke problemen in de opsporing, behandel ik in deze paragraaf het vereiste van algemene effectiviteit van de hackbevoegdheid. Het vereiste van effectiviteit is dusdanig nauw met het relevantiecriterium verbonden dat ik ze in het kader van dit onderzoek gezamenlijk behandel onder de vraag naar de relevantie van een hackbevoegdheid.[177]

Voor effectiviteit is vereist dat het overheidsoptreden waarmee inbreuk wordt gemaakt op het recht op privacy, überhaupt geschikt is voor het nastreven van het algemene doel van de opsporing van strafbare feiten.[178] In dit licht bezien is het de vraag of opsporingsambtenaren met toepassing van de hackbevoegdheid wel daadwerkelijk met acceptabele frequentie kunnen binnendringen in de betreffende geautomatiseerde werken. Hierbij treedt de technische complicatie op dat de beveiliging die criminele hackers en malware buiten de digitale deur moet houden, in beginsel ook hackpogingen door opsporingsambtenaren kan tegenhouden.[179] In de memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III wordt ook erkend dat een geautomatiseerd werk zodanig beveiligd kan zijn dat het niet lukt om binnen te dringen.[180] Tevens kunnen hacktechnieken en –software die op een bepaald *operating system* binnen kunnen dringen, machteloos staan tegenover een van de vele andere besturingssystemen die op een willekeurig geautomatiseerd werk geïnstalleerd kunnen zijn.[181] De vraag is of deze omstandigheden leiden tot een dusdanige beperking van een hackbevoegdheid dat moet worden geconcludeerd dat sprake is van ineffectiviteit in het licht van artikel 8 lid 2 EVRM. Het effectiviteitsvereiste komt zelden

[174] Zie <http://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html?_r=2&>.
[175] Vgl. <http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html>.
[176] In Frankrijk is deze bevoegdheid vastgelegd in artikel 706-102-1 van de *Code de Procédure Pénal*. In de Verenigde Staten kan de bevoegdheid (mede) worden gebaseerd op de *Fourth Amendment* van de *Constitution*; zie Brenner 2012, p. 54.
[177] Vgl. Gerards 2011, p. 156.
[178] Zie Gerards 2011, p. 156 en vgl. EHRM 18 mei 2004, nr. 58148/00 (*Éditions Plon/France*), § 53.
[179] Zie Oerlemans 2011, p. 892; Jacobs 2012, p. 2764.
[180] MvT p. 26. In de memorie van toelichting wordt niet gerefereerd aan de mogelijkheid om ontwikkelaars van antivirussoftware te verzoeken om uitzonderingen te maken voor politiesoftware. Uit de stelling dat het 'niet uitgesloten' is dat een geautomatiseerd werk vanwege de beveiliging niet kan worden binnengedrongen, lijkt te kunnen worden afgeleid dat dergelijke verzoeken momenteel geen onderdeel vormen van de plannen.
[181] Zie Oerlemans 2011, p. 892.

expliciet in de rechtspraak van het EHRM aan bod. Hierdoor is het lastig om een concreet percentage of ander minimumvereiste te plakken op de frequentie waarmee opsporingsambtenaren daadwerkelijk op geautomatiseerde werken moeten kunnen binnendringen. Voor daadwerkelijke ineffectiviteit is mijns inziens echter noodzakelijk dat toepassing van de hackbevoegdheid een onacceptabel lage succesratio heeft ten aanzien van het binnendringen in een geautomatiseerd werk, met inachtneming van de negatieve gevolgen voor het privéleven die ondanks (of juist vanwege) de mislukte hackpogingen ontstaan door beschadiging van geautomatiseerde werken en/of het openen van beveiligingslekken.[182] Van een dusdanig lage succesratio zal volgens mij geen sprake zijn. De beperkte statistieken die bekend zijn uit het buitenland laten zien dat de autoriteiten bij hackactiviteiten niet op grote schaal worden belemmerd door beveiliging van de geautomatiseerde werken waarop wordt binnengedrongen, al moet de gebruikte software vooralsnog van private derde partijen worden gekocht.[183] De technische kennis bij politie en justitie is nog verre van optimaal, maar hier wordt wel veel aandacht aan besteed en in geïnvesteerd.[184] Ik acht het dan ook redelijk om er als prognose van uit te gaan dat de politie in staat zal zijn om een dusdanige succesratio bij het binnendringen in geautomatiseerde werken te bereiken dat de hackbevoegdheid voldoet aan het effectiviteitsvereiste. Hierbij is dan wel van belang om de hackbevoegdheid goed te evalueren en na te gaan of deze daadwerkelijk aan het effectiviteitsvereiste voldoet: is de succesratio van het binnendringen in een geautomatiseerd werk in de praktijk zodanig dat dit opweegt tegen de negatieve gevolgen voor het recht op privéleven die voortvloeien uit mislukte hackpogingen?

§ 3. Bijdrage aan de oplossing van problemen in de opsporing

§ 3.1. Ten aanzien van versleuteling van elektronische gegevens

Versleuteling van opgeslagen gegevens

Met de voorgestelde bevoegdheid tot het binnendringen in een geautomatiseerd werk met het oog op het overnemen van gegevens kunnen op de harde schijf opgeslagen sleutels, te weten wachtwoorden en andere inloggegevens, worden overgenomen. Deze gegevens kunnen worden overgenomen door spyware op het geautomatiseerde werk te installeren, bijvoorbeeld een ‘keylogger’ die toetsaanslagen registreert. Hiermee komen de sleutels ter beschikking van de opsporingsambtenaren en kunnen de gegevens die (in ieder geval potentieel) informatie opleveren ten behoeve van de opsporing weer begrijpelijk en bruikbaar worden gemaakt.[185]

[182] Vgl. EHRM 18 mei 2004, nr. 58148/00 (*Éditions Plon/France*), § 53 en Jacobs 2012, p. 2763 – 2764.
[183] Zie bijvoorbeeld <http://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html?_r=2&>; destijds (in 2011) gebruikte de Duitse overheid software van DigiTask, een Duits softwarebedrijf. In afwachting van de ontwikkeling van eigen software, die eind 2014 gereed zou moeten zijn, heeft de Duitse overheid nieuwe software gekocht van een andere private derde partij: zie <http://pastebin.com/0twgvkZD > en <https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/>.
[184] Vgl. o.a. Stol, Leukfeldt & Klap 2012, p. 37; *Kamerstukken II* 2012/13, 26 643, nr. 285 (bijlage), p. 56 – 57 (Cybersecuritybeeld Nederland 3).
[185] Zie MvT, p. 16; Koops e.a. 2012, p. 47; Oerlemans 2011, p. 907.

Versleuteling van internetcommunicatie

Bij toepassing van de hackbevoegdheid met het oog op een bevel tot het aftappen en opnemen van telecommunicatie ex artikel 126m Sv kunnen opsporingsambtenaren spyware plaatsen om internetcommunicatie te onderscheppen vóórdat deze wordt versleuteld en vervolgens verstuurd, of juist nádat de communicatie is ontvangen en vervolgens ontsleuteld.[186] Wanneer de bevoegdheid wordt toegepast met het oog op een bevel tot het opnemen van vertrouwelijke communicatie ex artikel 126l Sv kan eenzelfde effect worden bereikt met softwareapplicaties die op afstand de microfoon van een computer kunnen aanzetten om VoIP-gesprekken af te luisteren.[187] Met deze wijze van aftappen en/of opnemen 'op het apparaat' wordt de versleuteling van de communicatie omzeild, waardoor de inhoud van de communicatie begrijpelijk wordt en informatie kan opleveren ten behoeve van het opsporingsonderzoek.

Benadrukt moet worden dat de relevantie van een hackbevoegdheid alleen geldt ten aanzien van *versleutelde* communicatie. Het binnendringen in een geautomatiseerd werk om vervolgens middels het activeren van bijvoorbeeld een microfoonfunctionaliteit 'face-to-face' gesprekken tussen personen in dezelfde ruimte af te luisteren, voldoet dan ook niet aan het relevantiecriterium aangezien in deze gesprekken naar de aard geen versleuteling (en ook geen van de overige in dit onderzoek behandelde problemen) optreedt. Onduidelijk is of het voorgestelde artikel 125ja lid 1 aanhef en onder d Sv mede beoogt face-to-face gesprekken te kunnen afluisteren. De commentaren op het conceptwetsvoorstel lijken (impliciet) wel aan te nemen dat een dergelijke toepassing wordt beoogd.[188] Voor zover dit daadwerkelijk het geval is, is het voorgestelde artikel 125ja lid 1 aanhef en onder d Sv in zoverre ontoelaatbaar, aangezien het de relevantietoets niet kan doorstaan en dus niet noodzakelijk is in een democratische samenleving in de zin van artikel 8 lid 2 EVRM.

§ 3.2. Ten aanzien van gebruik van draadloze netwerken

Het probleem dat gebruik van draadloze netwerken veroorzaakt voor de opsporing is dat de aftapbevoegdheid ex artikel 126m Sv niet effectief kan worden toegepast. Een internettap dient geplaatst te worden 'op' een IP-adres en tapt dan alleen de communicatie af die via dat IP-adres wordt gevoerd; internetcommunicatie die met hetzelfde geautomatiseerde werk maar via een ander IP-adres wordt gevoerd, komt niet over die tap. Wanneer een verdachte zijn communicatieverkeer over meerdere IP-adressen verspreidt blijft dan ook een deel van zijn communicatie verborgen wanneer niet alle IP-adressen bij de opsporingsdiensten bekend zijn en (derhalve) niet op alle IP-adressen een tap is geplaatst.[189] Voor de relevantievraag is derhalve allereerst van belang of het door opsporingsambtenaren binnendringen in een geautomatiseerd werk ertoe kan leiden dat de IP-adressen bekend worden.

Middels het binnendringen in een geautomatiseerd werk kan het IP-adres van het geautomatiseerde werk worden geregistreerd, zoals ook beoogd met het voorgestelde artikel

[186] Zie MvT, p. 8; Boek 2000, p. 591; Oerlemans 2011, p. 907.
[187] Zie MvT, p. 19 en p. 26.
[188] Zie Oerlemans 2013, p. 240; vgl. Engelfriet 2013.
[189] Zie ook Oerlemans 2012, p. 21 en p. 30 – 31.

125ja lid 1 aanhef en onder a Sv.[190] Op deze manier kan het probleem dat een geautomatiseerd werk van een verdachte gebruik maakt van meerdere verschillende IP-adressen, waardoor niet alle 'identiteiten' van het geautomatiseerde werk bekend zijn, worden omzeild door binnen te dringen in het geautomatiseerde werk en telkens het IP-adres te registreren dat het geautomatiseerde werk krijgt toegekend bij verbinding met een draadloos netwerk. De vaststelling van (in ieder geval één van) de IP-adressen biedt de mogelijkheid tot het aftappen van telecommunicatie 'op het apparaat', waardoor de problematiek van de verspreiding van internetverkeer over meerdere IP-adressen volledig wordt omzeild en het volledige internetverkeer van een verdachte kan dienen als informatie ten behoeve van het opsporingsonderzoek.

§ 3.3. Ten aanzien van cloud computing

Cloud computing leidt tot verschuiving van gegevensopslag van de harde schijf van het geautomatiseerde werk van de gebruiker naar een cloudserver, waardoor de problemen van onzichtbaarheid van gegevens en van '*loss of location*' ontstaan, zo is in hoofdstuk 3 vastgesteld. De gegevens bevinden zich dan alleen op de harde schijf van het geautomatiseerde werk wanneer de verdachte deze uit de cloud ophaalt om op zijn geautomatiseerde werk te verwerken. Een hackbevoegdheid kan voor dit probleem een oplossing bieden door opsporingsambtenaren de mogelijkheid te geven gedurende een bepaalde periode op de harde schijf van het geautomatiseerde werk 'aanwezig' te zijn zodat zij gegevens kunnen overnemen wanneer de verdachte deze vanuit de cloud ophaalt. De bevoegdheid hiertoe is ook opgenomen in het voorgestelde artikel 125ja Sv: gegevens die op het geautomatiseerde werk worden verwerkt gedurende de duur van toepassing van de hackbevoegdheid mogen worden overgenomen.[191] Op deze manier kunnen de gegevens die gedurende hun opslag in de cloud onzichtbaar en niet traceerbaar zijn, toch worden overgenomen.

Een andere oplossing die een hackbevoegdheid zou kunnen bieden, en die eveneens in het voorgestelde artikel 125ja Sv is inbegrepen, is het binnendringen van een cloudserver zodat opsporingsambtenaren de gegevens rechtstreeks vanuit die cloudserver kunnen overnemen.[192] Met deze toepassing hoeven de opsporingsambtenaren niet te wachten tot de verdachte de gegevens uit de cloud ophaalt (hoogstens om de cloudaanbieder vast te kunnen stellen). Ook op deze wijze zouden de onzichtbaarheid van gegevens en de '*loss of location*' worden omzeild. De rechtsmachtproblematiek verbonden aan deze toepassing valt buiten het bereik van dit onderzoek.[193]

Hoe dan ook zorgen de beide genoemde toepassingen van een hackbevoegdheid ervoor dat de onzichtbaarheid van gegevens en de '*loss of location*', veroorzaakt door het gebruik van cloud

[190] Zie MvT, p. 15.
[191] Zie MvT, p. 16.
[192] Zie MvT, p. 12.
[193] Een korte blik op de literatuur leert dat de discussie hieromtrent nog volop woedt, maar dat er wel tendensen zichtbaar zijn richting toelaatbaarheid van grensoverschrijdende toepassing van opsporingsbevoegdheden in cyberspace.

computing, worden omzeild. Hiermee voldoet de hackbevoegdheid aan het relevantiecriterium ten aanzien van het probleem van cloud computing.

§ 3.4. Ten aanzien van anonimiteit

Middels het binnendringen in een geautomatiseerd werk kan het IP-adres van het geautomatiseerde werk worden vastgesteld. Dit resultaat kan ook worden bereikt wanneer het IP-adres in kwestie is verborgen middels gebruik van anonimiseringstechnieken. Met het IP-adres kan tevens de locatie van het geautomatiseerde werk worden gevonden. Kennis van het IP-adres biedt derhalve informatie op basis waarvan verdere strafvorderlijke bevoegdheden kunnen worden toegepast, zoals het plaatsen van een internettap op dat IP-adres (of 'op het apparaat') met toepassing van de bevoegdheid ex artikel 126m Sv. Gezien het doel van anonimiteit op internet, namelijk het voorkomen van verspreiding van persoonlijke informatie over de betreffende internetgebruiker, zal vaak ook de identiteit en de locatie van de gebruiker/verdachte door anonimiseringstechnieken worden verborgen. Hiervan zal naar de aard vooral sprake zijn in het geval van cybercriminaliteit en kinderporno. Met name in die gevallen kan het bepalen van het IP-adres van het geautomatiseerde werk derhalve tevens leiden tot informatie over de identiteit en de locatie van de gebruiker c.q. verdachte.

In hoofdstuk 3 is opgemerkt dat het probleem van anonimiteit ook toepasselijk is op de afscherming van smartphones en tablets om de uitvoering van stelselmatige observatie te belemmeren. Aangezien smartphones en tablets ook geautomatiseerde werken zijn, kan hierop middels een hackbevoegdheid eveneens worden binnengedrongen, waarna er mogelijkheden bestaan om de locatie van het geautomatiseerde werk en daarmee in beginsel van de gebruiker/verdachte vast te stellen. Deze mogelijkheid wordt ook geboden met het voorgestelde artikel 125ja lid 1 aanhef en onder e Sv, dat de bevoegdheid inhoudt om op afstand software te installeren op een smartphone of een tablet zodat de GPS-functie kan worden geactiveerd en zo de locatiegegevens kunnen worden doorgegeven. Tevens kan bijvoorbeeld na het binnendringen worden geobserveerd welke Wi-Fi netwerken op een bepaald moment zichtbaar zijn op de smartphone of tablet om aan de hand hiervan een locatiebepaling te verrichten.[194] Op genoemde wijzen kan een hackbevoegdheid een bijdrage leveren aan het omzeilen van anonimiseringstechnieken bij het gebruik van smartphones en tablets en zo de vervolgtoepassing van stelselmatige observatie faciliteren. In zoverre voldoet ook deze toepassing aan het relevantiecriterium. Opgemerkt zij dat voor relevantie wel vereist is dat de stelselmatige observatie daadwerkelijk door anonimiseringstechnieken wordt belemmerd. Wanneer dit op andere wijze plaatsvindt, zoals in het voorbeeld in de memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III van de verdachte die een observatieteam voortdurend weet af te schudden, wordt niet voldaan aan het relevantiecriterium.[195]

Om dezelfde reden is ook niet toegestaan dat met de hackbevoegdheid een webcam en/of een in het geautomatiseerde werk ingebouwde camera wordt geactiveerd om personen te

[194] Zie MvT, p. 20.
[195] Vgl. MvT, p. 20.

identificeren en te observeren: hiermee wordt immers de overstap gemaakt van het enkele vaststellen van de locatie van een verdachte naar de daadwerkelijke fysieke observatie. De fysieke observatie ondervindt na het vaststellen van de locatie echter geen hinder meer van het probleem van anonimiseringstechnieken (of een van de andere in het kader van dit onderzoek behandelde verschijnselen). De memorie van toelichting bij het conceptwetsvoorstel Computercriminaliteit III *lijkt* mijns inziens ook zo geïnterpreteerd te moeten worden dat het voorgestelde artikel 125ja lid 1 aanhef en onder e Sv slechts beoogt stelselmatige observatie mogelijk te maken door een locatiebepaling van de te observeren persoon te verrichten.[196] Mocht het op afstand aanzetten van een webcam of ingebouwde camera echter wel beoogd zijn, dan zou deze wijze van toepassing dus niet voldoen aan het relevantiecriterium en in zoverre niet toelaatbaar zijn.

§ 4. Conclusie: de relevantie van een hackbevoegdheid

Hoewel er weinig tot geen empirische resultaten beschikbaar zijn van de resultaten van toepassing van een hackbevoegdheid, is de prognose van de effectiviteit en relevantie van een bevoegdheid tot het binnendringen in een geautomatiseerd werk mijns inziens voldoende positief. Mogelijk zal de toepassing in ieder geval aanvankelijk nog tegen enkele technische barrières oplopen waardoor geautomatiseerde werken niet kunnen worden binnengedrongen, maar de beperkte statistieken uit het buitenland en de inspanningen in het binnenland wekken de verwachting dat de technische beperkingen van een hackbevoegdheid praktisch gezien geen onoverkomelijke belemmering zullen vormen. Er van uitgaande dat de hackbevoegdheid bij toepassing in staat is de eerste horde te nemen, te weten het binnendringen in een geautomatiseerd werk, biedt deze bevoegdheid in zijn verschillende mogelijke modaliteiten een oplossing voor een of meer van de problemen veroorzaakt door versleuteling, gebruik van draadloze netwerken, cloud computing en/of anonimiseringstechnieken.

§ 5. Conclusie: het dringende belang van de opsporing

Vanwege de omvang van de problemen die door de technologische ontwikkelingen in de opsporing van strafbare feiten worden veroorzaakt, het gebrek aan subsidiaire alternatieven en de (verwachte) mogelijkheden van een hackbevoegdheid om een oplossing te bieden voor de problemen, kom ik tot de conclusie dat de opsporingspraktijk een dringend belang heeft bij de invoering van een bevoegdheid tot het binnendringen in een geautomatiseerd werk. Er is derhalve sprake van een *pressing social need* in de Nederlandse maatschappij. Dit standpunt ligt ook ten grondslag aan het conceptwetsvoorstel Computercriminaliteit III.[197] Op basis van artikel 8 lid 2 EVRM is vervolgens de vraag aan de orde hoe de belangen van de Nederlandse burgers bij waarborging van hun recht op bescherming van de persoonlijke levenssfeer zich hiertegen verhouden, hetgeen in de volgende hoofdstukken uitgebreid aan bod komt.

[196] Zie MvT, p. 20 – 21. Aldus ook Korteweg 2013, p. 14. Anders: Engelfriet 2013, Oerlemans 2013, p. 240.
[197] Zie MvT, p. 39. Het relevantiecriterium wordt niet expliciet benoemd maar wel behandeld in paragraaf 2.3 (bijdrage) en 2.5 (effectiviteit) van de memorie van toelichting.

Hoofdstuk 6: Het belang van het recht op privéleven

§ 1. Inleiding

Met de vaststelling van het dringende belang van de opsporing bij de invoering van een hackbevoegdheid resteert de vraag hoe het belang van de Nederlandse burgers bij waarborging van hun recht op bescherming van de persoonlijke levenssfeer zich hier tot verhoudt. In dit hoofdstuk zal dan ook de vraag aan bod komen hoe zwaar het belang van burgers bij bescherming van hun recht op privacy weegt, meer specifiek of het recht op integriteit en vertrouwelijkheid van ICT-systemen (als geformuleerd in paragraaf 2 van hoofdstuk 2) moet worden geacht zwaarder te wegen dan de algemene bescherming van gegevens en (tele-) communicatie binnen de reikwijdte van artikel 8 EVRM. Dit zal worden vastgesteld op basis van de in paragraaf 3 van hoofdstuk 2 genoemde factoren: de aard en het gewicht van het grondrecht en de aard en de ernst van de inbreuk hierop.

§ 2. Belangen van burgers bij bescherming van privéleven

§ 2.1. Aard en gewicht van het grondrecht

De verschillende grondrechten die binnen de reikwijdte van artikel 8 EVRM vallen, verschillen onderling in gewicht. Hoe gewichtiger het betreffende grondrecht, hoe zwaarder het maatschappelijke belang moet zijn dat de overheid aanvoert als rechtvaardiging voor een inbreuk.[198] Het EHRM kent vooral een bijzonder gewicht toe aan grondrechten die het meest intieme aspect van de persoonlijke levenssfeer raken: '*intimate or key rights*' of '*a particularly important facet of an individual's existence or identity*'.[199] Het Hof kent dit gewicht altijd expliciet toe en heeft dit onder andere gedaan ten aanzien van het seksuele leven en de seksuele identiteit van burgers en de confidentialiteit van medische informatie.[200] Aan de bescherming van privégegevens, locatiegegevens en vertrouwelijke (tele-) communicatie in het algemeen is door het EHRM niet expliciet een bijzonder gewicht toegekend, waaruit kan worden afgeleid dat het Hof deze door heimelijke opsporingsbevoegdheden geraakte aspecten van het privéleven in het algemeen geen bijzondere bescherming wenst te verlenen. Dit kan mogelijk in specifieke gevallen anders zijn, wanneer het concreet gaat om gegevens omtrent het seksuele leven, de seksuele identiteit, medische informatie of om andere gegevens die zien op dimensies van het privéleven die een bijzondere bescherming genieten onder artikel 8 EVRM.[201] Als uitgangspunt heeft mijns inziens echter te gelden dat de gegevens die met heimelijke opsporingsbevoegdheden worden verzameld geen bijzonder zware bescherming onder artikel 8 EVRM genieten.

---

[198] Zie Gerards 2011, p. 158.

[199] EHRM 27 mei 2004, nr. 66746/01 (*Connors/United Kingdom*), § 82 respectievelijk EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 102.

[200] EHRM 22 oktober 1981, nr. 7525/76 (*Dudgeon/United Kingdom*), § 41 en 52 respectievelijk EHRM 25 februari 1997, nr. 22009/93 (*Z/Finland*), § 94 – 96.

[201] Opgemerkt zij dat wat betreft gegevens omtrent deze elementen van de persoonlijke levenssfeer alleen de confidentialiteit van medische informatie expliciet door het EHRM een bijzonder gewicht is toegekend; voor het overige leid ik de bijzonder zware bescherming van de gegevens af uit de bescherming die de betreffende elementen van de persoonlijke levenssfeer is toegekend. In de Nederlandse interpretatie van artikel 8 EVRM krijgen deze gegevens in ieder geval wel een bijzonder zware bescherming op basis van artikel 16 Wbp, en op basis van deze bepaling genieten mijns inziens ook gegevens omtrent godsdienst of levensovertuiging, ras en politieke gezindheid deze bijzonder zware bescherming. Vgl. ook artikel 126nf Sv.

De vraag resteert dan of dit oordeel omtrent de mate van bescherming van gegevens anders moet luiden wanneer het gaat om gegevens die op geautomatiseerde werken worden opgeslagen en die met geautomatiseerde werken worden verstuurd, oftewel als het gaat om het recht op integriteit en vertrouwelijkheid van ICT-systemen. Weegt het belang van de integriteit van ICT-systemen en van de vertrouwelijkheid van de daarop opgeslagen gegevens en daarmee verstuurde communicatie zo zwaar dat het recht op integriteit en vertrouwelijkheid van ICT-systemen daarom een groter gewicht toekomt dan de bescherming van elders opgeslagen gegevens, elders vastgestelde locatiegegevens en op andere wijze verstuurde (tele-) communicatie, in die zin dat er een zwaarder maatschappelijk belang tegenover moet staan om een inbreuk hierop te kunnen rechtvaardigen?

Een dergelijke interpretatie lijkt in zijn algemeenheid niet beoogd te zijn met de formulering van het recht op integriteit en vertrouwelijkheid van ICT-systemen. Uit de Nederlandse formulering van dit recht valt mijns inziens enkel af te leiden dat er sprake is van een element van de persoonlijke levenssfeer dat vanwege haar specifieke kenmerken moet worden onderscheiden van de algemene bescherming van gegevens en (tele-) communicatie, niet dat dit element ook zwaarder zou moeten wegen.[202] Het BVerfG lijkt in zijn 'Online-Durchsuchung' uitspraak eenzelfde interpretatie te hebben beoogd. Het overwoog dat de (Duitse) grondrechten van dat moment onvolledige bescherming boden en geen recht deden aan het belang van de informatietechnische systemen in de informatiemaatschappij.[203] Het biedt hiervoor ook een duidelijke uitleg, waaruit blijkt dat het BVerfG het recht op integriteit en vertrouwelijkheid heeft geformuleerd als erkenning dat het privéleven dat plaatsvindt in de digitale wereld via ICT-systemen zijn eigen specifieke kenmerken heeft waarop moet worden ingespeeld om te voorkomen dat er een lacune in de wet bestaat, zonder hierbij dit element van het privéleven zwaarder te willen doen wegen dan de andere.[204] Burgers slaan al dan niet bewust enorme hoeveelheden privacygevoelige gegevens op in de digitale omgeving.[205] Deze verzameling gegevens vormt een vrijwel pasklaar en volledig beeld van het privéleven van de betreffende burgers. Het grote belang dat de persoonlijkheid en de persoonlijke ontplooiing daarom hebben bij het vertrouwelijk houden van deze gegevens behoeft geen discussie.[206] Hierop moet worden ingespeeld middels een specifieke bescherming van de gegevens en de systemen waarop ze zijn opgeslagen of vanaf waar ze worden verzonden, waarmee de risico's worden onderkend die verbonden zijn aan de digitale beschikbaarheid van zo'n verzamelingen privacygevoelige gegevens.[207]

Het recht op integriteit en vertrouwelijkheid van ICT-systemen is mijns inziens niet ontwikkeld om aan dit recht een bijzonder gewicht toe te kennen ten opzichte van de

[202] Vgl. Oerlemans 2011, p. 898; MvT, p. 38 – 39.
[203] Vgl. BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 181.
[204] Vgl. Steenbruggen 2008, p. 233.
[205] Onbewust vooral bij internetgebruik; zie bijvoorbeeld BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 178 – 179.
[206] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 200.
[207] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 181.

algemene bescherming van gegevens en (tele-) communicatie op basis van artikel 8 EVRM. Met dit nieuwe recht wordt slechts beoogd te erkennen dat het privéleven in een digitale omgeving specifieke risico's kent die ook hun eigen specifieke, maar niet méér bescherming vereisen: in zoverre verschilt enkel de 'aard' van dit recht ten opzichte van de algemene bescherming van gegevens en (tele-) communicatie.[208] Aan de betreffende risico's zal in het kader van de aard en de ernst van de inbreuk in paragraaf 2.2.4, en uiteindelijk de inkleding van de hackbevoegdheid in hoofdstuk 7, nog nadere aandacht worden besteed.

Verandert de conclusie omtrent de aard en het gewicht van het recht op integriteit en vertrouwelijkheid van ICT-systemen wanneer dit recht naar analogie van het huisrecht een absolute bescherming biedt van ICT-systemen, zoals geopperd in paragraaf 2 van hoofdstuk 2? Mijns inziens niet. Het huisrecht wordt in het licht van artikel 8 lid 2 EVRM evenmin door het EHRM expliciet als een *key right* gekwalificeerd en wordt doorgaans in de rechtspraak van het Hof inbegrepen in het algemene recht op privéleven ex artikel 8 EVRM.[209] De bescherming van de 'kernrechten' treedt ook in het kader van de eerbiediging van de woning op zijn vroegst in werking wanneer daadwerkelijk gegevens worden verzameld of activiteiten worden waargenomen die specifiek onder de meest intieme aspecten van de persoonlijke levenssfeer vallen. Dit houdt in dat aan het huisrecht weliswaar een groot gewicht en een absolute bescherming toekomt, maar eveneens geen bijzonder gewicht en dus geen bijzonder zware bescherming ten opzichte van het algemene recht op privéleven. Hetzelfde heeft naar mijn mening dan ook te gelden voor een analoge interpretatie van het recht op integriteit van ICT-systemen. Ook deze interpretatie ziet vooral op een erkenning van de risico's verbonden aan het privéleven dat via geautomatiseerde werken plaatsvindt.

§ 2.2. Aard en ernst van de inbreuk

De aard en de ernst van de inbreuk van een bevoegdheid tot het binnendringen in een geautomatiseerd werk zijn reeds deels behandeld in hoofdstuk 4. Wat betreft de toepassing van de voorgestelde hackbevoegdheid ten behoeve van het bepalen van de identiteit of locatie van een geautomatiseerd werk of de gebruiker, van het aftappen of opnemen van (tele-) communicatie en van stelselmatige observatie is in dat hoofdstuk reeds overwogen dat de inbreuk van een hackbevoegdheid op zichzelf niet (significant) zwaarder is dan die van de bestaande opsporingsbevoegdheden. In deze paragraaf zal ik dan ook vooral nader ingaan op de toepassing van de hackbevoegdheid om daadwerkelijk op de harde schijf van een geautomatiseerd werk (of eventueel een cloudserver) heimelijk onderzoek te doen om gegevens over te nemen of de aanwezigheid van gegevens vast te stellen. De inbreuk van deze toepassing is mijns inziens sowieso zwaarder dan die van de overige toepassingen van de

[208] Zie voor zeer vergelijkbare overwegingen als die van de 'Online-Durchsuchung' uitspraak ook het recente arrest Supreme Court of Canada 7 november 2013, *R. v. Vu*, 2013 SCC 60, § 41 – 43. Ook de *Supreme Court* erkent de risico's van de grote verzamelingen (vaak onbewust) opgeslagen gegevens op computers, waardoor immers potentieel een alomvattend beeld van het privéleven van een persoon kan worden verkregen.

[209] Jacobs, White & Ovey 2010, p. 359. Vgl. EHRM 24 november 1986, nr. 9063/80 (*Gillow/United Kingdom*), § 55, waarin het Hof wel een bijzonder gewicht toekende aan het recht op eerbiediging van de woning. Dit zag echter specifiek op het recht om in de eigen woning te kunnen (blijven) wonen, waarbij grotere belangen op het spel staan dan enkel de privacy van gegevens en activiteiten in de eigen woning waar het in het kader van dit onderzoek om gaat. Mijns inziens kan dit niet leiden tot de conclusie dat het huisrecht in zijn algemeenheid een 'kernrecht' is.

hackbevoegdheid en de bestaande opsporingsbevoegdheden. Enerzijds bieden geen van de bestaande heimelijke opsporingsbevoegdheden de mogelijkheid om rechtstreeks kennis te nemen van op een (al dan niet digitale) besloten locatie opgeslagen gegevens. Anderzijds kunnen de bevoegdheden tot het doorzoeken van woningen, die wel de mogelijkheid bieden om van op een besloten locatie opgeslagen gegevens kennis te kunnen nemen, niet heimelijk plaatsvinden. De vraag is dan echter of de inbreuk van de hackbevoegdheid, die wél heimelijkheid en kennisneming van opgeslagen gegevens combineert, zodanig ernstiger of anders is dat dit gevolgen heeft voor de proportionaliteit van de bevoegdheid. Bij de beoordeling hiervan komt belang toe aan de vraag of de hackbevoegdheid een algemeen en absoluut en/of een bijzonder ingrijpend karakter heeft en welke nadelige gevolgen de bevoegdheid met zich meebrengt. De vierde factor in de beoordeling van de aard en de ernst van de inbreuk, te weten de mogelijkheden voor misbruik van de bevoegdheid, geldt weer voor de hackbevoegdheid als geheel.

§ 2.2.1. Algemeen en absoluut karakter

Wanneer een inbreuk een algemeen en absoluut karakter heeft, moet het een bijzonder zwaarwegend belang dienen om toegestaan te zijn.[210] Een vergelijking van het voorgestelde artikel 125ja Sv met de recent onthulde NSA-methoden maakt duidelijk waarom de voorgestelde hackbevoegdheid niet algemeen en absoluut van karakter geacht kan worden. De Amerikaanse *National Security Agency* zet met het Prism programma al jaren grootschalige heimelijke surveillance in om telecommunicatie te monitoren.[211] Tevens heeft de NSA ook de mogelijkheid om met het programma *XkeyScore* praktisch alle internetactiviteit van internetgebruikers over de hele wereld af te tappen, op te slaan en te onderzoeken.[212] Een dergelijke grootschalige verzameling van data over burgers (*bulk collection* en *blanket surveillance*) is volgens de maatstaven van het EHRM niet toegestaan.[213] Het staat ook in duidelijk contrast met de hackbevoegdheid die ik in dit onderzoek behandel. Aansluiting kan worden gezocht bij het voorgestelde artikel 125ja Sv: deze bevoegdheid mag enkel worden toegepast in geval van een specifieke verdenking in de zin van artikel 27 Sv. Hierdoor is er in ieder geval geen sprake van een algemeen en absoluut karakter van de hackbevoegdheid.

§ 2.2.2. Bijzonder ingrijpend karakter

Het bijzonder ingrijpende karakter van een maatregel kan van invloed zijn op de factor ‘aard en ernst van een inbreuk’.[214] Het EHRM beschouwt heimelijke opsporingsbevoegdheden en bevoegdheden tot doorzoeking niet als ‘bijzonder’ ingrijpend of vergaand, zo kan worden afgeleid uit de omstandigheid dat het Hof aan deze factor nooit enige aandacht besteedt wanneer het gaat om dergelijke bevoegdheden. In Nederland lijkt de opvatting van

[210] Vgl. EHRM 27 september 1999, nrs. 33985/96 en 33986/96 (*Smith and Grady/United Kingdom*), § 93 – 94; EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 119.
[211] <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
[212] <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.
[213] Vgl. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 51: *exploratory or general surveillance* staat het EHRM niet toe, zelfs niet ten behoeve van de nationale veiligheid.
[214] Zie EHRM 27 september 1999, nrs. 33985/96 en 33986/96 (*Smith and Grady/United Kingdom*), § 91 en Gerards 2011, p. 221.

voorstanders van de hackbevoegdheid te zijn dat het door opsporingsambtenaren binnendringen in een geautomatiseerd werk weliswaar ingrijpend is, maar geen bijzonder ingrijpend of vergaand karakter heeft vergeleken met de reeds bestaande heimelijke opsporingsbevoegdheden en bevoegdheden tot doorzoeking.[215] Dit is een logische opvatting: met het binnendringen in een geautomatiseerd werk kan immers in beginsel van dezelfde gegevens kennis worden genomen als middels de reeds bestaande bevoegdheden tot doorzoeking van woningen en geautomatiseerde werken.[216] Weliswaar vindt het binnendringen in een geautomatiseerd werk op heimelijke wijze plaats, in tegenstelling tot de bevoegdheden tot doorzoeking, maar dit leidt mijns inziens niet tot een bijzonder ingrijpend karakter mits het heimelijk binnendringen zich beperkt tot die gegevens die noodzakelijk zijn in het belang van het onderzoek. In dit 'mits' zit evenwel ook besloten dat er wel degelijk bepaalde risico's verbonden zijn aan het toestaan van heimelijke toegang tot een grote verzameling vertrouwelijke gegevens.[217] Zie nader paragraaf 2.2.4.

§ 2.2.3. Nadelige gevolgen

Bij de beoordeling van de aard en de ernst van een inbreuk op de persoonlijke levenssfeer komt ook belang toe aan de nadelige gevolgen die een maatregel kan hebben ten aanzien van de persoonlijke levenssfeer.[218] Onderscheid kan worden gemaakt tussen de nadelige gevolgen van het bestaan van de wettelijke bevoegdheid en van de toepassing van de bevoegdheid. Het EHRM erkent dat het enkele bestaan van een heimelijke bevoegdheid op zich al nadelige gevolgen kan hebben voor het recht op bescherming van de persoonlijke levenssfeer, doordat het bestaan van zo'n bevoegdheid een bedreiging van heimelijke surveillance met zich draagt voor iedereen ten aanzien van wie de bevoegdheid kan worden toegepast; deze bedreiging raakt de vrijheid van communicatie van gebruikers van telecommunicatiediensten.[219] Wat betreft de bevoegdheid tot het binnendringen in geautomatiseerde werken bestaat er tevens een nadelig gevolg voor de vrijheid van het gebruik van geautomatiseerde werken; de ernst hiervan kan mijns inziens ongeveer gelijk gesteld worden met de gevolgen van heimelijke bevoegdheden voor de vrijheid van communicatie.

Toepassing van heimelijke bevoegdheden, inclusief de bevoegdheid tot het binnendringen in een geautomatiseerd werk, levert op zichzelf geen verdere nadelige gevolgen op mits deze op de juiste manier worden toegepast: van de toepassing zelf merken de betreffende personen praktisch gezien niets en het enige negatieve resultaat is dat zij of iemand tot wie zij in verhouding staan mogelijk verdachten worden in een strafrechtelijk onderzoek, hetgeen echter in lijn is met de beoogde doelstellingen.[220] De nadelige gevolgen van de bevoegdheid tot het

[215] MvT p. 38 – 39; Oerlemans 2011, p. 898; vgl. Conings & Oerlemans 2013, p. 26.
[216] De praktische complicaties waar de andere opsporingsbevoegdheden tegenaan kunnen lopen zijn in dit kader niet relevant.
[217] Zie Steenbruggen 2008, p. 233 – 235; De Hert, De Vries & Gutwirth 2009, p. 5; Groothuis & De Jong 2010, p. 282; Koning 2012, p. 48 – 49.
[218] EHRM 27 mei 2004, nr. 66746/01 (*Connors/United Kingdom*), § 85; EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 122. Dit betreft nadelige gevolgen van het binnendringen in een geautomatiseerd werk. De nadelige gevolgen van het *niet* kunnen binnendringen zijn reeds aan bod geweest in de relevantietoets.
[219] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 41; EHRM 2 augustus 1984, nr. 8691/79 (*Malone/United Kingdom*), § 64; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 106 en § 78.
[220] Vgl. EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 122, waarin enkel de nadelige gevolgen van misbruik van de bevoegdheid worden behandeld.

binnendringen in een geautomatiseerd werk zijn in overeenstemming met die van de bestaande heimelijke opsporingsbevoegdheden en vormen derhalve geen verzwarende factor in de belangenafweging. De nadelige gevolgen die door misbruik van de toepassing kunnen ontstaan komen in paragraaf 2.2.4 afzonderlijk aan bod.

§ 2.2.4. Mogelijkheden voor misbruik

In paragraaf 2.1 is in het kader van de aard en het gewicht van het recht op integriteit en vertrouwelijkheid van ICT-systemen reeds uiteengezet dat gebruikers enorme hoeveelheden privacygevoelige gegevens opslaan in de digitale omgeving waarin zij zich met hun geautomatiseerde werken begeven. Deze volledige verzameling gegevens is relatief eenvoudig toegankelijk als eenmaal op het geautomatiseerde werk is binnengedrongen, en hier komt nog eens bij dat de gebruiker van het betreffende geautomatiseerde werk zich niet op adequate wijze kan verweren tegen het binnendringen, aangezien dit binnendringen naar de aard heimelijk plaatsvindt en hij dus doorgaans niet door heeft dat er iemand is binnengedrongen in zijn geautomatiseerde werk.[221] Deze combinatie van relatief eenvoudige toegang tot een grote verzameling opgeslagen gegevens en de heimelijke aard van toepassing van de bevoegdheid leidt tot een risico dat grote hoeveelheden privacygevoelige gegevens kunnen worden verzameld en gebruikt op een wijze die niet in verhouding staat tot het belang van het onderzoek of zelfs voor andere doeleinden dan de opsporing van strafbare feiten.[222] Het gevolg hiervan is dat een hackbevoegdheid een risico met zich draagt van misbruik, waarbij 'misbruik' vrij ruim opgevat kan worden, namelijk als toepassing van de bevoegdheid met schending van de beginselen van proportionaliteit en subsidiariteit (al dan niet opzettelijk). Dit risico van misbruik vormt vanwege de combinatie van heimelijkheid, de omvang van de verzameling privégegevens en de relatief eenvoudige toegankelijkheid en bruikbaarheid van deze gegevens, een groter risico voor de persoonlijkheid en de persoonlijke ontwikkeling van burgers dan tot op heden mogelijk is: de bestaande heimelijke opsporingsbevoegdheden hebben immers niet de mogelijkheid zo'n volledige verzameling pasklare gegevens te vergaren, terwijl de huiszoekingsbevoegdheden niet heimelijk zijn en daardoor minder grote risico's van buitenproportionele toepassing met zich brengen.[223]

Een tweede risico voor misbruik ten aanzien van de privacy van burgers is de mogelijkheid voor opsporingsambtenaren om na het binnendringen in een geautomatiseerd werk webcams of ingebouwde camera's te activeren.[224]

Een derde risico voor misbruik van een hackbevoegdheid is het risico van manipulatie van bewijsmateriaal. Na te zijn binnengedrongen in een geautomatiseerd werk hebben opsporingsambtenaren de mogelijkheid om niet alleen te lezen of te luisteren (en te registreren respectievelijk op te nemen), maar ook om zelf te 'schrijven' op het geautomatiseerde werk en

[221] BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 180.
[222] Vgl. BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 180 en Steenbruggen 2008, p. 233. Vgl. ook EHRM 2 augustus 1984, nr. 8691/79 (*Malone/United Kingdom*), § 81.
[223] Vgl. BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07, § 200.
[224] Zie ook Oerlemans 2011, p. 892.

zo de gegevens die moeten dienen als bewijsmateriaal te manipuleren.[225] Voor een groot deel betreft deze kwestie de integriteit van het bewijsmateriaal en speelt het voornamelijk in het kader van artikel 6 EVRM, waardoor het in zoverre buiten het bereik van dit onderzoek valt. Evenwel vormt dit risico voor misbruik ook een gevaar voor het privéleven in de zin van artikel 8 EVRM, namelijk indien door het plaatsen van valse informatie een geheel ander beeld van de betreffende persoon wordt gecreëerd dan de werkelijke.[226]

De risico's voor misbruik van een hackbevoegdheid moeten zo veel mogelijk geneutraliseerd worden door waarborgen aan de toepassing van de bevoegdheid te verbinden. Hieraan wordt in hoofdstuk 7 nadere aandacht besteed.

§ 3. Conclusie

Het belang van op geautomatiseerde werken opgeslagen gegevens en daarmee verstuurde communicatie voor het privéleven van burgers staat buiten kijf. Noch de genoemde gegevens en communicatie, noch de integriteit van de ICT-systemen op zich (naar analogie van het huisrecht) vormen echter een element van de persoonlijke levenssfeer dat op zichzelf zwaarder weegt dan de algemene bescherming van gegevens en (tele-) communicatie onder het recht op privéleven als vastgelegd in artikel 8 lid 2 EVRM. Het recht op integriteit en vertrouwelijkheid van ICT-systemen dient enkel ter erkenning van de risico's verbonden aan het privéleven in een digitale omgeving. Wat betreft de aard en de ernst van de inbreuk heeft te gelden dat een hackbevoegdheid in beginsel geen zwaardere of meer omvangrijke inbreuk maakt op het recht op bescherming van de persoonlijke levenssfeer dan het geval is bij andere heimelijke opsporingsbevoegdheden. De bevoegdheid is niet algemeen en absoluut, noch bijzonder ingrijpend van karakter, terwijl de nadelige gevolgen dezelfde zijn als die van de bestaande heimelijke opsporingsbevoegdheden. Het belang van burgers bij waarborging van het recht op integriteit en vertrouwelijkheid van geautomatiseerde werken weegt derhalve even zwaar als hun belang bij de algemene bescherming van gegevens en (tele-) communicatie onder artikel 8 EVRM.

Wel bevat deze opsporingsmethode enkele specifieke kenmerken die in onderlinge samenhang leiden tot een risico dat de bevoegdheid in concrete situaties wordt toegepast met schending van de beginselen van proportionaliteit en subsidiariteit, oftewel dat misbruik van de bevoegdheid plaatsvindt. Bovendien zijn de gevolgen van misbruik potentieel aanzienlijk groter dan die tot op heden uit misbruik van opsporingsbevoegdheden kunnen ontstaan. Om deze redenen komt bij de zoektocht naar de *fair balance* een groot gewicht toe aan de waarborgen waarmee de bevoegdheid wordt omkleed.[227] In het volgende hoofdstuk zullen de waarborgen dan ook worden meegenomen in de afweging tussen de belangen van de opsporing en de belangen van burgers bij hun recht op bescherming van de persoonlijke levenssfeer.

[225] Zie Oerlemans 2011, p. 892 en Jacobs 2012, p. 2762 – 2763.
[226] Vgl. Jacobs 2012, p. 2762.
[227] Vgl. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 49 – 50; EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 153.

Hoofdstuk 7: '*Fair balance*'

§ 1. Inleiding: de twee vereisten voor een fair balance

Het uiteindelijke doel van de noodzakelijkheidstoets is zoals reeds gesteld het zoeken naar een *fair balance* tussen de belangen van de samenleving enerzijds en de grondrechten van burgers anderzijds.[228] Wanneer een *fair balance* wordt gerealiseerd, is de invoering en toepassing van een hackbevoegdheid gerechtvaardigd naar de maatstaven van het noodzakelijkheidsvereiste ex artikel 8 lid 2 EVRM. Alle factoren die in de voorgaande hoofdstukken aan bod zijn gekomen, worden nu gewogen in de beoordeling van de *fair balance*.

Het eerste vereiste voor een *fair balance* is dat er voldoende grond is voor de invoering van een hackbevoegdheid; een abstracte noodzakelijkheidstoets. Hebben de Nederlandse opsporingsdiensten, gezien de problemen in de opsporing veroorzaakt door versleuteling, gebruik van draadloze netwerken, cloud computing en anonimiseringstechnieken, het gebrek aan subsidiaire oplossingen hiervoor en de mogelijkheden die een hackbevoegdheid biedt om de problemen wél op te lossen, een dusdanig dringend belang bij een hackbevoegdheid dat invoering van deze bevoegdheid, met inachtneming van de ernstige inbreuk die dit maakt op de bescherming van de persoonlijke levenssfeer van burgers, in redelijke verhouding staat tot het belang van de opsporing?

Wanneer vaststaat dat er voor de invoering van de wettelijke bevoegdheid voldoende grond is (proportionaliteit en subsidiariteit *in abstracto*), is op basis van de rechtspraak van het EHRM voor de realisatie van een *fair balance* het tweede en laatste vereiste dat de bevoegdheid met voldoende waarborgen is omkleed ten behoeve van de proportionaliteit en subsidiariteit *in concreto*. Dit komt voort uit de risico's die zijn verbonden aan de toepassing van een hackbevoegdheid, als vastgesteld in hoofdstuk 6. De waarborgen dienen te garanderen dat de bevoegdheid daadwerkelijk enkel wordt toegepast wanneer dit in redelijke verhouding staat tot het belang van de opsporing van strafbare feiten.[229]

§ 2. Voldoende grond voor een hackbevoegdheid?

Voor voldoende grond voor een hackbevoegdheid is allereerst vereist dat deze bevoegdheid beantwoordt aan een dringend belang van de opsporing om een dergelijke bevoegdheid toe te voegen aan hun arsenaal: er moet een *pressing social need* in de maatschappij bestaan. Het dringende belang is in hoofdstuk 3 tot en met 5 uitgebreid behandeld, met de conclusie dat de hackbevoegdheid inderdaad beantwoordt aan een dringend belang van de opsporing.

[228] Zie Gerards 2011 en EHRM 7 juli 1989, nr. 14038/88 (*Soering/United Kingdom*) *supra* noot 50.
[229] Vgl. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 50; EHRM 26 maart 1987, nr. 9248/81 (*Leander/Sweden*), § 60; EHRM 24 augustus 1998, nr. 23618/94 (*Lambert/France*), § 31; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 106; EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 153; EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*), § 57; EHRM 25 februari 1993, nr. 11471/85 (*Crémieux/France*), § 40; EHRM 25 februari 1993, nr. 12661/87 (*Miailhe/France*), § 38.

De bovenstaande constatering leidt mijns inziens vervolgens ook vrij snel tot de conclusie dat er sprake is van een *voldoende* dringend belang van de opsporing, in die zin dat de inbreuk van een hackbevoegdheid in redelijke verhouding staat tot het belang van de opsporing. Wanneer er een leemte in de opsporing bestaat zoals in hoofdstuk 3 tot en met 5 geconstateerd, is het acceptabel dat er een (ernstige) inbreuk wordt gemaakt op de privacy van burgers om deze leemte op te vullen.[230] Het is dan vooral van belang om kritisch te overwegen ten aanzien van welke typen delicten de inbreuk in redelijke verhouding staat tot het belang van de opsporing.[231] Het EHRM acht de inbreuk van heimelijke opsporingsbevoegdheden proportioneel ten aanzien van *'serious criminal acts'*.[232] Deze maatstaf is bij de totstandkoming van de Wet BOB uitgewerkt in de gronden voor toepassing van de zwaarste heimelijke opsporingsbevoegdheden (te weten de bevoegdheden tot het aftappen van telecommunicatie en het direct afluisteren): deze mogen enkel worden toegepast in geval van een verdenking van 'zeer zware misdrijven', oftewel misdrijven als omschreven in artikel 67 lid 1 Sv die bovendien gezien hun aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde opleveren.[233] Eenzelfde maatstaf kan worden gehanteerd ten aanzien van een hackbevoegdheid: voor proportionaliteit van deze bevoegdheid is vereist dat deze alleen mag worden ingezet in opsporingsonderzoeken naar strafbare feiten in de categorie 'zeer zware misdrijven' als hierboven omschreven.

De discussie omtrent het al dan niet introduceren van een hackbevoegdheid is in eerste instantie voornamelijk ontstaan vanwege de ernstige gevaren van cybercriminaliteit en kinderporno voor de huidige Nederlandse samenleving.[234] Mijns inziens is het echter niet wenselijk om de bevoegdheid tot het binnendringen in een geautomatiseerd werk ook alleen toepasbaar te laten zijn tegen deze vormen van computercriminaliteit en niet tegen de overige delicten opgenomen in artikel 67 lid 1 Sv. Het onderscheid tussen 'klassieke' delicten en computercriminaliteit is immers niet (meer) heel strikt; klassieke delicten kunnen ook worden gepleegd met behulp van moderne technologische middelen en dan onder de noemer 'computercriminaliteit' worden geplaatst.[235] In die gevallen doen zich ook de problemen van gebruik van versleuteling, draadloze netwerken, cloud computing en/of anonimiseringstechnieken voor, welke ten grondslag liggen aan het dringende belang van de opsporing bij de hackbevoegdheid. Er lijkt, met inachtneming van artikel 8 lid 2 EVRM, dan ook geen noodzaak te zijn om de toepasbaarheid van de bevoegdheid tot het binnendringen in een geautomatiseerd werk te beperken tot cybercriminaliteit en kinderporno.

---

[230] Eenzelfde overweging lag ten grondslag aan de invoering van de bijzondere opsporingsbevoegdheden met de Wet BOB, zie *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 11.
[231] Het EHRM plaatst de delicten ten aanzien waarvan heimelijke bevoegdheden mogen worden toegepast als onderdeel van de waarborgen. Mijns inziens is deze kwestie echter zo nauw verbonden met het algemene bestaansrecht van de hackbevoegdheid dat deze in dat kader behandeld dient te worden.
[232] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 51; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 115.
[233] Zie *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 11.
[234] Zie paragraaf 1 van hoofdstuk 1.
[235] Zie H.W.K. Kaspersen in Koops 2007, p. 14 – 17 en Europol 2013, p. 15 – 16. Zie ook <http://www.economist.com/news/britain/21587839-keeping-up-crooks>.

Aparte overweging verdient de mogelijkheid dat de voorgestelde hackbevoegdheid in het conceptwetsvoorstel Computercriminaliteit III ook de bevoegdheid omvat om op afstand webcams of ingebouwde camera's aan te zetten ten behoeve van stelselmatige observatie, of om microfoons te activeren om face-to-face gesprekken tussen personen in dezelfde ruimte af te luisteren. Deze modaliteit van de hackbevoegdheid is niet proportioneel: zij is reeds stukgelopen op de relevantietoets, waardoor de opsporing geen dringend belang heeft bij de invoering van deze specifieke modaliteit en derhalve de *pressing social need* ontbreekt.[236]

Met de vaststelling van de *pressing social need* voor het bestaan van een wettelijke hackbevoegdheid en de redelijke verhouding hiervan ten aanzien van de opsporing van de categorie 'zeer zware misdrijven' resteert voor de realisatie van een *fair balance* de beoordeling van de te stellen waarborgen ter garantie van proportionaliteit en subsidiariteit bij concrete toepassing.

§ 3. Waarborgen voor proportionaliteit en subsidiariteit

Met de toets van voldoende waarborgen zijn we eindelijk aanbeland bij een criterium waarvoor het EHRM in het kader van heimelijke opsporingsbevoegdheden concrete handvatten biedt ter toetsing.[237] Dit betekent dat, in tegenstelling tot de voorgaande hoofdstukken, de maatstaven die het EHRM doorgaans hanteert en de maatstaven die op nationaal niveau moeten gelden, ten aanzien van de te stellen waarborgen ongeveer gelijk zijn. Wanneer ik toch een strengere nationale maatstaf noodzakelijk acht zal ik dit aangeven.

Het noodzakelijkheidsaspect van de waarborgentoets dient te worden onderscheiden van het legaliteitsaspect, waarmee het enige overlapping vertoont.[238] De eis van het stellen van waarborgen kan ook onder het legaliteitsvereiste worden gebracht, in die zin dat met de waarborgen voor de burger voorzienbaar moet zijn wanneer en onder welke voorwaarden de opsporingsdiensten de opsporingsbevoegdheid mogen toepassen.[239] Een onderscheid tussen het noodzakelijkheidsaspect en het legaliteitsaspect van het waarborgenvereiste is mijns inziens evenwel duidelijk te maken. Het noodzakelijkheidsaspect van de waarborgen ziet op de grenzen en beperkingen die door deze waarborgen worden gesteld aan de toepassing van de opsporingsbevoegdheid en de controle hierop, zodat wordt gegarandeerd dat de concrete toepassingen van de hackbevoegdheid voldoen aan de vereisten van proportionaliteit en subsidiariteit. Het legaliteitsaspect van de waarborgen ziet op de wijze waarop de grenzen en beperkingen worden vastgelegd: zijn de waarborgen voldoende toegankelijk voor burgers en is voldoende duidelijk geformuleerd wat de grenzen en beperkingen zijn aan toepassing van de opsporingsbevoegdheid in kwestie?[240] In deze paragraaf zal ik mij, in lijn met de rest van dit onderzoek, beperken tot het noodzakelijkheidsaspect van de waarborgen van een

[236] Zie hierover ook paragraaf 2 van hoofdstuk 8.
[237] Zie de rechtspraak *supra* noot 229.
[238] Zie ook Vlemminx 2013, p. 254 – 255.
[239] Zie paragraaf 2 van hoofdstuk 1; zie ook Vlemminx 2013, p. 254 – 259.
[240] Dit verschil tussen het legaliteitsaspect en het noodzakelijkheidsaspect van waarborgen komt duidelijk naar voren in de behandeling van deze twee aspecten in EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 92 – 102 respectievelijk § 103 – 136. Vgl. voorts Vlemminx 2013, p. 259 – 265.

hackbevoegdheid. De mate van duidelijkheid van de waarborgen zal in dit kader ook aan bod komen, maar dan zien op de duidelijkheid voor de autoriteiten die de bevoegdheid moeten toepassen, ten behoeve van de garantie van proportionaliteit en subsidiariteit, in plaats van de duidelijkheid ten opzichte van burgers ten behoeve van de voorzienbaarheid.

De waarborgen waarmee een hackbevoegdheid moet worden omkleed in het licht van het noodzakelijkheidsvereiste dienen te garanderen dat de praktische toepassing in concreto van de bevoegdheid de maatstaven van proportionaliteit en subsidiariteit respecteert, oftewel dat de praktische toepassing in concrete gevallen ook aansluit op een *pressing social need* en in redelijke verhouding staat tot het belang van de opsporing.[241] Hiertoe dienen de waarborgen het volgende te bepalen: de gronden op basis waarvan de bevoegdheid mag worden toegepast, de omvang en duur van toepassing van de bevoegdheid, de procedure voor toestemming en controle van toepassing, en de '*remedy*' naar nationaal recht.[242] Het in het conceptwetsvoorstel Computercriminaliteit III voorgestelde artikel 125ja Sv wordt ook in de bespreking in deze paragraaf betrokken, zodat kan worden beoordeeld in hoeverre de voorgestelde hackbevoegdheid reeds met voldoende waarborgen is omkleed.

§ 3.1. Gronden voor toepassing bevoegdheid

De algemene gronden voor toepassing van een bevoegdheid tot het binnendringen in een geautomatiseerd werk, te weten de delicten ten aanzien waarvan een hackbevoegdheid toepasbaar mag zijn, zijn in paragraaf 2 aan bod geweest. Daarbij is gesteld dat een hackbevoegdheid gerechtvaardigd kan worden toegepast tegen de zwaarste categorie misdrijven. Echter moet wel bij daadwerkelijke toepassing worden getoetst of de vereisten van proportionaliteit en subsidiariteit ook in het concrete geval toestaan dat de bevoegdheid wordt toegepast; hiertoe moeten dan ook voldoende waarborgen worden gesteld.

Vanwege het beginsel van subsidiariteit mag de hackbevoegdheid enkel worden ingezet wanneer het vergaren van informatie ten behoeve van de opsporing van strafbare feiten met gebruik van een andere, minder bezwarende methode naar verwachting geen resultaat zal opleveren of in ieder geval aanzienlijk gecompliceerder zal zijn.[243] In hoofdstuk 4 is vastgesteld dat er geen consequente subsidiaire alternatieven zijn voor een hackbevoegdheid wanneer sprake is van gebruik van versleuteling, draadloze netwerken, cloud computing en/of anonimiseringstechnieken. Echter is eveneens opgemerkt dat andere opsporingsbevoegdheden wel degelijk subsidiaire alternatieven (kunnen) bieden wanneer de betreffende verschijnselen zich níét voordoen.[244] Ook kunnen in voorkomende gevallen subsidiaire alternatieven toepasbaar zijn ondanks het gebruik van versleuteling, draadloze netwerken, cloud computing

[241] Vgl. de rechtspraak *supra* noot 229.
[242] Vgl. m.n. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 50 – 51; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 106. Voor huiszoekingen gelden vergelijkbare waarborgen, vgl. o.a. EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*), § 57 en EHRM 30 maart 1989, nr. 10461/83 (*Chappell/United Kingdom)*, § 60.
[243] Vgl. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 51; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 115. Vgl. voorts EHRM 28 april 2005, nr. 41604/98 (*Buck/Germany*), § 49.
[244] Uitzondering hierop vormt de omstandigheid dat netwerkzoeking ex artikel 125j Sv niet door de genoemde verschijnselen wordt belemmerd, maar dat het opsporingsonderzoek wel heimelijk moet plaatsvinden; zie paragraaf 4 van hoofdstuk 4.

en/of anonimiseringstechnieken. Bij concrete toepassing moet dan ook steeds worden afgewogen of er in het specifieke geval geen subsidiaire alternatieven mogelijk zijn.[245]

De subsidiariteitswaarborg moet naar voren komen in de wettelijke omschrijving van de bevoegdheid en de constitutieve vereisten voor toepassing. Het voorgestelde artikel 125ja Sv schrijft in lid 1 voor dat toepassing van de bevoegdheid enkel is toegelaten 'indien het onderzoek dit dringend vordert'.[246] Dit vereiste is mijns inziens een voldoende sterke subsidiariteitswaarborg in het licht van artikel 8 lid 2 EVRM. Het 'dringend onderzoeksbelang' is een term die vast wordt gehanteerd in het Wetboek van Strafvordering om subsidiariteit te garanderen.[247] In de praktijk moet daarom bekend worden verondersteld wat de betekenis is van de term. Op deze manier kan worden bewerkstelligd dat de hackbevoegdheid alleen wordt toegepast wanneer andere opsporingsmethoden niet bruikbaar zijn doordat de verdachte gebruik maakt van versleuteling, draadloze netwerken, cloud computing en/of anonimiseringstechnieken. Zo wordt door middel van de subsidiariteitseis en de daartoe gestelde waarborgen toch invulling gegeven aan de gedachte dat de wens voor een hackbevoegdheid vooral is ontstaan in het kader van de bestrijding van computercriminaliteit.

Enkele kanttekeningen zijn wel op zijn plaats: een scherpe controle op naleving van de subsidiariteitswaarborg is onontbeerlijk en vormt een aparte waarborg die aan bod komt in paragraaf 3.3. Tevens valt het mijns inziens aan te bevelen om de specifieke betekenis van de term 'dringend onderzoeksbelang' nog eens nader te specificeren in bijvoorbeeld een 'Aanwijzing' van het OM, om concreet te benadrukken dat de hackbevoegdheid alleen mag worden ingezet wanneer het gebruik van versleuteling, draadloze netwerken, cloud computing en/of anonimiseringstechnieken andere opsporingsbevoegdheden onbruikbaar maakt.[248]

Wat betreft de proportionaliteit in concreto overweeg ik het volgende. Wanneer is vastgesteld dat toepassing van de hackbevoegdheid in een concreet geval subsidiair is, heeft deze toepassing mijns inziens in beginsel ook als proportioneel in concreto te gelden: wanneer er geen lichtere opsporingsbevoegdheid resultaat kan bereiken, brengt de ernst van de toepasselijke typen delicten mee dat de toepassing automatisch proportioneel is. Een ander uitgangspunt zou het onwenselijke gevolg hebben dat zich situaties zouden kunnen voordoen waarin ten aanzien van bepaalde ernstige delicten geen effectieve opsporingsmethoden beschikbaar zijn en een leemte met zich brengen die juist met de invoering van de hackbevoegdheid moet worden voorkomen c.q. opgelost.[249] Voor de hanteerbaarheid van dit uitgangspunt is wel van belang dat het delict waar het om gaat ook in concreto een ernstige inbreuk op de rechtsorde vormt (althans dat de verdenking hier van uit gaat); dit zal

[245] Zie ook Franken 2009, p. 83.
[246] MvT, p. 39.
[247] Binnen het systeem van de Wet BOB, zie *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 12.
[248] Vgl. bijvoorbeeld artikel 3 lid 2 van het Duitse *Gesetz zur Beschränkung des Brief-, Post- under Fernmeldegeheimnisses*, waarin specifiek wordt bepaald dat de heimelijke opsporingsbevoegdheid alleen mag worden ingezet wanneer opsporing op andere wijze uitzichtloos of bijzonder bezwarend is.
[249] Interessant zijn in dit kader de overwegingen van Van Kempen omtrent de subsidiariteitstoets in het kader van noodweer (artikel 41 Sr); ook hierbij geldt dat het wel aannemen van subsidiariteit maar niet van proportionaliteit leidt tot een eigenlijk onacceptabele leemte in de mogelijkheden van toepassing van de betreffende regeling. Zie Van Kempen 2011, p. 318 – 319.

gemotiveerd aangevoerd moeten worden in de vordering tot een machtiging voor toepassing van de hackbevoegdheid (zie nader paragraaf 3.3).
Anderzijds heeft uiteraard te gelden dat wanneer toepassing van de hackbevoegdheid niet subsidiair is, deze ook niet proportioneel kan zijn aangezien er dan in concreto geen *pressing social need* bestaat in de vorm van een dringend belang voor de opsporingsdiensten.

§ 3.2. Omvang en duur van de bevoegdheid[250]

Wanneer eenmaal is vastgesteld dat het dringend onderzoeksbelang toepassing van een hackbevoegdheid vereist, moet nog worden gegarandeerd dat de toepassing ook qua omvang en duur beperkt blijft tot hetgeen in een concreet geval in redelijke verhouding staat tot het dringende belang van de opsporing. De waarborgen voor beperking van de omvang van toepassing van de bevoegdheid kunnen worden onderverdeeld in beperkingen ten aanzien van de personen waartegen de bevoegdheid kan worden ingezet en ten aanzien van de gegevens die mogen worden verzameld.

Het EHRM acht het van belang dat de omvang van toepassing van heimelijke opsporingsbevoegdheden beperkt blijft tot de verdachte en/of personen die rechtstreeks bij de verdachte betrokken zijn en acht derhalve *'exploratory or general surveillance'* niet toegestaan.[251] Het is in dit kader dan ook noodzakelijk, en daar is in de overwegingen gedurende dit onderzoek ook van uit gegaan, om de toepassing van de hackbevoegdheid te beperken tot een geautomatiseerd werk van de verdachte of een rechtstreeks betrokkene, althans een geautomatiseerd werk dat door deze categorieën personen wordt gebruikt. Het voorgestelde artikel 125ja Sv voldoet aan dit criterium: de bevoegdheid tot het binnendringen in een geautomatiseerd werk wordt beperkt tot een werk dat bij een verdachte in gebruik is.[252]

Een groot deel van de inbreuk van een hackbevoegdheid komt voort uit het risico dat opsporingsambtenaren na binnendringen in een geautomatiseerd werk onbeperkt toegang hebben tot de vaak grote hoeveelheden privacygevoelige gegevens die daar zijn opgeslagen.[253] Om die reden dient tevens te worden gegarandeerd dat de toepassing van de voorgestelde bevoegdheid beperkt blijft tot enkel die gegevens die relevant (kunnen) zijn voor het opsporingsonderzoek. Deze waarborg is ook opgenomen in het voorgestelde artikel 125ja Sv: toepassing van de bevoegdheid moet worden beperkt tot een zo beperkt mogelijk en gespecificeerd deel van het geautomatiseerde werk in kwestie.[254] Wanneer tijdens de toepassing blijkt dat binnendringen in een ander deel van het geautomatiseerde werk nodig is, dan is daarvoor een aangepast bevel en uitdrukkelijke toestemming van de rechter-commissaris nodig.[255] Wegens het unieke risico van onbeteugelde kennisneming van

[250] Strikt genomen hecht het EHRM belang aan de *aard*, omvang en duur van de bevoegdheid (zie bijvoorbeeld EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 50); de heimelijke aard van de bevoegdheid is echter juist de overkoepelende factor naar aanleiding waarvan de overige waarborgen moeten worden ingevuld en hieraan komt dan ook geen zelfstandige betekenis toe.
[251] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 51. Zie ook paragraaf 2.2.1 van hoofdstuk 6.
[252] MvT, p. 39.
[253] Zie paragrafen 2.2.2 en 2.2.4 van hoofdstuk 6.
[254] Zie het voorgestelde artikel 125ja lid 2 aanhef en onder e Sv en MvT, p. 40.
[255] MvT, p. 40.

gegevens verbonden aan een hackbevoegdheid ontbreken specifieke maatstaven van het EHRM en een specifieke nationale regeling om aansluiting bij te zoeken. Evenwel past deze procedure binnen het stelsel van waarborgen voor proportionaliteit en subsidiariteit dat tot stand is gebracht met het oog op artikel 8 lid 2 EVRM.[256]
Opgemerkt zij dat het praktisch gezien vrijwel onmogelijk zal zijn om voorafgaand aan toepassing van een hackbevoegdheid reeds met zekerheid vast te stellen welke gegevens precies relevant (kunnen) zijn voor het opsporingsonderzoek, waardoor het onvermijdelijk is dat ook kennis zal worden genomen van niet relevante (maar mogelijk wel privacygevoelige) gegevens.[257] De maatstaf moet mijns inziens bij de voorafgaande toetsing, inclusief de toetsing van eventuele uitbreiding van de toepassing, dan ook zijn dat 'voor zover redelijkerwijs mogelijk' enkel kennis mag worden genomen van voor het onderzoek relevante gegevens, en bij toetsing achteraf of aan deze beperking 'in redelijkheid' gehoor is gegeven bij het kennisnemen van de gegevens.

Veranderen de bovenstaande overwegingen omtrent de kennisneming van gegevens wanneer sprake is van 'gevoelige' gegevens, zoals die omtrent het seksuele leven of medische informatie, die (mogelijk) een bijzonder zware bescherming genieten binnen artikel 8 EVRM en waarvan verwacht kan worden dat deze regelmatig op een geautomatiseerd werk worden opgeslagen?[258] Mijns inziens is dit niet het geval. Weliswaar genieten 'gevoelige' gegevens mogelijk een bijzonder zware bescherming onder artikel 8 EVRM, maar de toepassing van een hackbevoegdheid is reeds beperkt tot gevallen van een specifieke verdenking van de zwaarste categorie strafbare feiten die het Nederlandse Wetboek van Strafvordering kent, met het extra criterium dat het strafbare feit ten aanzien waarvan een verdenking plaatsvindt een ernstige inbreuk op de rechtsorde veroorzaakt. Gezien die omstandigheden geldt mijns inziens dat ten aanzien van gevoelige gegevens niet een nog zwaardere proportionaliteitseis kan gelden, ondanks dat deze gegevens mogelijk strikt genomen een zwaardere bescherming verdienen onder artikel 8 EVRM. Wanneer er geen mogelijkheid is om zonder kennisneming van gevoelige gegevens voldoende informatie te verzamelen in een opsporingsonderzoek naar een zeer ernstig strafbaar feit en de toepassing in die zin dus subsidiair is, heeft de kennisneming van deze gegevens mijns inziens ook als proportioneel te gelden omdat onacceptabel is dat geen effectief opsporingsonderzoek naar zulke ernstige strafbare feiten kan worden uitgevoerd. Ook ten aanzien van gevoelige gegevens geldt derhalve de waarborg dat deze mogen worden verzameld indien en voor zover zij relevant (kunnen) zijn voor het opsporingsonderzoek.

Wat betreft de duur van toepassing van de hackbevoegdheid kan aansluiting worden gezocht bij de maximale duur voor toepassing van andere heimelijke opsporingsbevoegdheden in

[256] Vgl. *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 79 – 80 en EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 52 wat betreft heimelijke surveillance; *Kamerstukken II* 2003/04, 29 441, nr. 3 en EHRM 30 maart 1989, nr. 10461/83 (*Chappell/United Kingdom)*, § 60 wat betreft huiszoekingen.
[257] Vgl. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.
[258] Zie ook *supra* noot 200 en 201.

binnen- en buitenland.[259] In zoverre is de maximale duur van vier weken, vastgelegd in lid 3 van het voorgestelde artikel 125ja Sv, ook als proportioneel te beschouwen. Dat de duur van toepassing verlengd kan worden doet hier niet aan af.[260]
Het EHRM hecht evenwel vooral belang aan de waarborgen die garanderen dat de duur van de toepassing van de bevoegdheid in specifieke gevallen in verhouding staat tot het delict in kwestie.[261] Een van zulke waarborgen is de eis dat verlenging van de toepassing plaatsvindt op basis van een apart bevel, dat aan dezelfde vereisten moet voldoen als het oorspronkelijke bevel tot toepassing.[262] Deze waarborg is ook opgenomen in het voorgestelde artikel 125ja lid 3 Sv: voorafgaand aan de verlenging dient te worden beoordeeld of nog wordt voldaan aan de vereisten voor toepassing van de bevoegdheid, zo volgt uit de aansluiting van het voorgestelde artikel bij de artikelen 126l en 126m Sv, die deze waarborg ook kennen.[263]
Tevens is het van belang dat de toepassing van de bevoegdheid onmiddellijk wordt beëindigd wanneer (een van) de voorwaarden voor toepassing ophoud(t)(en) te bestaan.[264] Ook deze waarborg is in het voorgestelde artikel 125ja Sv opgenomen door de aansluiting bij artikel 126l (lid 6) en artikel 126m (lid 5) Sv. Wanneer de officier van justitie tussentijds oordeelt dat de gronden waarop het bevel is gegeven zijn vervallen, dient hij op dat moment de toepassing van de bevoegdheid te beëindigen.[265]

§ 3.3. Toestemming en controle

Om te garanderen dat de waarborgen ten behoeve van proportionaliteit en subsidiariteit van toepassing van een heimelijke opsporingsbevoegdheid worden nageleefd, is een systeem van toestemming en controle nodig. Dit is ook het standpunt van het EHRM: het Hof acht in het kader van dit criterium doorslaggevend het bestaan van een procedure die garandeert dat maatregelen alleen op zorgvuldige wijze worden toegepast.[266] Mijns inziens moet de maatstaf echter nog iets specifieker zijn: de procedure dient te garanderen dat specifiek de proportionaliteit en subsidiariteit van toepassing van de bevoegdheid voldoende worden betrokken in de overwegingen, zodat wordt gegarandeerd dat de toepassing plaatsvindt in aansluiting op een *pressing social need* en de inbreuk op de privacy in redelijke verhouding staat tot het opsporingsbelang.[267]

[259] Voor het binnenland zie artikel 126l lid 5 Sv en artikel 126m lid 5 juncto artikel 126l lid 5 Sv. Voor het buitenland zie bijvoorbeeld de tijdslimiet gesteld in de Duitse G10-regeling, goedgekeurd door het EHRM in EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 116.
[260] Zie EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 116, waarin het EHRM de mogelijkheid tot verlenging van de duur van toepassing van een heimelijke bevoegdheid goedkeurt.
[261] Zie EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 161.
[262] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 52; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 116; EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 161.
[263] Zie ook MvT, p. 78 en *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 80.
[264] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 52; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 116; EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 161.
[265] Zie ook MvT, p. 78 en *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 80.
[266] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 51; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 115. Vgl. EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*), § 57.
[267] Vgl. EHRM 27 mei 2004, nr. 66746/01 (*Connors/United Kingdom*), § 83, waarin het EHRM ook deze strengere maatstaf hanteert vanwege de beperkte *margin of appreciation*.

Mijns inziens kan de procedure van toestemming en controle worden gebaseerd op de procedure die met de Wet BOB is ingevoerd voor de bestaande heimelijke opsporingsbevoegdheden. Dit lijkt mij een logisch basismodel voor een toetsingsprocedure van een hackbevoegdheid. Immers is deze procedure reeds afgestemd op de risico's en complicaties die heimelijkheid van opsporingsbevoegdheden met zich meebrengt, en kunnen de specifieke toevoegingen aan de procedure die nodig zijn vanwege de bijzondere kenmerken van een hackbevoegdheid aan dit basismodel worden toegevoegd. Ook het conceptwetsvoorstel Computercriminaliteit III, waarnaar ik meermaals zal terugkoppelen, baseert de procedure van toestemming en controle op de Wet BOB.

De rol van de officier van justitie en de rechter-commissaris zal in de voorafgaande toetsingsprocedure vergelijkbaar moeten zijn met de rol die zij reeds vervullen op basis van de Wet BOB.[268] De officier van justitie is daarbij de autoriteit die bevoegd is om een bevel tot binnendringen in een geautomatiseerd werk te geven. Alvorens hij dit bevel kan geven dient hij een schriftelijke machtiging van de rechter-commissaris te vorderen. Deze vordering is in het conceptwetsvoorstel Computercriminaliteit III reeds nader gespecificeerd: de officier moet specifiek vermelden voor welk doel de bevoegdheid in het betreffende opsporingsonderzoek wordt ingezet, de aard en de functionaliteit van het technische hulpmiddel vermelden en aangeven ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens de bevoegdheid wordt toegepast.[269] Uiteindelijk vindt de voorafgaande toetsing van de proportionaliteit en de subsidiariteit vooral plaats door de rechter-commissaris, en de nadruk dient derhalve op zijn rol te liggen.[270]

De voorafgaande toetsing door een onafhankelijke rechterlijke ambtenaar vormt een sterke en wenselijke waarborg voor de proportionaliteit en subsidiariteit: er wordt immers voorzien in *'supervisory control'* door een rechter.[271] Over de daadwerkelijke invulling van de rol bestaat wel kritiek, inhoudende dat rechters-commissarissen nog maar zijdelings betrokken zijn bij opsporingsonderzoeken en dat machtigingen voor het aftappen of opnemen van communicatie zelden worden afgewezen.[272] Overigens zij opgemerkt dat hierbij waarschijnlijk ook een rol speelt dat het enkele vooruitzicht van een toetsing er reeds voor zorgt dat alleen de vorderingen met een hoge kans van slagen naar de rechter-commissaris worden gestuurd.[273]

Mijns inziens moet een wettelijk vastgelegde waarborg van voorafgaande rechterlijke toetsing reeds als voldoende worden beschouwd.[274] De discussie of de rol van de rechter-commissaris in de praktijk naar tevredenheid wordt ingevuld is uiteraard van belang, maar heeft mijns

[268] Vgl. MvT, p. 28 – 29 en *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 14 – 16.
[269] MvT, p. 29.
[270] Zie ook Beijer e.a. 2004, waarin geen evaluatie plaatsvindt van de afweging door de officier van justitie.
[271] Zie o.a. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 56; *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 15. Vgl. EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*), § 57.
[272] Beijer e.a. 2004, p. 193; Franken 2009, p. 85 – 86.
[273] Franken 2009, p. 86 – 87.
[274] Zie ook het 'advies Wetsvoorstel computercriminaliteit III' van de Raad voor de Rechtspraak d.d. 4 juli 2013, p. 2, te raadplegen via <http://www.rechtspraak.nl/Organisatie/Raad-Voor-De-Rechtspraak/Wetgevingsadvisering/Wetgevingsadviezen2013/2013-27-Advies-Wetsvoorstel-computercriminaliteit-III.pdf>.

inziens geen directe invloed op de toereikendheid van de wettelijk vastgelegde waarborg.[275] Een perfecte score kan ook niet worden verwacht en de omstandigheid dat er nog steeds naar wordt gestreefd de functie van de rechter-commissaris een zo goed mogelijke invulling te geven (recent weer met de op 1 januari 2013 in werking getreden Wet versterking positie rechter-commissaris) is mijns inziens ook een positieve factor in de toereikendheid van de waarborg van toetsing door de rechter-commissaris in het licht van artikel 8 lid 2 EVRM.

Voor toepassing van de bevoegdheid tot het binnendringen in een geautomatiseerd werk dient, zoals voor toepassing van alle heimelijke opsporingsbevoegdheden, als vereiste te worden gesteld dat vooraf toestemming wordt gevraagd aan het College van procureurs-generaal (het College), de landelijke leiding van het OM.[276] Het College wordt weer geadviseerd door de CTC, een intern adviesorgaan van het OM samengesteld uit leden van het OM en de politie.[277] Dit systeem van toestemming en advisering wordt eveneens in het conceptwetsvoorstel Computercriminaliteit III aangedragen.[278] Dat noch het College noch de CTC een democratisch of onafhankelijk orgaan is, is niet problematisch: de democratische inkleding en onafhankelijkheid van toezichthoudende organen wordt in de rechtspraak van het EHRM weliswaar als belangrijke waarborg voor proportionaliteit en subsidiariteit beschouwd, maar vooral wanneer hiermee een gebrek aan rechterlijke controle in de procedure moet worden gecompenseerd.[279] Het Hof geeft er sterk de voorkeur aan dat de toezichthoudende taak (ook) wordt toebedeeld aan een rechter.[280] Wanneer de nationale wetgeving wél voorziet in controle door een onafhankelijke rechterlijke ambtenaar, zoals in Nederland het geval is met de rol van de rechter-commissaris, acht het Hof de specifieke inkleding van de overige betrokken organen beduidend minder van belang.[281] Zo bezien vormt het vooral een pluspunt dat er nog een extra toetsing plaatsvindt, die de grote lijnen bewaakt en bovendien in de praktijk ook daadwerkelijk leidt tot een kritische beoordeling of toepassing van een heimelijke opsporingsbevoegdheid daadwerkelijk noodzakelijk is.[282] Het Nederlandse systeem van toetsing op centraal niveau kan dan ook door de Europese beugel.

Het EHRM heeft ingestemd met het Duitse systeem van toekenning van de beslissing tot toepassing van heimelijke opsporingsbevoegdheden aan een minister, die over de toepassing van de bevoegdheden periodiek verantwoording moet afleggen tegenover toezichthoudende

[275] Dit geldt voor de toetsing *in abstracto* zoals in dit onderzoek uitgevoerd; in een concrete toetsing van een specifiek geval door het EHRM kan een gebrekkige toetsing door de rechter-commissaris natuurlijk wel leiden tot een schending van het vereiste van voldoende waarborgen en daarmee een schending van artikel 8 EVRM.
[276] Zie <http://www.om.nl/organisatie/college_van/>.
[277] Zie de 'Aanwijzing opsporingsbevoegdheden (2012A012)', par. 5.1, te raadplegen via <http://www.om.nl/organisatie/beleidsregels/overzicht/opsporing/@158933/aanwijzing-1/>.
[278] MvT, p. 28.
[279] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 55; aansluiting hierop in EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 117.
[280] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 56; EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 167. Vgl. EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*), § 57.
[281] Zie EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 166. Vgl. EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*), § 57.
[282] Zie Beijer e.a. 2004, p. 162 – 163.

organen met daarin vertegenwoordigers van het parlement.[283] Ook het systeem van de Britse RIPA, dat de bevoegdheid tot het bevelen van toepassing van heimelijke strafvorderlijke bevoegdheden toekent aan de *Secretary of State*, kreeg de goedkeuring van het Hof.[284] Het Nederlandse systeem ziet er anders uit en biedt niet een dergelijke specifieke verdeling van bevoegdheden en verantwoordelijkheden tussen de minister van Veiligheid en Justitie en toezichthoudende organen. De minister is niet zelf bevoegd om het bevel te geven tot toepassing van een opsporingsbevoegdheid: de opsporingsbevoegdheden zijn zuiver geattribueerd aan het OM (zie o.a. artikel 148 Sv).[285] De minister heeft ook geen verplichting om periodiek verantwoording af te leggen aan een toezichthoudend orgaan; het College dient juist aan de minister periodiek verslag te doen over het aantal ter toetsing en registratie aangeboden bevoegdheden tot het binnendringen in een geautomatiseerd werk.[286]

Is het Nederlandse systeem toelaatbaar in het licht van artikel 8 lid 2 EVRM? Mijns inziens is dit wel het geval. Ten eerste is er geen indicatie om te geloven dat het algemene Nederlandse systeem van bevoegdheid- en verantwoordelijkheidverdeling tussen minister en OM door het EHRM niet wordt of zou worden geaccepteerd. Ten tweede betrekt het EHRM de rol van de minister in de toepassing van heimelijke opsporingsbevoegdheden wel in de beoordeling van de waarborgtoets, maar is dit slechts één van de factoren waaraan het Hof belang toekent. Het belangrijkste is dat er een voorafgaande onafhankelijke en/of democratische toetsing van de toepassing van de opsporingsbevoegdheid plaatsvindt, bij voorkeur door een rechterlijk ambtenaar: in het Nederlandse systeem wordt deze toetsing uitgevoerd door de rechter-commissaris. Ten derde heeft de minister wel de verplichting om inlichtingen te verschaffen die door leden van het parlement worden verlangd (artikel 68 Gw) en is de minister tegenover het parlement verantwoordelijk voor de uitvoering van opsporingsbevoegdheden door het OM.[287] Derhalve kan door het parlement democratische controle op de toepassing van de hackbevoegdheid worden uitgeoefend.

In aansluiting op de voorafgaande toetsingen en de algemene democratische controle van toepassing van de hackbevoegdheid komt ook een belangrijke rol toe aan de rechterlijke toetsing achteraf. Zoals Jacobs in 2012 naar aanleiding van de hackplannen van de minister reeds opmerkte, heeft de rechter-commissaris in beginsel vrijwel geen controle meer wanneer hij een machtiging voor toepassing heeft afgegeven. Vanaf dat moment kan de rechter-commissaris, in tegenstelling tot bijvoorbeeld tijdens een doorzoeking van een woning, zelf geen rechtstreeks toezicht meer houden op de wijze van toepassing en dus niet beoordelen of de hackbevoegdheid op de voorgeschreven wijze wordt toegepast.[288] Hij blijft wel degene die eventuele uitbreiding van de omvang van de bevoegdheid moet bevelen, maar kan tijdens het onderzoek niet zelf beoordelen of hij al dan niet hiervoor moet worden benaderd. Op die

[283] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 18 en 21; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 20 en 24.
[284] EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 31.
[285] Zie Corstens 2011, p. 99.
[286] Zie MvT, p. 28; artikel 129 lid 1 Wet RO.
[287] Zie Corstens 2011, p. 149.
[288] Zie Jacobs 2012, p. 2762.

manier blijft er een risico bestaan van onjuist gebruik of misbruik van de bevoegdheid zoals uiteengezet in paragraaf 2.2.4 van hoofdstuk 6. Dit is grotendeels een probleem waarmee alle heimelijke opsporingsbevoegdheden kampen, een probleem dat moet worden bestreden door controle achteraf. In dat kader worden strenge eisen gesteld aan de technische hulpmiddelen waarmee de opsporingsbevoegdheden worden ingezet, zodat de wijze van toepassing wordt geregistreerd en achteraf kan worden gecontroleerd: zie met name de artikelen 10 en 11 van het Besluit technische hulpmiddelen strafvordering.[289] Voor een hackbevoegdheid dient ook een dergelijke applicatie te worden ontwikkeld en ingezet (Jacobs spreekt van '*secure logging*'), die (onder andere) bijhoudt op welke delen van een geautomatiseerd werk de bevoegdheid wordt toegepast, van welke gegevens kennis wordt genomen en hoe lang de bevoegdheid wordt toegepast.[290] Tevens dient de *logging* functionaliteit te registreren welke gegevens door opsporingsambtenaren op het binnengedrongen geautomatiseerde werk worden geplaatst, zodat getoetst kan worden of sprake is geweest van manipulatie van gegevens waardoor een heel ander beeld van iemand kan worden gecreëerd (zie paragraaf 2.2.4 van hoofdstuk 6). De nadere uitwerking van de eisen die aan het technisch hulpmiddel en de toepassing hiervan moeten worden gesteld is te specifiek (en te technisch) voor dit onderzoek. Waarschijnlijk zullen deze vereisten wederom worden uitgewerkt bij AMvB, hetgeen ook reeds is voorgesteld in het conceptwetsvoorstel Computercriminaliteit III.[291] Toepassing van een eventuele hackbevoegdheid zal uiteraard pas toegestaan zijn wanneer de technische en processuele eisen daadwerkelijk bij AMvB zijn uitgewerkt en accurate controle achteraf dus mogelijk is.

In Nederland kan de procedure van toestemming en controle worden gebaseerd op de procedure uit de Wet BOB, met enkele specifieke toevoegingen op basis van de kenmerken van een hackbevoegdheid, op de wijze zoals hierboven uiteengezet. Een dergelijk systeem vormt een sterke waarborg voor proportionaliteit en subsidiariteit van toepassing van de hackbevoegdheid, en wordt ook in het conceptwetsvoorstel Computercriminaliteit III aangedragen.

§ 3.4. De 'remedy' naar nationaal recht

De eis van een '*effective remedy*' betreft de mogelijkheden voor burgers om tegen toepassing van opsporingsbevoegdheden op te komen.[292] De '*effective remedy'* vormt hiermee een laatste redmiddel tegen onjuiste toepassing van opsporingsbevoegdheden, wanneer de in paragraaf 3.1 tot en met 3.3 besproken waarborgen onverhoopt tekortschieten. Het EHRM heeft overwogen dat betrokkenen niet in de voorafgaande beoordeling van de toepassing van een heimelijke opsporingsbevoegdheid kunnen worden betrokken, juist vanwege het heimelijke

[289] Besluit van 20 oktober 2006, *Stb*. 2006, 524. Zie ook T. Blom, aant. 3 op artikel 126ee Sv, in: C.P.M. Cleiren & M.J.M. Verpalen (red.), *Tekst en Commentaar Strafvordering* 2011.
[290] Zie ook Jacobs 2012, p. 2762.
[291] Het voorgestelde artikel 125ja lid 6 Sv; zie ook MvT, p. 24.
[292] Hoewel de eis van een '*effective remedy before a national authority*' is vastgelegd in artikel 13 EVRM, wordt deze vaak (in ieder geval deels) 'geabsorbeerd' door de vraag of artikel 8 EVRM is geschonden: zie o.a. Van Dijk e.a. 2006, p. 1021; Jacobs, White & Ovey 2010, p. 133; EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 50 en 55 – 57; EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/United Kingdom*), § 167 – 169 en 196.

karakter.[293] Om die reden kan van staten maximaal gevergd worden dat zij voorzien in een *effective remedy* ná toepassing van een heimelijke opsporingsbevoegdheid.

Wat betreft de (naar de aard heimelijke) hackbevoegdheid is de eerste stap in het garanderen van een *effective remedy* dan ook het op de hoogte brengen van de betrokkene(n) dat de bevoegdheid is toegepast, hetgeen dient te gebeuren middels notificatie.[294] Het conceptwetsvoorstel Computercriminaliteit III sluit zich hierbij aan en het voorgestelde artikel 125ja Sv is onderworpen aan de regeling van artikel 125m en artikel 126bb Sv waarin de notificatieplicht van de officier van justitie is opgenomen.[295] Op basis van artikel 125m lid 2 en artikel 126bb Sv geldt de notificatieplicht evenwel pas zodra 'het belang van het onderzoek' dat toelaat.[296] Deze beperking van de notificatieplicht is op basis van de rechtspraak van het EHRM toegestaan: het Hof accepteert dat notificatie aan een verdachte in bepaalde gevallen strijdig kan zijn met de doelen van een heimelijk onderzoek, zelfs na beëindiging van de toepassing van de heimelijke opsporingsbevoegdheid zelf.[297] Voldoende is dat er een plicht tot notificatie bestaat zodra het belang van het onderzoek dit toelaat. De regeling inzake de notificatieplicht van het voorgestelde artikel 125ja Sv is derhalve toelaatbaar, al acht ik het wel van belang om de eis te stellen dat de officier van justitie zijn beroep op het onderzoeksbelang onderbouwt met concrete redenen en deze op schrift stelt bij de beslissing om notificatie achterwege te laten, zodat toetsing van deze beslissing achteraf mogelijk is en zo misbruik kan worden voorkomen. Hiermee kan worden voorkomen dat de notificatieplicht bij toepassing van de hackbevoegdheid een dode letter wordt zoals in het kader van het aftappen van telecommunicatie reeds het geval lijkt te zijn.[298] Waar ten aanzien van de notificatieplicht bij aftappen nog gesteld kan worden dat het aantal afgetapte personen en hun contactpersonen te groot is om daadwerkelijk de notificatieplicht te kunnen hanteren, hoeft dit ten aanzien van de hackbevoegdheid niet te gelden. Het uitgangspunt moet immers zijn dat de hackbevoegdheid alleen in bijzondere gevallen wordt gebruikt en niet massaal wordt ingezet (zie ook paragraaf 2.2.1 van hoofdstuk 6).

De tweede stap in de beoordeling van een *effective remedy* is de rechtsgang die de betrokkene ter beschikking staat. Deze stap treedt mijns inziens echter te ver in het gebied van artikel 13 EVRM en kan hier verder achterwege blijven. Ik volsta met de constatering dat de betrokkene in het Nederlandse rechtsstelsel na notificatie een rechtsgang openstaat bij de civiele rechter om schadevergoeding te vorderen op basis van onrechtmatige daad, hetgeen in beginsel kwalificeert als een *effective remedy* in de zin van het EVRM.[299]

---

[293] Zie EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 55; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 117.
[294] Vgl. EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 57; *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 11 – 12; Buruma 2001, p. 28.
[295] MvT, p. 30.
[296] Zie ook MvT, p. 30.
[297] EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 58; EHRM 29 juni 2006, nr. 54934/00 (*Weber and Saravia/Germany*), § 135 – 136; zie ook Buruma 2001, p. 29.
[298] Zie ook Beijer e.a. 2004, p. 145 – 147.
[299] Zie EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*), § 71.

§ 4. Conclusie: een *fair balance*

Het dringende belang van de opsporing bij invoering van een hackbevoegdheid vormt een *pressing social need* en wanneer het gaat om de zwaarste categorie delicten (de delicten opgenomen in artikel 67 lid 1 Sv die bovendien een ernstige inbreuk maken op de rechtsorde) staat de inbreuk op het privéleven die een hackbevoegdheid met zich brengt in redelijke verhouding tot het belang van de opsporing, en is er in Nederland voldoende grond voor een hackbevoegdheid. Deze conclusie sluit naar mijn mening aan op de realiteit van de moderne samenleving, waarin cybercriminaliteit en kinderporno wijdverspreid plaatsvinden zonder dat daartegen momenteel consequent effectief opgetreden kan worden, en waarin daarnaast vrijwel alle delicten op zodanige wijze kunnen (en steeds meer zullen) worden gepleegd dat hierbij gebruik wordt gemaakt van versleuteling, draadloze netwerken, cloud computing en anonimiseringstechnieken. Het kan niet worden geaccepteerd dat deze verschijnselen de opsporing van de ernstigste delicten die het Nederlandse strafrecht kent praktisch onmogelijk maken. Wel dienen de risico's van verkeerd gebruik of zelfs misbruik die aan de hackbevoegdheid zijn verbonden middels waarborgen te worden geneutraliseerd, zodat wordt gegarandeerd dat de toepassing van de hackbevoegdheid ook in concrete gevallen aansluit op een *pressing social need* en in redelijke verhouding staat tot het belang van het opsporingsonderzoek.

Wanneer toepasbaarheid van een hackbevoegdheid wordt beperkt tot de zwaarste categorie delicten en de bevoegdheid met de in de vorige paragraaf uiteengezette waarborgen voor proportionaliteit en subsidiariteit wordt omkleed, is er mijns inziens sprake van een *fair balance* tussen de belangen van de opsporing en de belangen van de bescherming van de privacy van burgers.

De waarborgen komen ook naar tevredenheid naar voren in het in het conceptwetsvoorstel Computercriminaliteit III opgenomen artikel 125ja Sv. De eis van aanwezigheid van een 'dringend onderzoeksbelang' garandeert dat de hackbevoegdheid enkel wordt toegepast wanneer de opsporing van ernstige strafbare feiten gehinderd wordt door gebruik van versleuteling, draadloze netwerken, cloud computing en/of anonimiseringstechnieken; de beperkingen die worden gesteld aan de omvang en duur van toepassing van de bevoegdheid leiden ertoe dat toepassing enkel mogelijk is ten aanzien van de verdachte, ten aanzien van een beperkt en gespecificeerd aantal gegevens en voor een beperkte duur; de procedure voor toepassing van de bevoegdheid biedt rechterlijke en/of democratische toetsing zowel vooraf als achteraf; en tot slot biedt de notificatieplicht in het licht van de rechtspraak van het EHRM een *effective remedy*.

Hoofdstuk 8: De mogelijkheden voor een hackbevoegdheid in Nederland

§ 1. Beantwoording hoofdvraag: het belang van een *fair balance*

De hoofdvraag die ten grondslag lag aan dit onderzoek is '*Wat zijn de mogelijkheden voor de invoering van een wettelijke bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk in Nederland, met inachtneming van het vereiste 'noodzakelijk in een democratische samenleving' als vastgelegd in artikel 8 lid 2 EVRM?'*. Middels de in paragraaf 2 van hoofdstuk 1 geformuleerde deelvragen, welke ik in respectievelijk hoofdstuk 2, hoofdstuk 5, hoofdstuk 6 en hoofdstuk 7 heb beantwoord, kom ik tot de volgende conclusie en beantwoording van de hoofdvraag.

Door de inbreuk die een hackbevoegdheid maakt op het recht op integriteit en vertrouwelijkheid van ICT-systemen, welk recht valt onder de bescherming van het recht op privéleven ex artikel 8 EVRM, staat buiten kijf dat de mogelijkheden voor de invoering van een hackbevoegdheid afhankelijk zijn van de maatstaven van artikel 8 lid 2 EVRM en de invulling die hier door het EHRM aan gegeven wordt. Dit betekent dat de inbreuk op het recht op privéleven, zowel van de hackbevoegdheid op zich als van concrete toepassing hiervan, moet aansluiten op een *pressing social need* en in een redelijke verhouding moet staan tot het belang van de opsporing van strafbare feiten. Er moet derhalve een *fair balance* worden gecreëerd tussen het dringende belang van de opsporing bij invoering (en uiteindelijk: toepassing) van een hackbevoegdheid enerzijds en het belang van burgers bij de waarborging van hun recht op privéleven anderzijds. Wanneer bij de inkleding van een hackbevoegdheid deze *fair balance* wordt bewaard, kan de bevoegdheid worden beschouwd als 'noodzakelijk in een democratische samenleving' in de zin van artikel 8 lid 2 EVRM. De mogelijkheden om een hackbevoegdheid in overeenstemming met het noodzakelijkheidscriterium in te voeren worden dus bepaald door de eisen die worden gesteld aan de realisatie van een *fair balance*.

De eerste eis voor een *fair balance* is dat er voldoende grond is voor de hackbevoegdheid: de bevoegdheid moet beantwoorden aan een *pressing social need* in de Nederlandse maatschappij en in abstracto in redelijke verhouding staan tot het belang van de opsporing van strafbare feiten. In Nederland hebben de opsporingsdiensten een dringend belang bij de invoering van een wettelijke hackbevoegdheid, zoals vastgesteld in hoofdstuk 3 tot en met 5. De opsporingspraktijk wordt ernstig belemmerd door met name de versleuteling van elektronische gegevens en het gebruik van anonimiseringstechnieken en tevens door het gebruik van draadloze netwerken, terwijl cloud computing naar verwachting in de nabije toekomst ernstige belemmeringen zal veroorzaken in opsporingsonderzoeken. De huidige opsporingsbevoegdheden schieten tekort om hiertegen consequent een oplossing te bieden en een hackbevoegdheid kan deze problemen juist wel stelselmatig oplossen. Er bestaat dus een *pressing social need* in de Nederlandse maatschappij.
Een hackbevoegdheid staat in redelijke verhouding tot de categorie 'zeer zware misdrijven' (zie paragraaf 2 van hoofdstuk 7). Een van de bestaansredenen van artikel 8 lid 2 EVRM is

om de nationale overheid de mogelijkheid te bieden om ten behoeve van de opsporing van deze delicten een (ernstige) inbreuk op het recht op privéleven te maken; om die reden mogen ten aanzien van de betreffende delicten reeds de zwaarste bestaande heimelijke opsporingsbevoegdheden worden toegepast. Dat een hackbevoegdheid een inbreuk maakt op het recht op integriteit en vertrouwelijkheid van ICT-systemen doet niet af aan het uitgangspunt: dit recht weegt niet zwaarder dan de algemene bescherming van privégegevens, locatiegegevens en (tele-) communicatie, ook niet wanneer dit recht analoog aan het huisrecht wordt geïnterpreteerd. Wanneer toepasbaarheid van de hackbevoegdheid wordt beperkt tot de categorie 'zeer zware delicten', staat de inbreuk in redelijke verhouding tot het belang van de opsporing van strafbare feiten en is voldaan aan het eerste vereiste voor een *fair balance*.

De tweede eis voor een *fair balance* is dat de hackbevoegdheid wordt omkleed met voldoende waarborgen om te garanderen dat de beginselen van proportionaliteit en subsidiariteit ook bij concrete toepassingen van de hackbevoegdheid voldoende in acht worden genomen, zodat toepassing van de hackbevoegdheid ook in de concrete gevallen waarin het wordt toegepast aansluit op een *pressing social need* en in redelijke verhouding staat tot het belang van de opsporing. De combinatie van de heimelijke aard van een hackbevoegdheid met de potentieel enorme hoeveelheid privacygevoelige gegevens die na het binnendringen in een geautomatiseerd werk voor het oprapen liggen, brengt risico's van verkeerd gebruik of zelfs misbruik van deze bevoegdheid mee die in potentie ongekend grote negatieve gevolgen kunnen hebben voor de persoonlijkheid en de persoonlijke ontwikkeling van burgers. Deze negatieve gevolgen moeten worden voorkomen door waarborgen te stellen die toepassing van de hackbevoegdheid beperken tot die gevallen waarin andere opsporingsbevoegdheden niet volstaan, vereisen dat de omvang en duur van de toepassing worden gespecificeerd, voorzien in een strenge toetsing en controle van de toepassing van de bevoegdheid (zowel voorafgaand aan de toepassing als achteraf), en een voldoende *effective remedy* bieden aan de burger ten aanzien van wie de hackbevoegdheid is toegepast. Deze waarborgen moeten worden ingekleed op de wijze als in paragraaf 3 van hoofdstuk 7 uiteengezet. In dat geval is ook aan het tweede vereiste voor een *fair balance* voldaan.

Door aan de hierboven uiteengezette vereisten voor een *fair balance* tussen opsporing en privacy te voldoen, kan de hackbevoegdheid de noodzakelijkheidstoets van artikel 8 lid 2 EVRM doorstaan en wat het noodzakelijkheidsvereiste betreft in Nederland worden ingevoerd. Uiteraard moet ook aan het legaliteitsvereiste worden voldaan, maar een hackbevoegdheid als hierboven omschreven is in Nederland mijns inziens fundamenteel toelaatbaar.

§ 2. Wetsvoorstel Computercriminaliteit III

Met het conceptwetsvoorstel Computercriminaliteit III ligt er reeds een concreet voorstel voor een hackbevoegdheid op tafel, en de voorgestelde bevoegdheid is tijdens dit onderzoek meermaals aan bod gekomen in het kader van de verschillende toetsingen. Ter afsluiting van het onderzoek zal ik in deze paragraaf nog een concrete beoordeling geven van de toelaatbaarheid van het voorgestelde artikel 125ja Sv (zoals het er nu ligt) in het licht van het

noodzakelijkheidsvereiste van artikel 8 lid 2 EVRM en benadrukken welke punten nog aandacht verdienen. Tevens zal ik nagaan hoe de argumentatie in de memorie van toelichting moet worden beoordeeld met het oog op de indringende toetsing aan het noodzakelijkheidsvereiste die de nationale overheid geacht wordt uit te voeren.

De argumentatie van de noodzakelijkheid van een hackbevoegdheid in de memorie van toelichting is vrij uitgebreid en duidelijk. Er wordt een indringende toetsing aan artikel 8 lid 2 EVRM uitgevoerd en de Nederlandse overheid kwijt zich vooralsnog dus goed van de taak die het EHRM haar stelt in de waarborging van het recht op privéleven ex artikel 8 EVRM. Het dringende belang van de opsporing en de belangen van burgers bij hun recht op privéleven komen aan bod en de argumenten snijden mijns inziens grotendeels hout. De memorie van toelichting weet de *pressing social need* voor een hackbevoegdheid goed aan te dragen, op basis van de factoren zoals ik die in paragraaf 3 van hoofdstuk 2 heb uiteengezet en in dit onderzoek nader heb behandeld. Tevens wordt de toepasbaarheid van het voorgestelde artikel 125ja Sv beperkt tot de zwaarste delicten, te weten de delicten genoemd in artikel 67 lid 1 Sv die bovendien een ernstige inbreuk op de rechtsorde vormen. Duidelijk is dat de voorgestelde bevoegdheid aan het eerste vereiste van de *fair balance* voldoet. Desondanks zijn er wel enkele aandachtspunten in de memorie van toelichting aan te stippen.

In het kader van de subsidiariteit wordt in de memorie van toelichting niet of nauwelijks aandacht besteed aan een aantal alternatieven die ik in dit onderzoek wel heb besproken. Voor de meeste van deze alternatieven geldt dat deze in dit onderzoek duidelijk zijn afgewezen als subsidiaire opties, waardoor hun omissie in de memorie van toelichting geen groot bezwaar is. Uitzondering hierop vormt de mogelijkheid van toepassing van de bevoegdheid tot het vorderen van inhoudelijke opgeslagen gegevens ex artikel 126ng lid 2 Sv, in geval van versleuteling van telecommunicatie. Deze wordt in de memorie van toelichting volledig genegeerd, en hoewel ik in hoofdstuk 4 heb geconcludeerd dat deze optie waarschijnlijk geen subsidiair alternatief vormt voor een hackbevoegdheid, is het mijns inziens van belang om deze optie wel aan bod te laten komen in het wetgevingsproces en de praktische mogelijkheden en onmogelijkheden van de bevoegdheid ex artikel 126ng lid 2 Sv duidelijk te beargumenteren. Mijn oordeel is immers gebaseerd op inschattingen op basis van onvolledige gegevens. Juist de overheid beschikt over de gegevens (die zij niet openbaar wil maken) die nodig zijn om de kans van slagen van de bevoegdheid met meer zekerheid te beoordelen. Behandeling van artikel 126ng lid 2 Sv en de situaties waarin deze wel en niet effectief kan zijn in het wetgevingsproces kan er tevens aan bijdragen dat deze optie uiteindelijk daadwerkelijk voldoende in acht wordt genomen bij de beslissingen om de bevoegdheid tot het binnendringen in een geautomatiseerd werk in concrete gevallen al dan niet toe te passen.

Tevens bespreekt (of impliceert) de memorie van toelichting enkele gevallen van toepassing van de hackbevoegdheid die in het licht van het relevantiecriterium niet toelaatbaar zijn, te weten het hacken van smartphones om een verdachte die observatieteams weet af te schudden alsnog te kunnen observeren en (mogelijk) het activeren van een webcam of ingebouwde camera ten behoeve van stelselmatige observatie dan wel het activeren van een microfoon om

face-to-face gesprekken tussen personen in dezelfde ruimte af te luisteren. Voor zover deze toepassingen daadwerkelijk worden voorgesteld, moeten deze mijns inziens worden afgewezen en gedurende het wetgevingsproces worden verwijderd uit de mogelijke toepassingen van het voorgestelde artikel 125ja Sv.

Wat betreft het tweede vereiste van de *fair balance* ben ik van mening dat de voorgestelde hackbevoegdheid met voldoende waarborgen wordt omkleed om aan dit vereiste te voldoen. Ik heb nog enkele suggesties kunnen plaatsen om de effectiviteit van de waarborgen mogelijk nog wat te verhogen, maar de juridische inkleding van de waarborgen is mijns inziens duidelijk omschreven in de memorie van toelichting en ook inhoudelijk naar tevredenheid in het licht van het noodzakelijkheidsvereiste van artikel 8 lid 2 EVRM. Uitzondering hierop vormt vooralsnog het gebrek aan een duidelijk mechanisme voor de *logging* van de handelingen die opsporingsambtenaren op een binnengedrongen geautomatiseerd werk verrichten. Deze moet uiteraard, gezien het overwogene in paragraaf 3.3 van hoofdstuk 7, wel worden ontwikkeld voordat de hackbevoegdheid daadwerkelijk kan worden ingevoerd en toegepast.

Belangrijke kritieken, zoals die van Jacobs, komen vooral voort uit zorgen omtrent de praktische uitvoering van de hackbevoegdheid en de nadelige gevolgen die deze kan hebben voor de privacy.[300] De praktijk na invoering van de hackbevoegdheid ligt in beginsel buiten het bereik van dit onderzoek, maar desondanks acht ik ook ten aanzien hiervan een korte overweging nog op zijn plaats.

Mijns inziens kunnen de kritieken en de zorgen omtrent de praktische uitvoering van de hackbevoegdheid niet in de weg staan aan de introductie van een hackbevoegdheid, gezien de in dit onderzoek vastgestelde noodzakelijkheid van deze bevoegdheid voor de Nederlandse opsporing. Technische kinderziektes zullen er ongetwijfeld zijn en fouten zullen worden gemaakt. De complexiteit van toepassing van de hackbevoegdheid zal het uiterste vergen van de technische capaciteiten van politie en justitie. Dat is de realiteit die echter hoe dan ook zal gelden in de beginjaren van een hackbevoegdheid, ongeacht wanneer deze zal worden ingevoerd. Weliswaar zullen de technische capaciteiten van de politie over enkele jaren groter zijn dan nu (zie paragraaf 2 van hoofdstuk 5), maar zonder bevoegdheden bestaat er ook geen impuls om de technische capaciteiten significant uit te breiden. Uitstel heeft in zoverre mijns inziens geen zin. Uiteraard zijn het noodzakelijkheidsvraagstuk en zelfs het algehele privacyvraagstuk niet de enige kwesties die kunnen leiden tot juridische en praktische complicaties en zijn kwesties als de rechtsmachtproblematiek en de integriteit van bewijs in het kader van artikel 6 EVRM (kort aangestipt in hoofdstuk 5 respectievelijk hoofdstuk 6) ook van groot belang voor een effectieve uitvoering van een hackbevoegdheid. Voor zover het gaat om de bescherming van privéleven zijn er mijns inziens echter geen juridische bezwaren verbonden aan het voorgestelde artikel 125ja Sv, en worden de praktische problemen voor een groot deel reeds zoveel mogelijk beperkt door de gestelde waarborgen. De overige,

[300] Zie Jacobs 2012, p. 2761 – 2764.

onvermijdelijke problemen zullen in de praktijk moeten worden opgelost. In dit kader is het uiteraard wel van belang om de hackbevoegdheid regelmatig te evalueren, om na te kunnen gaan of de bevoegdheid daadwerkelijk effectief is, de waarborgen daadwerkelijk garanties bieden en de bevoegdheid daadwerkelijk met inachtneming van de vereisten van proportionaliteit en subsidiariteit wordt toegepast.

Wat betreft het voorgestelde artikel 125ja Sv is mijn conclusie dat deze in beginsel de noodzakelijkheidstoets van artikel 8 lid 2 EVRM kan doorstaan. Wel is het van belang dat in het wetgevingsproces nog kritisch wordt gekeken naar de subsidiaire alternatieven, ook om bij te dragen aan de ontwikkeling van een criterium wanneer een hackbevoegdheid al dan niet als subsidiair moet worden beschouwd, en dienen kritische vragen te worden gesteld omtrent de reikwijdte van de beoogde toepassingen van de hackbevoegdheid. Tevens is het noodzakelijk dat een bruikbare *logging* functionaliteit wordt ontwikkeld om de toepassing van de hackbevoegdheid te registreren. Tot slot is een periodieke evaluatie van de hackbevoegdheid in de praktijk van groot belang om te controleren of de waarborgen daadwerkelijk effectief zijn in het voorkomen van disproportionele en dissubsidiaire toepassing van de bevoegdheid.

§ 3. Slotoverweging: de hackbevoegdheid in andere landen

De invloed van de rechtsvergelijking op de proportionaliteitstoets, die in de rechtspraak van het EHRM ook doorschijnt,[301] is in dit onderzoek voornamelijk beperkt gebleven tot enkele referenties aan de Duitse en Britse stelsels van heimelijke surveillance en aan de 'Online-Durchsuchung' uitspraak van het BVerfG. Een echte vergelijking met hackbevoegdheden uit andere rechtsstelsels is achterwege gebleven om twee redenen. Allereerst is het aantal rechtsstelsels dat momenteel een hackbevoegdheid kent beperkt. Naar mijn weten hebben onder de lidstaten van de Raad van Europa alleen Frankrijk en Duitsland een hackbevoegdheid.[302] Frankrijk kent met artikel 706-102 van de *Code de Procédure Pénale* een hackbevoegdheid in het kader van de opsporing van ernstige misdrijven, terwijl de Duitse (post-'Online-Durchsuchung') bevoegdheid op basis van artikel 20k van de zogenoemde BKA-wet enkel door het *Bundeskriminalamt* mag worden toegepast ten aanzien van terrorisme.[303] Geen van beide bevoegdheden is nog door het EHRM getoetst, terwijl het BVerfG momenteel klachten tegen de Duitse hackbevoegdheid nog in behandeling heeft.[304] De betreffende wettelijke regelingen bieden dan ook weinig inzicht in wat al dan niet toelaatbaar is in het kader van het noodzakelijkheidsvereiste van artikel 8 lid 2 EVRM.

[301] Zie o.a. EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (*S & Marper/United Kingdom*), § 107 – 112.
[302] De Britse RIPA wordt door de overheid aldaar gebruikt als basis voor het toepassen van '*remote searches*', maar het valt mijns inziens zeer te betwijfelen of deze wet een voldoende duidelijke wettelijke grondslag biedt in het kader van het legaliteitsvereiste van artikel 8 lid 2 EVRM en als zodanig als een 'hackbevoegdheid' kan worden gekwalificeerd.
[303] De volledige naam van de Duitse BKA-wet is *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*.
[304] De Hert, De Vries & Gutwirth 2009, p. 205.

Bronvermelding

LITERATUUR

Arai-Takahashi 2002
Y. Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Antwerpen - Oxford - New York: Intersentia 2002.

Beijer e.a. 2004
A. Beijer, *De Wet bijzondere opsporingsbevoegdheden – Eindevaluatie*, Den Haag: Boom Juridische Uitgevers 2004.

Boek 2000
J.L.M. Boek, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB* 2000, p. 589 – 593.

Brenner 2012
S.W. Brenner, 'Law dissonance and remote computer searches', *North Carolina Journal of Law and Technology* 2012, 14-1, p. 43 – 92.

Buruma 2001
Y. Buruma, *Buitengewone opsporingsmethoden*, Deventer: W.E.J. Tjeenk Willink 2001.

Cleiren & Verpalen 2011
C.P.M. Cleiren & M.J.M. Verpalen (red.), *Tekst en Commentaar Strafvordering*, Deventer: Kluwer 2011 (online bijgewerkt t/m 2013).

Conings & Oerlemans 2013
C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013/5, p. 23 – 32.

Corstens 2011
G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2011.

Van Dijk e.a. 2006
P. van Dijk e.a. (eds), *Theory and Practice of the European Convention on Human Rights*, Antwerpen – Oxford: Intersentia 2006.

Dommering 2000
E.J. Dommering, 'De nieuwe Nederlandse Constitutie en de informatietechnologie. Bespreking van het rapport van de Commissie Grondrechten in het digitale tijdperk.', *Computerrecht* 2000, 4, p. 177 – 185.

Eijpe & Van Essen 2007
L.H.M. Eijpe & T.T. van Essen, 'VoIP: juridische stand van zaken', *Computerrecht* 2007, 3, p. 14 – 21.

Van den Eshof e.a. 2002
G. Van den Eshof e.a., *Opsporing van verborgen informatie: technische mogelijkheden en juridische beperkingen*, Den Haag: Sdu Uitgevers 2002 (ITeRReeks, nr. 56).

Ferreira Pires 2011
L. Ferreira Pires, 'Wat is Cloud computing?', *Computerrecht* 2011/63, p. 104 – 107.

Franken 2009
A.A. Franken, 'Proportionaliteit en subsidiariteit in de opsporing', *Delikt en Delinkwent* 2009, 8, p. 79 – 92.

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

Groothuis & De Jong 2010
M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk? Een verkenning', *Privacy & Informatie* 2010-6, p. 278 – 283.

De Hert, De Vries & Gutwirth 2009
P. de Hert, K. de Vries & S. Gutwirth, 'Duitse rechtspraak over remote searches, datamining en afluisteren op afstand. Het arrest Bundesverfassungsgericht 27 februari 2008 (Online-Durchsuchung) in breder perspectief', *Computerrecht* 2009, 189, p. 200 – 211.

Jacobs 2012
B.P.F. Jacobs, 'Policeware', *NJB* 2012/2240, p. 2761 – 2764.

Jacobs, White & Ovey 2010
R.C.A. White & C. Ovey, *The European Convention on Human Rights*, Oxford: Oxford University Press 2010.

Van Kempen 2011
P.H.P.H.M.C. van Kempen, 'Drie basisvereisten voor noodweer. Een pleidooi voor subsidiariteit als centrale voorwaarde', in: P.H.P.H.M.C. van Kempen, A.J. Machielse, H.J.B. Sackers & P.C. Vegter (red.), *Levend strafrecht. Strafrechtelijke vernieuwingen in een maatschappelijke context* (Liber Amoricum Ybo Buruma), Kluwer: Deventer 2011, p. 303 – 321.

Kindt & Van der Hof 2009
E. Kindt & S. van der Hof, 'Identiteitsgegevens en -beheer in een digitale omgeving: een juridische benadering', *Computerrecht* 2009, 36, p. 44 – 52.

Koning 2012
M.E. Koning, 'Van teugelloos 'terughacken' naar 'digitale toegang op afstand'', *Privacy & Informatie* 2012-2, p. 46 – 52.

Koops 2000
B.J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000 (IteRReeks, nr. 31).

Koops 2007
B.J. Koops (red.), *Strafrecht & ICT*, Den Haag: Sdu Uitgevers 2007.

Koops 2012
B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel: nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Den Haag: Boom Lemma Uitgevers 2012.

Koops e.a. 2012
B.J. Koops e.a., *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Tilburg/Den Haag: TILT/WODC 2012.

Koops, Van Schooten & Prinsen 2004
B.J. Koops, H. van Schooten & M.M. Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu Uitgevers 2004 (ITeRReeks, nr. 70).

Korteweg 2013
D.A. Korteweg, 'Wetsvoorstel Computercriminaliteit III gepubliceerd', *Juridisch up to Date* 2013-10, p. 13 – 17.

Lünneman e.a. 2006
K. Lünneman e.a., *Kinderen beschermd tegen seksueel misbruik: evaluatie van de partiële wijziging in de zedelijkheidswetgeving*, Utrecht: Verwey-Jonker Instituut 2006.

Mell & Grance 2011
P. Mell & T. Grance, 'The NIST definition of Cloud Computing', *NIST Special Publication* 800-145, september 2011.

Odinot e.a. 2012
G. Odinot e.a., *Het gebruik van de telefoon- en internettap in de opsporing*, Den Haag: Boom Lemma Uitgevers 2012.

Oerlemans 2010
J.J. Oerlemans, *Opsporing en bestrijding van kinderpornografie op internet*, Tilburg: Celsus Juridische Uitgeverij 2010.

Oerlemans 2011
J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *Delikt en Delinkwent* 2011, 62, p. 888 – 908.

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

Oerlemans 2013
J.J. Oerlemans, 'Conceptwetsvoorstel Computercriminaliteit III', *Computerrecht* 2013/146, p. 239 – 240.

Schokkenbroek 1996
J.G.C. Schokkenbroek, *Toetsing aan de vrijheidsrechten van het Europees Verdrag tot Bescherming van de Rechten van de Mens* (diss. Leiden), Zwolle: W.E.J. Tjeenk Willink.

Spoenle 2010
J. Spoenle, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Council of Europe Project on Cybercrime Discussion Paper, augustus 2010.

Steenbruggen 2008
W.A.M. Steenbruggen, annotatie bij: BVerfG 27 februari 2008 (*Online-Durchsuchung*) 1 BvR 370/07, 1 BvR 595/07, *Tijdschrift voor Media en Communicatierecht* 2008-5, p. 232 – 235.

Stol, Leukfeldt & Klap 2012
W.Ph. Stol, E.R. Leukfeldt & H. Klap, 'Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012', *Justitiële Verkenningen* 2012-1, p. 25 – 39.

Vande Lanotte 2005
J. Vande Lanotte, *Handboek EVRM Deel I: Algemene beginselen*, Antwerpen: Intersentia 2005.

Vlemminx 2013
F.M.C. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische Uitgevers 2013.

Wiemans 2004
F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken*, Nijmegen: Wolf Legal Publishers 2004.

JURISPRUDENTIEREGISTER

Europees Hof van de Rechten van de Mens

EHRM 7 december 1976, nr. 5493/72, *NJ* 1978, 235, m.nt. E.A. Alkema (*Handyside/United Kingdom*).

EHRM 6 september 1978, nr. 5029/71 (*Klass and Others/Germany*).

EHRM 26 april 1979, nr. 6538/74, *NJ* 1980, 146, m.nt. E.A. Alkema (*Sunday Times/United Kingdom*).

EHRM 22 oktober 1981, nr. 7525/76 (*Dudgeon/United Kingdom*).

EHRM 25 maart 1983, nr. 5947/72 (*Silver and Others/United Kingdom*).

EHRM 2 augustus 1984, nr. 8691/79, *NJ* 1988, 534, m.nt. J.V. van Dijk (*Malone/United Kingdom*).

EHRM 24 november 1986, nr. 9063/80 (*Gillow/United Kingdom*).

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

EHRM 30 maart 1989, nr. 10461/83 (*Chappell/United Kingdom).*

EHRM 7 juli 1989, nr. 14038/88, *NJ* 1990, 158, m.nt. E.A. Alkema (*Soering/United Kingdom*).

EHRM 16 december 1992, nr. 13710/88, *NJ* 1993, 400, m.nt. E.J. Dommering (*Niemietz/Germany*).

EHRM 25 februari 1993, nr. 10828/84 (*Funke/France*).

EHRM 25 februari 1993, nr. 11471/85 (*Crémieux/France*).

EHRM 25 februari 1993, nr. 12661/87 (*Miailhe/France*).

EHRM 25 februari 1997, nr. 22009/93, *NJ* 1999, 516, m.nt. G. Knigge (*Z/Finland*).

EHRM 24 augustus 1998, nr. 23618/94 (*Lambert/France*).

EHRM 27 september 1999, nrs. 33985/96 en 33986/96 (*Smith and Grady/United Kingdom*).

EHRM 12 mei 2000, nr. 35394/97, *NJ* 2002, 180, m.nt. T.M. Schalken (*Khan/United Kingdom*).

EHRM 28 januari 2003, nr. 44647/98, *EHRC* 2003/24 (*Peck/United Kingdom*).

EHRM 18 mei 2004, nr. 58148/00 (*Editions Plon/France*).

EHRM 27 mei 2004, nr. 66746/01, *EHRC* 2004/67, m.nt. K. Henrard (*Connors/United Kingdom*).

EHRM 28 april 2005, nr. 41604/98, *EHRC* 2005/59, m.nt. F. Fernhout (*Buck/Germany*).

EHRM 6 juni 2006, nr. 62332/00, *NJ* 2009, 449, m.nt. E.J. Dommering (*Segerstedt-Wiberg and Others/Sweden*).

EHRM 29 juni 2006, nr. 54934/00, *EHRC* 2007/13, m.nt. J.P. Loof (*Weber and Saravia/Germany*).

EHRM 2 november 2006, nr. 59909/00, *EHRC* 2007/7, m.nt. M. Peeters (*Giacomelli/Italy*).

EHRM 1 juli 2008, nr. 58243/00, *NJ* 2010, 324, m.nt. E.J. Dommering (*Liberty and Others/United Kingdom*).

EHRM 4 december 2008, nrs. 30562/04 en 30566/04, *NJ* 2009, 410, m.nt. E.A. Alkema; *EHRC* 2009/13, m.nt. B.J. Koops; *NJCM-Bulletin* 2009, 34-4, m.nt. M.G.J.M. van der Staak (*S & Marper/United Kingdom*).

EHRM 1 maart 2010, nr. 46113/99, *EHRC* 2010/54 (*Demopoulos and Others/Turkey*).

EHRM 18 mei 2010, nr. 26839/05, *NJ* 2011/333 (*Kennedy/United Kingdom*).

EHRM 2 september 2010, nr. 35623/05, *EHRC* 2010/123, m.nt. P. de Hert & J. van Caeneghem (*Uzun/Germany*).

Bundesverfassungsgericht

BVerfG 27 februari 2008 (*Online-Durchsuchung*), 1 BvR 370/07, 1 BvR 595/07.

Supreme Court of Canada

Supreme Court of Canada 7 november 2013, *R. v. Vu*, 2013 SCC 60.

PARLEMENTAIRE STUKKEN

Tweede Kamer

Kamerstukken II 1989/90, 21 551, nr. 3.

Kamerstukken II 1996/97, 25 403, nr. 3.

Kamerstukken II 1998/99, 26 671, nr. 3.

Kamerstukken II 2003/04, 29 441, nr. 3.

Kamerstukken II 2004/05, 26 671, nr. 10.

Kamerstukken II 2008/09, 28 684, nr. 232.

Aanhangsel Handelingen II 2009/10, nrs. 2010Z04067 en 2010Z04074.

Aanhangsel Handelingen II 2010/11, nr. 201015331.

Kamerstukken II 2011/12, 33 240 VI, nr. 1.

Aanhangsel Handelingen II 2011/12, nr. 2011Z23302.

Aanhangsel Handelingen II 2011/12, nr. 2012Z02969.

Aanhangsel Handelingen II 2011/12, nr. 2012Z11858.

Kamerstukken II 2012/13, 28 684, nr. 363.

Kamerstukken II 2012/13, 30 517, nr. 26.

Kamerstukken II 2012/13, 26 643, nr. 285 (bijlage).

Eerste Kamer

Kamerstukken I 1998/99, 25 403 en 23 251, nr. 119b.

ELEKTRONISCHE BRONNEN

Publicaties

Postel 1980

J. Postel, *RFC-760 – DoD standard Internet Protocol*, januari 1980 <http://tools.ietf.org/html/rfc760>, laatst geraadpleegd op 20 november 2013.

Veiligheid en Justitie Bulletin 2013

'Aanpak van meer grote, internationale cybercrime-zaken', *Veiligheid en Justitie Bulletin*, Jaargang 5, Nummer 8, 17 september 2013, <https://abonneren.rijksoverheid.nl/article/veiligheid-en-justitie-bulletin/prinsjesdageditie-veiligheid-en-justitie-bulletin/aanpak-van-meer-grote-internationale-cybercrime-zaken/1952/20680?preview=false>, laatst geraadpleegd op 20 november 2013.

Rapporten

Openbaar Ministerie 2011

Landelijk parket Openbaar Ministerie, *Kinderporno op anonieme, diep verborgen websites*, <http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/>, laatst geraadpleegd op 20 november 2013.

Gartner 2012

Gartner, *Gartner's 2012 Hype Cycle for Emerging Technologies Identifies "Tipping Point" Technologies That Will Unlock Long-Awaited Technology Scenarios*, 16 augustus 2012, <http://www.gartner.com/newsroom/id/2124315>, laatst geraadpleegd op 20 november 2013, afbeelding helaas niet meer beschikbaar.

Newcom 2013

Newcom, *Social Media in Nederland 2013*, februari 2013, <http://www.slideshare.net/newcomresearch/social-media-in-nederland-2013-smo13-newcom-actuele-cijfers>, laatst geraadpleegd op 20 november 2013.

Europol 2013

Europol, *Serious and Organised Crime Threat Assessment*, maart 2013, <https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf>, laatst geraadpleegd op 20 november 2013.

Raad voor de Rechtspraak 2013

Raad voor de Rechtspraak, 'Advies Wetsvoorstel computercriminaliteit III, 4 juli 2013, <http://www.rechtspraak.nl/Organisatie/Raad-Voor-De-Rechtspraak/Wetgevingsadvisering/Wetgevingsadviezen2013/2013-27-Advies-Wetsvoorstel-computercriminaliteit-III.pdf>, laatst geraadpleegd op 20 november 2013.

Internetconsultatie

Conceptwetsvoorstel Computercriminaliteit III

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), mei 2013, <http://www.internetconsultatie.nl/computercriminaliteit>, laatst geraadpleegd op 20 november 2013.

Memorie van toelichting conceptwetsvoorstel Computercriminaliteit III

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), mei 2013, <http://www.internetconsultatie.nl/computercriminaliteit>, laatst geraadpleegd op 20 november 2013.

Weblogs

Engelfriet 2013

A. Engelfriet, *Wetsvoorstel computercriminaliteit: terughackbevoegdheid, webcammeekijkrecht, decryptiebevel en wereldwijde rechtsmacht bij cybercrime*, mei 2013, <http://blog.iusmentis.com/2013/05/03/wetsvoorstel-computercriminaliteit-terughackbevoegdheid-webcammeekijkrecht-decryptiebevel-en-wereldwijde-rechtsmacht-bij-cybercrime/>, laatst geraadpleegd op 20 november 2013.

Nieuwsartikelen

<https://www.bof.nl/2013/05/02/opstelten-grijpt-overhaast-naar-hackbevoegdheid/>, laatst geraadpleegd op 20 november 2013.

<http://gmailblog.blogspot.nl/2010/01/default-https-access-for-gmail.html>, laatst geraadpleegd op 20 november 2013.

<http://www.nbcnews.com/technology/yahoo-mail-enables-encryption-battles-security-flaw-1B7911843>, laatst geraadpleegd op 20 november 2013.

<http://www.microsoft.com/investor/EarningsAndFinancials/Earnings/Kpi/fy13/q3/Detail.aspx>, laatst geraadpleegd op 20 november 2013.

<http://www.guardian.co.uk/technology/2013/may/07/viber-skype-desktop-service>, laatst geraadpleegd op 20 november 2013.

< http://www.nu.nl/internet/3608352/whatsapp-heeft-350-miljoen-gebruikers.html>, laatst geraadpleegd op 20 november 2013.

<http://www.guardian.co.uk/technology/shortcuts/2012/dec/04/whatsapp-new-text-messaging>, laatst geraadpleegd op 20 november 2013.

<http://www.marketingfacts.nl/berichten/1-op-de-3-huishoudens-bezit-een-tablet>, laatst geraadpleegd op 20 november 2013.

<http://www.nytimes.com/2011/10/15/world/europe/uproar-in-germany-on-police-use-of-surveillance-software.html?_r=1&>, laatst geraadpleegd op 20 november 2013.

<http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html>, laatst geraadpleegd op 20 november 2013.

<https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/>, laatst geraadpleegd op 20 november 2013.

<http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/>, laatst geraadpleegd op 20 november 2013.

<global.samsungtomorrow.com/?p=28713>, laatst geraadpleegd op 20 november 2013.

<https://www.bof.nl/live/wp-content/uploads/20120217-bevragingen-sociale-netwerken.pdf>, laatst geraadpleegd op 20 november 2013.

<http://www.wired.com/beyond_the_beyond/2012/10/gartner-hype-cycle-2012/>, laatst geraadpleegd op 20 november 2013.

<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>, laatst geraadpleegd op 20 november 2013.

<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>, laatst geraadpleegd op 20 november 2013.

<http://www.economist.com/news/britain/21587839-keeping-up-crooks>, laatst geraadpleegd op 20 november 2013.

Websites

<http://www.truecrypt.org/>, laatst geraadpleegd op 20 november 2013.

<http://www.openpgp.org/>, laatst geraadpleegd op 20 november 2013.

<http://www.whatsapp.com/faq/general/21864047>, laatst geraadpleegd op 20 november 2013.

<http://vpnservice.nl/>, laatst geraadpleegd op 20 november 2013.

<https://www.torproject.org/about/overview.html.en>, laatst geraadpleegd op 20 november 2013.

<https://www.torproject.org/eff/tor-legal-faq.html.en>, laatst geraadpleegd op 20 november 2013.

<http://www.skype.com/en/legal/privacy/>, laatst geraadpleegd op 20 november 2013.

<http://www.whatsapp.com/legal/>, laatst geraadpleegd op 20 november 2013.

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>, laatst geraadpleegd op 20 november 2013.

<https://www.facebook.com/about/privacy/your-info>, laatst geraadpleegd op 20 november 2013.

<http://www.skype.com/en/legal/privacy/#disclosureOfInformation>, laatst geraadpleegd op 20 november 2013.

<http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>, laatst geraadpleegd op 20 november 2013.

<http://www.google.com/transparencyreport/>, laatst geraadpleegd op 20 november 2013.

<http://www.om.nl/organisatie/college_van/>, laatst geraadpleegd op 20 november 2013.

< http://www.om.nl/organisatie/beleidsregels/overzicht/opsporing/@158933/aanwijzing-1/>, laatst geraadpleegd op 20 november 2013.