MASTER'S THESIS

De hackbevoegdheid van art. 126nba SV getoetst aan het recht op privacy

Kruithof-Kanmphuis, R.M.

Award date:
2022

Awarding institution:
Department of Public Law

De hackbevoegdheid van art. 126nba SV getoetst aan het recht op privacy

Masterscriptie Rechtsgeleerdheid

Naam student: R.M. Kruithof-Kamphuis

Studentnummer: 851843346

Begeleider: I. Braber

Examinator: S. Naber

Woonplaats: Zwanenburg

E-mailadres: rm.kruithof-Kamphuis@studie.ou.nl

Telefoonnummer: 06

Aantal woorden: 13.604

Datum van inleveren: 8 juli 2022

Inhoudsopgave

1. Inleiding

1.1. Aanleiding onderwerp 4
1.2. De centrale onderzoeksvraag en deelvragen 5
1.3. Afbakening en maatschappelijke relevantie 6

2. Het doel en de reikwijdte van art. 126nba Sv

2.1. Inleiding 8
2.2. Het doel en de noodzaak van art. 126nba Sv 8
2.3. De reikwijdte van art. 126nba Sv 10
2.4. Conclusie 11

3. De criteria voor een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM

3.1. Inleiding 14
3.2. De reikwijdte van art. 8 EVRM 14
3.3. Beperking van het recht op privacy op grond van art. 8 lid 2 EVRM 15
3.4. Conclusie 18

4. Art 126nba Sv: De kritische adviezen in het licht van art. 8 EVRM

4.1. Inleiding 20
4.2. Adviezen en kritieken 20
4.3. Drie fasen van inzet 23
4.4. Conclusie 25

5. Art. 126nba Sv: De inzet in de praktijk

5.1. Inleiding 28
5.2. Jurisprudentie met betrekking tot art. 126nba Sv 28
5.3. De inspectieverslagen 30
5.4. Conclusie 31

6. Toetsing

6.1. Inleiding 34
6.2. De toetsing van art. 126nba Sv aan art. 8 EVRM 34
6.3. Conclusie 37

7. Eindconclusie

7.1. Bevindingen 38

Literatuur- en bronnenlijst 40
Jurisprudentielijst 46

Hoofdstuk 1 - Inleiding

1.1. Aanleiding onderwerp

Na een lange voorbereiding is op 1 maart 2019 de Wet Computercriminaliteit III in werking getreden met als doel de opsporing en vervolging van (computer) criminaliteit te verbeteren.[1] Een van de veelbesproken bepalingen uit deze wet is art. 126nba van het Wetboek van Strafvordering (hierna: 126nba Sv) waarvan lid 1 bepaalt:

''In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vaststelling daarvan;
b. de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m;[2]
c. de uitvoering van een bevel als bedoeld in artikel 126g (.....);[3]

en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen:

d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;
e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid (....).''

Deze bepaling geeft de opsporingsdiensten onder voorwaarden de mogelijkheid tot het heimelijk binnendringen in een geautomatiseerd werk ten dienste van het strafrechtelijk onderzoek en de bewijsvergaring tegen verdachten. De noodzaak van deze bepaling zou zijn gelegen in het feit dat verdachten door de voortschrijdende techniek en het gebruik van geautomatiseerde werken voor communicatie en verwerking van opslag en gegevens zeer lastig te identificeren en lokaliseren zijn.[4] Zo maken criminelen gebruik van alle technische mogelijkheden om hun identiteit te verhullen en anoniem te blijven en opereren zij vaak van buiten de Nederlandse landsgrenzen. Daarbij wordt er veelal informatie versleuteld en opgeslagen bij aanbieders van 'Cloudcomputing'.[5] Traditionele opsporingsmethoden schieten dan tekort en zijn niet effectief. Zonder de hackbevoegdheid van art. 126nba Sv zouden de opsporingsdiensten daarom in veel onderzoeken met lege handen staan.

Tijdens de behandeling van het wetsvoorstel zijn door verschillende deskundigen en leden van de Eerste Kamer zorgen geuit over de waarborg van het recht op privacy van art. 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EHRM).[6] Ook in de literatuur is kritiek geuit op de

---

[1] *Kamerstukken II* 2015/16, 34 372, nr. 2.
[2] Art. 126l Sv en art. 126m Sv zien beide op het opnemen van vertrouwelijke informatie.
[3] Art. 126g Sv ziet op het stelselmatig volgen van een persoon.
[4] *Kamerstukken II* 2015/16, 34372, 3, p. 6-7.
[5] Oerlemans *Strafblad* 2017.
[6] *Kamerstukken I* 2016/17, 34 372, E, (Verslag I). Als ook: *Kamerstukken II* 2017/18, 34 372, nr. 27., Als ook: *Kamerstukken II* 2018/19, 34 372, nr. 29.

hackbevoegdheid in relatie tot het recht op privacy en met name op de mogelijke schending daarvan.[7]
Nu de wet ruim twee jaar geleden in werking is getreden, zal in deze scriptie worden onderzocht of en in hoeverre de vele kritiek terecht is en zal specifiek worden onderzocht of de hackbevoegdheid van art. 126nba Sv verenigbaar is met art. 8 lid 2 EVRM.
Gezien het feit dat de ten tijde van het wetsvoorstel geuite kritiek op art. 126nba Sv en de mogelijke schending van privacy hoofdzakelijk twijfels over de inzet van de hackbevoegdheid in de praktijk betrof,[8] is een analyse op de daadwerkelijke toepassing en inzet van art. 126nba Sv in de praktijk van wezenlijk belang voor de in deze scriptie onderzochte verenigbaarheid van art. 126nba Sv met art. 8 lid 2 EVRM. Daarom zal art. 126nba Sv niet alleen worden getoetst aan art. 8 EVRM, maar ook aan de hand van de opgetekende ervaringen met art. 126nba Sv in de praktijk.

1.2. De Centrale onderzoeksvraag en deelvragen

De centrale onderzoeksvraag die in deze scriptie zal worden beantwoord is:

'Is de hackbevoegdheid van art. 126nba van het Wetboek van Strafvordering verenigbaar met art. 8 lid 2 EVRM, zoals uitgelegd in de rechtspraak van het EHRM?'

Om tot een antwoord op de hoofdvraag te komen zullen achtereenvolgens de volgende deelvragen worden onderzocht en beantwoord:

- *Wat is het doel en de reikwijdte van de hackbevoegdheid van art. 126nba Sv?*
- *Wat zijn de criteria voor een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM?*
- *Op welke wijze zijn de waarborgen tegen een onrechtmatige schending van art. 8 EVRM in het huidige art. 126nba Sv ingekleed en waar liggen de kritiekpunten?*
- *Hoe verloopt de toepassing van art. 126nba Sv sinds de invoering ervan in de praktijk?*

Beantwoording van de eerste deelvraag strekt tot doel om de noodzaak en reikwijdte van het huidige art. 126nba Sv in kaart te brengen. Naast het Wetboek van Strafvordering (hierna: WvSv) zal in hoofdstuk 2 ook de het wetsvoorstel Computercriminaliteit III en de aanloop daartoe worden besproken.

Ter beantwoording van de tweede deelvraag '*Wat zijn de criteria voor een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM*?', zullen in hoofdstuk 3 met name het EVRM en de jurisprudentie van het EHRM aan de orde komen en met name de criteria voor een gerechtvaardigde beperking op grond van lid 2 van dit grondrecht. Ook zullen relevante uitspraken van het EHRM met betrekking tot heimelijke opsporingsmethoden worden belicht.

In hoofdstuk 4 zal worden ingegaan op de derde deelvraag '*Op welke wijze zijn de waarborgen tegen een schending van art. 8 EVRM in de huidige Wet computercriminaliteit III ingekleed en waar liggen de kritiekpunten?*' Daartoe zal worden bezien hoe de criteria van de tweede deelvraag in art. 126nba Sv zijn gewaarborgd door deze te toetsen aan de hand van de kamerstukken bij het wetsvoorstel Computercriminaliteit III, de daarbij behorende Memorie van Toelichting en de literatuur. Ook het belang van toetsing achteraf zal daarbij ter sprake komen.[9]

---

[7] Aink *TPWS* 2016/46. Als ook: Oerlemans *Strafblad* 2017. Als ook: Van der Sloot *TBS&H* 2017. Als ook: Preadvies Adviescommissie Strafrecht 2013.
[8] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 78-80.
[9] Oerlemans *Strafblad* 2017.

In hoofdstuk 5 zal de vierde deelvraag '*Hoe verloopt de toepassing van art. 126nba Sv sinds de invoering ervan in de praktijk?*' worden beantwoord aan de hand van de beschikbare Nederlandse jurisprudentie sinds de invoering van de wet en de onderzoeksverslagen van de Inspectie Justitie en Veiligheid (hierna: de Inspectie). Daarbij komt ook de relatie met art. 6 EVRM aan bod.[10]

De toetsing van art. 126nba Sv aan art. 8 EVRM is opgenomen in hoofdstuk 6. Tot slot volgt in hoofdstuk 7 de eindconclusie en daarmee ook het antwoord op de centrale onderzoeksvraag.

1.3. Afbakening en maatschappelijke relevantie

Het grondrecht op privacy is opgenomen in meerdere mensenrechtelijke verdragen en ook in de Nederlandse grondwet.[11] In deze scriptie zal ik mij beperken tot het recht op privacy zoals bedoeld in art. 8 EVRM. Met oog op de beperkte omvang van deze scriptie zal het grensoverschrijdende aspect grotendeels onbesproken blijven.

De centrale onderzoeksvraag en daarbij behorende deelvragen zijn op meerdere vlakken maatschappelijk relevant. Enerzijds is er de noodzaak van de hackbevoegdheid ter bescherming van de maatschappij tegen steeds groeiende en verdergaande grensoverschrijdende (digitale) criminaliteit.[12] Anderzijds bestaat het risico dat door de invoering van deze bijzondere opsporingsbevoegdheid een belangrijk grondrecht als het recht op privacy zoals neergelegd in art. 8 EVRM onder grote druk komt te staan.[13] Ofwel: enerzijds worden burgers beter beschermd tegen criminaliteit maar tegelijkertijd kunnen zij daardoor worden geschonden in hun recht op privacy.

Omdat de Wet Computercriminaliteit III nog jong is en de meeste literatuur en artikelen dateren van voor de inwerkingtreding daarvan, zal ik in deze scriptie proberen te achterhalen of de kritiek en zorgen die naar voren komen uit de literatuur en wetsgeschiedenis, terecht zijn in het kader van de bescherming van art. 8 EVRM. Door art. 126nba Sv niet alleen te toetsen aan jurisprudentie en de criteria van art. 8 EVRM, maar ook aan de onderzoeksverslagen van de Inspectie, zal duidelijk worden in hoeverre het recht op privacy is gewaarborgd bij de toepassing van art. 126nba Sv.

[10] EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman.
[11] Art. 10 Gw.
[12] *Kamerstukken II* 2015/16, 34372, 3, p. 7-12; *Kamerstukken II* 2016/17, 34372, 6, p. 14-22.
[13] Aink *TPWS* 2016/46.

Hoofdstuk 2 – Het doel en de reikwijdte van art. 126nba Sv

2.1. Inleiding

In het wetsvoorstel Computercriminaliteit I van 1985 stond de opkomende digitalisering centraal. Daarbij was de strafbaarstelling van 'hacken' de meest besproken wijziging van het Wetboek van Strafrecht. Hacken werd gezien als een opkomende nieuwe technologische dreiging, waar door de media veel aandacht aan werd besteed. De sterk toenemende digitalisering van de samenleving maakte dat het gevaar van 'hacken' steeds groter werd. Omdat deze nieuwe vormen van criminaliteit in veel gevallen niet zonder analoge toepassing onder een strafbepaling waren te brengen was het nodig het Wetboek van Strafrecht te moderniseren en zodoende lacunes in de wet te voorkomen.[14] Zo was Ronald O. in 1992, voor de totstandkoming van de wet Computercriminaliteit I wegens hacken - en bij gebrek aan een passende strafbepaling - aangehouden op verdenking van valsheid in geschrifte en oplichting. Na invoering van de wet was Ronald O. in 1993 vervolgens de eerste persoon die op grond van art. 138ab Sr wegens computervredebreuk kon worden vervolgd.[15] Evenzo is de strafbaarstelling van het delict 'computervredebreuk' van art. 138ab Sr in de Wet Computercriminaliteit I een verbijzondering op strafbaarstelling van de reguliere fysieke 'huisvredebreuk' van art. 138 Sr.[16]

De Wet Computercriminaliteit III trad exact 26 jaar na de Wet Computercriminaliteit I op 1 maart 2019 in werking.[17] In tegenstelling tot de strafbaarstelling van 'hacken' in de Wet Computercriminaliteit I in 1993, voorziet deze jonge wet uit 2019 juist in een 'hackbevoegdheid' ten behoeve van het strafrechtelijke opsporingsonderzoek. Dat klinkt tegenstrijdig, omdat opsporingsdiensten daarmee feitelijk bevoegdheden hebben gekregen die zij juist proberen op te sporen.[18]

In dit hoofdstuk zal daarom de vraag '*Wat is het doel en de reikwijdte van de hackbevoegdheid van art. 126nba Sv?*' worden beantwoord.
Daartoe zal in paragraaf 2.2. eerst het doel en daarmee de noodzaak van de hackbevoegdheid van art. 126nba Sv worden besproken. In paragraaf 2.3. wordt de reikwijdte van de bevoegdheden die voortvloeien uit art. 126nba Sv onderzocht. Daarbij worden eerst de verschillende onderzoeksbevoegdheden die uit het wetsartikel voortvloeien besproken. Gelet op de beperkte omvang van deze scriptie wordt het internationale aspect niet of slechts zeer beperkt behandeld. In paragraaf 2.4. volgt een eerste conclusie.

2.2. Het doel en de noodzaak van art. 126nba Sv

Met de opkomst van het internet en de eerste kennismakingen met cybercrime,[19] was het doel van de Wet computercriminaliteit I om ervoor te zorgen dat digitale criminaliteit op gelijke wijze kon worden opgespoord en vervolgd als traditionele delicten.[20] Inmiddels zijn we na inwerkingtreding van de Wet Computercriminaliteit I[21] bijna 30 jaar verder en behoeft het geen betoog dat de digitale wereld in de afgelopen drie decennia explosief is gegroeid. Het leven vindt tegenwoordig misschien zelfs meer ín de digitale omgeving plaats dan daarbuiten. Geen wonder dat de criminaliteit daarin

[14] Stol & Strikwerda 2017, p. 116.
[15] Stol & Strikwerda 2017, p. 117.
[16] Vergelijk art. 138 Sr en art. 138ab Sr.
[17] *Stb.* 2019, 167. Als ook: *Stb.* 1993, 33.
[18] Jacobs, *NJB* 2012/2240, p. 2761.
[19] Bijvoorbeeld: Hacken in plaats van fysiek ergens inbreken of illegale verkoop via internet etc.
[20] *Kamerstukken II* 1989/90, 21551, nr. 3, p. 1-4.
[21] *Stb.* 1993, 33.

net zo hard is meegegroeid.[22] Om dit te illustreren gaf Jacobs in 2012 een treffend voorbeeld. Hij noemt de bancaire sector en wijst daarbij enerzijds op de enorme daling van *fysieke* bankovervallen in de afgelopen jaren, terwijl anderzijds het aantal *digitale* aanvallen op bankrekeningen en geldstromen juist explosief blijft stijgen.[23]

Blijkens de Memorie van Toelichting is het doel van de hackbevoegdheid van art. 126nba Sv om het voor opsporingsdiensten mogelijk te maken om rechtmatig en onder strikte voorwaarden heimelijk binnen te kunnen dringen in, of toegang te krijgen tot, een geautomatiseerd werk,[24] dat in gebruik is bij een verdachte van ernstige vormen van (computer)criminaliteit zoals het verspreiden van kinderpornografie of het handelen in verdovende middelen.[25] Daarmee verschaft de Wet computercriminaliteit III nieuwe juridische munitie ten behoeve van de opsporing en vervolging van (computer)criminaliteit.[26]

In algemene zin is de noodzaak van de hackbevoegdheid gelegen in de bescherming van de maatschappij tegen de groeiende en steeds verdergaande (grensoverschrijdende en digitale) criminaliteit.[27] Meer specifiek komt de noodzaak voort uit de enorm snelle technologische ontwikkelingen waar criminelen zeer dankbaar en steeds laagdrempeliger van gebruikmaken. De wettelijke opsporingsbevoegdheden schieten om die reden tekort voor een doelmatige opsporing en vervolging zonder een bevoegdheid als die van art. 126nba Sv.[28] De drie meest wezenlijke technologische ontwikkelingen waar het om gaat zullen hierna kort worden toegelicht.

Allereerst wordt in de Memorie van Toelichting bij het Wetsvoorstel de versleuteling ofwel encryptie van elektronische gegevens genoemd.[29] Daarbij worden berichten met behulp van speciale programma's via een algoritme omgezet in onleesbare tekens.[30] Zo zijn er legale softwareprogramma's op de markt die de gebruiker zelf kan installeren en waarmee een grote hoeveelheid aan bestanden versleuteld kan worden. Ook grote providers waaronder Gmail en WhatsApp maken standaard gebruik van versleuteling. Daardoor zijn echter niet alleen goedwillende burgers, maar ook kwaadwillende criminelen steeds beter beveiligd in hun onderlinge onlinecommunicatie. Het aftappen of opnemen van onlinecommunicatie wordt daardoor steeds lastiger of zelfs onmogelijk. De bestaande bepalingen in het Wetboek van Strafvordering die erop zien om versleuteling door de aanbieder of provider van de versleutelingsdienst verplicht ongedaan te laten maken (126m, zesde lid, en 126nh, eerste lid, Sv), leveren in veel gevallen niet het gewenste resultaat op. Ook als de aanbieder verplicht is om mee te werken aan ongedaan making van encryptie blijkt het afdwingen daarvan vaak onmogelijk. Zo is de aanbieder in veel gevallen niet in Nederland gevestigd of is er sprake van meerdere 'lagen' beveiliging waarbij elke 'laag' aan een andere aanbieder toebehoort. Daarbij wordt er soms niet voldaan aan de definitie van 'aanbieder',

[22] Stol & Strikwerda 2017, p. 13.
[23] Jacobs, *NJB* 2012/2240, p. 2761.
[24] Voor een algemene definitie van een geautomatiseerd werk zie art. 80sexies Sr. Ook kan een apparaat als geautomatiseerd werk worden aangemerkt als het geschikt is voor opslag, verwerking en overdracht van gegevens. Uit de jurisprudentie (zie o.a. HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.) en de Memorie van Toelichting bij het wetsvoorstel (*Kamerstukken II* 2015/16, 34372, 3, p. 98.) volgt dat externe gegevensdragers die met een dergelijk apparaat in verbinding staan, zoals een usb-stick, harde schijf of externe server ook onder het begrip 'geautomatiseerd werk' vallen.
[25] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 6-7.
[26] *Stb.* 2018, 340, p. 10.
[27] *Kamerstukken II* 2015/16, 34372, 3, p. 7-12; *Kamerstukken II* 2016/17, 34372, 6, p. 14-22.
[28] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 7-10.
[29] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 8.
[30] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 7-8.

hetgeen vereist is om medewerking te kunnen vorderen (art. 126la Sv). Mede hierom meende de wetgever dat de opsporingsdiensten zowel moeten kunnen beschikken over een bevoegdheid tot decryptie (ontsleuteling) van digitale berichten als over de bevoegdheid om communicatie te onderscheppen voordat deze is versleuteld. De hackbevoegdheid van art. 126nba Sv maakt dit mogelijk.[31]

Als tweede ontwikkeling noemt de wetgever het veelvuldig gebruik van draadloze verbindingen. Iedereen kan tegenwoordig vrijwel overal en gratis gebruikmaken van wifi-verbindingen en hotspots. In dergelijke situaties is het aftappen van alle communicatie van een verdachte alleen effectief en mogelijk als alle hotspots of wifi-verbindingen waar de verdachte gebruik van maakt afgetapt zouden worden. Behalve dat dit zo goed als ondoenlijk is, staat - gelet op het aantal derden dat met een dergelijke handelwijze in hun privacy kunnen worden geraakt - ook het proportionaliteitsbeginsel hieraan in de weg. De communicatie van vele andere personen die niet als verdachte zijn aangemerkt zou op deze manier, zonder dat zij daarvan op de hoogte zijn, immers ook worden afgetapt. De bevoegdheid van art. 126nba Sv maakt het echter mogelijk om gericht binnen te dringen in het geautomatiseerd werk van de verdachte zelf, bijvoorbeeld in diens smartphone. Hierdoor kan een inbreuk op de privacy van derden grotendeels worden voorkomen en kan alle communicatie van verdachte worden onderschept.[32]

Als derde reden voor de noodzaak van art. 126nba Sv wordt het gebruik van zogenoemde 'Cloud computingdiensten' aangevoerd. Opslaan van gegevens gebeurt tegenwoordig steeds minder vaak op een lokale harde schijf. In plaats daarvan wordt data opgeslagen in de 'cloud', dat wil zeggen op servers van een Cloudcomputingdienst, waarvan de fysieke locatie vaak onbekend is en die zich niet zelden buiten Nederland bevindt.[33] Daarbij komt het voor dat bestanden van één persoon in meerdere delen en over meerdere servers in verschillende landen zijn opgeslagen.[34] Op grond van art. 125j Sv bestaat weliswaar de bevoegdheid om onderzoek in een geautomatiseerd werk te verrichten dat zich elders bevindt - ook wel netwerkdoorzoeking genoemd - maar daarbij wordt ervan uitgegaan dat het geautomatiseerd werk met de opgeslagen gegevens zich op een vaste plek bevindt en slechts binnengetreden hoeft te worden.[35] Zoals hiervoor beschreven is dat tegenwoordig echter steeds vaker niet het geval.

Criminelen kunnen met behulp van dit soort technologische ontwikkelingen dus steeds makkelijker te werk gaan. Door daarnaast gebruik te maken van anonimiseringstechnieken zoals 'The Onion Router System' (TOR) - die ervoor zorgen dat het IP-adres van de gebruiker verborgen blijft - wordt de pakkans steeds kleiner.[36] De hackbevoegdheid van art. 126nba Sv geeft de opsporingsdiensten diverse instrumenten om deze ongewenste ontwikkeling te bestrijden.

2.3. De reikwijdte van art. 126nba Sv

Art. 126nba Sv is een bijzondere opsporingsbevoegdheid, op grond waarvan heimelijk kan worden binnengedrongen in een geautomatiseerd werk. Nadat het binnendringen heeft plaatsgevonden kunnen de opsporingsdiensten vervolgens diverse opsporingsbevoegdheden toepassen binnen het apparaat of netwerk waarin is binnengedrongen. Die bevoegdheden bestaan uit het vaststellen van

[31] *Kamerstukken II* 2015/16, 34372, 3, p. 7-9.
[32] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 10.
[33] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 11.
[34] Van der Sloot, *TBS&H* 2017, p. 196.
[35] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 11.
[36] Oerlemans, *Strafblad* 2017, p. 356.

de identiteit of locatie van de verdachte, het opnemen of afluisteren van gesprekken, het vastleggen van opgeslagen gegevens, het ontoegankelijk maken van gegevens en uit stelselmatige observatie.[37]

Gezien het heimelijke karakter van de bepaling, en ook de inhoudelijke overeenkomsten met de overige bijzondere opsporingsbevoegdheden, heeft de wetgever ervoor gekozen de hackbevoegdheid op te nemen in Titel IVA van het WvSv. Het gevolg daarvan is dat er meer rechtswaarborgen van toepassing zijn dan op de 'traditionele' opsporingsbevoegdheden van titel IV van het WvSv.[38] Gelet op het indringende karakter van art. 126nba Sv ten opzichte van het recht op privacy van de verdachte, lijkt dit een logische keuze.

De voorwaarden waaronder de bevoegdheid van art. 126nba Sv mag worden ingezet zijn dan ook strikt gesteld en komen neer op het volgende. Allereerst mag de hackbevoegdheid slechts worden ingezet wanneer op grond van feiten en omstandigheden kan worden aangenomen dat het geautomatiseerde werk ook daadwerkelijk door verdachte zelf in gebruik is. Daarbij is het niet relevant of verdachte het apparaat alleen in gebruik heeft of samen met anderen.[39]

Daarbij staat de bevoegdheid van art. 126nba Sv slechts open ingeval er sprake is van verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten op grond van art. 67 lid 1 Sv, het strafbare feit een ernstige inbreuk op de rechtsorde oplevert én in geval het strafrechtelijk onderzoek dit dringend vordert. Denk bijvoorbeeld aan een delict als valsheid in geschrift (art 225 Sr).[40] Fraude wordt steeds vaker online gepleegd waarbij burgers en bedrijven op grote schaal de dupe kunnen worden, hetgeen een grote maatschappelijke impact kan hebben.[41] Maar ook delicten als witwassen (art. 420bis Sr), mensensmokkel (art. 197a Sr) en opruiing en rekrutering voor de gewapende strijd (art. 131 en 205 Sr) zijn voorbeelden van delicten die zich steeds meer via digitale kanalen afspelen.[42]

Van de bevoegdheid tot vastlegging van gegevens en het ontoegankelijk maken van gegevens kan overigens pas sprake zijn in geval van verdenking van een misdrijf waarop een maximum gevangenisstraf van acht jaar of meer op is gesteld.[43]

Een extra waarborg ligt in de tijdelijkheid van de rechterlijke machtiging. Art. 126nba lid 3 Sv bepaalt dat het bevel voor maximaal vier weken wordt gegeven. Wel biedt art 126nba lid 5 Sv de mogelijkheid tot verlenging, in welk geval de officier van justitie een nieuwe met redenen omklede machtiging moet aanvragen en er opnieuw een voorafgaande rechterlijke toetsing moet plaatsvinden.

2.4. Conclusie

De technologische mogelijkheden zijn de afgelopen jaren razendsnel gegroeid en de criminaliteit maakt daar veelvuldig en dankbaar gebruik van. Het gebruik van draadloze netwerken, encryptie, Cloudcomputingdiensten en diverse anonimiseringstechnieken maken het opsporingsonderzoek steeds lastiger en stellen de opsporingsdiensten voor grote uitdagingen. Om niet stuk te lopen in het

[37] Art. 126nba Sv.
[38] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 16.
[39] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 98.
[40] Art. 225 Sr.
[41] *Kamerstukken I* 2018/19, 34 372, M.
[42] *Kamerstukken II* 2017/18, 34 372, nr. 27.
[43] Art. 126nba lid 1 Sv.

opsporingsonderzoek is de Wet computercriminaliteit III en daarmee de hackbevoegdheid van art. 126nba Sv in het leven geroepen.[44]

Op grond van art. 126nba Sv kan aan opsporingsdiensten de bevoegdheid worden gegeven om binnen te dringen in een geautomatiseerd werk en vervolgens onderzoek te doen in dat geautomatiseerd werk.

Door haar heimelijke karakter kan deze bevoegdheid vergaande inbreuken op de privacy van een verdachte opleveren. Daarom en gelet op de overeenkomsten met de andere bijzondere opsporingsbevoegdheden, is de hackbevoegdheid opgenomen als bijzondere opsporingsbevoegdheid in Titel IVA van het WvSv die ziet op de 'Bijzondere bevoegdheden tot opsporing'. Daardoor zijn meer rechtswaarborgen van toepassing dan bij de 'gewone' opsporingsbevoegdheden van Titel IV van het WvSv.[45]

Die waarborgen zijn dat het bij de inzet van art. 126nba Sv minimaal moet gaan om een delict waarvoor voorlopige hechtenis is toegelaten op grond van art. 67 lid 1 Sv, het strafbare feit een ernstige inbreuk op de rechtsorde oplevert én het strafrechtelijk onderzoek dit dringend vordert.[46] Ook vindt er een rechterlijke toetsing vooraf plaats. De officier van justitie kan pas het bevel ex art. 126nba Sv aan de opsporingsdiensten geven nadat daarvoor een machtiging is afgegeven door de rechter-commissaris, met als extra waarborg dat dat de afgegeven machtiging tijdelijk is. Bij verlenging van de machtiging zal dus altijd en vooraf een rechterlijke toetsing moeten plaatsvinden.[47]

Of en in hoeverre de inzet van de hackbevoegdheid van art. 126nba Sv te ver reikt en kan leiden tot ongerechtvaardigde inbreuken op de privacy van een verdachte, zal in de volgende hoofdstukken worden bezien. Allereerst zal in hoofdstuk 3 worden gekeken naar de criteria voor een gerechtvaardigde inbreuk op het recht op privacy, zoals neergelegd in artikel 8 lid 1 EVRM, waarna in hoofdstukken 4 en 5 zal worden bezien op welke wijze daar invulling aan wordt gegeven, zowel in formele zin als in de rechtspraktijk.

[44] *Kamerstukken II* 2015/16, 34372, 3, p. 7-12; *Kamerstukken II* 2016/17, 34372, 6, p. 14-22.
[45] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 16.
[46] Art. 126nba lid 1 Sv.
[47] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 29.

Hoofdstuk 3 – De criteria voor een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM

3.1. Inleiding

Tot op heden heeft het Europees Hof voor de Rechten van de Mens (hierna: EHRM) zich niet expliciet uitgesproken over de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk zoals in art. 126nba Sv. Wel zijn er aanknopingspunten te vinden in diverse uitspraken van het EHRM. Het EHRM heeft zich bijvoorbeeld wel uitgesproken over de rechtmatigheid van andere heimelijke opsporingsbevoegdheden zoals de tapbevoegdheid van art. 126l Sv jo. 126m Sv.[48]

Zo heeft het EHRM in meerdere uitspraken geoordeeld dat de inzet van heimelijke opsporingsbevoegdheden zoals het aftappen/afluisteren van gesprekken, het onderscheppen en opslaan van post- en e-mails alsmede het volgen van een verdachte in zijn online-gedragingen, per definitie een inbreuk op artikel 8 lid 1 EVRM opleveren.[49] Daarbij is niet relevant of de verkregen gegevens daadwerkelijk belastende informatie tegen een verdachte bevatten of dat de gegevens al dan niet tegen verdachte worden gebruikt in het strafproces.[50] Hieruit volgt dat de inzet van dergelijke heimelijke opsporingsbevoegdheden altijd moeten kunnen worden gerechtvaardigd op grond van de uitzonderingsbepaling zoals opgenomen in art. 8 lid 2 EVRM.

Het doel van deze scriptie is om vast te stellen of en in hoeverre de hackbevoegdheid van art. 126nba Sv in overeenstemming is met de eisen die gelden voor een rechtmatige inbreuk ex art. 8 lid 2 EVRM. In het voorgaande hoofdstuk zijn het doel en de reikwijdte van art. 126nba Sv bepaald. In dit hoofdstuk zal art. 8 EVRM onder de loep worden genomen. De centrale vraag daarbij luidt:

'Wat zijn de criteria voor een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM?'

Daartoe zal in paragraaf 3.2. eerst de reikwijdte van art. 8 EVRM worden uiteengezet. Vervolgens zullen in paragraaf 3.3. de criteria worden besproken waaraan een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM moet voldoen. Daarbij wordt specifiek ingegaan op de door het EHRM vastgestelde criteria voor een gerechtvaardigde inbreuk op art. 8 EVRM in geval van de inzet van heimelijke opsporingsbevoegdheden. Daarbij zal de relevante rechtspraak van het EHRM worden besproken. In paragraaf 3.4. volgt een conclusie.

3.2. De reikwijdte van art. 8 EVRM

Art. 8 lid 1 EVRM bepaalt ''*Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie*''.

In meerdere uitspraken heeft het EHRM geoordeeld dat er geen uitputtende uitleg mogelijk is voor het begrip privéleven.[51] De rechtspraak over art. 8 EVRM betreft dan ook zeer uiteenlopende zaken. Ondanks dat het begrip privéleven zich volgens het EHRM niet leent voor een uitputtende uitleg kan uit de rechtspraak van het EHRM toch enigszins worden afgeleid op welke rechten de bescherming die voortvloeit uit art. 8 EVRM ziet. Zo heeft het EHRM in de zaak *Pretty/Verenigd Koninkrijk*

---

[48] Zie bijvoorbeeld: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman.

[49] Loof e.a. 2015, p. 8. Als ook: EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48. Als ook: EHRM 2 augustus 1984, nr. 8691/79 *(Malone/Verenigd Koninkrijk),* par. 64. Als ook: EHRM 25 maart 1998, nr. 23224/94 (*Kopp/Zwitersland)*, p. 53. Als ook: EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par. 65-70. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, par. 77.

[50] EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par. 70.

[51] EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Duitsland),* par. 29. Als ook: EHRM 6 februari 2001, nr. 44599/98 (*Bensaid/Verenigd Koninkrijk),* par. 47. Als ook: EHRM 27 juli 2004, nr. 55480/00 en nr. 59330/00 *(Sidrabas & Dziautas/Litouwen),* par. 43. Als ook: EHRM 4 december 2008, nr.30562/04 en nr. 30566/04 *(S. & Marper/Verenigd Koninkrijk),* par. 66.

bijvoorbeeld overwogen dat zowel persoonlijke autonomie als persoonlijke ontwikkeling deel uitmaken van het recht op privéleven.[52] Een nadere uitleg heeft het EHRM daarbij niet gegeven.[53]

Een wat duidelijker aspect van het recht op privéleven is het recht op privacy. Het recht op privacy vloeit voort uit het recht op privéleven zoals bedoeld in art. 8 lid 1 EVRM en komt erop neer dat eenieder het recht heeft om zijn leven te kunnen leiden zonder dat de overheid of anderen zich hier ongewenst in mengen.[54] Met oog op de strafrechtspleging is dit wellicht het belangrijkste uitvloeisel van art. 8 lid 1 EVRM. Het zorgt er immers voor dat de opsporingsdiensten geen onbeperkte inmenging in het leven van een verdachte mogen of kunnen maken.[55]

Bij de uitoefening van (heimelijke) opsporingsbevoegdheden zullen er vaak meerdere rechten in het geding zijn. Zo omvat het recht op privacy in de strafrechtelijke context mede het huisrecht, het recht op bescherming van persoonsgegevens en van correspondentie.[56] De reden daarvoor is dat deze verschillende uit art. 8 lid 1 EVRM voortvloeiende grondrechten zodanig met elkaar samenhangen, dat in veel gevallen niet goed te bepalen is welke van deze specifieke rechten in het gedrang is.[57] Zoals in de inleiding reeds besproken levert de inzet van heimelijke opsporingsbevoegdheden zoals het afluisteren en het onderscheppen van post van verdachten per definitie een inbreuk op de privacy op.[58] Inzet van dergelijke bevoegdheden kan vanwege het heimelijke karakter en de kans op misbruik van de bevoegdheid door de opsporingsdiensten een gevaar opleveren voor de democratische rechtsstaat en moeten volgens het EHRM slechts in uitzonderlijke gevallen kunnen worden ingezet.[59]

Tot slot is het met betrekking tot de reikwijdte van art. 8 EVRM van belang om te vermelden dat het EHRM beoogt met de tijd mee te gaan. In 1978 is in de zaak *Tyrer/Verenigd Koninkrijk* overwogen dat het EVRM een 'levend' verdrag is en dat bij de uitleg ervan moet worden gekeken naar de 'present day conditions'.[60] Hieruit volgt dat hedendaagse communicatiemiddelen zoals e-mail en WhatsApp ook onder de reikwijdte van art. 8 EVRM vallen.

3.3. Beperking van het recht op privacy op grond van art. 8 lid 2 EVRM

Art. 8 lid 2 EVRM bepaalt *''Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen''.*[61]

---

[52] EHRM 29 april 2002, nr. 2346/02 (*Pretty/Verenigd Koninkrijk)*, par. 61.
[53] De Vries 2013, p. 202.
[54] De Vries 2013, p. 202.
[55] De Vries 2013, p. 202.
[56] De Vries 2013, p. 202. Als ook: EHRM 24 juli 2003, nrs. 46133/99 en 48183/99 *(Smirnova/Rusland)*, par. 95. Als ook: EHRM 28 mei 2009, nr. 26713/05 (*Bigaeval/Griekenland),* par. 22.
[57] De Vries 2013, p. 202.
[58] Loof e.a. 2015, p. 8. Als ook: EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48. Als ook: EHRM 2 augustus 1984, nr. 8691/79 *(Malone/Verenigd Koninkrijk),* par. 64. Als ook: EHRM 25 maart 1998, nr. 23224/94 (*Kopp/Zwitersland)*, p. 53. Als ook: EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par. 65-70. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, par. 77.
[59] EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48.
[60] EHRM 25 april 1978, nr. 5856/72 (*Tyrer/Verenigd Koninkrijk)*, par. 31.
[61] Art. 8 lid 2 EVRM.

Daarmee kan een inbreuk op het recht op privacy zoals dat voortvloeit uit art. 8 lid 1 EVRM slechts gerechtvaardigd zijn wanneer wordt voldaan aan de cumulatief gestelde eisen van bovengenoemde bepaling, te weten dat:

1. De beperking moet een legitiem doel dienen;
2. De beperking moet zijn voorzien bij wet;
3. De beperking moet noodzakelijk zijn in een democratische samenleving.

Allereerst moet er dus sprake zijn van een legitiem doel. Deze doelen staan uitputtend vermeld in de tekst van art. 8 lid 2 EVRM. De hackbevoegdheid van art. 126nba Sv valt zonder enige twijfel onder het voorkomen van wanordelijkheden en strafbare feiten. Op dit criterium zal daarom verder niet worden ingegaan.

Het tweede criterium omvat het voorzienbaarheidsvereiste (*forseeability*). Uit de rechtspraak van het EHRM die ziet op de invulling van het voorzienbaarheidsvereiste in het kader van heimelijke opsporingsbevoegdheden volgen de cumulatieve eisen dat de bevoegdheid a) moet zijn gegrond op een nationale wettelijke bepaling die b) duidelijk en toegankelijk is voor verdachten en, vooral dat c) de wettelijke bepaling voldoende voorzienbaar is voor verdachten, in die zin dat een verdachte de gevolgen van een dergelijke bepaling moet kunnen begrijpen.[62] In *Weber en Savaria/Duitsland* overwoog het EHRM bijvoorbeeld; *''... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly'' en "....It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*.[63] De overweging die het EHRM hier maakt lijkt er vrij vertaald op neer te komen dat voorzienbaarheid in het kader van heimelijke opsporingsbevoegdheden redelijkerwijs niet kan betekenen dat het voor een persoon precies kenbaar moet kunnen zijn welke bevoegdheden op welk moment tegen hem worden ingezet, maar dat hij op grond van de wettelijke opsporingsbevoegdheid logischerwijs een inschatting moet kunnen maken van de mogelijke inzet van deze bevoegdheid tegen hem.

In *Kennedy/Verenigd Koninkrijk* benadrukt het EHRM nogmaals dat in de betreffende wetsbepaling duidelijk moet zijn weergegeven onder welke omstandigheden bedoelde opsporingsbevoegdheden kunnen worden ingezet.[64]

Ook stelt het EHRM aan geheime opsporingsbevoegdheden de eis dat er voldoende effectieve waarborgen tegen misbruik aanwezig moeten zijn. In de hiervoor aangehaalde zaak *Kennedy/ Verenigd Koninkrijk* overwoog het EHRM bijvoorbeeld: *'In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance*

[62] EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par.50.
[63] EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par. 93.
[64] De Vries 2013, p. 203-204. Als ook o.a.: EHRM 18 mei 2010, nr. 26839/05 *(Kennedy/Verenigd Koninkrijk),* par. 152.

powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court.'[65] Daarmee stelt het EHRM dat in geval er onvoldoende waarborgen tegen misbruik van een dergelijke bevoegdheid zouden zijn ingebouwd in de nationale wet, dit onder het grote publiek terecht de indruk zou kunnen wekken dat er misbruik kan worden gemaakt van de betreffende bevoegdheid en dat die bevoegdheid daarmee onrechtmatig zou zijn.

In aanvulling daarop heeft het EHRM in meerdere uitspraken over heimelijke opsporingsbevoegdheden nog een opsomming gegeven van de criteria waaraan een nationale wettelijke bepaling moet voldoen in het kader van voorzienbaarheid en ter voorkoming van machtsmisbruik.[66] Daarbij zijn zes cumulatieve eisen gesteld waaraan de nationale wettelijke bepalingen moeten voldoen, te weten:

1. De aard van het misdrijf waarop de bevoegdheid mag worden ingezet moet duidelijk zijn omschreven;
2. Er moet duidelijk blijken op welke categorie van personen de bevoegdheid betrekking heeft;
3. Er moet een maximale tijdsduur aan de inzet van de bevoegdheid worden gesteld;
4. De procedure voor het verwerken en opslaan van gegevens die verkregen zijn bij de inzet van de heimelijke bevoegdheid moet kenbaar zijn;
5. Er moeten regels zijn die gelden bij het delen van de onderschepte gegevens met derde instanties;
6. Er moeten regels zijn die bepalen wanneer en in welke gevallen de onderschepte gegevens worden vernietigd.[67]

Daarbij stelde het EHRM dat deze sub-criteria de minimale waarborg tegen machtsmisbruik omvatten, die voor justitiabelen een duidelijk kader schept voor de omstandigheden waarin de overheid gebruik kan maken van dergelijke heimelijke opsporingsbevoegdheden.[68] Daar heeft het EHRM in 2010 aan toegevoegd dat de aard, de reikwijdte, de duur en de rechtsgrond van de ingezette bevoegdheid moeten worden afgezet tegen de omstandigheden van het specifieke geval.[69] Daarbij kan worden gedacht aan de aard en omvang van de zaak, de ernst van de verdenking, mogelijke schade of afbreukrisico als gevolg van het delict, of er sprake is van een geschokte rechtsorde, enz.

Uit het voorgaande volgt mijns inziens dat elke afzonderlijke inbreuk op de privacy die voortkomt uit de inzet van een heimelijke opsporingsbevoegdheid, afzonderlijk moet worden getoetst aan de uitzondering van art. 8 lid 2 EVRM. Het is immers alleen dan mogelijk om de omstandigheden van het specifieke geval in de beoordeling mee te nemen.

In de zaak *Zakharov/Rusland,* die zag op de bevoegdheid tot het onderscheppen van telefoon- en internetcommunicatie, heeft het EHRM bovenstaande overwegingen herhaald en daarbij de criteria nog eens aangescherpt door ook het laatste criterium van het noodzakelijkheidsvereiste aan controle onderhevig te maken door een onderscheid te maken in drie fases van toezicht.[70] Dit derde en laatste criterium 'noodzakelijk in een democratische samenleving' houdt in dat er sprake moet zijn

[65] EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk)*, par. 124.
[66] EHRM 24 april 1990, nr. 11801/85 (*Kruslin-Huvig/Frankrijk).* Als ook: EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par. 95. Als ook: EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland).*
[67] EHRM 24 april 1990, nr. 11801/85 (*Kruslin-Huvig/Frankrijk).* Als ook: EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par. 95. Als ook: EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland).*
[68] EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par.101.
[69] EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk),* par. 153.
[70] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland).*

van een 'pressing social need' voor de beperking van, - in dit geval-, het recht op privacy.[71] Er moet aldus een dringende maatschappelijke behoefte bestaan die rechtvaardigt dat er een inbreuk wordt gemaakt op het recht op privacy van de verdachte. Daarbij moet acht worden geslagen op het proportionaliteitsbeginsel, dat wil zeggen dat het doel en gevolg van de inzet van de bevoegdheid moet worden afgewogen en in verhouding moet staan tot het recht op privacy van de verdachte. Op grond van het subsidiariteitsbeginsel mag de bevoegdheid bovendien slechts worden ingezet als vaststaat dat geen ander minder ingrijpend middel voorhanden is.[72] Daarbij moet het doel en de grond van de inbreuk 'relevant and sufficient' zijn, wat inhoudt dat de bevoegdheid ook geschikt moet zijn voor het behalen van het doel van de inzet van de opsporingsbevoegdheid.[73] Daarin komt aan de bevoegde instanties van de lidstaten een zekere 'margin of appreciation' ofwel beoordelingsruimte toe. Dat werd herhaald in de uitspraak van het EHRM in de zaak *S. en Marper tegen het Verenigd Koninkrijk* waarin het ging om het opslaan van o.a. DNA-materiaal en vingerafdrukken in databanken van de Britse overheid. Daarin toetste het EHRM op verzoek van de twee klagers de Britse regelgeving aan het EVRM en concludeerde dat die in strijd was met art. 8 EVRM en kende vervolgens aan klagers ten laste van de Britse overheid een immateriële schadevergoeding toe.[74]

Met betrekking tot de 'noodzakelijkheid in een democratische samenleving' heeft het EHRM in *Zakharov/Rusland* - waarin het ging om een tapbevoegdheid - een onderscheid gemaakt in drie fases waarin afzonderlijk toezicht door de bevoegde nationale instanties is vereist, te weten 1) voorafgaand toezicht aan de inzet van de heimelijke bevoegdheid, 2) toezicht tijdens de daadwerkelijke inzet van de heimelijke bevoegdheid en 3) toezicht achteraf.[75] In elk van deze fases zal de 'pressing social need' opnieuw en bij voorkeur door een bevoegde rechter moeten worden beoordeeld. Op deze wijze kunnen de rechten van een verdachte beter worden gewaarborgd, doordat in elk opvolgend stadium opnieuw wordt getoetst of er nog steeds sprake is van een 'pressing social need' voor de inzet van de bevoegdheid.[76]

3.4. Conclusie

In dit hoofdstuk is in het kader van heimelijke opsporingsbevoegdheden onderzocht wat de criteria zijn voor een gerechtvaardigde inbreuk op art. 8 lid 1 EVRM.

Het EHRM heeft zich nog niet expliciet uitgesproken over een hackbevoegdheid als in art. 126nba Sv in relatie tot schending van art. 8 EVRM. Er zijn echter wel degelijk aanknopingspunten te vinden in EHRM-jurisprudentie over andere bijzondere opsporingsbevoegdheden, zoals het afluisteren of het onderscheppen van communicatie in e-mails of post van een verdachte.[77]

Uit de jurisprudentie van het EHRM die ziet op de heimelijke opsporingsbevoegdheden volgt onder meer dat de inzet van een dergelijke bevoegdheid per definitie een inbreuk op artikel 8 lid 1 EVRM

---

[71] EHRM 7 december 1976, nr. 5493/72 (*Handyside/Verenigd Koninkrijk),* par. 48-49.
[72] Oerlemans 2017, p. 76. Als ook: EHRM 25 maart 1983, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75. Als ook: 7136/75 (*Silver and others/Verenigd Koninkrijk)*, par. 97. Als ook: EHRM 26 Maart 1987, nr. 9248/81 *(Leander v. Sweden)*, par. 81.
[73] EHRM 3 oktober 2013, appl. nr. 12430/11 *(Vosgien v. France).*
[74] EHRM 4 december 2008, nr. 30562/04 (*S. & Marper/Verenigd Koninkrijk),* par. 101-102.
[75] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.
[76] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.
[77] EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk).* Als ook: Zie bijvoorbeeld: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman. Als ook: EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland).*

oplevert die moet kunnen worden gerechtvaardigd op grond van art. 8 lid 2 EVRM.[78] Daarvoor is vereist dat de beperking een legitiem doel dient, bij wet is voorzien en noodzakelijk is in een democratische samenleving.[79]

Het voorzienbaarheidsvereiste dat geldt voor heimelijke opsporingsbevoegdheden is door het EHRM zo uitgelegd dat een verdachte logischerwijs een inschatting moeten kunnen maken van de kans op een mogelijke inzet van deze bevoegdheid tegen hem.[80] Dit klinkt logisch. Een dergelijke bevoegdheid zou zinloos zijn als het voorzienbaarheidsvereiste hier zo ver zou reiken dat precies kenbaar moet zijn welke bevoegdheid wanneer tegen een verdachte wordt ingezet. Wie vooraf weet dat zijn online communicatie wordt onderschept, zal immers geen belastende informatie via dat kanaal prijsgeven. Toch is enige voorzienbaarheid wel aanwezig. Het EHRM stelt als eis dat duidelijk moet zijn omschreven onder welke omstandigheden die bevoegdheid kan worden ingezet.[81]

Vanwege het heimelijke karakter en de daarmee samenhangende kans op misbruik en het gevaar dat dit mee kan brengen voor de democratische rechtstaat, mogen heimelijke opsporingsbevoegdheden slechts in uitzonderlijke gevallen worden ingezet.[82] Daartoe heeft het EHRM in het kader van de voorzienbaarheid bij heimelijke opsporingsbevoegdheden en ter voorkoming van machtsmisbruik een zestal sub-criteria ontwikkeld en die nadien nog aangescherpt door de inzet van de bevoegdheid in drie fases te verdelen.[83] Omdat in elke fase opnieuw wordt beoordeeld of nog steeds sprake is van een dringende maatschappelijk behoefte voor de inzet van de heimelijke bevoegdheid, zullen de rechten van een verdachte beter zijn gewaarborgd.[84]

---

[78] Loof e.a. 2015, p. 8. Als ook: EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48. Als ook: EHRM 2 augustus 1984, nr. 8691/79 *(Malone/Verenigd Koninkrijk),* par. 64. Als ook: EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par. 65-70. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, par. 77.

[79] Art. 8 lid 2 EVRM.

[80] EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par. 93.

[81] De Vries 2013, p. 203-204. Als ook o.a.: EHRM 18 mei 2010, nr. 26839/05 *(Kennedy/Verenigd Koninkrijk),* par. 152.

[82] EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48.

[83] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.

[84] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.

Hoofdstuk 4 – Art 126nba Sv: De kritische adviezen in het licht van art. 8 EVRM

4.1. Inleiding

In aanloop naar de Wet computercriminaliteit III is veelvuldig gediscussieerd over de hackbevoegdheid die voortvloeit uit art. 126nba Sv. Zowel voorafgaand aan als tijdens de parlementaire behandeling van de wet zijn er met name in het licht van art. 8 EVRM de nodige kritieken opgeworpen.[85] In dit hoofdstuk zal aan de hand van de bij het wetsvoorstel Computercriminaliteit III behorende Memorie van Toelichting (hierna: MvT) en de ten tijde van het wetsvoorstel uitgebrachte adviezen worden besproken wat die kritieken waren en zijn en welke waarborgen art. 126nba Sv biedt ter voorkoming van mogelijke onrechtmatige schendingen van de privacy.

De centrale vraag van dit hoofdstuk is '*Wat zijn de voornaamste kritiekpunten op de inzet van art. 126nba Sv en welke waarborgen tegen een ongerechtvaardigde schending van art. 8 EVRM in relatie tot die kritiekpunten zijn in de huidige wet ingekleed?'*

In paragraaf 4.2. worden eerst de voornaamste kritieken in het licht van art. 8 EVRM en de reactie daarop van de regering besproken. De kritiek met betrekking tot het grensoverschrijdende aspect van de inzet van de hackbevoegdheid wordt daarbij buiten beschouwing gelaten omdat die vooral ziet op schending van soevereiniteit en daarmee het kader van deze scriptie te buiten gaat.

In paragraaf 4.3. worden achtereenvolgens de drie fasen bij de inzet van art. 126nba Sv besproken. Daarbij wordt ook kort aandacht besteed aan de relatie met het recht op een eerlijk proces als neergelegd in art. 6 EVRM. In paragraaf 4.4. volgt een tussentijdse conclusie.

4.2. Adviezen en kritieken

In hoofdstuk 2 is weergegeven dat de voorwaarden waaronder de bevoegdheid van art. 126nba Sv mag worden ingezet in beginsel strikt lijken te zijn gesteld. Zo valt de hackbevoegdheid onder de bijzondere opsporingsbevoegdheden van Titel IVA van het WvSv en mag deze slechts worden ingezet wanneer uit feiten en omstandigheden kan worden aangenomen dat het geautomatiseerd werk ook daadwerkelijk door verdachte zelf in gebruik is. Het maakt daarbij echter niet uit waar het geautomatiseerd werk zich bevindt en of dat ook door anderen dan verdachte zelf in gebruik is.[86] Het gevolg daarvan kan zijn dat de inzet van art. 126nba Sv ook voor anderen dan verdachten, zoals onschuldige burgers, een schending van hun privacy kan opleveren zonder dat zij zich hiervan bewust zijn.[87] Denk bijvoorbeeld aan een computer in een hotellobby, waarvan alle hotelgasten desgewenst gebruik kunnen maken.

De regering heeft diverse organisaties geconsulteerd over het conceptwetsvoorstel, waaronder de Stichting Bits of Freedom (hierna BoF), die opkomt voor de digitale Burgerrechten en privacy van de Nederlandse burgers. BoF heeft zich kritisch uitgelaten over het wetsvoorstel en gesteld dat de hackbevoegdheid van art. 126nba Sv in feite een onbegrensde bevoegdheid is, waarbij onschuldige burgers evengoed in hun grondrechten worden geraakt als verdachten. Juist omdat criminelen doorgaans niet alleen hun eigen computer gebruiken, bestaat de kans dat ook onschuldige burgers door inzet van deze bevoegdheid in hun privacy worden geraakt. Daarnaast wijst BoF erop dat met inzet van de hackbevoegdheid ook hele servers kunnen worden gehackt. Daarbij krijgen

---

[85] Zie *Kamerstukken II,* 34372. Als ook: Verslag internetconsultatie bij Wet computercriminaliteit III.
[86] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 98.
[87] Van der Sloot, *TBS&H* 2017, p. 202.

opsporingsdiensten toegang tot en de mogelijkheid tot gebruik van een veelheid aan data van onschuldige burgers. BoF noemt de hackbevoegdheid in dat kader 'technisch onbeperkt'.[88]

In reactie hierop stelt de regering dat het onwaarschijnlijk is dat een onschuldige burger wiens IP-adres door een verdachte wordt gebruikt, persoonlijk wordt geraakt door inzet van de hackbevoegdheid. Daarvoor is de bevoegdheid volgens de regering te nauw ingekleed, door een uitgebreide, zorgvuldige en langdurige voorbereiding én uitoefening. Om die reden acht de regering ook onwaarschijnlijk dat de hackbevoegdheid wordt ingezet op een computer waar een verdachte slechts eenmaal gebruik van heeft gemaakt. Daarnaast wordt de opvatting dat criminelen voornamelijk gebruikmaken van andermans computer door de regering afgewezen omdat verdachten juist en voornamelijk gebruik zouden maken van draadloze netwerken en anonimiseringstechnieken.[89]

Naast de privacy van onschuldige burgers komt volgens BoF ook die van de verdachte zelf ernstig in het gedrang, omdat immers ook alle communicatie en data van verdachte die niet binnen het strafrechtelijk onderzoek vallen bij inzet van de hackbevoegdheid in handen van de opsporingsdiensten komen. BoF meent dat de noodzakelijkheid en proportionaliteit hiervoor niet voldoende zijn aangetoond.[90] Daarmee zegt BoF dat de inbreuk op de privacy van individuele burgers alsmede van verdachten disproportioneel groot is en niet in verhouding staat tot het doel van het wetsvoorstel. Ook de Nederlandse Orde van Advocaten (hierna: NOvA) heeft zich in zijn advies op dit punt kritisch uitgesproken en aangegeven dat de hackbevoegdheid te vergaand is om zonder deugdelijke en cijfermatige onderbouwing van de noodzaak in te voeren.[91] Het College van procureurs-generaal (hierna: het College) meent daarentegen dat zonder de hackbevoegdheid van art. 126nba Sv de opsporingsdiensten niet in staat zijn om de criminaliteit effectief en met gelijke wapens te bestrijden en dat de noodzaak daarvan besloten ligt in het moeten kunnen bijhouden van de snelle technologische ontwikkelingen.[92] In reactie op de kritieken dat de noodzaak van de hackbevoegdheid niet voldoende en deugdelijk is aangetoond, overweegt de regering in de MvT dat de noodzaak en proportionaliteit wel degelijk voldoende zijn aangetoond en uiteengezet. Daarbij verwijst de regering net als het College naar de technologische ontwikkelingen zoals de mogelijkheid tot versleuteling van gegevens en het gebruik van Cloudcomputing door criminelen. Ook verwijst de regering naar de MvT.[93] Op de kritiek van de NOvA dat enige cijfermatige onderbouwing met betrekking tot de noodzaak ontbreekt is door de regering evenwel niet ingegaan.

Het advies van de Raad voor de Rechtspraak (hierna: Rvdr) ziet met name op de reikwijdte van de hackbevoegdheid. De reikwijdte van de hackbevoegdheid wordt ook door de NOvA bekritiseerd.[94] Er zou te veel ruimte zijn voor inzet van de hackbevoegdheid in verwaarloosbaar kleine, zogenoemde bagatelzaken.[95] De regering wijst die kritiek van de hand en stelt dat een brede toepassing van de hackbevoegdheid is uitgesloten omdat de hackbevoegdheid is bedoeld als een 'laatste redmiddel'.[96] De procedurele vereisten en de vereiste voorafgaande machtiging van de rechter-commissaris bieden volgens de regering voldoende waarborgen voor een zorgvuldige afweging van de inzet van de hackbevoegdheid. De eerste voorafgaande toetsing daarvan vindt plaats door de Centrale

[88] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 78-80.
[89] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 79.
[90] Bijlage 651730 bij *Kamerstukken II* 2015/2016, 34372, 3.
[91] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 77.
[92] Bijlage 651723 bij *Kamerstukken II* 2015/2016, 34372, 3.
[93] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 77.
[94] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 76.
[95] Preadvies Adviescommissie Strafrecht 2013.
[96] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 79.

Toetsingscommissie (hierna: CTC). Dit is een intern adviesorgaan dat bestaat uit leden van het openbaar ministerie en politie. Bij een positief advies wordt het verzoek van art. 126nba Sv voorgelegd aan de rechter-commissaris, waarbij de subsidiariteit wordt getoetst. Pas als vaststaat dat er geen andere, minder vergaande opsporingsbevoegdheden zijn waarmee hetzelfde onderzoeksresultaat kan worden bereikt, kan de hackbevoegdheid worden ingezet.[97]

Andere kritiek met oog op de reikwijdte van art. 126nba Sv is dat de hackbevoegdheid ziet op *alle* geautomatiseerde werken, dus ook alle apparaten die vallen onder de noemer van het *'internet of things'*. Dit betekent dat bijvoorbeeld een 'slimme' koelkast of een tuinlamp op grond van art. 126nba Sv zou kunnen worden gehackt. Gezien het grote aantal 'slimme apparaten' dat wordt ontwikkeld en op termijn in Nederland gebruikt kan gaan worden is het potentiële bereik van art. 126nba Sv enorm groot.[98] Dat zou nuttig kunnen zijn in een strafrechtelijk onderzoek, maar zorgt voor een grenzeloze reikwijdte aan te hacken apparaten. Zo zou de politie kunnen aanvoeren dat een verdachte thuis was omdat hij zijn slimme thermostaat en/of smart-tv aan had staan.[99] Er zijn echter ook situaties denkbaar waarin hacken een technisch risico met zich mee kan brengen, zoals het hacken - en daardoor mogelijk storen of uitvallen - van een pacemaker of slimme auto.[100] Het voor de inzet van de hackbevoegdheid uitsluiten van specifieke apparaten is wat de regering betreft echter onwenselijk.[101] Criminelen zouden er daardoor toe bewogen worden juist van dergelijke apparaten gebruik te maken.[102] Als het de politie bijvoorbeeld verboden zou worden om een 'slimme auto' op afstand te stoppen om een verdachte staande te houden zou dat een goede reden zijn voor criminelen om gebruik te maken van een dergelijke auto.

Tot slot kan als kritiekpunt het gebruik van zogenoemde systeemkwetsbaarheden, zoals fouten of onbekende openingen in software, worden genoemd.[103] De bevoegdheid van opsporingsdiensten om heimelijk binnen te dringen in een geautomatiseerd werk is onder andere mogelijk door gebruik te maken van kwetsbaarheden in software of apparatuur waarvan de producent zelf geen weet heeft. BoF meent dat opsporingsdiensten belang hebben bij het laten bestaan van onbekende kwetsbaarheden en dat door die kwetsbaarheden niet te melden bij de producent, software bewust kwetsbaar wordt gehouden, waardoor ook anderen gebruik kunnen maken van die kwetsbaarheden, hetgeen een averechts effect kan hebben.[104] De regering wijst dit van de hand en stelt dat het ook voor de opsporingsdiensten zeer onwenselijk is om kwetsbaarheden lange tijd stil te houden omdat het risico op mogelijk misbruik door derden afbreuk doet aan de betrouwbaarheid van het bewijs. Daarnaast is het risico voor de maatschappij als geheel te groot om dergelijke kwetsbaarheden langere tijd stil te houden.[105]

De betrouwbaarheid van digitaal bewijs dat is verkregen door gebruik te maken van kwetsbaarheden is overigens per definitie problematisch. Wanneer opsporingsdiensten een geautomatiseerd werk hacken door gebruik te maken van een kwetsbaarheid dan kan dat immers ook door een kwaadwillende derde worden gedaan en kan op deze wijze vergaard digitaal bewijs bewust worden gemanipuleerd of vervalst.[106] Van der Sloot concludeert dat het in dit licht nog maar de vraag is of

---

[97] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 79.
[98] 'Bijna drie kwart van de Nederlanders maakt gebruik van slimme apparaten', *CBS.nl,* 1 december 2021.
[99] Prins, *TPWS 2017/15,* p. 1.
[100] Oerlemans *Strafblad* 2017, p. 358.
[101] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 32.
[102] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 32.
[103] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 34.
[104] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 79.
[105] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 34.
[106] Van der Sloot, *TBS&H* 2017, p. 203.

het gebruik van kwetsbaarheden in de software daadwerkelijk kan leiden tot een effectieve manier om betrouwbaar bewijsmateriaal te verzamelen.[107]

Ondanks dat ook de wetgever het niet melden van kwetsbaarheden aan de producent onwenselijk acht, is in art. 126ffa Sv toch een uitzonderingsbepaling opgenomen op grond waarvan de officier van justitie na een schriftelijke machtiging van de rechter-commissaris de bekendmaking van de kwetsbaarheid aan de producent kan uitstellen. Er moet dan wel sprake zijn van een 'zwaarwegend onderzoeksbelang'.[108]

4.3. Drie fasen van inzet

In hoofdstuk 3 is uiteengezet dat het EHRM in de zaak *Zakharov/Rusland* de inzet van heimelijke opsporingsbevoegdheden verdeeld ziet in drie fasen van toezicht, mede omwille van de waarborging van de rechten van de verdachte.[109] De daarbij beschreven bevoegdheden zijn voor wat betreft hun heimelijke aard vergelijkbaar met de hackbevoegdheid van art. 126nba Sv. Het belang van toetsing in verschillende fasen is dan ook veelbesproken tijdens de totstandkoming van de Wet Computercriminaliteit III.[110] Nu het gaat om de inzet van een heimelijke bevoegdheid, waarvan de inzet reële risico's met zich meebrengt op onrechtmatige schendingen van art. 8 EVRM, is voor een goed begrip een duidelijke en zo volledig mogelijke weergave van de daadwerkelijke inzet van de bevoegdheid op zijn plaats. De drie fasen zoals die ter waarborging bij de inzet van art. 126nba Sv zijn ingekleed zullen hierna aan de hand van de MvT worden besproken.

In de eerste 'verkennende fase' dienen de risico's die gepaard gaan met de inzet van de bevoegdheid in het specifieke geval door de Officier van Justitie te worden ingeschat en afgewogen.[111] Pas na dit vooronderzoek, waarin alle onderzoeks-aspecten door de Officier van Justitie in beeld zijn gebracht, maakt hij de afweging om al dan niet een bevel tot onderzoek in een geautomatiseerd werk af te geven. Daarbij dient het belang van de inzet van de bevoegdheid te worden afgewogen tegen de bescherming van de persoonlijke levenssfeer van de verdachte en eventuele derden.[112]

Nadat de officier van justitie heeft besloten tot het bevel legt hij zijn voornemen voor aan de CTC. De CTC toetst de voorgenomen inzet van de hackbevoegdheid vervolgens aan wet- en regelgeving en aan rechtspraak en beoordeelt naast de effectiviteit van de beoogde inzet ook de proportionaliteit en subsidiariteit. Na akkoord van de CTC vraagt de officier van justitie de rechter-commissaris om een schriftelijke machtiging. De rechter-commissaris beoordeelt vervolgens opnieuw de proportionaliteit en subsidiariteit van de beoogde inzet. Ook beoordeelt hij of het geautomatiseerd werk voldoende aanwijsbaar en identificeerbaar is en bepaalt hij de reikwijdte en de duur van het onderzoek.[113]

De tweede fase bestaat uit 'het onderzoek in het geautomatiseerd werk' en vangt aan nadat de eerste fase is afgerond en de officier van justitie heeft vastgesteld welk geautomatiseerd werk moet worden binnengedrongen met het oog op het verkrijgen van welk soort gegevens. Daarbij is een niet-limitatief aantal technieken mogelijk, zoals gebruikmaken van 'Artificial Intelligence' ('AI') of 'social engineering', wat wil zeggen het per telefoon of e-mail manipuleren van verdachte met het doel om bijvoorbeeld malware te plaatsen in zijn computersysteem, dan wel om 'keyloggers' te plaatsen om wachtwoorden van verdachte te achterhalen. Ook kan een 'bug' geplaatst worden. Daarbij kan, zoals

[107] Van der Sloot, *TBS&H* 2017, p. 204.
[108] Art. 126ffa Sv.
[109] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.
[110] Zie o.a. *Kamerstukken I* 2016/17, 34 372, E, (Verslag I).
[111] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 33.
[112] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 32-34.
[113] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 38.

in de vorige paragraaf besproken, gebruik worden gemaakt van bestaande kwetsbaarheden in het systeem van verdachte. Uitgangspunt daarbij is dat er geen nieuwe kwetsbaarheden worden gecreëerd.[114]

Het toezicht in de tweede fase bestaat uit vastlegging ofwel 'logging' (vastlegging) van de gegevensstromen.[115] Dit gebeurt geautomatiseerd en dient de controleerbaarheid en voorkoming van misbruik van de bevoegdheid. Bij gebruik van technische hulpmiddelen is vereist dat de handelingen van die hulpmiddelen op eenzelfde automatische wijze worden vastgelegd.[116] Daardoor kan het gevolgde proces en de kwaliteit daarvan ook achteraf worden gecontroleerd en daarmee de integriteit van het proces worden gewaarborgd.[117]

De derde en laatste fase omvat 'de afsluiting van het onderzoek in een geautomatiseerd werk'. Het onderzoek wordt beëindigd als het doel van de inzet is bereikt, of als de termijn waarvoor de machtiging is afgegeven is verstreken. Geplaatste technische hulpmiddelen worden verwijderd door een speciaal technisch team dat niet betrokken is geweest bij het onderzoek zelf. Omwille van de controleerbaarheid van de door dit team verrichte handelingen worden deze op grond van art. 152 Sv opgenomen in een proces-verbaal. Het technisch team is gehouden om het geautomatiseerd werk zoveel mogelijk achter te laten in de staat waarin het was voordat de bevoegdheid werd ingezet. Wanneer dit niet mogelijk is dient de officier van justitie de beheerder van het geautomatiseerd werk daarvan op de hoogte te stellen en aanwijzingen te geven op welke wijze de achtergebleven software kan worden verwijderd.[118] Zowel in de adviezen als in de literatuur is het belang van toezicht achteraf veelbesproken.[119]

Het toezicht in de derde fase ligt bij de Inspectie van Veiligheid en Justitie (hierna: de Inspectie). De Inspectie houdt toezicht op de kwaliteit van de politiële taakuitvoering en controleert voornamelijk of de inzet van art. 126nba Sv volgens de wettelijke procedures is toegepast. Jaarlijks brengt de Inspectie een verslag uit van de resultaten van dit toezicht en signaleert daarbij aandachtspunten.[120] Punt van kritiek hierbij is de betwiste onafhankelijkheid van de Inspectie.[121] De regering wijst er in dit kader op dat de Inspectie als rijksinspectie weliswaar onderdeel is van het ministerie, maar dat wel degelijk sprake is van volledige onafhankelijkheid. Zo stelt de Inspectie zijn eigen werkprogramma vast en beschikken de inspecteurs over wettelijke bevoegdheden die eenieder verplichten om medewerking te verlenen.[122] Of dat een garantie biedt voor volledige onafhankelijkheid is maar de vraag.

Ook luidt de kritiek dat een rechtmatigheidstoets achteraf in veel gevallen ontbreekt.[123] Bij een vergaande bevoegdheid als die van art. 126nba Sv is een rechtmatigheidstoets achteraf, wat bijvoorbeeld Oerlemans betreft, onmisbaar. Nu is echter niet duidelijk hoever de opsporingsdiensten zijn gegaan bij de inzet van de bevoegdheid, maar slechts of de procedures juist zijn gevolgd.[124] In gevallen waarbij niet tot vervolging wordt overgegaan is er geen rechter die zich buigt over de

[114] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 34.
[115] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 34.
[116] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 35.
[117] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 39.
[118] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 39, p. 105.
[119] Zie o.a. Oerlemans *Strafblad* 2017.
[120] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 82-83.
[121] *Kamerstukken I* 2016/17, 34 372, E, p. 22.
[122] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 82.
[123] *Kamerstukken I* 2016/17, 34 372, E, p. 9. Als ook: Oerlemans *Strafblad* 2017, p. 359.
[124] Oerlemans *Strafblad* 2017, p. 359.

rechtmatigheid van de ingezette bevoegdheid. Daarnaast is het in geval van niet-vervolging voor de verdachte niet mogelijk om van zijn klachtrecht gebruik te maken daar hij in de meeste gevallen niet eens weet dat de bevoegdheid tegen hem is ingezet. Daarmee komt de relatie met art. 6 EVRM dat ziet op het recht op een eerlijk proces om de hoek kijken.[125] Een onrechtmatige schending van art. 8 EVRM leidt in de praktijk namelijk zelden tot vaststelling door de rechter van een schending van art. 6 EVRM.[126] Wanneer de betrouwbaarheid van enig onrechtmatig verkregen bewijs niet ter discussie staat, zal het in de strafzaak tegen verdachte kunnen worden gebruikt. Meerdere wetenschappers menen dat de rechtmatigheidstoets juist om die reden van uiterst belang is.[127] Zonder gedegen rechtmatigheidstoets is de betrouwbaarheid van het bewijs immers niet te garanderen. Zo lang de betrouwbaarheid van bewijs louter op grond van juist gevoerde procedures wordt aangenomen, staat de bescherming van art. 8 EVRM in strafzaken onder grote druk. De feitelijke gang van zaken bij de inzet komt dan immers niet aan de orde. Lindemann meent dat het met een vergaande bevoegdheid als die van art. 126nba Sv een kwestie van tijd is tot het EHRM een andere koers zal gaan varen en dat de betrouwbaarheid van het bewijs bij een schending van art. 8 EVRM niet zomaar zal worden aangenomen en het EHRM een rechtmatigheidstoets zal eisen.

4.5. Conclusie

In dit hoofdstuk is onderzocht welke kritiek er in het licht van art. 8 EVRM is geleverd op de invoering van het wetsvoorstel tot invoering van de hackbevoegdheid in art. 126nba Sv en welke waarborgen tegen een ongerechtvaardigde schending van art. 8 EVRM er in de huidige wet zijn opgenomen.

Naast het vermeend ontbreken van de noodzakelijkheid en proportionaliteit van de bevoegdheid, zien de kritieken ook op de te verwachten problemen bij de inzet van de bevoegdheid in de praktijk. Zo is er kritiek op de reikwijdte van de bevoegdheid en op het gebruik van systeemkwetsbaarheden.[128] Ook zou er te veel ruimte zijn voor toepassing van de hackbevoegdheid in bagatelzaken en zouden er te veel soorten apparaten onder de bevoegdheid vallen.[129]

De waarborgen tegen misbruik van de bevoegdheid liggen met name in de drie fasen van toezicht zoals het EHRM bij heimelijke opsporingsbevoegdheden vereist en die ook zijn ingebouwd in art. 126nba Sv.[130] In ‘de verkennende fase’ toetst intern adviesorgaan CTC het voornemen en de wijze van inzet, waarna de officier van justitie de rechter-commissaris om een schriftelijke machtiging verzoekt.[131] Het toezicht in de tweede fase bestaat uit de geautomatiseerde vastlegging van de gegevensstromen ter voorkoming van misbruik van de bevoegdheid.[132] De controle in de derde fase ligt bij de Inspectie. De Inspectie houdt achteraf toezicht op de kwaliteit van de politiële taakuitvoering en controleert of de inzet van art. 126nba Sv volgens de wettelijke procedures is toegepast. Hier wordt jaarlijks verslag van uitgebracht.[133]

Dat de overheid als wetgever weinig risico’s ziet en optimistisch is mag niet verbazen. In de opsporing en vervolging van criminaliteit is een belangrijke taak weggelegd voor het Openbaar

---

[125] Art. 6 EVRM. Deze voetnoot verwijst letterlijk naar zichzelf
[126] Lindemann & Van Toor, *Ars Aequi* 2018/5, p. 377. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, p. 43.
[127] Oerlemans *Strafblad* 2017, p. 359. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, p. 44.
[128] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 77-80.
[129] Preadvies Adviescommissie Strafrecht 2013. Als ook: *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 79.
[130] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.
[131] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 32-34.
[132] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 35.
[133] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 82-83.

Ministerie. De vraag is daarom wat men mag verwachten van een intern orgaan als de CTC, nu die commissie bestaat uit leden van de politie en het OM. Het is zeer de vraag of een kritische opstelling met betrekking tot de vereiste proportionaliteit en subsidiariteit bij een dergelijke interne voorafgaande toetsing wel is gewaarborgd. Het lijkt wat op de slager die zijn eigen vlees keurt. Dezelfde vraag kan gesteld worden over het toezicht achteraf door de Inspectie, al is hier gelet op de onafhankelijke wettelijke taakstelling wellicht minder kans op tegengestelde belangen dan bij de toetsing door de CTC. Dat de Inspectie vooral toetst aan de formele regels en een rechtmatigheidstoets ontbreekt, kan ertoe leiden dat er maar weinig netelige kwesties op tafel komen. Als het OM op enig moment besluit om niet te vervolgen wordt er over een eventuele onrechtmatige inzet niet meer gesproken. Met Oerlemans meen ik daarom dat toezicht op de rechtmatigheid van de inzet door een onafhankelijke commissie de voorkeur verdient.[134]

In het volgende hoofdstuk zal aan de hand van Nederlandse jurisprudentie sinds de invoering van de wet en de onderzoeksrapporten van de Inspectie worden bezien hoe de toepassing van art. 126nba Sv in de praktijk verloopt. Daarna zal art. 126nba Sv worden getoetst aan art. 8 lid 2 EVRM en het antwoord van de centrale onderzoeksvraag worden gegeven.

[134] Oerlemans *Strafblad* 2017, p. 359.

Hoofdstuk 5 – Art 126nba Sv: De inzet in de praktijk

5.1. Inleiding

In het vorige hoofdstuk is vastgesteld dat de ten tijde van het wetsvoorstel geuite kritiek op art. 126nba Sv ook grotendeels betrekking heeft op de rechtmatigheid van de inzet van de hackbevoegdheid in de praktijk. Daarom is voor het beantwoorden van de centrale onderzoeksvraag naast een formele toetsing van art. 126nba Sv aan art. 8 EVRM ook een analyse van de daadwerkelijke inzet van art. 126nba Sv in de praktijk van belang.

Sinds de invoering van de wet Computercriminaliteit III op 1 maart 2019 heeft de Inspectie Justitie en Veiligheid twee verslagen die zien op het toezicht op de inzet van art. 126nba Sv. gepubliceerd.[135]

In dit hoofdstuk zal aan de hand van deze verslagen en de voorhanden zijnde jurisprudentie sinds de invoering van art. 126nba Sv daarom in kaart worden gebracht hoe de inzet van de hackbevoegdheid in de rechtspraktijk tot nu toe verloopt en hoe dit zich verhoudt tot het recht op privacy van art. 8 EVRM.

De centrale vraag die in dit hoofdstuk wordt beantwoord is;

'*Hoe verloopt de toepassing van art. 126nba Sv sinds de invoering ervan in de praktijk?',*

Daartoe zal in paragraaf 5.2. eerst de jurisprudentie worden besproken. Vervolgens zal in paragraaf 5.3. een analyse van de Inspectieverslagen worden gemaakt. Omdat ten tijde van schrijven van dit hoofdstuk over het jaar 2021 nog geen Inspectieverslag is gepubliceerd, zullen alleen de verslagen over 2019 en 2020 worden besproken. Een conclusie volgt in paragraaf 5.4.

5.2. Jurisprudentie met betrekking tot art. 126nba Sv

Er is op dit moment nog geen normbepalende jurisprudentie die expliciet ziet op de hackbevoegdheid van art. 126nba Sv. De wijze van inzet van de hackbevoegdheid is tot nu toe voornamelijk onderwerp van strafrechtelijk verweer geweest in de verschillende strafzaken die zijn voortgekomen uit de EncroChat-onderzoeken.[136]

Tegen de versleutelde chatdienst EncroChat en de natuurlijke personen die daarachter schuilgaan is in 2020 door de Nederlandse politie in samenwerking met de Franse politie een grootschalig strafrechtelijk onderzoek ingesteld waarbij toegang is verkregen tot tientallen miljoenen versleutelde berichten.[137] Het Nederlandse onderzoek 26Lemont onderzocht de medeplichtigheid van EncroChat en diens bestuurders aan misdrijven gepleegd door gebruikers van de versleutelde Chatdienst.[138]

Met het oog op een voorzienbare inbreuk op de persoonlijke levenssfeer van *alle* Nederlandse EncroChat-gebruikers heeft het OM in het 26Lemont-onderzoek de rechter-commissaris gevraagd om een algemene machtiging voor de inzet van de hackbevoegdheid op personen die zijn betrokken bij georganiseerde misdaad. Het argument daarbij was dat het redelijk vermoeden bestond dat gebruikers van EncroChat zich in het algemeen schuldig maken aan misdrijven in georganiseerd verband.[139] Daarop is door de rechter-commissaris ten behoeve van het 26Lemont-onderzoek op 27

---

[135] Verslag toezicht wettelijke hackbevoegdheid politie 2019; Verslag toezicht wettelijke hackbevoegdheid politie 2020.
[136] Zie bijvoorbeeld: Rb. Den Haag, 25-08-2021, ECLI:NL:RBDHA:2021:9368. Anders: Rb. Den Haag, 30-06-2021, ECLI:NL:RBDHA:2021:8421.
[137] Oerlemans, *Computerrecht* 2021/145, p. 237.
[138] Oerlemans, *Computerrecht* 2021/195, p. 200-201.
[139] Oerlemans, *Computerrecht* 2021/195, p. 200-201.

maart 2020 een machtiging op grond van art. 126uba Sv afgegeven.[140] Dit is eenzelfde bevoegdheid als die van art. 126nba Sv maar dan met betrekking tot georganiseerde misdaad. De aldus verzamelde gegevens mogen vervolgens niet zomaar door het OM in andere strafrechtelijke onderzoeken worden gedeeld. Hiervoor moet eerst toestemming worden gevraagd aan de rechter-commissaris, waarna de betreffende informatie op grond van art. 126dd Sv gedeeld mag worden met de behandelend officier van justitie.[141]

Opvallend is dat de rechtbank de inbreuk die binnen het 26Lemont-onderzoek wordt gemaakt op de privacy van EncroChat-gebruikers slechts als klein heeft ingeschat. De reden daarvoor is dat er specifiek zoeksleutels gericht op zware misdrijven werden ingezet én omdat EncroChat naar verwachting niet voor privédoeleinden zou worden gebruikt. Om voorgaande reden is de rechtbank van oordeel dat deze werkwijze geen strijd met art. 8 EVRM oplevert.[142] Oerlemans stelt zich met betrekking tot vorenstaande terecht kritisch op en meent dat wanneer het gaat om 25 miljoen berichten van 55.000 personen, hier ook makkelijk het tegenovergestelde kan worden betoogd.[143]

Uit het onderzoek onder de ongeveer 55.000 EncroChat gebruikers en 25 miljoen verstuurde berichten zijn inmiddels al diverse Nederlandse strafzaken voortgekomen en het zal niet verbazen dat in vrijwel alle gevallen de rechtmatigheid van het bewijs door de verdediging wordt betwist.[144]

De overweging die de rechtbanken in de individuele strafzaken maken komt er in het algemeen op neer dat het bewijs dat voortkomt uit het 26Lemont-onderzoek rechtmatig is, gezien het feit dat voor het onderzoek door de rechter-commissaris een 126uba-machtiging is afgegeven, waar vervolgens uit wordt afgeleid dat er een subsidiariteits- en proportionaliteitstoets heeft plaatsgevonden.[145] Daarnaast stellen de rechtbanken dat indien wel sprake zou zijn van een vormverzuim in het 26Lemont-onderzoek, het daarmee verkregen bewijs met oog op het Schutznorm-beginsel,[146] in onderhavige zaken gewoon gebruikt kan worden.[147] De verweren die zien op de oncontroleerbaarheid van het bewijs worden in zijn algemeenheid afgewezen op grond van het interstatelijke vertrouwensbeginsel.[148]

---

[140] Rb. Limburg, 26 januari 2022, ECLI:NL:RBLIM:2022:571, r.o. 3.3.2.3.

[141] Oerlemans, *Computerrecht* 2021/195, p. 200-201.

[142] Oerlemans, *Computerrecht* 2021/195, p. 200-201.

[143] Oerlemans, *Computerrecht* 2021/195, p. 200-201.

[144] Zie bijvoorbeeld: Rb. Limburg, 26 januari 2022, ECLI:NL:RBLIM:2022:571. Als ook: Rb. Den Haag, 20 januari 2021, ECLI:NL:RBDHA:2021:284. Als ook: Rb. Oost-Brabant 25 maart 2021, ECLI:NL:RBOBR:2021:1272.Als ook: Rb. Noord-Nederland 29 april 2021, ECLI:NL:RBNNE:2021:1704. Als ook: Rb. Noord-Nederland 29 april 2021, ECLI:NL:RBNNE:2021:1652.

[145] Oerlemans, *Computerrecht* 2021/238.

[146] Ook wel relativiteitstheorie genoemd. Zie o.a. het afvoerpijparrest (HR 30-03-2004, ECLI:NL:PHR:2004:AM2533, m.nt. Y. Buruma.) waarin de rechtbank in r.o. 3.5 naar de Schutznorm verwijst: *"Opmerking verdient dat indien het niet de verdachte is die door de niet-naleving van het voorschrift is getroffen in het belang dat de overtreden norm beoogt te beschermen, in de te berechten zaak als regel geen rechtsgevolg zal behoeven te worden verbonden aan het verzuim."*

[147] Rb. Den Haag, 20 januari 2021, ECLI:NL:RBDHA:2021:284.

[148] Zie bijvoorbeeld: Rb. Zeeland-West-Brabant 31 maart 2021, ECLI:NL:RBZWB:2021:1556, waarin de rechtbank de werking van het interstatelijk vertrouwensbeginsel in par. 3.3.3. op de volgende wijze uitlegt: *''Ten aanzien van onderzoekshandelingen waarvan de uitvoering plaatsvindt onder verantwoordelijkheid van de buitenlandse autoriteiten van een andere EVRM lidstaat, is de taak van de Nederlandse strafrechter ertoe beperkt te waarborgen dat de wijze waarop van de resultaten van dit onderzoek in de strafzaak tegen de verdachte gebruik wordt gemaakt, geen inbreuk maakt op zijn recht op een eerlijk proces, zoals bedoeld in artikel 6, eerste lid, EVRM. Het behoort niet tot de taak van de Nederlandse strafrechter om te toetsen of de*

In het vorige hoofdstuk is al verwezen naar het verband tussen een mogelijke schending van art. 8 EVRM door de inzet van art. 126nba Sv en het recht op een eerlijk proces van art. 6 EVRM. In de eerdergenoemde uit het EncroChat-onderzoek 26Lemont voortgekomen strafzaken is de relevantie van art. 6 EVRM heel duidelijk waarneembaar. Immers, als de rechtbank de kans op schending van art. 8 EVRM bij het onderscheppen van communicatie van meer dan 55.000 vooraf *onbekende* personen als klein aanmerkt *en* het Schutznorm-vereiste in de weg staat aan een rechtmatigheidstoets in individuele strafzaken, kan mijns inziens niet worden ontkomen aan de conclusie dat het recht op privacy van de individuele verdachte kennelijk zonder probleem geschonden kan worden zonder dat dat van invloed is op de behandeling van zijn of haar strafzaak, waardoor zijn of haar recht op een eerlijk proces ernstig in het gedrang kan komen.

5.3. De inspectieverslagen

Zoals in hoofdstuk 4 besproken is het belangrijk hier nogmaals te benadrukken dat het toezicht van de Inspectie geen inhoudelijke toetsing maar een procesmatige betreft. Het toezicht van de Inspectie ziet voornamelijk op de uitvoering van de hackbevoegdheid door het daarvoor verantwoordelijke technisch team.[149]

Uit de Inspectieverslagen blijkt dat de hackbevoegdheid in 2019 acht keer is ingezet en in 2020 veertien keer.[150] Uit de conclusie van het verslag van 2019 blijkt dat de toepassing van de hackbevoegdheid in grote lijnen aan de wettelijke eisen heeft voldaan, maar dat de automatische logging van bestanden in alle acht gevallen niet compleet was. Die onvolledigheid van de logging heeft volgens de inspectie de controle lastig gemaakt. Tegelijkertijd oordeelt de inspectie dat er geen sprake was van onregelmatigheden die de betrouwbaarheid en integriteit van het onderzoek hebben aangetast.[151]

Ook waren verbeteringen noodzakelijk ten behoeve van de betrouwbaarheid en integriteit van het bewijs bij de inzet van technische hulpmiddelen zoals de testfase en de aantoonbaarheid van de beheersing van veiligheidsrisico's.[152] Zo was in geen van de zes gevallen waarbij gebruik is gemaakt van een technisch hulpmiddel, de vereiste goedkeuring voor- of achteraf van het hulpmiddel aanwezig en heeft de politie de uit te voeren handelingen niet in alle gevallen voorafgaand getest. En ondanks dat de politie in 2019 een groot aantal beveiligingsmaatregelen heeft getroffen ontbrak zowel een intern kwaliteitssysteem als een integrale risicoanalyse.[153]

Genoeg ruimte voor verbetering dus, maar omdat 2019 het eerste jaar van inwerkingtreding van de wet was, ging de Inspectie ervan uit dat de oorzaak lag in de opbouwfase.[154]

Ook in 2020 was de logging echter in geen van de gevallen geheel op orde. Vooral de registratie van beeldschermopnames en het vastleggen van toetsaanslagen was niet volledig geschied. Ook was niet goed te controleren of alle ingezette technische hulpmiddelen na afloop van de inzet volledig waren verwijderd. Met betrekking tot de verplichte verslaglegging in een proces-verbaal van de handelingen van de politie geldt dat deze in sommige gevallen ontbrak. Ook in gevallen waar wel een proces-

---

wijze waarop dit onderzoek is uitgevoerd, strookt met de dienaangaande in het desbetreffende buitenland geldende rechtsregels.''.

[149] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 12.

[150] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 7.

[151] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 7-8.

[152] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 7-8.

[153] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 9-11.

[154] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 7. Als ook: 'Uitblijven verbeteringen in hackproces van politie is risico', *Inspectie Justitie en Veiligheid*, 29 juni 2021.

verbaal was opgesteld, ontbraken in de verslaglegging de namen van degenen die bij de uitvoering van de onderzoekshandelingen betrokken waren en ontbraken veelal ook tijdstippen van uitvoering van de handelingen.[155]

In 2020 werd in tien van de veertien gevallen gebruikgemaakt van commerciële software (in 2019 was dit in zeven van de acht keer het geval). De Inspectie geeft daarbij aan dat de leverancier in al die gevallen volledig en oncontroleerbaar toegang heeft tot dezelfde informatie als de politie en dat dit afbreuk doet aan de betrouwbaarheid van het bewijs en dit risico's op schending van de privacy van de verdachte met zich meebrengt.[156] Opvallend daarentegen is dat zowel in 2019 als 2020 geen nevenschade of veiligheidsrisico voortkomende uit het in stand houden van kwetsbaarheden werd ontdekt.[157]

Een nieuwsbericht van juni 2021 op de eigen website van de Inspectie wordt naar aanleiding van de uitkomst van het Inspectieverslag over 2020 gekopt in klinkende taal; *'Uitblijven verbeteringen in hackproces van politie is risico'*.[158] In dit artikel staat dat de Inspectie had verwacht dat alle tekortkomingen die over het jaar 2019 waren vastgesteld, in 2020 zouden zijn verholpen. Nu dit niet het geval is heeft de Inspectie aan de politie de opdracht gegeven om alle vastgestelde tekortkomingen te verhelpen en verbetering te tonen.[159]

Noemenswaardig is ook dat de Inspectie in het verslag van 2020 opmerkt dat op basis van de aantallen in elk geval geen sprake is van een 'ongecontroleerde inzet op grote schaal'.[160] Nu uit de Inspectieverslagen lijkt te volgen dat de hackbevoegdheid in 2019 en 2020 slechts is ingezet in 8 respectievelijk 14 gevallen, lijkt dat op het eerste gezicht geen onlogische conclusie. Of dit in werkelijkheid ook zo is kan niet worden nagegaan en is maar de vraag.

Opvallend is dat in het Inspectieverslag over 2020 bij de bespreking van de afbakening expliciet wordt vermeld dat het EncroChat-onderzoek buiten de reikwijdte van het toezicht van de Inspectie valt.[161] De reden daarvoor is dat het OM en de politie hebben gesteld dat in het betreffende onderzoek geen inzet van de hackbevoegdheid door Nederlandse opsporingsdiensten heeft plaatsgevonden. Bij het 26Lemont-onderzoek is echter wel een bevel op grond van art. 126uba Sv afgegeven. Het zou voor de hand liggen dat de inzet van art. 126uba Sv wel binnen het toezichtbereik van de Inspectie zou vallen. Juist in grotere onderzoeken als die naar georganiseerde misdaad is het goed voorstelbaar dat er fouten kunnen ontstaan of misbruik kan worden gemaakt bij de inzet van de bevoegdheid en lijkt een dergelijke toetsing daarom onmisbaar. Oerlemans leidt uit het voorgaande tevens af dat de Inspectie kennelijk ook geen onderzoek doet naar zaken waarin een machtiging op grond van art. 126ng Sv is afgegeven tot het verschaffen van toegang tot accounts op inbeslaggenomen geautomatiseerde werken van verdachten.[162]

Men zou zich dan ook kunnen afvragen of de conclusie van de Inspectie dat er geen sprake is van een inzet op 'ongecontroleerde schaal' niet heel anders zou kunnen uitvallen als de inzet van alle direct

---

[155] Verslag toezicht wettelijke hackbevoegdheid politie 2020, p. 11-12.
[156] Verslag toezicht wettelijke hackbevoegdheid politie 2020, p. 3.
[157] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 16. Als ook: Verslag toezicht wettelijke hackbevoegdheid politie 202, p. 3.
[158] 'Uitblijven verbeteringen in hackproces van politie is risico', *Inspectie Justitie en Veiligheid*, 29 juni 2021.
[159] Verslag toezicht wettelijke hackbevoegdheid politie 2020, p. 21. Als ook: 'Uitblijven verbeteringen in hackproces van politie is risico', *Inspectie Justitie en Veiligheid*, 29 juni 2021.
[160] Verslag toezicht wettelijke hackbevoegdheid politie 2020, p. 3.
[161] Verslag toezicht wettelijke hackbevoegdheid politie 2020, p. 5.
[162] Oerlemans, *Computerrecht* 2021/194.

aan art. 126nba Sv gerelateerde opsporingsbevoegdheden binnen de reikwijdte van de controle van de Inspectie zouden vallen.

5.4. Conclusie

In dit hoofdstuk is op basis van de voor handen zijnde jurisprudentie en de Inspectieverslagen over 2019 en 2020 onderzocht op welke wijze art. 126nba Sv in de praktijk wordt ingezet.

De jurisprudentie met betrekking tot art. 126nba Sv is schaars. Daarom is het lastig of in elk geval te vroeg om een duidelijke lijn in de rechtspraak te ontdekken. Wel kan uit het besproken EncroChat-onderzoek 26Lemont worden afgeleid dat het afgeven van een bevel op grond van art. 126uba Sv ten behoeve van het onderscheppen van de communicatie van meer dan 55.000 vooraf niet bekende personen - en daarmee tientallen miljoenen versleutelde berichten - door rechters klaarblijkelijk niet in strijd met art. 8 EVRM wordt geacht.[163] Het is daarbij opvallend dat de rechtmatigheid van de inzet van de hackbevoegdheid op deze wijze wel heel gemakkelijk lijkt te worden aangenomen en in geval van een schending van art. 8 EVRM, al snel rechtmatig wordt geacht.[164] Behalve het enorm grote aantal personen dat binnen het 26Lemont-onderzoek valt en die zeer wel onrechtmatig in hun privacy kunnen zijn geraakt, wordt diezelfde groep op grond van het Schutznorm-beginsel alsnog geacht niet onrechtmatig te zijn geraakt in hun recht op een eerlijk proces.[165]

Anderzijds is het opmerkelijk dat het toezicht van de Inspectie niet ziet op de inzet van art. 126uba Sv en een onderzoek als 26Lemont daarmee ook buiten de reikwijdte van de Inspectiecontrole valt. De verdachten in de individuele strafzaken die zijn voortgekomen uit het 26Lemont-onderzoek lijken daarmee zowel een rechtmatigheidstoets als een procedurele waarborg mis te lopen.

Concluderend kan gesteld worden dat het toezicht van de Inspectie zeer strak is afgebakend en uitsluitend ziet op de inzet van art. 126nba Sv en toetsing op de gevoerde procedures. Die toetsing achteraf lijkt geenszins een volledig en duidelijk beeld te schetsen van de inzet van de hackbevoegdheid in de praktijk. In dat licht bezien én gezien het gemak waarmee binnen het 26Lemont-onderzoek de rechtmatigheid van het bewijs wordt aangenomen valt mijns inziens moeilijk te verdedigen dat de toetsing van de Inspectie een sterke waarborg biedt tegen onrechtmatige schendingen van de privacy van art. 8 EVRM en daarmee ook op het recht op een eerlijk proces van art. 6 EVRM.

In het volgende hoofdstuk zal art. 126nba Sv eerst worden getoetst aan art. 8 lid 2 EVRM, waarna tot slot een eindconclusie en het antwoord op de centrale onderzoeksvraag volgt.

[163] Oerlemans, *Computerrecht* 2021/195, p. 200-201.
[164] Rb. Zeeland-West-Brabant 31 maart 2021, ECLI:NL:RBZWB:2021:1556. Als ook: Rb. Overijssel 29 maart 2021, ECLI:NL:RBOVE:2021:1307. Als ook: Oerlemans, *Computerrecht* 2021/195, p. 200-201.
[165] Rb. Den Haag, 20 januari 2021, ECLI:NL:RBDHA:2021:284.

Hoofdstuk 6 – Toetsing

6.1. Inleiding

Dit hoofdstuk omvat de toetsing van de hackbevoegdheid van art. 126nba Sv aan art. 8 EVRM. In hoofdstuk 3 van deze scriptie is toegelicht aan welke drie cumulatieve voorwaarden een gerechtvaardigde inbreuk op art. 8 EVRM in het licht van heimelijke opsporingsmethoden moet voldoen. De toetsing in paragraaf 6.2. zal daarom binnen dat kader worden gedaan en ziet zowel op een formele toetsing als op de inzet van de in art. 126nba Sv opgenomen hackbevoegdheid in de praktijk. In paragraaf 6.3. volgt een conclusie.

6.2. Toetsing van art. 126nba Sv aan art. 8 EVRM

Het doel van art. 126nba Sv is het voorkomen en opsporen van wanordelijkheden en strafbare feiten. Dit komt overeen met de legitieme doelen zoals genoemd in art. 8 lid 2 EVRM. Daaruit volgt dat aan het eerste criterium, het legitieme doel, is voldaan.

Het tweede criterium is het voorzienbaarheidsvereiste. Dat wil zeggen dat de heimelijke opsporingsbevoegdheden moeten zijn gegrond op een nationale wettelijke bepaling die duidelijk en toegankelijk is voor justitiabelen én voldoende voorzienbaar is, in die zin dat een verdachte de gevolgen van een dergelijke bepaling moet kunnen begrijpen.[166] Dit houdt in dat een verdachte op grond van de wettelijke opsporingsbevoegdheid een inschatting moet kunnen maken van de mogelijke inzet van deze bevoegdheid tegen hem.[167] Het EHRM stelt daarbij als eis dat duidelijk moet zijn omschreven onder welke omstandigheden die bevoegdheid kan worden ingezet.[168]

Daartoe heeft het EHRM de volgende zes sub-criteria geformuleerd:

1. De aard van het misdrijf waarop de bevoegdheid mag worden ingezet moet duidelijk zijn omschreven;
2. Er moet duidelijk blijken op welke categorie van personen de bevoegdheid betrekking heeft;
3. Er moet een maximale tijdsduur aan de inzet van de bevoegdheid worden gesteld;
4. De procedure voor het verwerken en opslaan van gegevens die verkregen zijn bij de inzet van de heimelijke bevoegdheid moet kenbaar zijn;
5. Er moeten regels zijn die gelden bij het delen van de onderschepte gegevens met andere instanties;
6. Er moeten regels zijn die bepalen wanneer en in welke gevallen de onderschepte gegevens worden vernietigd.[169]

Toetsing aan deze criteria levert het volgende op. Met betrekking tot de eerste twee eisen regelt art. 126nba lid 1 Sv de categorie misdrijven en personen waartegen de hackbevoegdheid kan worden ingezet. Zo mag de hackbevoegdheid slechts worden ingezet wanneer op grond van feiten en omstandigheden kan worden aangenomen dat het geautomatiseerd werk ook daadwerkelijk door verdachte zelf in gebruik is. Daarbij moet sprake zijn van verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten op grond van art. 67 lid 1 Sv, moet het strafbare feit een ernstige

---

[166] EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par.50.
[167] EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par. 93.
[168] De Vries 2013, p. 203-204. Als ook o.a.: EHRM 18 mei 2010, nr. 26839/05 *(Kennedy/Verenigd Koninkrijk),* par. 152.
[169] EHRM 24 april 1990, nr. 11801/85 (*Kruslin-Huvig/Frankrijk).* Als ook: EHRM 29 juni 2006, nr. 54934/00 (*Weber en Savaria/Duitsland*), par. 95. Als ook: EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk)*, par. 124.

inbreuk op de rechtsorde opleveren én moet het strafrechtelijk onderzoek dit dringend vorderen.[170] Voor wat betreft het onderzoeksbelang is voorafgaande rechterlijke toetsing vereist. De officier van justitie mag de bevoegdheid pas inzetten na een daartoe strekkende machtiging van de rechter-commissaris. Op basis van een proportionaliteits- en subsidiariteitstoets bepaalt de rechter-commissaris of er sprake is van een dringend onderzoeksbelang.[171]

De derde eis - de tijdelijkheid van de inzet - is neergelegd in art. 126nba lid 3 Sv, dat zegt dat het bevel voor de inzet van art. 126nba Sv voor maximaal vier weken wordt gegeven. Wel biedt art. 126nba lid 5 Sv de mogelijkheid tot verlenging. In dat geval moet de officier van justitie een nieuwe machtiging vragen die opnieuw door de rechter-commissaris moet worden getoetst.

Aan de vierde door het EHRM gestelde eis - een kenbare procedure - wordt bij de inzet van art. 126nba Sv voldaan door het verplichten van geautomatiseerde vastlegging van gegevensstromen.[172] Bovendien moeten door het technische team verrichte handelingen worden opgenomen in een proces-verbaal. Dit is vastgelegd in art. 126nba lid 8 sub b Sv.

De basis voor eis vijf – regels voor het delen van de onderschepte gegevens met andere instanties – is opgenomen in art. 126nba lid 8 sub a Sv en uitgewerkt in art. 6 van het Besluit technische hulpmiddelen Strafvordering.

Eis zes -met betrekking tot regels inzake vernietiging van onderschepte gegevens- vindt zijn grondslag in art. 126cc Sv.

Nu alle zes door het EHRM voorgeschreven sub-criteria zijn ingebed in de tekst en uitleg van art. 126nba Sv, lijkt formeel te zijn voldaan aan het voorzienbaarheidsvereiste.

Het derde en laatste criterium ‘noodzakelijk in een democratische samenleving’ behelst dat er sprake moet zijn van een ‘pressing social need’ voor de beperking van het recht op privacy.[173] Er moet dus een dringende maatschappelijke noodzaak bestaan die rechtvaardigt dat er een inbreuk wordt gemaakt op het recht op privacy. Daarbij moeten zowel het proportionaliteitsbeginsel als het subsidiariteitsbeginsel in acht worden genomen en moet de grond van de inbreuk ‘relevant and sufficient’ zijn. Hierbij komt aan de lidstaten een zekere ‘margin of appreciation’ toe, maar het uiteindelijke oordeel is aan het EHRM.[174]

Zoals uiteengezet in hoofdstuk 3 kan uit de eis van het EHRM dat de aard, reikwijdte, duur en de rechtsgrond van de ingezette bevoegdheid moeten worden afgezet tegen de verdenking en de omstandigheden van het specifieke geval, worden afgeleid dat elke afzonderlijke inbreuk op de privacy die voortkomt uit de inzet van een heimelijke opsporingsbevoegdheid, afzonderlijk moet worden getoetst aan de uitzonderingsbepaling van art. 8 lid 2 EVRM.[175] Afgaand op de gang van zaken in het EncroChat-onderzoek 26Lemont wordt in de praktijk niet aan dit vereiste voldaan. Uit voornoemd onderzoek blijkt immers dat een enkel beroep op grond van art. 126uba Sv voldoende was voor het onderscheppen van tientallen miljoenen versleutelde berichten van meer dan 55.000 personen.[176] Dat staat haaks op zowel de overweging van het EHRM dat de inzet van dit soort

[170] Art. 126nba lid 1 Sv.
[171] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 30.
[172] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 35.
[173] EHRM 7 december 1976, nr. 5493/72 (*Handyside/Verenigd Koninkrijk),* par. 48-49.
[174] EHRM 4 december 2008, nr. 30562/04 (*S. & Marper/Verenigd Koninkrijk),* par. 101-102.
[175] EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk),* par. 153.
[176] Rb. Limburg, 26 januari 2022, ECLI:NL:RBLIM:2022:571, r.o. 3.3.2.3.

heimelijke opsporingsbevoegdheden per definitie een inbreuk op artikel 8 lid 1 EVRM oplevert,[177] en dat elke afzonderlijke inbreuk op de privacy die voortkomt uit de inzet van heimelijke opsporingsbevoegdheden afzonderlijk moet worden getoetst aan de uitzonderingsbepaling van art. 8 lid 2 EVRM.[178]

Voor wat betreft de 'pressing social need' heeft het EHRM het toezicht op heimelijke opsporingsbevoegdheden verdeeld in drie fases waarin afzonderlijk toezicht is vereist. In elke fase moet de 'pressing social need' opnieuw worden beoordeeld.[179] Ook bij de invoering van art. 126nba Sv is een dergelijk drie fasen-toezicht ingesteld.

In de eerste fase vindt het vooronderzoek plaats. Op grond daarvan maakt de officier van justitie de afweging om al dan niet een bevel tot onderzoek in een geautomatiseerd werk af te geven.[180] Daarbij wordt het belang van inzet van die bevoegdheid afgewogen tegen de persoonlijke levenssfeer van de verdachte en eventuele derden.[181] In deze fase toetst het interne adviesorgaan CTC het voornemen en de wijze van inzet aan wet- en regelgeving en jurisprudentie en beoordeelt het naast de effectiviteit ook de proportionaliteit en subsidiariteit. Van onafhankelijke toetsing is hier feitelijk geen sprake nu de CTC bestaat uit leden van het OM en de politie. Na akkoord van de CTC vraagt de officier van justitie de rechter-commissaris om een schriftelijke machtiging. In tegenstelling tot de CTC is de rechter-commissaris volledig onafhankelijk.

De tweede fase bestaat uit 'het onderzoek in het geautomatiseerd werk' zelf. Het toezicht in deze fase bestaat uit de geautomatiseerde vastlegging van de gegevensstromen, mede ter voorkoming van misbruik van de bevoegdheid.[182] Of in deze fase de 'pressing social need' opnieuw wordt beoordeeld kan, -behoudens in het geval dat de termijn van de machtiging verloopt en de rechter-commissaris opnieuw moet oordelen over de inzet van art. 126nba Sv-, mijns inziens niet gesteld worden.

De derde fase omvat 'de afsluiting van het onderzoek in een geautomatiseerd werk'. In deze fase worden geplaatste technische hulpmiddelen verwijderd door een speciaal daarvoor aangesteld technisch team, dat niet betrokken is geweest bij het onderzoek zelf.
De controle in de derde fase ligt bij de Inspectie. Die houdt achteraf toezicht op de kwaliteit van de politiële taakuitvoering en controleert of de inzet van art. 126nba Sv volgens de wettelijke procedures is toegepast. Hiervan wordt jaarlijks verslag uitgebracht.[183] Zowel uit de verslagen van 2019 als 2020 blijkt dat de logging van de gegevensstromen en de verslaglegging van de onderzoeks-handelingen in processen-verbaal onvoldoende op orde waren.[184] Ondanks dat de Inspectie zich uitspreekt over risico's met betrekking tot de privacy van verdachten veroorzaakt door procedurefouten, ontbreekt het in de controles aan een rechtmatigheidstoets achteraf.[185] Daarbij kunnen er - net als bij de CTC - vraagtekens worden geplaatst bij de onafhankelijkheid van de

[177] Loof e.a. 2015, p. 8. Als ook: EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48. Als ook: EHRM 2 augustus 1984, nr. 8691/79 *(Malone/Verenigd Koninkrijk),* par. 64. Als ook: EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par. 65-70. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, par. 77.
[178] EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk),* par. 153.
[179] EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland),* par. 233.
[180] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 33.
[181] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 32-34.
[182] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 35.
[183] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 82-83.
[184] Verslag toezicht wettelijke hackbevoegdheid politie 2019, p. 7-8. Als ook: Verslag toezicht wettelijke hackbevoegdheid politie 2020, p. 11-12.
[185] *Kamerstukken I* 2016/17, 34 372, E, p. 9. Als ook: Oerlemans *Strafblad* 2017, p. 359.

Inspectie nu deze deel uitmaakt van het ministerie van Justitie en Veiligheid. Wel heeft de Inspectie een onafhankelijke wettelijke taakstelling heeft met eigen doelstellingen.[186]

6.3. Conclusie

Uit het voorgaande blijkt dat art. 126nba Sv tekstueel en formeel gezien in hoge mate beantwoordt aan de door het EHRM gestelde eisen en waarborgen voor een rechtmatige inbreuk op art. 8 EVRM. Uit de analyse van de (beperkte) jurisprudentie en de Inspectieverslagen 2019/2020 met betrekking tot de inzet van art. 126nba Sv blijkt echter dat het er bij de inzet van de hackbevoegdheid in de praktijk nog wel eens aan schort als het gaat om de logging van gegevensstromen en de verslaglegging van de handelingen in processen-verbaal. Daarnaast lijkt het in de tweede fase van de inzet van de hackbevoegdheid te ontbreken aan de noodzakelijkheidstoets en met name de toets aan de 'pressing social need'.

[186] *Kamerstukken II* 2016/17, 34372, nr. 6, p. 82.

Hoofdstuk 7 - Eindconclusie

7.1. Bevindingen

De centrale onderzoeksvraag die hierna zal worden beantwoord luidt:
'Is de hackbevoegdheid van art. 126nba van het Wetboek van Strafvordering verenigbaar met art. 8 lid 2 EVRM, zoals uitgelegd in de rechtspraak van het EHRM?'.

De kritieken op het wetsvoorstel zagen onder meer op het ontbreken van de noodzaak van de hackbevoegdheid.[187] De noodzaak daarvan is mijns inziens uitgebreid en veelvuldig door de regering toegelicht. De hackbevoegdheid dient ter bescherming van de maatschappij tegen steeds groeiende en verdergaande grensoverschrijdende (digitale) criminaliteit.[188] Dat neemt niet weg dat bij de inzet van de hackbevoegdheid van art. 126nba Sv het recht op privacy zoals neergelegd in art. 8 EVRM, onder grote druk kan komen te staan.

Andere kritieken op het wetsvoorstel betroffen de reikwijdte van de bevoegdheid, het risico van het gebruik van onbekende systeemkwetsbaarheden alsmede de toepassing in bagatelzaken en het schenden van de privacy van onschuldige burgers.[189] De regering heeft deze kritiek beargumenteerd van de hand gewezen en uit de inmiddels verschenen verslagen van de Inspectie blijkt niet dat dergelijke risico's aan de orde zijn geweest.[190]

Uit de toetsing aan de criteria voor een gerechtvaardigde inbreuk op art. 8 EVRM, zoals uiteengezet in hoofdstuk 3 van deze scriptie, blijkt dat art. 126nba Sv in hoge mate voldoet aan de door het EHRM gestelde formele eisen voor een rechtmatige inbreuk op art. 8 EVRM. De zes criteria die daarvoor door het EHRM zijn opgesteld zijn allen terug te vinden in art. 126nba Sv. Ook de door het EHRM vereiste drie fasen van toezicht gelden bij de inzet van art. 126nba Sv. Daarbij is het wel de vraag of in de tweede fase, die voornamelijk ziet op de automatische verslaglegging van de onderschepte gegevens, een nieuwe beoordeling van de 'pressing social need' wel mogelijk en haalbaar is. [191]

Uit analyse van jurisprudentie en de verslagen van de Inspectie in 2019 en 2020 over de inzet van art. 126nba Sv komt naar voren dat daar in de praktijk nog het nodige aan schort. Zo waren de logging van gegevensstromen en de verslaglegging van de handelingen in processen-verbaal niet voldoende op orde.

Met een machtiging op grond van art. 126uba Sv werd het rechtmatig geacht om in het EncroChat-onderzoek 26Lemont tientallen miljoenen versleutelde berichten van meer dan 55.000 personen te onderscheppen, zonder dat per individueel geval een toetsing van de hackbevoegdheid heeft plaatsgevonden.[192] Het uit 26Lemont verkregen bewijs werd in de individuele strafzaken op grond van het Schutznorm-beginsel vervolgens geacht rechtmatig te zijn.[193] Dit terwijl uit de jurisprudentie van het EHRM die ziet op heimelijke opsporingsbevoegdheden volgt dat de inzet van een dergelijke bevoegdheid per definitie een inbreuk op artikel 8 EVRM oplevert en dat élke afzonderlijke inbreuk

[187] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 77-80.
[188] *Kamerstukken II* 2015/16, 34372, 3, p. 7-12; *Kamerstukken II* 2016/17, 34372, 6, p. 14-22.
[189] Preadvies Adviescommissie Strafrecht 2013. Als ook: *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 77-80.
[190] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 34, p. 79. Als ook: *Kamerstukken II* 2016/17, 34372, nr. 6, p. 32. Als ook: Verslag toezicht wettelijke hackbevoegdheid politie 2019. Als ook: Verslag toezicht wettelijke hackbevoegdheid politie 2020.
[191] *Kamerstukken II* 2015/16, 34372, 3 (MvT), p. 35.
[192] Rb. Limburg, 26 januari 2022, ECLI:NL:RBLIM:2022:571, r.o. 3.3.2.3.
[193] Rb. Zeeland-West-Brabant 31 maart 2021, ECLI:NL:RBZWB:2021:1556. Als ook: Rb. Overijssel 29 maart 2021, ECLI:NL:RBOVE:2021:1307. Als ook: Oerlemans, *Computerrecht* 2021/195, p. 200-201.

op de privacy die voortkomt uit de inzet van een dergelijke heimelijke opsporingsbevoegdheid afzonderlijk moet worden getoetst aan de uitzonderingsbepaling van art. 8 lid 2 EVRM.[194]
Nu dat niet is geschied lijken de verdachten in de individuele strafzaken die zijn voortgekomen uit het 26Lemont-onderzoek daarmee zowel een rechtmatigheidstoets als een procedurele waarborg mis te lopen.

In het verlengde hiervan is ook het verband met art. 6 EVRM is van groot belang. Immers nu de inzet van een vergaande bevoegdheid als die van art. 126nba Sv raakt aan het belang en privacy van 55.000 personen en daarmee op hun recht op een eerlijk proces zoals neergelegd in art. 6 EVRM.

Daarmee valt het moeilijk te verdedigen dat de toetsing van de Inspectie een sterke waarborg biedt tegen onrechtmatige schendingen van de privacy van art. 8 EVRM en het recht op een eerlijk proces van art. 6 EVRM. Daarbij is opmerkelijk dat het toezicht van de Inspectie niet ziet op de inzet van art. 126uba Sv en dat een grootschalig onderzoek als 26Lemont daarmee buiten de reikwijdte van de Inspectiecontrole valt.

Hoewel art. 126nba Sv in formele zin grotendeels lijkt te voldoen aan de voorzienbaarheidseisen die het EHRM stelt aan de inzet tot heimelijke opsporingsbevoegdheden, lijkt het in de tweede fase van de inzet van de hackbevoegdheid te ontbreken aan de noodzakelijkheidstoets en met name de toets aan de ‘pressing social need’. Dit overwegende en gelet op het gemak waarmee binnen het 26Lemont-onderzoek en de daaruit voortvloeiende individuele strafzaken de rechtmatigheid van het bewijs werd aangenomen én omdat bij de toetsing achteraf in de meeste gevallen een rechtmatigheidstoets ontbreekt, moet mijns inziens geconcludeerd worden dat de hackbevoegdheid van art. 126nba van het Wetboek van Strafvordering niet zonder meer verenigbaar is met art. 8 lid 2 EVRM.

[194] Loof e.a. 2015, p. 8. Als ook: EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland),* par. 41-48. Als ook: EHRM 2 augustus 1984, nr. 8691/79 *(Malone/Verenigd Koninkrijk),* par. 64, 153. Als ook: EHRM 16 februari 2000, nr. 27798/95 *(Amann/Zwitserland),* par. 65-70. Als ook: EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman, par. 77.

Bronnenlijst

Geraadpleegde literatuur

Aink, *TPWS* 2016/46
J.R.J. Aink, 'Het wetsvoorstel Computercriminaliteit III: Een High Tech inhaalslag?', *TPWS* 2016/46.

De Vries 2013
K. de Vries, 'Het recht op privéleven en aanverwante rechten', in: J. Gerards e.a. (red.), *Grondrechten, de nationale, Europese en internationale dimensie,* Nijmegen: Ars Aequi Libri, p. 129-149.

Jacobs, *NJB* 2012/2240
B. Jacobs, 'Policeware' *NJB* 2012/2240, afl. 39, p. 2761-2764.

Lindemann & Van Toor, *Ars Aequi* 2018/5
M. Lindemann & D. van Toor, 'Protection of a suspect's privacy in criminal procedures', *Ars Aequi* 2018/5, p.376-384.

Loof e.a. 2015
J.P. Loof e.a., *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten,* Universiteit Leiden.

Oerlemans, *DD* 2011/41
J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid' *Delikt en Delinkwent* 2011/41, afl.8/62, p. 888-908.

Oerlemans, *Strafblad* 2017
J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op het internet', *Strafblad* 2017, afl. 4, p. 350-359.

Oerlemans, 2017
J.J. Oerlemans, *'Investigating Cybercrime'*, (diss. Leiden), Waddinxveen (Nederland): AlphaZet Prepress 2017.

Oerlemans, *Computerrecht* 2019/117
J.J. Oerlemans, 'Aanwijzing voor grensoverschrijdende inzet hackbevoegdheid, *Computerrecht* 2019/117, afl. 3, p. 221.

Oerlemans, *Computerrecht* 2021/145
J.J. Oerlemans, 'Veroordeling op basis van EncroChat-gegevens', *Computerrecht* 2021/145, afl. 5, p. 237-242.

Oerlemans, *Computerrecht* 2021/194
J.J. Oerlemans, 'Rapport inspectie J&V over de hackbevoegdheid', *Computerrecht* 2021/194, afl. 4, p. 389-390.

Oerlemans, *Computerrecht* 2021/195
J.J. Oerlemans, 'Meer duidelijkheid over EncroChat-operatie', *Computerrecht* 2021/195, afl. 4, p. 192-201.

Oerlemans, *Computerrecht* 2021/238
J.J. Oerlemans, 'Beslissing inzake inzet bevoegdheden Encrochat', *Computerrecht* 2021/238, afl. 5, p. 483-484.

Prins, *TPWS 2017/15*
M.A. Prins, 'Een koelkast als getuige', *TPWS* 2017/15, afl. 22, p. 112-117.

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

Van der Sloot, *TBS&H* 2017
B. van der Sloot, 'De bevoegdheid van de politie om computers binnen te treden: tijd voor een grondrecht op de bescherming van informatie-technische systemen?', *TBS&H* 2017, afl. 4, p. 195-206.

Aangehaalde literatuur

Jacobs, *NJB* 2012/2240
B. Jacobs, 'Policeware' *NJB* 2012/2240, afl. 39, p. 2761-2764.

Oerlemans, *Strafblad* 2017
J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op het internet', *Strafblad* 2017, afl. 4, p. 350-359.

Regelgeving en parlementaire stukken

***Stb.* 1993, 33**
Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van de informatietechniek *Stb.* 1993, 33).

***Stb.* 2018, 340**
Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan nite met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126 uba, eerste lid, en 126 zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), *(Stb.* 2018, 340).

***Stb.* 2019, 167**
Wet van 27 juni 2018 tot 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) (*Stb. 167*).

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

Kamerstukken II 2015/16, 34 372, nr. 2.

Kamerstukken II 2015/16, 34372, nr. 3 (MvT).

Kamerstukken II 2015/16, 34372, nr. 4.

Kamerstukken II 2015/16, 34372, nr. 5.

Bijlage 651723 bij *Kamerstukken II* 2015/2016, 34372, 3.

Bijlage 651730 bij *Kamerstukken II* 2015/2016, 34372, 3.

Kamerstukken II 2016/17, 34372, nr. 6.

Kamerstukken II 2016/17, 34 372, nr. 10.

Kamerstukken II 2016/17, 34 372, nr. 11.

Kamerstukken II 2016/17, 34 372, nr. 13.

Kamerstukken II 2016/17, 34 372, nr. 22.

Kamerstukken II 2016/17, 34372, nr. 23.

Kamerstukken II 2017/18, 34 372, nr. 27.

Kamerstukken II 2018/19, 34 372, nr. 29.

Kamerstukken I 2016/17, 34 372, A.

Kamerstukken I 2016/17, 34 372, E, (Verslag I).

Kamerstukken I 2018/19, 34 372, L.

Kamerstukken I 2018/19, 34 372, M.

Geraadpleegde adviezen en onderzoeksrapporten

Preadvies Adviescommissie Strafrecht 2013
Preadvies van de Adviescommissie Strafrecht inzake '*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)',* NOVA 2013.

Verslag toezicht wettelijke hackbevoegdheid politie 2019
http://www.inspectie-jenv.nl/Publicaties/rapporten/2020/08/20/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019.

Verslag toezicht wettelijke hackbevoegdheid politie 2020
http://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020.

Verslag internetconsultatie bij Wet computercriminaliteit III
https://www.internetconsultatie.nl/computercriminaliteit/document/726>.

Aangehaalde nieuwsberichten

'Uitblijven verbeteringen in hackproces van politie is risico', ***Inspectie Justitie en Veiligheid*****, 29 juni 2021.**

'Bijna drie kwart van de Nederlanders maakt gebruik van slimme apparaten', ***CBS.nl,*** **1 december 2021.**

Geraadpleegde wetscommentaren

Blom, in: ***T&C Strafvordering*** **2021**
T. Blom, commentaar op art. 126nba Sv, in: T. Blom, *Tekst en Commentaar Strafvordering,* Deventer: Wolters Kluwer 2021 (online, bijgewerkt 1 juli 2021).

Geraadpleegde jurisprudentie

EHRM 7 december 1976, nr. 5493/72 (*Handyside/Verenigd Koninkrijk).*

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

EHRM 26 april 1979, nr. 6538/74 *(Sunday Times/The United Kingdom)*.

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

EHRM 25 maart 1983, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, en 7136/75 (*Silver and others/Verenigd Koninkrijk).*

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

EHRM 2 augustus 1984, nr. 8691/79 *(Malone/Verenigd Koninkrijk).*

EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Duitsland).*

EHRM 25 maart 1998, nr. 23224/94 (*Kopp/Zwitersland)*.

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

EHRM 6 februari 2001, nr. 44599/98 (*Bensaid/Verenigd Koninkrijk).*

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

EHRM 24 juli 2003, nrs. 46133/99 en 48183/99 *(Smirnova/Rusland)*.

EHRM 27 juli 2004, nr. 55480/00 en nr. 59330/00 *(Sidrabas & Dziautas/Litouwen).*

EHRM 4 december 2008, nr.30562/04 en nr. 30566/04 *(S. & Marper/Verenigd Koninkrijk).*

EHRM 28 mei 2009, nr. 26713/05 (*Bigaeval/Griekenland).*

EHRM 18 mei 2010, nr. 26839/05 (*Kennedy/Verenigd Koninkrijk).*

EHRM 3 oktober 2013, appl. nr. 12430/11 *(Vosgien v. France).*

EHRM 15 januari 2015, nr. 68955/11, *JBP* 2015/57, m.nt. Lindeman.

EHRM 4 december 2015, nr. 47143/06 (*Zakharov/Rusland).*

HR 9 januari 1987, ECLI:NL:HR:1987:AG5500, *NJ* 1987, 928, m.nt. E.A. Alkema.

HR 30-03-2004, ECLI:NL:PHR:2004:AM2533, m.nt. Y. Buruma.

HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.

Hof Den Haag, 26-08-2021, ECLI:GHDHA:2021:1872.

Rb. Midden-Nederland 15 oktober 2019, ECLI:NL:RBMNE:2019:4766, *Computerrecht* 2020/9, m.nt. J.J. Oerlemans.

Rb. Den Haag 20 januari 2021, ECLI:NL:RBDHA:2021:284.

Rb. Oost-Brabant 25 maart 2021, ECLI:NL:RBOBR:2021:1272.

Rb. Overijssel 29 maart 2021, ECLI:NL:RBOVE:2021:1307.

Rb. Zeeland-West-Brabant 31 maart 2021, ECLI:NL:RBZWB:2021:1556.

Rb. Noord-Nederland 29 april 2021, ECLI:NL:RBNNE:2021:1704.

Rb. Noord-Nederland 29 april 2021, ECLI:NL:RBNNE:2021:1652.

Rb. Den Haag, 30 juni 2021, ECLI:NL:RBDHA:2021:8421.

Rb. Den Haag, 25 augustus 2021, ECLI:NL:RBDHA:2021:9368.

Rb. Limburg, 26 januari 2022, ECLI:NL:RBLIM:2022:571.

Rb. Den Haag, 15 maart 2022, ECLI:RBDHA:2022:4288.