Zoeken in computers naar Nederlands en Belgisch recht

Koops, Bert-Jaap; Conings, Charlotte; Verbruggen, Frank

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Zoeken in computers naar Nederlands en Belgisch recht

Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?

Bert-Jaap Koops
Charlotte Conings
Frank Verbruggen

NVVS 2016

Zoeken in computers naar Nederlands en Belgisch recht.
Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?
Preadvies voor de jaarvergadering van de Nederlands-Vlaamse Vereniging voor Strafrecht 2016

ISBN: 978-9462-4033-21

Opstellers Preadviezen
Prof.dr. Bert-Jaap Koops
Dra. Charlotte Conings
Prof.dr. Frank Verbruggen

Dit boek is een uitgave van:
Wolf Legal Publishers (WLP)
Postbus 313
5060 AH Oisterwijk
info@wolfpublishers.nl
www.wolfpublishers.com

Het onderzoek van B-J Koops voor dit preadvies werd mogelijk gemaakt door een VICI-beurs van NWO, projectnummer 453-14-004.

Inhoudsopgave

Inleiding: 'computer-geanimeerd' debat over strafprocedure[1]

BEWEGING – Op het vlak van strafvorderlijk onderzoek in computers is veel in beweging. Dat lijkt logisch: bij computers is altijd veel in beweging, niet in het minst de vele gegevens die in computers worden verwerkt en tussen computers worden uitgewisseld.[2] Ook op juridisch vlak is er het nodige in beweging. In Nederland is er het wetsvoorstel Computercriminaliteit III, dat een doorzoeking van computers op afstand voorstelt[3] en de modernisering van het Wetboek van Strafvordering[4], waar het onderzoek van computers en gegevensdragers een belangrijk onderdeel van vormt.[5] In België heeft de regering een wetsontwerp aangekondigd om van een aantal als te zwaar beschouwde procedures, zoals infiltratie, een 'lichtere versie' te scheppen voor een Internetcontext. De Belgische regering wil net zoals de Nederlandse het omstreden 'hacken' van computers door speurders formeel legaliseren. Nog belangrijker is het Belgische initiatief om op relatief korte termijn een volledig nieuw Wetboek van Strafvordering in te voeren dat uitdrukkelijk de sprong van de negentiende naar de eenentwintigste eeuw zou maken. Dat betekent dat het een wetboek zal moeten zijn voor de digitale, gemondialiseerde informatiemaatschappij. Dit doet erg denken aan het Nederlandse project Modernisering Strafvordering, waarmee wordt beoogd om in verschillende tranches het Nederlandse wetboek op systematische wijze bij de tijd te brengen, al gaan er in België minder

---

1 Verwijzingen naar wetsartikelen in dit preadvies betreffen het Wetboek van Strafvordering (Nl.Sv en B.Sv), tenzij anders vermeld. Verwijzingen naar wetgeving en literatuur zijn conform de *Leidraad voor juridische auteurs* (https://www.wolterskluwer.nl/documents/204355/809745/Leidraad+voor+juridische+auteurs+2013/)en *Juridische verwijzingen en afkortingen* (http://www.legalworld.be/legalworld/uploadedFiles/Other_content/V_A-BI15001_final_binnenwerk.pdf), alwaar de gebruikte tijdschriftafkortingen zijn te vinden.

2 Voor de leesbaarheid volgen we in dit preadvies meestal het algemene spraakgebruik, waarin de term '*computer*' is ingeburgerd, in plaats van de juridische termen. We hanteren de term '*computer*', het Nederlandse '*geautomatiseerd werk*', het Belgische '*informatica-systeem*' en ook '*IT-systeem*' als synoniemen, hoewel er nuanceverschillen tussen de definities zijn. Zie ook *infra*, hfd. 1.

3 *Kamerstukken II* 2015/16, 34 372, nrs. 1-3.

4 *Kamerstukken II* 2015/16, 29 279, nr. 278.

5 Zie *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014.

voorstudies[6] en consultatierondes aan vooraf dan in Nederland en lijkt de politieke druk om snel te gaan hoger.

RELATIEVE RUST – De regeling van het strafvorderlijk computeronderzoek was sinds begin jaren 1990 in Nederland, sinds het jaar 2000 in België, relatief stabiel gebleven. Voorafgaand had een dogmatische discussie plaatsgevonden hoe computers te positioneren waren in het strafrecht. In Nederland adviseerde de in 1985 ingestelde Commissie computercriminaliteit (Commissie-Franken) in 1987 om diverse bepalingen in het Wetboek van Strafrecht (Sr) en Wetboek van Strafvordering (Nl.Sv) aan te passen of in te voeren, vanuit het standpunt dat gegevens geen 'goed' zijn in strafrechtelijke zin. De wetgever nam in 1993 dit standpunt over in de Wet computercriminaliteit.[7] Anders dan de Commissie computercriminaliteit[8] vond de wetgever het niet nodig om computeronderzoek expliciet te regelen in Nl.Sv, aangezien de huiszoekingsbevoegdheid voldoende ruim was om bij een huiszoeking ook computers te kunnen doorzoeken en waar nodig gegevens te kopiëren (evenals vingerafdrukken kunnen worden 'gekopieerd' bij een huiszoeking).[9] Wel werden enkele aanpalende bevoegdheden ingevoerd, zoals de netwerkzoeking en het bevel tot ongedaanmaking van beveiliging, alsmede specifieke bepalingen ter rechtsbescherming van degenen die door computeronderzoek geraakt (kunnen) worden. Daarmee was het computeronderzoek hoofdzakelijk geregeld. In 2006 volgde nog een systematische wijziging met de invoering van de doorzoeking ter inbeslagneming van gegevens,[10] maar dat was het wel ongeveer.

De Belgische wetgever combineerde in 2000 in één wet op de Informaticacriminaliteit strafrechtelijke bepalingen, met nieuwe strafbaarstellingen als 'hacking', valsheid in informatica en informaticabedrog,[11] met de invoering van een aantal strafvorderlijke bevoegdheden op maat van een IT-context. Net zoals in Nederland gold wel als uitgangspunt dat de normale klassieke bevoegdheden, zoals huiszoeking en beslag, belangrijk bleven,

---

6 De UGent deed wel een knelpuntenonderzoek: G. VERMEULEN, W. DE BONDT, T. GOMBEER, S. RAATS en L. VAN PUYENBROECK, *Scenario's voor een nieuwe Belgische strafprocedure. Een praktijkgericht knelpuntenonderzoek,* Antwerpen, Maklu, 2015, 583 p.

7 *Stb.* 1993, 33; zie *Kamerstukken II* 1989/90, 21 551, nrs. 1-3.

8 Zie COMMISSIE COMPUTERCRIMINALITEIT, *Informatietechniek en strafrecht. Rapport van de Commissie Computercriminaliteit*, 's-Gravenhage, Staatsuitgeverij, 1987, 86-88.

9 *Kamerstukken II* 1989/90, 21 551, nr. 3, 12-13.

10 *Stb.* 2005, 390, i.w.tr. 1 januari 2006 (*Stb.* 2005, 609).

11 Ter voorbereiding van de ratificatie van het Cybercrime-verdrag, zijn de bepalingen in 2006 licht aangepast.

zeker om controle te krijgen over dragers van informatie. De wetgever voerde onder meer specifieke regels in voor het gegevensbeslag, de ontsleutelplicht en de netwerkzoeking. Bij deze laatste zou vooral de ruime mogelijkheid tot grensoverschrijdende toepassing door Belgische speurders internationaal als model worden gepropageerd (*infra*, 2.3). De wetgever had de uitdrukkelijke ambitie om met een technologie-neutrale formulering te beletten dat de wetgeving al te vaak zou moeten worden aangepast aan technologische evoluties. Dat leek relatief goed te lukken, al tastte het OM soms wel de grenzen af, wat bijvoorbeeld op het vlak van medewerkingsplichten van de ICT-sector enkele opmerkelijke rechtszaken opleverde.[12]

OPBORRELENDE ONRUST – Sinds een paar jaar is het strafvorderlijk computeronderzoek echter opnieuw onrustig geworden, grotendeels door veranderingen in het ICT-landschap. Computers zijn mobiel geworden, mobieltjes (in Vlaanderen prozaïsch '*GSM's*' genoemd) zijn computers geworden (smartphones), de cloud is opgekomen als opslagplaats van computergegevens en klassieke scheidslijnen – zoals tussen opslag en transport, tussen documenten en communicatie, tussen tekst, geluid en beeld – zijn aan het vervagen. De Nederlandse wetgever[13] vindt dat deze ontwikkelingen om een reactie vragen en met de genoemde initiatieven (Computercriminaliteit III, Modernisering Strafvordering) heeft hij de handschoen ook opgenomen. De Belgische regering kondigde, op uitdrukkelijk aandringen van politie en justitie, ook een korte-termijn-update aan in afwachting van het nieuwe wetboek.[14]

Dit biedt een goede aanleiding voor een preadvies voor de Nederlands-Vlaamse Vereniging voor Strafrecht, waarin we de keuzes in beide landen vergelijken. Daarbij bespreken we de huidige voorstellen, ten minste voor zover ze beschikbaar zijn.[15] Dat is echter niet voldoende. De NVVS is

12 *Infra*, voetnoten 99 en 496.

13 Natuurlijk krijgt ook de rechter vragen voorgeschoteld, in elk geval wanneer de wetgeving geen simpel antwoord meer biedt op rechtsvragen rond computeronderzoek. In dit preadvies ligt de nadruk op het systeem en de hoofdlijnen van de wet en minder op de uitwerking in details. Daarom spreken we in de eerste plaats over uitdagingen voor de wetgever en minder over uitdagingen voor de rechter.

14 *Persbericht Verbetering van de bijzondere opsporingsmethoden en gegevensverzameling inzake internet en telecommunicaties* (sic!) – *tweede lezing*, beschikbaar op de website van de minister van Justitie: http://www.koengeens.be/news/2016/06/29/verbetering-van-de-bijzondere-opsporingsmethoden-en-gegevensverzameling-inzake-internet-e.)

15 Dat was op het moment van de redactie niet het geval voor de Belgische wetswijzigingen inzake Internetinfiltratie of 'heimelijke toegang door speurders'. Op 30 juni 2016 kwam er een persbericht van de regering dat de grote lijnen schetste, maar de teksten

immers een forum bij uitstek om dieper en breder na te denken over de betekenis van de ICT-ontwikkelingen voor het systeem van de wet. De huidige wetgeving is al behoorlijk complex. De voorzienbare wijzigingen dreigen, ondanks hun ambitie om de regeling te vereenvoudigen, die complexiteit niet te verminderen. Computers zijn machines voor gegevensverwerking, maar (vanuit opsporingsperspectief) vooral een bepaald type gegevensdrager. De wetgevers moeten zich daarom afvragen wat computers bijzonder maakt, als object van onderzoek in de strafvordering. Is het dat zij, evenals elektronische opslagmedia, grote hoeveelheden gegevens bevatten, of wellicht vooral elektronische gegevens? Of is het eerder dat computers inmiddels een dermate centrale plaats in ieders leven innemen dat zij langzamerhand de klassieke plaatsen (fysieke plaatsen als huis, bedrijf, café en publieke ruimte) en de klassieke communicatievormen (brieven, telefoongesprekken en 'live' gesprekken) verdringen als het ankerpunt waarrond zich het menselijk leven centreert? Of zijn computers simpelweg een hulpmiddel voor de wetgever om verschillende vormen van gegevensvergaring compact aan te duiden? Anders gezegd: waarom en hoe hanteren we eigenlijk begrippen als 'geautomatiseerd werk' of 'informaticasysteem' in de strafvordering? Volgens ons is een fundamentele reflectie nodig over de plaats van computers in de wettelijke regeling van de opsporing, die verder moet gaan dan het aanpassen van enkele bepalingen in het licht van ICT-ontwikkelingen.

DUBBEL OPZET – Het doel van dit preadvies is daarmee tweeledig. Eerst proberen we een kritisch-constructief overzicht te bieden van de bestaande regeling van het strafvorderlijk onderzoek in computers naar huidig en voorgesteld Nederlands en Belgisch recht. Daarbij krijgen de mogelijke verschillen tussen de landen bijzondere aandacht. Het gaat dus over onderzoek van computers en hun inhoud in het kader van de opsporing van strafbare feiten. De nadruk ligt daarbij op de bevoegdheden tot doorzoeking en inbeslagneming. Het vorderen van gegevens uit computers laten we als zodanig buiten beschouwing, behalve waar het vanuit wetssystematisch of rechtsbeschermend oogpunt relevant is in relatie tot computeronderzoek. Ook ligt de nadruk op het onderzoek van opgeslagen gegevens: het onderzoek van stromende gegevens (interceptie) blijft als zodanig bui-

van het wetsontwerp waren ook dan nog niet beschikbaar. (*Persbericht Verbetering van de bijzondere opsporingsmethoden en gegevensverzameling inzake internet en telecommunicaties* (sic!) – *tweede lezing*, http://www.koengeens.be/ news/2016/06/29 /verbetering-van-de-bijzondere-opsporingsmethoden-en-gegevensverzameling-inzake-internet-e.)

ten beschouwing, behalve voor zover dit verbonden is met onderzoek van of in computers. Vervolgens kijken we vanuit conceptueel-theoretisch en wetssystematisch oogpunt hoe de opsporing moet omgaan met een steeds meer door computers gedetermineerde samenleving. Daartoe schetsen we in het tweede deel de contouren van de manier waarop computeronderzoek ingebed zou kunnen worden in het systeem van opsporingsbevoegdheden.

Dit preadvies tracht aldus twee centrale vragen te beantwoorden. Hoe ziet de huidige en voorgestelde regeling van strafvorderlijk onderzoek in computers er uit in Nederland en België? Het eerder beschrijvende, kritisch-rechtspositieve en rechtsvergelijkende antwoord staat in Deel 1. We hebben daar de thema's uitgelicht die representatief lijken voor het algemeen debat of die misschien omstreden zijn. Tegen deze achtergrond trachten we een tweede vraag te beantwoorden: moeten computers conceptueel een bijzondere plaats innemen in het systeem van opsporingsbevoegdheden (in het bijzonder de doorzoeking) en zo ja, welke plaats? Voor die meer systematisch-theoretisch kwestie, die tamelijk onontgonnen terrein is, geven we een aanzet voor een NVVS-debat in het meer essayistische Deel 2.

Deel 1. Huidig en voorgesteld recht

In dit deel bespreken we de huidige en voorgestelde regeling van het strafvorderlijk computeronderzoek in Nederland en de (in de mate van het mogelijke) corresponderende regeling in België.[16] Na een korte analyse van de wettelijke definities die het begrip 'computer' vormgeven (hfd. 1), bestaat de hoofdmoot van dit deel uit de vier verschillende vormen van computeronderzoek, voor België nu nog nauw verbonden met de algemene doorzoekingsbevoegdheden (hfd. 2). Aansluitend komen aanpalende bevoegdheden zoals het ontsleutelbevel en de ontoegankelijkmaking (hfd. 3) aan bod. Tot slot gaan we specifiek in op enkele rechtsbeschermingsbepalingen, om te kijken of en hoe bij computeronderzoek bepaalde typen van gegevens aanvullend worden beschermd (hfd. 4).

[16] Hierbij bouwt de Nederlandse preadviseur voort op zijn eerdere besprekingen van de wetgeving (B.J. KOOPS & Y. BURUMA, 'Formeel strafrecht en ICT', in: B.J. KOOPS (red.), *Strafrecht en ICT*, 2e druk, Den Haag, Sdu 2007, 77-121; B.J. KOOPS, 'Cryptografie en strafvordering', in: B.J. KOOPS (red.), *Strafrecht en ICT*, 2e druk, Den Haag, Sdu, 2007, 123-136; B.J. KOOPS, 'Cybercriminaliteit', in: S. VAN DER HOF, A.R. LODDER EN G.J. ZWENNE (red.), *Recht en computer*, 6e druk, Deventer, Kluwer, 2014, 213-241), waaruit enkele tekstpassages zijn overgenomen. Co-auteur Buruma heeft toestemming gegeven voor dit hergebruik. Ook de Vlaamse preadviseurs putten extensief uit gepubliceerd en aankomend werk van Charlotte Conings (doctoraatsscriptie KU Leuven, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld*).

Hoofdstuk 1. De definitie van computers

NEDERLAND: GEAUTOMATISEERD WERK– Noch het Nederlandse, noch het Belgische Wetboek van Strafvordering bevat een definitie van het begrip 'computer'. In het Nederlandse Wetboek van Strafrecht is wel een definitie te vinden, die volgens de wetsgeschiedenis zich '*kennelijk*' ook uitstrekt over het gebruik van het begrip in Nl.Sv[17]. '*Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen*' (art. 80sexies Sr).[18] Computers zijn meer dan enkel gegevensdragers: de definitie omvat niet '*werken die uitsluitend bestemd zijn voor de opslag van gegevens of eenvoudige werken die in beginsel slechts bestemd zijn om te functioneren zonder interactie met hun omgeving, zoals een elektronisch klokje*'.[19] Het gaat dus vooral om een apparaat dat gegevens verwerkt, met name in interactie met de omgeving (invoer/ verwerking/uitvoer). Om te voorkomen dat puur mechanische gegevensverwerkers onder de definitie zouden vallen, is het begrip '*elektronisch*' opgenomen in de definitie (die per amendement is ingevoerd in een laat stadium van de wetsbehandeling). Daarbij is over het hoofd gezien dat dit de definitie beperkt ten opzichte van computers die op niet-elektronische basis functione-

---

17 '*De definitiebepalingen van deze begrippen zijn destijds door middel van een amendement alleen in het Wetboek van Strafrecht opgenomen. Uit de praktijk is mij evenwel niet bekend dat er problemen zijn ontstaan doordat een aparte definitiebepaling in het Wetboek van Strafvordering ontbreekt. De begrippen worden kennelijk gehanteerd in de betekenis die daarin is gegeven in de definitiebepalingen in het Wetboek van Strafrecht.*' *Kamerstukken I* 2005/06, 26 671 en 30 036 (R 1784), D, 6-7. Zie ook F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125i-125o, aant. 4.
Opmerkelijk is overigens wel dat de eerste consultatieversie van wat later het wetsvoorstel Computercriminaliteit III werd, voorstelde de definities van '*gegevens*' en '*geautomatiseerd werk*' op te nemen in Sv (art. 138e en 138f), om uitvoering te geven aan de toezegging bij de behandeling van Computercriminaliteit II (Handelingen I 2005/06, 30-1351) om '*bij een latere gelegenheid te zullen bezien in hoeverre er aanleiding is tot het opnemen van termen als "gegevens" en "geautomatiseerd werk" [in] het Wetboek van Strafvordering*'; zie Conceptwetsvoorstel versterking bestrijding computercriminaliteit, 2010. Dit is in de volgende versies verdwenen. Aangezien de toezegging van de minister in 2006 verwees naar de algemene herziening van Sv, is het mogelijk dat de wetgever hier alsnog op terugkomt bij de operatie Modernisering Sv. De Contourennota (*Kamerstukken II* 2015/16, 29 279, nr. 278) geeft daarvan echter nog geen blijk.

18 Het element van overdracht ontbrak in de definitie in de Wet computercriminaliteit (*Stb.* 1993, 33), maar is in de Wet computercriminaliteit II (*Stb.* 2006, 300) toegevoegd.

19 *Kamerstukken II* 1989/90, 21 551, nr. 3, 6.

ren.[20] Wiemans doet opmerken dat '*alle optische systemen en opslagmedia*' hierdoor buiten de definitie vallen.[21] Voor zover het optische opslagmedia (zoals cd's) betreft, is dat terecht – een opslagmedium is immers geen computer; voor zover het optische systemen betreft, zou dat een omissie kunnen zijn, maar vooralsnog zijn er geen computers die puur op basis van optische gegevensverwerking functioneren. Relevanter lijkt dat quantumcomputers buiten de definitie vallen; hoewel deze nog lang niet op de markt zijn, worden op dat vlak de laatste tijd wel significante vorderingen gemaakt. De definitie zal dus op zeker moment moeten worden aangepast om ook quantumcomputers te omvatten.[22]

AANPASSING CC III – Het wetsvoorstel Computercriminaliteit III (hierna ook: CC III) wil misschien daarom de definitie in artikel 80sexies Sr te vervangen door het volgende: '*Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.*'[23] De reden van de wijziging is echter niet bijzonder duidelijk. Aanvankelijk was het de bedoeling om een uitspraak van de Hoge Raad te consolideren, namelijk dat een router ook onder de definitie van geautomatiseerd werk valt (en dus als zodanig gehackt kan worden). Een router verwerkt weliswaar niet zelfstandig gegevens maar is wel onderdeel van een netwerk van computers en/of telecommunicatievoorzieningen en zulke netwerken vallen naar de bedoeling van de wetgever ook onder het begrip geautomatiseerd werk.[24] Het naar de Raad van State gestuurde wetsontwerp nam de definitie over uit Richtlijn 2013/40/EU over aanvallen op informatiesys-

---

20 CHR.H. VAN DIJK EN J.M.J. KELTJENS, *Computercriminaliteit*, Zwolle, Tjeenk Willink, 1995, 85.

21 F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125i-125o, aant. 5.

22 In de oorspronkelijke Memorie van Toelichting werd overigens ook al gewezen op '*biotechnische ontwikkelingen*' die zich in de toekomst kunnen voordoen (*Kamerstukken II* 1989/90, 21 551, nr. 3, 6); hoewel de wetgever in de omschrijving in de MvT daarmee rekening hield, vallen biotechnische computers door het latere amendement buiten de definitie. Ook B.J. KOOPS EN TH. DE ROOS, 'Materieel strafrecht en ICT', in: B.J. KOOPS (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, 23-75 wijzen op p. 24 op '*biologische computers*' die niet onder de definitie vallen. De ontwikkeling van op biomateriaal gebaseerde computers (bijvoorbeeld bacteriën) is, in tegenstelling tot quantumcomputers, echter niet zo ver ontwikkeld als destijds werd overwogen.

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

24 HR 26 maart 2013, LJN BY9718.

temen.[25] De Raad bekritiseerde terecht deze definitie, omdat hiermee het begrip computer ook de computergegevens in de computer zou gaan omvatten, wat een categoriefout lijkt. De Raad beval daarom aan om het begrip 'computergegevens' niet op te nemen in de definitie en eerder aan te sluiten bij de definitie uit het Cybercrime-verdrag.[26] Deze aanbeveling is volgens de MvT opgevolgd: de definitie volgt nu het Cybercrime-verdrag.[27] Dat is echter niet bepaald geslaagd: de definitie hanteert nog steeds het begrip '*computergegevens*', daar waar het Verdrag de term '*gegevens*' hanteert.[28] Dit is verwarrend, omdat hiermee een zekere circulariteit ontstaat: het begrip '*geautomatiseerd werk*' is immers, ook door de wetgever, bedoeld als synoniem voor '*computer*' en het is dan onhandig om de term '*computer*' terug te laten keren in de definitie. Bovendien is onduidelijk wat het begrip '*computergegevens*' inhoudt; het is niet dezelfde term als het begrip '*gegevens*' dat in de computercriminaliteitswetgeving wordt gebruikt.[29] Uit het oogpunt van zowel logica als wetssystematiek ligt het voor de hand om '*computergegevens*' in de voorgestelde definitie te vervangen door de term '*gegevens*'.

Ondertussen is de precieze grondslag voor de wijziging bepaald onduidelijk geworden. In de toelichting wordt nog verwezen naar het router-arrest, maar (anders dan in de consultatieversie) zonder de toevoeging dat het wenselijk is om ook de router onder het computerbegrip te brengen. In plaats daarvan stelt de MvT nu: '*Niettemin bestaat er aanleiding tot aanpassing van het begrip «geautomatiseerd» werk vanwege de technologische ontwikkelingen, die*

---

25 De Richtlijn definieert in art. 2 onder a '*informatiesysteem*' als '*apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken,* ***alsmede de computergegevens*** *die met dat apparaat of die groep van apparaten worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan*' (nadruk toegevoegd).

26 *Kamerstukken II* 2015/16, 34 372, nr. 4, 37.

27 *Kamerstukken II* 2015/16, 34 372, nr. 3, 86.

28 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, *Trb.* 2002, 18, Nederlandse vertaling *Trb.* 2004, 290 (hierna: Cybercrime-verdrag), art. 1 onder a. Opmerkelijk is dat de wetgever nu in artikel 80sexies Sr wel aansluit op de definitie uit het Verdrag, maar niet de definitie uit de Nederlandse vertaling van het Verdrag volgt. Die definieert een computersysteem in art. 1 onder a als '*ieder apparaat of geheel van onderling verbonden of samenhangende apparaten, waarvan een of meer overeenkomstig een programma geautomatiseerde gegevensverwerking uitvoert*' (*Trb.* 2004, 290).

29 Art. 80quinquies Sr: '*Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken.*'

ertoe leiden dat apparaten zelfstandig op basis van een programma automatisch gegevens verwerken, zonder dat deze onderdeel vormen van een netwerk.'[30]
Deze cryptische toelichting legt niet uit welke technische ontwikkelingen er dan precies zijn, noch wat het probleem precies is met apparaten die wel zelfstandig geautomatiseerd gegevens verwerken maar niet onderdeel vormen van een netwerk. Dat kan niet op een router slaan, die immers deel is van een (tenminste intern) netwerk, en voor zover het op stand-alone apparaten slaat, is onduidelijk waarom die niet onder de huidige definitie van een geautomatiseerd werk zouden vallen (de apparaten verwerken immers geautomatiseerd gegevens en kunnen daarmee naar men mag aannemen gewoon als computer worden beschouwd). Overigens maakt het niet zoveel uit dat de definitie wordt vervangen, of waarom precies, als de definitie maar hout snijdt en vooral voldoende duidelijk is wat er wel of niet onder valt.

In dat licht is het belangrijk om de toelichting nader te citeren, omdat hieruit de enorme reikwijdte van het computerbegrip blijkt: '*In de voorgestelde begripsomschrijving vormt het op basis van een programma automatisch verwerken van computergegevens een essentieel vereiste. Deze definitie omvat computers, servers, modems, routers, smartphones en tablets. In het advies van Bof wordt erop gewezen dat in het conceptwetsvoorstel voorgestelde de begripsomschrijving van het conceptwetsvoorstel dat in consultatie is gegeven ook technische apparaten omvat die in verbinding staan met een netwerk, zoals de SCADA-systemen die worden gebruikt bij industriële productiesystemen, navigatiesystemen, televisies, een digitaal fototoestel met Wifi-compatibiliteit of een pacemaker. Deze apparaten vallen ook onder de thans voorgestelde begripsomschrijving. Dit is echter niet zozeer een gevolg van de wens tot verruiming van de omschrijving van het geautomatiseerd werk als wel van de ontwikkeling van de techniek, die ertoe leidt dat steeds meer apparaten beschikken over functies die voorheen waren voorbehouden aan de computer.*'[31]

COMPUTER ALS DEELVERZAMELING? – Opvallend in dit citaat is dat de wetgever hier de term '*computer*' hanteert als kleine deelverzameling van '*geautomatiseerd werk*', waarbij vermoedelijk gedacht wordt aan de pc en schootcomputer; de '*computer*' is dus iets anders dan de andere genoemde apparaten. Dat sluit aan bij het gewone spraakgebruik, maar miskent dat de wetgever tegelijkertijd de nadruk legt op de functionaliteit die al deze apparaten gemeen hebben, namelijk geautomatiseerde gegevensverwerking. Dat maakt ze tot '*geautomatiseerd werk*' – maar daarmee ook, zouden wij zeggen,

30 *Kamerstukken II* 2015/16, 34 372, nr. 3, 85.
31 *Kamerstukken II* 2015/16, 34 372, nr. 3, 86.

tot '*computer*'. De apparaten voeren immers berekeningen (*computing*) uit, oftewel automatische bewerkingen van gegevens. Dat blijkt ook uit het feit dat de wetgever kennelijk wel meent dat al deze apparaten '*computergegevens*' verwerken, waarin het '*computer*'-element van SCADA-systemen of pacemakers niet voorbehouden is aan gegevens uit pc's of schootcomputers. Bovendien is het nauwelijks nog mogelijk om een onderscheid te maken tussen pc's en schootcomputers enerzijds, en tablets en smartphones anderzijds – er zijn zoveel verschillende formaten in de omloop dat er een continu spectrum is van slimme horloges (een omissie in de opsomming) via smartphones, tablets en notebooks tot klassieke bureaucomputers en supercomputers. Het zal duidelijk zijn dat al deze apparaten een '*computer*' zijn, min of meer functioneel equivalent van de klassieke (bureau)computer, zij het in verschillende formaten met enigszins verschillende vormen van invoer en uitvoer.

Dat daarnaast ook andere typen apparaten die geautomatiseerd gegevens verwerken, zoals industriële systemen, navigatiesystemen, digitale camera's met WiFi en pacemakers (en allerlei andere apparaten die in de nabije toekomst op het Internet der Dingen worden aangesloten), een '*geautomatiseerd werk*' zijn en dus onder de computercriminaliteitswetgeving vallen, zal minder duidelijk zijn voor de burger (en vermoedelijk ook voor menig politieagent en officier van justitie). Het lijkt wel een terechte keuze, zeker voor het materiële recht – het onrechtmatig binnendringen in pacemakers of gegevens manipuleren in een digitale koelkast is in beginsel even strafwaardig als klassieke vormen van hacken of gegevensbeschadiging.[32] Voor het formele recht is het misschien minder nodig om de definitie zo ruim te hebben, maar zoals de wetgever zegt, kunnen zich situaties voordoen waarin ook in dit type apparaten moet kunnen worden gezocht naar gegevens.[33] Tegelijkertijd is het ook een wat beangstigend idee als justitie de bevoegd-

---

32 Wel kan het onbedoelde neveneffecten hebben. Wanneer een slimme koelkast als geautomatiseerd werk kan worden gekwalificeerd, zal ook het zonder toestemming openen van de koelkastdeur onder de omschrijving van computervredebreuk (art. 138ab Sr) vallen, en het zonder toestemming plaatsen van een blikje bier ter afkoeling in een slimme koelkast zal gekwalificeerde computervredebreuk opleveren (namelijk onrechtmatig binnendringen en vervolgens gebruik maken van de verwerkingscapaciteit van het geautomatiseerde werk, art. 138ab lid 3 onder a Sr). Dit, naar we aannemen onbedoelde, gevolg valt te voorkomen door de in 2006 afgeschafte beveiligingseis weer in ere te herstellen in art. 138ab Sr. We kunnen ons echter voorstellen dat de ruime definitie in Sr meer van dat soort neveneffecten heeft waarvan de wetgever zich rekenschap zou moeten geven alvorens deze definitie in te voeren. Dat valt echter buiten het bestek van dit preadvies.

33 Zie *infra*, 2.2 onder '*Terminologie*'.

heid zou hebben om op afstand binnen te dringen in navigatiesystemen van auto's, pacemakers of bionische protheses; de noodzaak van een dergelijke bevoegdheid zal stevig onderbouwd moeten worden.[34]

Discussiepunt:
Moeten apparaten als navigatiesystemen, slimme koelkasten, tv's en pacemakers (die wel geautomatiseerd gegevens verwerken, maar een ander karakter hebben dan de traditionele computer) onder de (strafvorderlijke) definitie van 'geautomatiseerd werk' vallen?

BELGIË: INFORMATICASYSTEEM – De Belgische wetgever koos van meet af aan (al was dat pas in het symbolische jaar 2000)[35] voor het begrip '*informaticasysteem*', dat hij tegelijkertijd in het Strafwetboek[36] en in het Wetboek van Strafvordering[37] invoerde. In de parlementaire voorbereidingen[38] wordt '*een informaticasysteem*' gedefinieerd als: '*Een systeem voor opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT*'. De Belgische wetgever had uitdrukkelijk de bedoeling een technologie-neutrale definitie aan te reiken om te vermijden dat nieuwe technologische evoluties de wet al snel onbruikbaar zouden maken. Door de keuze voor het begrip '*informaticasysteem*' is vooral de functie (wat doet het en hoe?) doorslaggevend, zeker niet het fysieke voorwerp. Hoewel '*informatica*' historisch vooral op het studiegebied sloeg, lijkt het in de omgangstaal meer als synoniem te gelden voor '*geautomatiseerde informatie(verwerkings)technologie*'[39]. Toch maakte de wetgever meteen duidelijk dat ook de dragers ('*chipkaarten*') en fysieke apparatuur ('*computers*') onder het begrip vallen, op zich en als '*onderdeel van het systeem*'. Met de keuze van '*systeem*' staat de interactie tussen software en hardware centraal, ook als onderdeel van netwerken. Niet alleen personal computers

34 Zie *infra*, 2.2.

35 Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.* 3 november 2001.

36 Bv. 504quater Sw. (informaticabedrog) of 550bis (hacking) e.v. Sw.

37 Bv. 88ter§1 B.Sv

38 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 12.

39 Zo spreekt de Vlaamse Dienst voor Arbeidsbemiddeling over de '*Informatica-sector*' (https://www.vdab.be/beroepen/sector_informatica.shtml), ook de dagbladpers hanteert het begrip: TY, 'Informaticasector wanhopig op zoek naar meisjes', *Het Nieuwsblad* 11 februari 2013, in het Vlaamse onderwijs bestaat er een richting '*Informaticabeheer*' (http://data-onderwijs.vlaanderen.be/onderwijsaanbod /lijst .aspx?hs=311&studie=0787)

en schootcomputers zijn dus informaticasystemen, ook bankautomaten, smartphones, PDA's en tablets vallen onmiskenbaar onder die term. Het lijdt weinig twijfel dat onder deze ruime definitie ook routers vallen en ook de ingebouwde IT-systemen van voorwerpen (auto's, koelkasten, verwarmingsinstallaties e.d.) die zijn ingepast in een '*Internet of Things*'. De loskoppeling van de hardware leidt er toe dat ook socialemediaomgevingen (zoals Facebook, Twitter of Instagram) en e-mailapplicaties (zoals Hotmail en gmail), draadloze netwerken en WiFi-hotspots allemaal binnen deze definitie vallen. Het koepelbegrip '*informatica*' sluit klassieke papieren en andere niet-digitale informatieverwerking uit en maakt het o.i. mogelijk futuristische niet-elektronische verwerkingssystemen (zoals quantumcomputers) eronder te laten vallen. De veralgemeende digitalisering van informatie en de verwerking van informatie[40] maakt natuurlijk dat heel veel speurwerk in of met informaticasystemen gebeurt. Anders dan in Nederland is er in België geen uitdrukkelijke uitsluiting van '*werken die uitsluitend bestemd zijn voor de opslag van gegevens of eenvoudige werken die in beginsel slechts bestemd zijn om te functioneren zonder interactie met hun omgeving, zoals een elektronisch klokje*'.

De Belgische strafwet koppelt de bescherming van de informaticasystemen uitdrukkelijk aan die van de gegevens.[41] Zoekingen in informaticasystemen zullen noodzakelijk een zoeking inhouden naar (informatica)-gegevens, ook wel data genoemd. In België moet onder '*gegevens*' worden verstaan '*voorstellingen van informatie die geschikt zijn voor opslag, verwerking en overdracht via een informaticasysteem*'. Ook dat is natuurlijk een circulaire definiëring, nu gegevens ('*data*') mee omschrijven wat een informaticasysteem is (*supra*). De materiële vormgeving van de gegevens (elektromagnetisch, optisch of anderszins) is irrelevant.

Discussiepunt:
De Belgische definitie van informaticasysteem is heel ruim. Te ruim of is dat juist een voordeel?
Is het wenselijk om, anders dan in Nederland, digitale gegevensdragers (zoals usb-staafjes of geheugenkaarten) onder de (strafvorderlijke) definitie te laten vallen?

---

40 Vlaanderen kondigde aan dat alle (landelijke) radiostations digitaal zullen worden, digitale televisie is al de norm, talloze procedures voor bedrijven, zoals BTW-aangifte of de heffing op vrachtverkeer, bestaan uitsluitend in de elektronische variant, net als de stemprocedure voor verkiezingen in grote delen van het land.

41 Titel IXbis Sw luidt: '*Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen*'.

Hoofdstuk 2. Onderzoek in computers

2.1. Doorzoeking van plaatsen

2.1.1. Doorzoeking ter inbeslagneming

NEDERLAND – De meest gebruikelijke vorm waarbij computers voorwerp zijn van strafvorderlijk onderzoek is in het kader van een doorzoeking. Traditioneel vindt een doorzoeking plaats ter inbeslagneming van voorwerpen of ter aanhouding van de verdachte. In het laatste geval (art. 55a Nl.Sv) zal de opsporingsambtenaar wel computers kunnen tegenkomen, maar daar vanwege subsidiariteit en proportionaliteit niet in mogen zoeken – de verdachte zal zich immers niet in de computer verstoppen (toekomstige uitzonderingen als slimme koelkasten daargelaten).[42]

De doorzoeking ter inbeslagneming is vormgegeven op basis van de plaats waar het onderzoek plaatsvindt. Voor 2000 betrof dit hoofdzakelijk loci delicti, woningen alsmede koffiehuizen en andere voor het publiek toegankelijke plaatsen (art. 97 Nl.Sv-1926, de 'huiszoeking'). Sinds 2000[43] is een doorzoeking van verschillende plaatsen mogelijk onder uiteenlopende voorwaarden, afhankelijk van de (privacy)gevoeligheid van de plaats.

a) *Voertuigen*: opsporingsambtenaren kunnen bij heterdaad of verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten,[44] ter inbe-

---

42 De enige relevante situatie van computeronderzoek bij een doorzoeking ter aanhouding van de verdachte is wanneer op een computerscherm bewijsmateriaal zichtbaar is (bijvoorbeeld een kinderpornografische afbeelding); dan kan, in het kader van zoekend rondkijken waarbij relevant materiaal wordt aangetroffen, de computer in beslag worden genomen en onderzocht. Elke handeling om in een computer te kijken buiten wat op het scherm zelf zichtbaar is (een toetsaanslag, het naar beneden rollen van de scherminhoud) gaat verder dan zoekend rondkijken en is buiten een doorzoeking dus niet toegestaan (vgl. *Kamerstukken II* 1989/90, 21 551, nr. 3, 13); en voor aanhouding van een verdachte is elke doorzoeking van een computer disproportioneel. De genoemde situatie dat op het scherm een strafbaar feit of bewijsmateriaal te zien is, zal zich zelden voordoen. Wij beperken ons daarom verder tot de doorzoeking ter inbeslagneming.

43 Zie *Stb.* 1999, 243.

44 De wettelijke formulering is misdrijven als omschreven in art. 67, eerste lid, dat bepaalt dat voorlopige hechtenis is toegestaan voor misdrijven met een maximumgevangenisstraf van vier jaar of meer, alsmede voor een aantal specifiek genoemde misdrijven (waaronder de meeste computercriminaliteitsdelicten). Voorlopige hechtenis is ook mogelijk, volgens lid 2, als van de verdachte geen vaste woon- of verblijfplaats in Nederland kan worden vastgesteld en op het misdrijf gevangenisstraf staat. Waar in dit

slagneming vervoermiddelen (met uitzondering van woongedeelten) doorzoeken (art. 96b Nl.Sv).

b) *Alle plaatsen, behalve woningen en geheimhouderkantoren*: de officier van justitie kan bij ontdekking op heterdaad of verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, elke plaats doorzoeken, behalve woningen zonder toestemming van de bewoner[45] en kantoren van professionele verschoningsgerechtigden[46] (art. 96c Nl.Sv).
c) *Woningen en geheimhouderkantoren*:[47] de rechter-commissaris kan op vordering van de officier van justitie of ambtshalve elke plaats, in het bijzonder dus ook woningen en geheimhouderkantoren, doorzoeken (art. 110 Nl.Sv). Bij dringende noodzakelijkheid, als het optreden van de rechter-commissaris niet kan worden afgewacht, kan de (hulp)officier van justitie ook, met machtiging van de rechter-commissaris (bijvoorbeeld gegeven via de mobiele telefoon), woningen en geheimhouderkantoren doorzoeken (art. 97 Nl.Sv). Doorzoeking van plaatsen ter inbeslagneming, inclusief woningen en geheimhouderkantoren, is voorts mogelijk in het kader van een strafrechtelijk financieel onderzoek; dit geschiedt door de rechter-commissaris (art. 126b lid 2-3 Nl.Sv). Bij dringende noodzakelijkheid kan de officier echter, ook zonder toestemming van de rechter-commissaris, elke plaats, inclusief woningen en geheimhouderkantoren, doorzoeken om gegevens te vergaren teneinde inzicht te krijgen in de vermogenspositie van de onderzochte persoon of voor conservatoir beslag op (waardevolle) voorwerpen (art. 126c j° art. 126a en art. 94a Nl.Sv).

Tijdens een doorzoeking zijn de autoriteiten bevoegd in de te doorzoeken ruimtes aangetroffen computers te onderzoeken; dat is inbegrepen in de doorzoekingsbevoegdheid en behoefde, aldus de wetgever bij de Wet

---

preadvies termen als voorlopigehechtenismisdrijf worden gehanteerd, wordt uitsluitend gedoeld op de situatie van het eerste lid van art. 67.

45 De officier kan op basis van dit artikel dus wel woningen doorzoeken met toestemming van de bewoner. Wanneer en hoe dergelijke toestemming gegeven kan worden, valt buiten het bestek van dit preadvies. Waar in het navolgende gesproken wordt van het doorzoeken van woningen, gaan we uit van situaties waarin bewoners geen toestemming hebben verleend.

46 Zie *infra*, noot 283.

47 In de Contourennota wordt voorgesteld de regeling te splitsen en meer te differentiëren tussen doorzoekingen van woningen en van geheimhouderkantoren, zie *Kamerstukken II* 2015/16, 29 279, nr. 278, 61. We gaan daar niet verder op in.

computercriminaliteit, geen wetswijziging.[48] Een doorzoeking bestaat immers uit gericht en stelselmatig onderzoek van de locatie naar relevante voorwerpen of sporen. Daarbij mogen bijvoorbeeld kasten worden geopend en doorzocht, en vloeren, plafonds en kluizen mogen worden opengebroken en doorzocht op inhoud. Daarom is men bij gericht en stelselmatig onderzoek ook bevoegd een computer aan te zetten, de beveiliging daarvan te doorbreken en de inhoud te onderzoeken. En evenals autoriteiten bij een doorzoeking kopieën van vingerafdrukken of van schoenzoolprofielen mogen maken, mogen zij kopieën maken van aangetroffen computergegevens.[49] Bij een doorzoeking ter inbeslagneming kunnen computers dus op twee manieren worden onderzocht: door inbeslagneming van de computer (waarvan de inhoud dan later op het bureau of in het lab kan worden onderzocht) of door ter plekke de gegevens in de computer te onderzoeken en over te nemen. Omdat onderzoek van gegevens tijdens de doorzoeking vaak niet mogelijk of afdoende is (omdat lang niet altijd duidelijk is waar relevante gegevens staan), wordt meestal een één-op-één-kopie gemaakt van de harde schijf (die dan later op het bureau of in het lab kan worden onderzocht).

BELGIË – Ook België maakt een onderscheid tussen de plaatsen waar opsporings- en onderzoekshandelingen[50] doorgaan. Hoe privacygevoeliger de plaats, hoe strikter de regels voor strafrechtelijk onderzoek op die plaats. Bij de fysieke plaatsen is er een onderscheid tussen openbare plaatsen, plaatsen toegankelijk voor het publiek, private plaatsen en woningen. Verder geldt er zoals in Nederland een specifieke regelgeving waar grondrechten om bijzondere redenen (extra) in het gedrang komen, omwille van het onderzochte of doorzochte voorwerp (bv. bij beroepsgeheimhouders, *infra*, 4.1), de gezochte informatie (bv. informatie over bronnen bij journalisten) of de manier van zoeken (bv. heimelijk).

---

48 Vgl. COMMISSIE COMPUTERCRIMINALITEIT, *Informatietechniek en strafrecht*, 's-Gravenhage, Staatsuitgeverij, 1987, 88, die eenzelfde benadering voorstond maar, omdat '*eventuele twijfels omtrent bevoegdheden moeten worden verneden*', een expliciete bepaling voorstelde in art. 99 Nl.Sv: '*Indien het belang van het onderzoek dat vordert, kan de opsporende ambtenaar tijdens de huiszoeking onderzoek verrichten in aanwezige geautomatiseerde werken.*'

49 Zie *Kamerstukken II* 1989/90, 21 551, nr. 3, 10-13 en F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125i-125o, aant. 6.

50 Beide termen gebruiken we hierna als synoniemen.

OPENBARE EN PUBLIEK TOEGANKELIJKE PLAATSEN BELGIË – Vereenvoudigd gesteld, heeft de Belgische politie[51] vrije toegang tot openbare plaatsen (art. 8 B.Sv en 15 Wet Politieambt, WPA), tot voor het publiek toegankelijke plaatsen en tot gelijkgestelde plaatsen, zoals verlaten onroerende goederen (26 WPA). Indien zij op niet-openbare plaatsen niet louter willen rondkijken maar tot doorzoekingen willen overgaan, hebben ze in beginsel een bevel van een onderzoeksrechter nodig.[52] Daarop bestaat echter een belangrijke uitzondering, namelijk wanneer zij op heterdaad betrappen.[53]

DOORZOEKINGEN VOERTUIG BELGIË – Het begrip '*voertuig*' moet ruim worden begrepen. Het gaat om vervoermiddelen in het algemeen: wagens, boten, luchtvaartuigen, bussen, trams en treinen.[54] In principe is doorzoeking van een voertuig enkel mogelijk op bevel van de onderzoeksrechter of na uitdrukkelijke toestemming van de eigenaar, bestuurder en passagiers. Wanneer tijdens een geldige huiszoeking een voertuig wordt aangetroffen in een woning of aanhorigheid daarvan, is wel geen afzonderlijk bevel of afzonderlijke toestemming nodig. Ook het voertuig kan worden doorzocht op grond van het huiszoekingsbevel. Art. 29 WPA voorziet echter in een zeer ruim geformuleerde uitzondering voor het doorzoeken van voertuigen die worden aangetroffen in openbare plaatsen of plaatsen toegankelijk voor het publiek.[55] In drie gevallen kan iedere politieambtenaar zonder bevel of

---

51 Het betreden van de plaatsen toegankelijk voor het publiek op grond van art. 26 WPA vindt in principe openlijk plaats. Ook het heimelijk (in burger) betreden en rondkijken is mogelijk voor zover het niet in strijd is met de redelijke privacyverwachting. (Vgl. MvT, *Parl. St.* Kamer 2001-02, nr. 50K1688/001, 56.)

52 Cass. 19 juni 1957, *RDPC* 1957-58, 612; L. ARNOU, 'De zoeking en de inbeslagname: de bestaande en nieuwe regelgeving' in C. FIJNAUT en F. HUTSEBAUT (eds), *De nieuwe politiewetgeving in België,* Deurne, Kluwer, 1993, (171) 193-194; R. VERSTRAETEN, *Handboek strafvordering,* Antwerpen, Maklu, 2012, 332.

53 C. ROMBOUX, 'Huiszoeking en opsporing' in *Postal Memorialis. Lexicon strafrecht, strafvordering en bijzondere wetten*, Mechelen, Kluwer, 2013, H130/27; R. VERSTRAETEN, *Handboek strafvordering,* Antwerpen, Maklu, 2012, 332.

54 MvT, *Parl. St.* Kamer 1990-91, nr. 47K1637/001, 52; Omzendbrief van 2 februari 1993 met betrekking tot de wet van 5 augustus 1992 op het politieambt, *BS* 20 maart 1993, nr. 6.2.3.; L. ARNOU, 'Zoeking in voertuigen', in *Comm. Straf.* 1998, 2.

55 Het artikel spreekt van de openbare weg en voor het publiek toegankelijke plaatsen. De openbare weg moet echter ruim begrepen worden. Het artikel is bijgevolg ook van toepassing op voertuigen die worden aangetroffen in andere openbare plaatsen, zoals een openbare parkeerplaats, een haven of station. Plaatsen toegankelijk voor het publiek zijn bv. een parkeerplaats van een restaurant of een drive-in-bioscoop. L. ARNOU, 'Zoeking in voertuigen', in *Comm. Straf.* 1998, 10.

toestemming overgaan tot het doorzoeken van voertuigen op die plaatsen.[56] Het gaat om de situaties waarin zij op grond van de gedragingen van de bestuurder of de passagiers, op grond van materiële aanwijzingen of op grond van omstandigheden van tijd en plaats, redelijkerwijze kunnen denken dat het voertuig werd gebruikt, wordt gebruikt of zou kunnen worden gebruikt om (1) een misdrijf te plegen, (2) opgespoorde personen of personen die aan een identiteitscontrole willen ontsnappen, een schuilplaats te geven of te vervoeren of (3) voor de openbare orde gevaarlijk voorwerpen, overtuigingsstukken of bewijsmateriaal in verband met een misdrijf, op te slaan of te vervoeren.[57] Het gaat dus om een andere formulering dan in Nederland, maar in de praktijk zal de Belgische politie even gemakkelijk of nog gemakkelijker voertuigen kunnen doorzoeken. De bevoegdheid geldt bijvoorbeeld in het kader van een politiealarm, d.i. de systematische opsporing binnen een bepaalde zone en gedurende een bepaalde periode, bevolen door een magistraat of officier van gerechtelijke politie ingevolge een gepleegd misdrijf.[58] Het toepassingsgebied van art. 29 WPA is erg vaag geformuleerd waardoor er van de bijzondere bescherming van voertuigen weinig overblijft.

DOORZOEKING PRIVATE PLAATS, GEEN WONING BELGIË – Private plaatsen zijn ruimtes die niet toegankelijk zijn voor het algemene publiek. Er geldt slechts een beperkte toegangsmogelijkheid: verschillende personen hebben toegang, maar voorwaarden beperken die.[59] Het gaat wel niet om woningen of aanhorigheden, die in art. 15 B.Gw een bijzondere bescherming krijgen. Ook art. 22 B.Gw vereist echter een bescherming tegen onrechtmatige overheidsinmengingen in het privéleven, net zoals het EHRM. Dat hof interpreteert het begrip '*woning*' trouwens erg ruim. Private plaatsen (zoals een private vergaderzaal, club, garagebox of opslagplaats) verdienen volgens ons dan ook een bescherming, al moet die niet noodza-

---

56 Het is belangrijk dat het voertuig niet als woning is ingericht en fungeert, want dan gelden de regels inzake de huiszoeking. (zie art. 29 *in fine* WPA)

57 Zie voor een toepassing van art. 29 WPA: Antwerpen 10 maart 1999, *RW* 2000-01, afl. 18, 695.

58 MvT, *Parl. St.* Kamer 1990-91, nr. 47K1637/001, 52.

59 Cass. 16 januari 1939, *Pas.* 1939, I, 22; Cass. 25 mei 1972, *Pas.* 1972, I, 885; L. ARNOU, 'De zoeking en de inbeslagname: de bestaande en nieuwe regelgeving' in C. FIJNAUT en F. HUTSEBAUT (eds), *De nieuwe politiewetgeving in België,* Deurne, Kluwer, 1993, (171) 176; C. DE VALKENEER, 'La perquisition: principes généraux' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 16; R. VERSTRAETEN, *Handboek strafvordering,* Antwerpen, Maklu, 2012, 332.

kelijk dezelfde zijn als bij de woning. België heeft geen specifieke wettelijke regel die uitdrukkelijk bepaalt wie, over het algemeen,[60] bevoegd is tot het doen van opsporingen in private plaatsen die geen woning zijn. De regelgeving inzake *heimelijke* opsporing wijdt er wel specifieke bepalingen aan. (*infra,* 2.2). Het Hof van Cassatie lijkt aan te geven dat geen rechterlijk bevel vereist is voor het doorzoeken van private plaatsen die geen woning zijn. Een toegangsbevoegdheid tot private plaatsen op grond van de algemene opsporingsbevoegdheid uit art. 8 B.Sv en 15 WPA, waardoor politieambtenaren, belast met de gerechtelijke politietaak zonder specifieke waarborgen toegang kunnen nemen tot private plaatsen, lijkt ons in strijd met het recht op eerbiediging van de woning zoals geïnterpreteerd door het EHRM. Auteurs als De Valkeneer en Verstraeten verdedigen dat op dit ogenblik de regels inzake huiszoeking wel van toepassing zijn op private plaatsen die geen woning uitmaken in de zin van art. 15 B.Gw.[61] Ook het Hof van Beroep te Brussel oordeelde reeds in die zin voor een garagebox die geen aanhorigheid uitmaakte van een woning en voor het private gedeelte van een winkel.[62] Bockstaele en Viaene komen tot dezelfde conclusie, maar dan via een ruime interpretatie van het begrip '*woning*' en '*aanhorigheid*'.[63]

DOORZOEKING WONING BELGIË – Een doorzoeking van een woning of aanhorigheden (met inbegrip van werkelijke verblijfplaatsen[64] en beroeps-

---

60 Een doorzoeking op grond van bijzondere bevoegdheden laten we buiten beschouwing. Bv. art. 6bis van de wet van 24 februari 1921 betreffende het verhandelen van gifstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica, *BS* 6 maart 1921.

61 C. DE VALKENEER, 'La perquisition: principes généraux' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 15; R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 332.

62 Brussel 26 november 2002, onuitg. resp. Brussel 30 april 2003, onuitg., aangehaald in C. DE VALKENEER, 'La perquisition: principes généraux' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 15.

63 M. BOCKSTAELE, 'Huiszoeking, vaststellingen en beslag vanuit het perspectief van het plaatsbezoek' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 32-33 met verwijzing naar Cass. 16 januari 1939, *Pas.* 1939, I, 22; L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR*, Brussel, Larcier, 1962, 52, 57 en 202 e.v. (telkens m.b.t. besloten vergaderplaatsen, die enkel toegankelijk zijn voor bepaalde personen). Zie eveneens L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR,* Brussel, Larcier, 1962, 56 (m.b.t. een gehuurde opslagplaats waar meubels uit de woning (tijdelijk) worden bewaard. Dit zou in aanmerking komen als een voortzetting van de woning).

64 Cass. 21 oktober 1992, AR 9804, *Pas.* 1992, I, 1180-1183, concl. B. JANSSENS DE BISTHOVEN; Cass. 23 juni 1993, AR P.93.0374.F, *Arr.Cass.* 1993, 624; Cass. 21 april

lokalen) vereist een huiszoekingsbevel van een onderzoeksrechter (art. 87 B.Sv). Tot 2016 betekende dat meteen ook dat voor het verdere onderzoek de zware procedure van het gerechtelijk onderzoek onder leiding van die onderzoeksrechter nodig was. Sinds de zgn. Potpourri-II-wet is de huiszoeking mogelijk via een mini-instructie, een door de onderzoeksrechter geleid intermezzo in het opsporingsonderzoek onder leiding van het OM.[65] De onderzoeksrechter heeft echter steeds de mogelijkheid om het onderzoek naar zich toe te trekken en het verder af te handelen als een gerechtelijk onderzoek. Bij een heterdaadsituatie (art. 41 B.Sv)[66] bevatten de artikelen 32 en 36 B.Sv specifieke regels voor de huiszoeking. De procureur des Konings heeft dan de bevoegdheid om de woning van de verdachte (inclusief diens verblijf- of schuilplaats[67]) en de woning die de plaats delict uitmaakt, te doorzoeken. De officieren van gerechtelijke politie, hulpofficieren van de procureur des Konings, genieten dezelfde bevoegdheid op grond van art. 49 B.Sv.[68] De achterliggende *ratio* ligt in het risico op verlies van bewijselementen, die juist na het misdrijf nog wel voorhanden zijn en dus een snel en efficiënt optreden noodzakelijk maken.[69] Ook is het risico

---

1998, AR P.96.1470.N, *Arr.Cass.* 1998, 446, *RW* 1998-99, 1452, noot A. VANDEPLAS; Cass. 20 december 2000, AR P.00.1384.F, *Arr.Cass.* 2000, afl. 10, 2057; Cass. 19 februari 2002, AR P.00.1100.N, *Arr.Cass.* 2002, afl. 2, 535; Cass. 8 september 2004, AR P.04.0466.F, *Arr.Cass.* 2004, afl. 9, 1329, *RW* 2005-06, afl. 14, 540, noot F. VANNESTE; Cass. 26 oktober 2004, AR P.04.1129.N, *Arr.Cass.* 2004, afl. 10, 1695.

65 Art. 28septies B.Sv, zoals gewijzigd door art. 63 van de wet van 2 februari 2016.

66 De volgende situaties worden door art. 46 B.Sv aan heterdaad gelijkgesteld: (1) de situatie waarin het misdrijf binnenshuis wordt gepleegd en het hoofd van het huis de procureur des Konings verzoekt het vast te stellen en (2) de situatie waarin het slachtoffer van partnergeweld de procureur des Konings verzoekt om een binnenshuis gepleegd misdrijf vast te stellen.

67 L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR,* Brussel, Larcier, 1962, 168. Het artikel laat echter niet toe toegang te nemen tot de woning van derden, zelfs niet indien de verdachte zich daar verschuilt, tenzij de verdachte een medebewoner is van die woning. R. VERSTRAETEN, *Handboek strafvordering,* Antwerpen, Maklu, 2012, 380.

68 Aangezien het artikel verwijst naar het hoofdstuk uit het Wetboek van Strafvordering over de Procureur des Konings, geldt deze bijzondere heterdaadbevoegdheid niet voor heterdaadbevoegdheden die zijn ingeschreven in het hoofdstuk over de onderzoeksrechter. Het gaat daarbij om de heterdaadbevoegdheid tot het openen van post (88sexies B.Sv), het observeren van elektronische communicatie (art. 88bis B.Sv) en het onderscheppen van (elektronische) communicatie (90ter e.v. B.Sv).

69 M. BOCKSTAELE, 'Huiszoeking, vaststellingen en beslag vanuit het perspectief van het plaatsbezoek' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 35; F. KUTY, 'La notion de preuve pénale admissible, la sanction infligée à une preuve illicite, le surcroît de pouvoir en cas de flagrance et les suites qu'il y a eu de réserver à une infraction découverte lors d'une perquisition' (noot onder Cass. 7 februari 1995),

op een willekeurige vervolging bij betrapping op heterdaad beperkter.[70] Bij een voortdurend misdrijf kan een heterdaadsituatie zijn zolang de ongeoorloofde toestand voortduurt.[71] Of er al dan heterdaadsituatie bestond, is een feitenkwestie die de rechter ten gronde beoordeelt, die daarbij de *ratio* van de bijzondere procedure in het achterhoofd moet houden. Bij talloze computermisdrijven, zoals het bezit van kinderpornografie, grooming, stalking, het aanbieden van hackertools of van andere illegale goederen of diensten zullen speurders, in het kader van een al lopend opsporingsonderzoek, bewust streven naar een heterdaadbetrapping van de verdachte.

BELGIË: GEEN ONDERSCHEID IN DOEL ZOEKING – Het Belgisch recht maakt geen onderscheid naar gelang het doel van de zoeking, zoals dat in Nederland wel het geval is. Of de zoeking gericht is op een inbeslagname dan wel louter de vastlegging van gegevens, is bijgevolg niet van belang om uit te maken van welke soort doorzoeking sprake is. Het verschil vertaalt zich louter naar een onderscheid op het niveau van de beslagbevoegdheid. Zo kent het Belgisch recht een klassiek beslag (art. 35 e.v. en 89 B.Sv) en het modernere databeslag (art. 39bis B.Sv). Op grond van het klassiek beslag kunnen speurders een informaticasysteem, dat zij tijdens een doorzoeking aantreffen, in beslag nemen. Het databeslag laat toe het systeem ter plaatse te laten en louter computergegevens in beslag te nemen door ze te kopiëren (en eventueel te blokkeren en verwijderen). Het Hof van Cassatie leidt uit die laatste bevoegdheid af dat informaticasystemen doorzocht kunnen worden zodra ze het voorwerp kunnen uitmaken van een beslag, al blijkt dat niet duidelijk uit de wet.[72] Dat betekent dat de bovenstaande doorzoekingsbevoegdheden zich op grond van de Cassatierechtspraak ook uitstrekken tot de ter plaatse aangetroffen informaticasystemen. We verwijzen naar die bevoegdheid tot het doorzoeken van informaticasystemen ter plaatse als de '*informaticazoeking*'.[73] We gaan in de volgende titel dieper in op die bevoegdheid.

JLMB 1997, afl. 12, (474) 476–477; L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR,* Brussel, Larcier, 1962, 162.

70 M-A BEERNAERT, H.D. BOSLY, D. VANDERMEERSCH, *Droit de la procédure pénale*, Brugge, La Charte, 2014, 371.

71 C. ROMBOUX, 'Huiszoeking en opsporing' in *Postal Memorialis. Lexicon strafrecht, strafvordering en bijzondere wetten*, Mechelen, Kluwer, 2013, H130/8.

72 Cass. 11 februari 2015, AR P.14.1739.F, *RW* 2015-16, afl. 16, 621 noot C. CONINGS.

73 Het zoeken naar gegevens die op een aangetroffen informaticasysteem staan opgeslagen, noemt men in de praktijk vaak '*uitlezen*', maar wij gebruiken liever informatica-

2.1.2. Doorzoeking ter vastlegging van gegevens

NEDERLAND: ART. 125i Nl.Sv – Aangezien gegevens niet kunnen worden inbeslaggenomen, kan justitie theoretisch geen reguliere doorzoeking aanvragen als ze alleen beoogt om een computer te doorzoeken en gegevens te kopiëren. In de praktijk kan natuurlijk altijd een doorzoeking ter inbeslagneming van een gegevens*drager* plaatsvinden. Dat is echter, zoals de Commissie computercriminaliteit al constateerde, mogelijk een te zwaar middel (als door inbeslagneming van de computer de 'continuïteit van vitale verwerkingsprocessen' in gevaar komt) of soms onmogelijk. De Commissie stelde daarom voor om artikel 97 en artikel 111-oud (huidig art. 110) uit te breiden met een clausule, na 'ter inbeslagneming': 'of ter vergaring of opneming van daarvoor vatbare gegevens'.[74] De wetgever nam dat bij de Wet computercriminaliteit echter niet over, wat vervolgens kritiek opleverde omdat nu, ook als justitie op voorhand een doorzoeking wil doen enkel om gegevens te kopiëren en niet om hele gegevensdragers in beslag te nemen, hiervoor een oneigenlijke doorzoeking 'ter inbeslagneming' van de gegevensdrager moet worden aangevraagd.[75] Dit (tamelijk theoretische) probleem is opgelost in 2005 door een zelfstandige bevoegdheid in te voeren in art. 125i Nl.Sv:

'*Aan de rechter-commissaris, de officier van justitie, de hulpofficier van justitie en de opsporingsambtenaar komt onder dezelfde voorwaarden als bedoeld in de artikelen 96b, 96c, eerste, tweede en derde lid, 97, eerste tot en met vierde lid, en 110, eerste en tweede lid, de bevoegdheid toe tot het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd. In het belang van het onderzoek kunnen zij deze gegevens vastleggen. De artikelen 96, tweede lid, 98, 99 en 99a zijn van overeenkomstige toepassing.*'

Hoewel de bepaling vooral bedoeld was voor computers, is zij generieker geformuleerd: het gaat om alle gegevensdragers, dus naast computers ook elektronische gegevensdragers (zoals usb-staafjes), optische gegevensdragers (bijvoorbeeld dvd's) en papieren gegevensdragers (bijvoorbeeld ordners).[76]

---

zoeking voor toegang tot gegevens in informaticasystemen die opsporingsinstanties op geldige wijze in handen krijgen.

74 COMMISSIE COMPUTERCRIMINALITEIT, *Informatietechniek en strafrecht*, 's-Gravenhage, Staatsuitgeverij, 1987, 87.

75 Zie COMMISSIE-MEVIS (2001), *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, 2001, 88-90 en 100; F.P.E. WIEMANS, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen, Wolf Legal Publishers, 2004, 234-238.

76 G.J.M. CORSTENS, *Het Nederlands strafprocesrecht*, bewerkt door M.J. BORGERS, 8e druk, Deventer, Kluwer, 572; *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en door-*

De doorzoeking ter vastlegging van gegevens is door artikel 125i mogelijk onder dezelfde voorwaarden als de reguliere doorzoeking ter inbeslagneming in genoemde artikelen. Het voorstel van Wiemans om in plaats van deze vrij ingewikkelde verwijzingsbepaling een veel simpeler bepaling in de betekenissentitel op te nemen dat onder '*doorzoeking ter inbeslagneming*' ook '*doorzoeking ter vastlegging van gegevens*' wordt verstaan,[77] heeft de wetgever helaas niet gevolgd. Dat heeft belangrijke (en mogelijk onbedoelde) wetssystematische gevolgen. Het betekent immers dat doorzoekingen ter vastlegging van gegevens (als mogelijk minder ingrijpend alternatief voor doorzoekingen ter inbeslagneming) alleen mogelijk zijn in situaties als bedoeld in artikelen 96b, 96c, 97 en 110. Doorzoekingen op basis van bijzondere wetgeving (art. 49 Wet wapens en munitie) kunnen niet plaatsvinden ter vastlegging van gegevens.[78] Dat lijkt niet zo'n probleem, omdat bij dergelijke doorzoekingen vrijwel nooit alleen naar gegevens gezocht zal worden, maar ook naar wapens, zodat altijd wel een doorzoeking ter inbeslagneming aangewezen zal zijn. Problematischer lijkt echter dat doorzoekingen in het kader van een strafrechtelijk financieel onderzoek (art. 126b en 126c Nl.Sv) beperkt zijn tot doorzoekingen ter inbeslagneming, terwijl juist bij het zoeken naar gegevens die inzicht geven in de vermogenspositie van de onderzochte personen het relevant kan zijn om de doorzoeking primair te richten op het vastleggen van gegevens, en niet op inbeslagneming van gegevensdragers. Financiële en administratieve gegevens staan immers steeds meer in computers opgeslagen en het valt moeilijk in te zien waarom artikel 125i zich niet ook tot sfo-doorzoekingen uitstrekt. De oplossing van Wiemans om in plaats van het opsommende artikel 125i een bepaling in de betekenissentitel op te nemen, zou dat hebben ondervangen, en daarmee niet alleen eleganter maar ook generieker en systematischer zijn geweest.

Terecht merkt Wiemans verder op dat de formulering van artikel 125i onsystematisch is, nu de volgorde van de artikelvermelding niet correspondeert met de volgorde van functionarissen.[79] De kritiek van Wiemans op het opnemen van een verwijzing naar de rechtsbeschermende artikelen 98, 99 en 99a kan deels worden gevolgd.[80] De verwijzing naar artikel 98 (ge-

---

zoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2), versie 4 juni 2014, 44.

77 F.P.E. WIEMANS, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen, Wolf Legal Publishers, 2004, 236-237.

78 F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125i, aant. 4.

79 *Ibid*., art. 125i, aant. 5.

80 Zie *Ibid*., art. 125i, aant. 5.

heimhouderbescherming) is ongelukkig, omdat voor computeronderzoek daarvoor juist een specialis, artikel 125l, is geschapen (zie par. 4.1), en de verwijzing naar artikel 99a (bijstand door raadsman) is overbodig omdat die bepaling voor elke doorzoeking van plaatsen geldt en dus ook automatisch voor een doorzoeking ex 125i. De verwijzing naar artikel 99 vinden we echter, anders dan Wiemans, niet zinledig, omdat de subsidiariteitseis (eerst uitnodigen tot vrijwillige afgifte, art. 99 lid 1) een ander karakter heeft dan de bevoegdheid om gegevens te vorderen (wat verplichte afgifte van gegevens inhoudt), en omdat het zinvol is om de bewoner, huisgenoten of, indien aanwezig, verdachte in de gelegenheid te stellen zich omtrent de gekopieerde gegevens te verklaren (art. 99 lid 2 j° 125i) – bijvoorbeeld om aan te geven dat de opsporingsambtenaar op een verkeerd spoor zit en dat het niet nodig is de gegevens te kopiëren.[81]

Tegelijkertijd toont dit ook een lacune aan in de rechtsbescherming wanneer tijdens een doorzoeking *ter inbeslagneming* computers worden onderzocht en daaruit gegevens worden gekopieerd. De bescherming van geheimhouders is afdoende gewaarborgd via artikel 125l (zie par. 4.1) en de mogelijkheid van bijstand door een raadsman (zonder de doorzoeking daardoor op te houden) (art. 99a) geldt voor elke doorzoeking. Artikel 99 is echter beperkt tot de inbeslagneming van voorwerpen, wat betekent dat bij inbeslagnemingsdoorzoekingen waarbij gegevens worden gekopieerd, niet eerst (waar het belang van het onderzoek dat toestaat) om vrijwillige afgifte van de gegevens hoeft te worden gevraagd, noch dat betrokkenen in de gelegenheid worden gesteld zich over de gekopieerde gegevens te verklaren. Dat laatste lijkt een omissie: als de wetgever de bepaling relevant acht bij een doorzoeking ter vastlegging van gegevens (zoals blijkt uit de verwijzing in art. 125i), moet de bepaling ook relevant zijn bij andere doorzoekingen waarbij gegevens worden vastgelegd.

Evenzo ontbreekt een gegevensanaloge bepaling voor artikel 96 Nl.Sv. Artikel 96 lid 1 bepaalt dat bij ontdekking op heterdaad of een misdrijf waarvoor voorlopige hechtenis is toegelaten, de opsporingsambtenaar bevoegd is om elke plaats te betreden om daarvoor vatbare voorwerpen in beslag te nemen. Aangezien artikel 125i beperkt is tot doorzoekingen, geldt de gegevensvastleggingsmogelijkheid niet voor het betreden van plaatsen. Nu zullen zich niet vaak situaties voordoen dat een opsporingsambtenaar gegevens wil vastleggen en daartoe een plaats wil betreden (zonder dat hij ook een gegevensdrager in beslag zou willen nemen), maar theoretisch wekt het bevreemding dat hier geen equivalent voor in het leven is geroe-

81 Vgl. WÖRETSHOFER, T&C Strafvordering, 11e druk 2015, art. 99 Sv, aant. 1.

pen. Aangezien de wetgever inbeslagneming van een gegevensdrager over het algemeen als ingrijpender beschouwt dan het overnemen van gegevens uit de gegevensdrager, ligt het voor de hand dat artikel 96 lid 1 ook een equivalent zou moeten krijgen voor het betreden van plaatsen ter vastlegging van gegevens.

Hetzelfde geldt voor de bevriezingsmogelijkheid van artikel 96 lid 2: bij een doorzoeking ter inbeslagneming kan de opsporingsambtenaar, in afwachting van de bevoegde autoriteit, de nodige maatregelen nemen om te voorkomen dat voor inbeslagneming vatbare voorwerpen verdwijnen of beschadigd raken. Zoals Wiemans doet opmerken, is het zinvol dat dit ook van overeenkomstige toepassing verklaard is bij doorzoekingen ter vastlegging van gegevens ex artikel 125i;[82] dat zal dan betekenen dat de opsporingsambtenaar ook maatregelen kan treffen om vernietiging of beschadiging van vast te leggen gegevens te voorkomen. Indien echter een doorzoeking plaatsvindt ter inbeslagneming, bijvoorbeeld een doorzoeking van een bedrijfspand door een hulpofficier op basis van artikel 96c lid 2, is artikel 96 lid 2 wel van overeenkomstige toepassing (namelijk door art. 96c lid 3), maar dat beperkt zich dan tot maatregelen die de hulpofficier kan nemen om verdwijning of beschadiging van *voorwerpen* te voorkomen. Bevriezingsmaatregelen bestemd om *gegevens* te beveiligen tegen vernietiging of beschadiging, vallen daar niet onder. Nu kan de hulpofficier wel de computer zelf verzegelen, als voor inbeslagneming vatbaar voorwerp, maar de verzegeling strekt dan niet om beschadiging te voorkomen van het voorwerp zelf, maar van de (niet voor inbeslagneming vatbare) inhoud ervan, en dat valt, strikt genomen, niet onder artikel 96. Dit kan opgelost worden door in artikel 96 lid 2 na 'beschadiging van voor inbeslagneming vatbare voorwerpen' in te voegen 'of van gegevens'.

Al met al kunnen we concluderen dat de invoering van de doorzoeking ter vastlegging van gegevens in artikel 125i wel een verbetering is ten opzichte van de oorspronkelijke regeling uit 1993, maar ook dat het feit dat computeronderzoek niet alleen kan plaatsvinden door inbeslagneming van computers (en vervolgens onderzoek van de inhoud daarvan) maar ook door het kopiëren van gegevens, duidelijk nog onvoldoende systematisch is doorgevoerd in het Wetboek van Strafvordering.

INFORMATICAZOEKING BELGIË – Ook Belgische opsporingsinstanties die tijdens zoekingen op een fysieke plaats, een persoon (cf. fouillering) of

82 F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125i, aant. 5.

voertuig een informaticasysteem aantreffen dat mogelijks voor het strafrechtelijk onderzoek relevante gegevens bevat, kunnen dat onder bepaalde voorwaarden doorzoeken. Deze zogenaamde informaticazoeking is niet in een uitdrukkelijke bepaling omschreven en lijkt daarom, zoals de klassieke zoekingen (fysieke plaats, persoon of voertuig), plaatsgebonden. Het gaat om een dwangmaatregel. Daarom menen wij dat de bevoegdheid tot het uitvoeren van een informaticazoeking, net zoals bij de huiszoeking, de overheid meteen ook het recht geeft om een eventuele verhindering van toegang op om het even welke loyale wijze ongedaan te maken. Dus houdt de zoekingsbevoegdheid meteen de mogelijkheid in om een beveiliging (encryptie) te doorbreken. Dat kan bijvoorbeeld via het exploiteren van een zwakheid in het systeem, het gebruik van een in een strafonderzoek legaal verkregen paswoord of door een *brute force* aanval, d.w.z. dat een hele reeks paswoorden op geautomatiseerde wijze worden geprobeerd. Wel moet de overheid steeds rekening houden met de hieraan verbonden risico's: het onbewust wissen van gegevens, het beschadigen van het systeem of delen ervan, nadeel voor andere gebruikers van het systeem. Ook moet het doorbreken van de beveiliging steeds redelijk zijn en in verhouding staan tot het nagestreefde doel (art. 37 WPA).

BELGIË: BEVOEGDE INSTANTIES INFORMATICAZOEKING – België heeft nog geen tegenhanger van art. 125i Nl.Sv. Bij gebreke aan een uitdrukkelijke bepaling inzake de informaticazoeking in het kader van een klassiek strafonderzoek, zijn ook de voorwaarden voor de toepassing ervan niet onmiddellijk duidelijk. Toch vermeldt het Belgische Wetboek van Strafvordering tweemaal terloops de zoeking in een informaticasysteem: bij het databeslag en bij de netwerkzoeking. Art. 39bis B.Sv, dat handelt over het databeslag, vermeldt dat de procureur des Konings de verantwoordelijke van het informaticasysteem op de hoogte brengt van de '*zoeking in het informaticasysteem*'. De onderzoeksrechter moet hetzelfde doen (art. 89 B.Sv, dat verwijst naar art. 39bis B.Sv). Die vermelding maakt niet duidelijk wanneer de procureur des Konings dan wel de onderzoeksrechter bevoegd is voor de doorzoeking van de gegevens in een IT-systeem. Art. 88ter B.Sv regelt de netwerkzoeking nader en dat is eigenlijk een uitbreiding van de informaticazoeking (*infra*, 2.1.3). Het artikel vangt aan als volgt: '*Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, kan deze zoeking worden uitgebreid naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt: […]*'. Hier verschijnt dus blijkbaar plots het bevel van de onderzoeksrechter als

een wettelijke toepassingsvoorwaarde voor de informaticazoeking.[83] Uit het voorgaande en de algemene regels inzake zoeking en beslag, menen we te kunnen afleiden dat er een bevoegdheid tot het uitlezen van IT-systemen is weggelegd voor zowel de procureur des Konings als de onderzoeksrechter. De vraag naar de concrete bevoegdheidsverdeling tussen beide instanties beantwoordt de wet niet. Sommige auteurs[84] leiden uit het gebrek aan een duidelijke, specifieke grondslag af dat de bevoegdheid tot het rechtstreeks toegang nemen tot de gegevens in IT-systemen voortvloeit uit de zoekingsbevoegdheid ten aanzien van de plaats waar dat systeem wordt aangetroffen (bv. zoeking t.a.v. een fysieke plaats, voertuig of persoon). De mogelijkheid om tijdens zo een zoeking een IT-systeem in beslag te nemen of, wanneer een beslag op het systeem niet wenselijk is, enkele gegevens in beslag te nemen, betekent dat het systeem eveneens kan worden doorzocht ('*uitgelezen*') door de voor de zoeking bevoegde instanties. Zoals we reeds aanstipten, volgt het Hof van Cassatie deze visie in het arrest van 11 februari 2015.[85] Er zouden bijgevolg geen bijzondere voorschriften van toepassing zijn. Een informaticasysteem onderscheidt zich in die visie dan ook niet van andere zaken die tijdens de zoeking worden aangetroffen, zoals een portefeuille, agenda of koffer.[86] De zoeking in een informaticasysteem heeft het databeslag tot doel. Daarom zullen de beperkingen bij gegevensbeslag ook gelden. Dat betekent dat opsporingsinstanties de zoeking slechts mogen

---

83 Het woord 'wanneer' in art. 88ter B.Sv wijst erop dat het bevel van de onderzoeksrechter een voorwaarde is van de informaticazoeking en niet dat enkel een door de onderzoeksrechter bevolen informaticazoeking de aanleiding kan zijn voor een verregaandere netwerkzoeking. (T. INCALZA, 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', *Jura Falc.* 2010-11, afl. 2, (329) 333.) Het is immers absurd de onderzoeksrechter te verbieden een door het OM bevolen informaticazoeking uit te breiden.

84 Zie voor die visie: MvT, *Parl. St.* Senaat 2005-06, nr. 3-1824/1, 5; M. BOCKSTAELE, 'Huiszoeking, vaststellingen en beslag vanuit het perspectief van het plaatsbezoek' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 47; D. DEWANDELEER, 'Misdrijven en strafonderzoek in de IT-context' in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2009-2010, (125) 139, 141 en 144 die dit afleidt uit de algemene beslagbevoegdheid (art. 35 e.v. Sv.); E. FRANCIS, 'Algemene principes van de bijzondere verbeurdverklaring en het beslag in strafzaken', *T.Strafr.* 2011, afl. 5, (306) 324; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 167-171.

85 Cass. 11 februari 2015, AR P.14.1739.F., *RW* 2015-16, afl. 16, 621 noot C. CONINGS.

86 Zie voor kritiek op deze visie: C. CONINGS, 'Het uitlezen van een gsm of ander privaat IT-systeem: this is not America' (noot onder Cass. 11 februari 2015), *RW* 2015, afl. 16, 622-626.

uitvoeren als ze redelijkerwijze kunnen vermoeden dat zij in het informaticasysteem data zullen aantreffen die voor de bijzondere verbeurdverklaring in aanmerking komen of kunnen dienen om de waarheid aan de dag te brengen m.b.t. het onderzochte misdrijf. Andere auteurs menen nochtans dat op grond van de aanvang van art. 88ter §2 B.Sv de informaticazoeking wel degelijk een bijzondere regeling kent waarbij een bevel van de onderzoeksrechter centraal staat.[87] Ze vergelijken met de huiszoeking, zodat hun visie beperkt blijft tot zoekingen in private informaticasystemen.[88] Art. 88ter §2 B.Sv spreekt i.v.m. de informaticazoeking over '*personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken*'. Dit lijkt inderdaad aan te geven dat het niet gaat over publieke, maar enkel over private informaticasystemen. Een bevoegdheid van de procureur des Konings blijft dan overeind voor publieke informaticasystemen en eventueel voor een informaticazoeking met toestemming van de persoon in kwestie. Een huiszoekingbevel (of eventueel een bevel tot zoeking in een private plaats) zou zich uitstrekken tot de informaticasystemen die de opsporingsinstanties daar aantreffen.[89] Uiteraard moeten zij de uit het bevel voortvloeiende beperkingen steeds respecteren.[90] Een specifiek bevel zou dan vereist zijn voor private informaticasystemen die men in openbare of voor het publiek toegankelijke plaatsen aantreft, bv. tijdens een fouillering of aanhouding.[91] Het

---

87 Zie: M-A BEERNAERT, H.D. BOSLY, D. VANDERMEERSCH, *Droit de la procédure pénale*, Brugge, La Charte, 2014, 697; C. DE VALKENEER, *Manuel de l'enquête pénale*, Brussel, Larcier, 2011, 448; C. MEUNIER, 'La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique', *RDPC* 2001, (611) 663-664; R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 508.

88 Hiermee bedoelen we systemen die niet voor het publiek toegankelijk zijn. T. INCALZA, 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', *Jura Falc.* 2010-11, afl. 2, (329) 332-333; C. MEUNIER, 'La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique', *RDPC* 2001, (611) 663.

89 P. DE HERT en G. LICHTENSTEIN, 'Huiszoeking en beslag in geautomatiseerde omgevingen', in M. BOCKSTAELE (ed), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 64; R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 508; zie echter contra: C. DE VALKENEER, *Manuel de l'enquête pénale*, Brussel, Larcier, 2011, 448. (De auteur stelt dat twee bevelen vereist zijn die echter wel in hetzelfde instrument kunnen worden opgenomen.)

90 C. CONINGS en J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerr.* 2013, afl. 1, (23) 27, noot nr. 33.

91 R. VERSTRAETEN lijkt hier evenwel nog een bijkomend onderscheid in te voeren. Wanneer de onderzoeksrechter een informaticasysteem in beslag laat nemen zou een

verschil tussen beide visies in de rechtsleer situeert zich voornamelijk hier. De vraag rijst echter welk bevel de onderzoeksrechter in dat geval dient te geven. Enkele auteurs verwijzen voor de toe te passen voorwaarden naar het klassieke bevel van de huiszoeking.[92] Dat lijkt echter niet altijd geschikt. Zo kan een huiszoeking bijvoorbeeld slechts uitzonderlijk bij nacht omwille van de verhoogde intimiteit op dat ogenblik. De *ratio* van die tijdsvoorwaarden gaat niet op voor zoekingen in private informaticasystemen, die men bijvoorbeeld tijdens een nachtelijke fouillering aantreft.[93] Daarom zou de onderzoeksrechter zijn bevel (of kantschrift) eerder moeten baseren op artikel 56 B.Sv (over het gerechtelijk onderzoek)[94] of art. 88 B.Sv (over de ruime doorzoekingsbevoegdheid van "plaatsen"). De Belgische regering kondigde net voor de zomer van 2016 aan dat ze de niet-heimelijke informaticazoeking nu toch bij wet ging regelen. Dat zou een einde stellen aan de bestaande onduidelijkheid in de wet. De nieuwe wet zou werken met vier niveaus, waarin ook de huidige netwerkzoeking vervat zit: '*de zoeking waartoe de officier van gerechtelijke politie kan beslissen in een informaticasysteem dat in beslag is genomen; de door de procureur des Konings bevolen zoeking in een informaticasysteem dat niet in beslag is genomen, maar dat wel nog kan zijn* (sic!)*, de door de procureur bevolen uitbreiding van een zoeking tot een informaticasysteem dat verbonden is aan een informaticasysteem dat het onderwerp is van de eerste maatregel voor zover de informatie toegankelijk is zonder code in te voeren, elke andere niet-*

---

afzonderlijk bevel ook niet nodig zijn voor het uitlezen van het in beslag genomen systeem. R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 507.

92 C. DE VALKENEER, *Manuel de l'enquête pénale*, Brussel, Larcier, 2011, 448; C. MEUNIER, 'La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique', *RDPC* 2001, (611) 663-664; R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 508.

93 Zie eveneens C. CONINGS en J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerr.* 2013, afl. 1, (23) 27, noot nr. 32; T. INCALZA, 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', *Jura Falc.* 2010-11, afl. 2, (329) 335-336.

94 Zie in dit opzicht de voorbereidende werken van de kleine Franchimont-wet m.b.t. art. 56 B.Sv: '*Door het gebruik van de woorden « hij beslist of het noodzakelijk is dwang te gebruiken, » houdt het ontwerp rekening met het feit dat de onderzoeks- rechter bepaalde maatregelen neemt bij wege van beschikkingen, zelfs op niet-formele wijze.*' MvT, *Parl. St.* Kamer 1996-97, nr. 49K857/001, 42. Zie eveneens Verslag namens de commissie, *Parl. St.* Senaat 2002-03, nr. 2-1260/4, 15 i.v.m. de observatie voor de invoering van de BOM-regelgeving: '*Persoonlijk maakt hij* [D. VANDERMEERSCH] *steeds een kantschrift op voor een observatie omdat hij vindt dat hij daarvoor de verantwoordelijkheid op zich moet nemen. Spreker baseert zich op het huidige artikel 56 van het Wetboek van Strafvordering. Observatie is een aantasting van de privé-sfeer en hij vindt daarom dat ze door de onderzoeksrechter moet worden bevolen, zodat er een spoor van is in het dossier.*'

heimelijke zoeking in een informaticasysteem, bevolen door een onderzoeksrechter.'[95] Het ontwerp bouwt dus voort op de idee dat in principe geen rechterlijk bevel vereist is voor het doorzoeken van IT-systemen en breidt de bevoegdheden van het parket zelfs nog verder uit tot bepaalde vormen van netwerkzoekingen, die onder het huidig recht wel duidelijk aan de onderzoeksrechter toekomen (*infra*, 2.1.3).

BELGISCH STRAFUITVOERINSGONDERZOEK – De regelgeving voor de Belgische tegenhanger van het Nederlandse sfo, het strafuitvoeringsonderzoek (SUO), bevat, anders dan de klassieke regels voor het vooronderzoek, wél al een uitdrukkelijk voorschrift voor de informaticazoeking. Art. 464/8 B.Sv voorziet in de mogelijkheid tot het doorzoeken van een private plaats met toestemming van de persoon met werkelijk genot over die plaats. Het artikel vermeldt uitdrukkelijk dat speurders tijdens die zoeking informatiedragers mogen opsporen en in beslag nemen. Voor een zoeking in een privaat informaticasysteem dat zich in die private plaats bevindt, is overeenkomstig art. 464/8 §2 Sv echter een nieuwe toestemming vereist, namelijk van de concrete gebruiker van het systeem. De toestemming tot het doorzoeken van de private plaats en de daaruit voortvloeiende beslagbevoegdheid, houden dus blijkbaar geen bevoegdheid in om zonder meer alle informaticasystemen te doorzoeken die zich in die private plaats bevinden. Daarmee erkent de wetgever dat het informaticasysteem een afzonderlijk te beschermen rechtsgoed uitmaakt. Een houding die in contrast staat met die van het Hof van Cassatie. In het kader van de bevoegdheden onder dwang in het SUO vinden we dit onderscheid echter niet meer terug. Daar spreekt de wetgever in art. 464/22 en 464/23 B.Sv opnieuw enkel van een doorzoeking van een private plaats en de netwerkzoeking.

DATABESLAG BELGIË – Wanneer de informaticazoeking of de netwerkzoeking (*infra*, 2.1.3)[96] data onthult die voor bijzondere verbeurdverklaring in aanmerking komen of kunnen dienen om de waarheid aan de dag te brengen, kan de uitvoerende ambtenaar die overeenkomstig art. 39bis B.Sv kopiëren. Dat geldt ook voor de gegevens noodzakelijk om andere gegevens te kunnen verstaan. Daarnaast voorziet het artikel in de bevoegdheid om de

---

95 *Persbericht Verbetering van de bijzondere opsporingsmethoden en gegevensverzameling inzake internet en telecommunicaties* (sic!) – *tweede lezing*, http://www. koengeens .be/news/2016/06/29/verbetering-van-de-bijzondere-opsporingsmethoden-en-gegevensverzameling-inzake-internet-e.

96 Art. 39bis B.Sv juncto art. 35 B.Sv. Zie ook art. 89 B.Sv.

toegang tot de originele gegevens en kopieën daarvan te verhinderen en in de plicht om bepaalde specifiek in de wet omschreven gegevens[97] ontoegankelijk te maken.[98] Daarop bestaat echter een beperking. Bij een unilaterale grensoverschrijdende netwerkzoeking (*infra*, 2.1.3) aangetroffen gegevens mogen overeenkomstig art. 88ter §3 B.Sv enkel worden gekopieerd.[99] Zoals in Nederland vormt het databeslag op grond van art. 39bis B.Sv een alternatief voor het klassieke beslag op de materiële dragers op grond van art. 35 B.Sv e.v. resp. 89 B.Sv. Voor zover het artikel niet in afwijkende voorschriften voorziet, zijn de voorschriften van het klassieke beslag van toepassing. Art. 39bis B.Sv voorziet ook in de mogelijkheid tot een beslag met bewaring ter plaatse. In dat geval kopiëren de opsporingsinstanties de gegevens niet, maar beperken zij zich tot een soort loutere verzegeling ervan door de toegang daartoe te blokkeren.[100] Die mogelijkheid is bijvoorbeeld interessant wanneer de omvang van de aangetroffen data niet toelaat om alles te kopiëren.[101] Hoewel Kerkhofs en Van Linthout wel eens anders hebben beweerd[102], kan het databeslag enkel plaatsvinden in de openlijke fase van het strafonderzoek. Art. 39bis B.Sv stelt immers dat de verantwoordelijke van het informaticasysteem op de hoogte moet worden gebracht van de zoeking in het informaticasysteem. De wetgever wou met die informatieverplichting aangeven dat hij met art. 39bis B.Sv geen heimelijke maatregel wilde invoeren.[103] De verantwoordelijke van het IT-systeem moet bovendien een samenvatting krijgen van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd. De wetgever neemt, in tegen-

97 Zie art. 39bis §3 B.Sv: '*Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen* […].'

98 'Ontoegankelijk maken' is een ruim begrip dat verschillende maatregelen moet toelaten waaronder het verwijderen van de betrokken bestanden met behoud van een kopie voor justitie (dit om te vermijden dat de beslissing tot verwijdering definitief zou zijn, onafhankelijk van de einduitspraak). Zie Amendement, *Parl. St.* Senaat 1999-2000, nr. 2-392/002, 11.

99 Gelet op het *Pirate Bay*-arrest van het Hof van Cassatie kan de toegang tot de gegevens vanuit België in bepaalde gevallen eveneens worden geblokkeerd op grond van het databeslag. Zie Cass. 22 oktober 2013, AR P.13.0550.N, *Computerr.* 2014, afl. 2, 106, noot K. VANDERHAUWAERT, *T.Strafr.* 2014, afl. 2, 126, noot R. SCHOEFS.

100 Zie art. 39bis §4 B.Sv.

101 J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 172-173.

102 J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 175-176.

103 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 21: '*De bedoeling van het op de hoogte brengen van de maatregel is evenwel duidelijk te stellen dat het niet gaat om een geheime maatregel (vergelijk met de huiszoekingsbevoegdheid).*'

stelling tot bij het klassiek beslag, genoegen met een samenvatting aangezien een uitputtende inventarisering vaak niet realistisch is.[104] Aangezien art. 39bis B.Sv, onverminderd de eigen voorschriften, de regels uit het Wetboek van Strafvordering inzake het klassiek beslag van toepassing verklaart op het databeslag, menen we dat de verschillende vormvereisten van het beslag, zoals de aanwezigheid van de verdachte, diens erkenning van de inbeslaggenomen data en diens ondertekening van het proces-verbaal inzake het beslag, zonder meer van toepassing blijven.

INTEGRITEIT EN VERTROUWELIJKHEID DATA – De voor het beslag bevoegde ambtenaar moet steeds de passende technische middelen aanwenden bij de inbeslagname en de latere bewaring ter griffie van de data om de vertrouwelijkheid en integriteit van de gegevens te garanderen.[105] De wetgever stelt die vage beveiligingseis voorop in art. 39bis B.Sv, maar zonder verdere specificaties m.b.t. die technische middelen.[106] Vanuit dezelfde bekommernis moet de kopiëring plaatsvinden op dragers van de overheid. Enkel in spoedeisende gevallen of omwille van technische vereisten kan de kopiëring ook op dragers van de personen die gerechtigd zijn om het onderzochte IT-systeem te gebruiken. Ook de bevoegdheid om de toegang tot de originele data en eventuele kopieën daarvan te verhinderen, opnieuw door aanwending van de passende technische hulpmiddelen, is op de eerste plaats gericht op het verzekeren van de integriteit van het bewijs[107] en vormt een alternatief voor de klassieke verzegeling overeenkomstig art. 38 B.Sv. Daar art. 39bis B.Sv geen afwijking voorziet, gelden de voorschriften van het klassieke beslag ter verzekering van de integriteit van het bewijs in principe ook voor het databeslag. Op grond van het proportionaliteitsbeginsel dient het beslag zo beperkt mogelijk te blijven, ook een databeslag.[108] Gelet op de wijze van verzekering van de integriteit van het bewijs, is de keuze tussen de verschillende beslagbevoegdheden echter niet zo evident.

---

104 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 21.

105 Art. 39bis §6 B.Sv

106 Een voorbeeld van een nuttig technisch middel ter verzekering van de integriteit van het verzamelde digitale bewijs is het gebruik van hashwaardes. De hashwaarde van een bestand is als het ware een unieke code van dat bestand. Die waarde kan berekend worden op het ogenblik van de inbeslagname. Bij een later gebruik van het bestand als bewijsmateriaal voor de rechter ten gronde kan de hashwaarde van het bestand opnieuw worden berekend. Een gelijke hashwaarde geeft aan dat het bestand in tussentijd niet werd bewerkt. Zie hierover uitgebreid: J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 190-192.

107 J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 186.

108 Verslag namens de commissie, *Parl. St.* Kamer 1999-2000, nr. 50K0213/004, 90.

Het zal bijvoorbeeld vaak aangewezen zijn de volledige harde schijf te kopiëren om de integriteit en betrouwbaarheid van de data te vrijwaren.[109] Vanuit diezelfde zorg kan ook de inbeslagname van het volledige materiaal noodzakelijk zijn, omdat de aansluiting op andere hardware de opgeslagen gegevens kan wijzigen.[110] In bepaalde omstandigheden is een ruim beslag op materiaal dan weer niet wenselijk gelet op de nefaste economische weerslag ervan. Zo zal een bedrijf erg lijden onder een ruim beslag op informatiesystemen.[111] Ook is het denkbaar dat een klassiek beslag of forensische kopie niet tot de mogelijkheden behoort gelet op de omvang van de gegevens of wegens tijdsgebrek. De systemen zullen dan rechtstreeks worden doorzocht (*live forensics*). Bovendien kan het zijn dat om technische redenen een forensische kopie slechts stukken informatie oplevert. Dit is afhankelijk van het type van opslag van gegevens. In dat geval kan een *chip off* (het fysiek uit de machine verwijderen van een flashgeheugenchip[112]) een vollediger beeld opleveren. Zo een *chip off* kan achteraf niet meer volledig opnieuw worden uitgevoerd. Zowel in het geval van *live forensics* als in het geval van een *chip off* is een duidelijke verslaggeving en documentatie van het gevoerde onderzoek zeer belangrijk om de integriteit van het verkregen bewijs te verzekeren.

AANKOMEND RECHT BELGIË: BEVRIEZING – Volledigheidshalve voegen we hier nog aan toe dat België, volgens een aankondiging van de regering, weldra na art. 39bis B.Sv artikelen zou invoeren die een procedure bevatten voor de snelle bevriezing van gegevens op verzoek van een derde staat, in uitvoering van het Cybercrime-verdrag van 2001.

2.1.3. Netwerkzoeking

VAN COMPUTER NAAR VERBONDEN COMPUTERS – Een van de – in theorie – belangrijkste aanpalende bevoegdheden is om een onderzoek in een computer, dat plaatsvindt in het kader van een doorzoeking, uit te kunnen breiden tot met die computer verbonden computers. Deze bevoegdheid is in Nederland bij de Wet computercriminaliteit ingevoerd (en

---

109 P. DE HERT en G. LICHTENSTEIN, 'Huiszoeking en beslag in geautomatiseerde omgevingen', in M. BOCKSTAELE (ed), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 62.

110 Verslag namens de commissie, *Parl. St.* Kamer 1999-2000, nr. 50K0213/004, 45.

111 P. DE HERT en G. LICHTENSTEIN, 'Huiszoeking en beslag in geautomatiseerde omgevingen', in M. BOCKSTAELE (ed), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 62.

112 Flashgeheugen is niet-vluchtig (extern) geheugen, d.w.z. dat het data behoudt als het toestel wordt uitgeschakeld.

in 2006 geherformuleerd maar niet inhoudelijk herzien). Artikel 125j Nl.Sv bepaalt dat een doorzoeking, vanaf de plaats waar de doorzoeking plaatsvindt, kan worden voortgezet in een elders aanwezig computersysteem, mits de personen die op de plek van doorzoeking wonen, plegen te werken of te verblijven, met toestemming van de rechthebbende tot een dergelijke computer toegang hebben.

UITDRUKKELIJKE BEPERKINGEN – In de wat omslachtige formulering van 125j Nl.Sv zitten twee beperkingen, ook het dubbelebandcriterium genoemd.[113] Enerzijds vereist ze een feitelijke band tussen de persoon en de locatie waar de doorzoeking plaatsvindt. De persoon moet gewoonlijk op deze locatie verblijven, dus een netwerkzoeking is niet mogelijk vanaf de laptop van een toevallige bezoeker of de smartphone van een schoonmaker. Anderzijds moet er ook een juridische band (geautoriseerde toegang) zijn tussen de persoon en de computer (of delen daarvan) elders. Een netwerkzoeking mag zich dus niet uitstrekken tot door de verdachte gehackte computers. België schrijft deze tweede beperking uitdrukkelijk in art. 88ter §2 B.Sv[114], maar het is veel minder duidelijk of art. 88ter B.Sv zoals art. 125j Nl.Sv ook een band tussen de persoon en de plaats vereist. Doordat het zoekingsbevel van de onderzoeksrechter centraal staat en dat bevel het voorwerp van de zoeking strikt moet omschrijven, lijkt het onwaarschijnlijk dat het zou kunnen slaan op aangetroffen computersystemen van toevallige bezoekers. Het zal meestal moeilijk aan te nemen vallen dat het bevel die systemen tot voorwerp had. Een aanvullende voorwaarde is dat het onderzoek in het aangesloten computersysteem redelijkerwijs nodig is voor de waarheidsvinding, en, voor België, een expliciete subsidiariteitseis.[115] De ambtenaar[116] zal dus niet zomaar elke netwerkverbinding kunnen onderzoeken, maar eerst moeten bepalen of het redelijkerwijs aannemelijk

---

113 *Kamerstukken II* 1989/90, 21 551, nr. 3, 27.

114 Art. 88ter §2 B.Sv: '*De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben*.'

115 In België verwoord met de dubbele eis in art. 88ter §1 B.Sv: '*indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking en indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan*.' In Nederland verwoord met de clausule: '*[onderzoek naar elders] opgeslagen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen*'.

116 Dat is naar Belgisch recht een afweging die de onderzoeksrechter moet maken wanneer hij zijn bevel uitschrijft.

is dat zich elders relevante gegevens bevinden.[117] Verder mogen alleen reeds opgeslagen gegevens in het externe werk worden gezocht en overgenomen: de bevoegdheid mag niet worden gebruikt om heimelijk de externe computer een tijd te monitoren op nieuwe binnenkomende gegevens. Toevallig binnenkomende gegevens mogen naar Nederlands recht wel als bijvangst worden gebruikt.[118] Dat ligt in België in principe moeilijker. Het opvangen van stromende gegevens die als private communicatie in aanmerking komen, maakt immers een tap uit. Zolang de nietigheidssanctie gold voor de tap, werd daarom in de praktijk gewerkt met dubbele bevelen voor dezelfde zoeking, namelijk een bevel voor de netwerkzoeking en één voor de tap.[119] Nu de nietigheidssanctie uit de tapwetgeving is verdwenen, valt te verwachten dat men hier in de praktijk soepeler mee zal omspringen.

NEDERLAND: GEEN GEGEVENSDRAGERS – Naast deze expliciet geformuleerde beperkingen, vallen ook enkele andere beperkingen op (naast de territoriale beperking, *infra*, 2.3). Ten eerste kan naar Nederlands recht alleen in externe computers worden gezocht, niet in externe gegevensdragers. Naar de stand van de techniek begin jaren '90 zal de wetgever hebben geoordeeld dat met een computer verbonden externe gegevensdragers zich altijd wel in de ruimte van de doorzoeking zullen bevinden. Inmiddels zijn externe harde schijven en draadloze verbindingen echter gemeengoed geworden. Het is dan ook denkbaar dat iemand gegevens op een externe schijf buiten in een belendend pand opslaat die via WiFi of doorgetrokken kabel verbonden is met de computer. Hoewel dit een theoretisch voorbeeld is, lijkt het niet bij de systematiek van het computeronderzoek te passen dat externe, via het netwerk toegankelijke elektronische gegevensdragers niet binnen het bereik van een netwerkzoeking vallen. De Belgische bepaling laat uitbreiding toe '*naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt*', wat voornoemde situaties wel dekt.

NIET VANAF POLITIEKANTOOR – Ten tweede kan de bevoegdheid in Nederland alleen worden ingezet tijdens een doorzoeking en ter plekke wor-

---

117 In de praktijk zal zo'n afweging niet veel voorstellen, althans het valt achteraf nauwelijks vast te stellen of een onderzoek niet redelijkerwijs nodig kon worden gevonden voor de waarheidsvinding; zie F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 4.3.

118 *Ibid*., art. 125j, aant. 4.2.

119 P. VAN LINTHOUT, J. KERKHOFS, 'Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel', *T.Strafr.* 2008, 93; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 290-295.

den uitgeoefend. Dat blijkt uit de zinsnede '*kan **vanaf de plaats waar de doorzoeking plaatsvindt**, in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan*' (art. 125j Nl.Sv, nadruk toegevoegd). Het onderzoek kan dus niet vanaf het politiebureau plaatsvinden, ook niet als dat nog gelijktijdig met de doorzoeking zou zijn.[120]

Dat levert voor de praktijk een enorme beperking op. De politie onderzoekt computers bij een doorzoeking veelal niet ter plekke, maar neemt ze mee of maakt een één-op-één-kopie van de harde schijf. Tegenwoordig gebeurt dat steeds vaker, wanneer de computer tijdens een doorzoeking aan staat, met behoud van stroom (met speciale apparatuur). Zo voorkomt men dat gegevens in het tijdelijke geheugen verdwijnen door het uit- en later weer aanzetten van de computer. Die tijdelijke gegevens kunnen vooral ook netwerkverbindingen betreffen, zoals wachtwoorden waarmee is ingelogd op een externe mailserver. Indien dergelijke netwerkverbindingen echter, bij onderzoek op het bureau, worden aangetroffen, mogen ze niet meer op basis van artikel 125j Nl.Sv worden gebruikt voor onderzoek in de systemen elders.[121] Het lijkt, gezien de manier waarop computeronderzoek in het kader van een doorzoeking veelal plaatsvindt, ten minste te overwegen om artikel 125j Nl.Sv uit te breiden tot situaties '*bij of terstond na*' een doorzoeking (vergelijkbaar met de steunbevoegdheid van het ontsleutelbevel, die mogelijk is '*bij of terstond na de toepassing van*' het vorderen van gegevens, zie art. 126nh/uh/zp Nl.Sv). Dat vergt dan wel een herformulering van het artikel: '*vanaf de plaats waar de doorzoeking plaatsvindt*' zou moeten worden vervangen door iets als '*vanaf een geautomatiseerd werk dat is onderzocht in het kader van een doorzoeking*', en de consequenties ervan zouden nog nader moeten worden onderzocht.

De huidige Belgische tekst is dubbelzinniger en laat misschien nu al netwerkzoeking vanaf meegenomen computers toe. Art. 88ter B.Sv vangt immers aan als volgt: '*Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, kan deze zoeking worden uitgebreid naar een informaticasysteem of deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt:…*' In België bestaat er eerder discussie over de vraag of de netwerkzoeking ook kan plaatsvinden vanaf de systemen van de

---

120 CHR.H. VAN DIJK EN J.M.J. KELTJENS, *Computercriminaliteit*, Zwolle, Tjeenk Willink, 1995, 235-236.

121 En ook als de doorzoeking op afstand (*infra*,. 2.2), zou worden ingevoerd, is het de vraag of die bepaling een dergelijk onderzoek zou toestaan; het is niet evident dat het systeem elders valt onder een '*een geautomatiseerd werk dat bij de verdachte in gebruik is*'. Bovendien is die bevoegdheid veel beperkter inzetbaar dan alle gevallen waarvoor een doorzoeking kan plaatsvinden.

overheid zelf. Kerkhofs en Van Linthout menen van wel, omdat ook de verdachte doorgaans vanop elke computer ter wereld toegang kan nemen tot zijn online accounts zoals zijn webmailaccount[122]. Dit lijkt echter in strijd met de nog erg 'plaatsgebonden' bewoordingen van de Belgische wet. Die beperking van de wet heeft nochtans een averechts effect. Wanneer opsporingsinstanties bv. gericht willen zoeken in een online account van een persoon (bv. de verdachte) zouden zij dit naar huidig recht via een huiszoeking of fouillering moeten doen, ook al zijn die in principe niet noodzakelijk. Zij zouden immers eerst een informaticazoeking moeten opzetten vooraleer zij kunnen overgaan tot de netwerkzoeking. Een rechtstreekse toegangsmogelijkheid via de computers van de overheid verdient de voorkeur, want die is minder indringend.[123] De wet zal waarschijnlijk in het najaar van 2016 veranderen en dan regelt men het best ondubbelzinnig. Uit het persbericht van de regering blijkt dat nog steeds wordt uitgegaan van een *uitbreiding van een zoeking tot een informaticasysteem dat verbonden is aan een informaticasysteem dat het onderwerp is van de eerste maatregel.* Het ontwerp lijkt nochtans te werken met een restcategorie, namelijk '*elke andere niet-heimelijke zoeking in een informaticasysteem*', waarvoor de onderzoeksrechter bevoegd is. Die restcategorie kan de leemte in de wetgeving opvangen. Wel ontstaat hierdoor een vreemd onderscheid. De plaats van waaruit de doorzoeking vanop afstand gebeurt, bepaalt immers welke instantie bevoegd is. De procureur des Konings is zo bevoegd voor de openlijke uitbreiding van de zoeking ter plaatse terwijl enkel de onderzoeksrechter bevoegd is voor de openlijke zoeking in hetzelfde systeem vanaf de systemen van de overheid.

ENKEL DOORZOEKING – Ten derde is de netwerkzoeking in Nederland beperkt tot situaties van een doorzoeking.[124] In Nederland vallen andere situaties waarbij een computer in beslag is genomen en wordt onderzocht

---

122 J. KERKHOFS en P. VAN LINTHOUT, 'Cybercriminaliteit doorgelicht', *T.Strafr.* 2008, afl. 4, (179) 199.

123 De persoon op wie de zoeking betrekking heeft, moet hiervan wel in kennis worden gesteld en zou daarbij bovendien best aanwezig zijn om de rechten van verdediging te waarborgen. (C. CONINGS en J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerr.* 2013, afl. 1, (23) 31.)

124 Volgens F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 4.1, is de netwerkzoeking beperkt tot de doorzoeking uit de commune strafvordering; toepassing bij een doorzoeking ex art. 49 WWM zou dus niet mogelijk zijn. Dit volgt echter niet uit de formulering van art. 125j, noch uit art. 125i Nl.Sv (dat onderzoek van computers tijdens een doorzoeking ter inbeslagneming onverlet laat).

(zie alle situaties *infra*, 2.4) erbuiten.[125] Hiervoor is bewust gekozen in de Wet computercriminaliteit: een voorstel van Harteveld en Knigge om de netwerkzoeking ook mogelijk te maken bij andere situaties dan (wat toen nog heette) een huiszoeking, werd door de minister '*resoluut van de hand gewezen*',[126] met de volgende argumentatie: '*Het gaat om een ingrijpende bevoegdheid. Het zou niet juist zijn deze ter gelegenheid van elke inbeslagneming te kunnen uitoefenen. Het onderzoek in netwerken dient aan dezelfde waarborgen te worden onderworpen als een huiszoeking.*'[127] Voor dat standpunt viel, anno 1992, veel te zeggen. De doorzoeking was een 'huiszoeking' en computers stonden meestal bij verdachten in huis, zodat deze situatie verreweg het meest zou voorkomen. Inmiddels is het juridische landschap veranderd, nu sinds 2000 de doorzoeking in meer typen plaatsen, onder lagere voorwaarden, mogelijk is dan de huiszoeking. Ook het computerlandschap ziet er aanzienlijk anders uit: computers zijn mobiel geworden en dus lang niet altijd meer gebonden aan een plaats van doorzoeking. Daar komt bij dat ook gegevensopslag nu fundamenteel anders plaatsvindt dan in de jaren 1990: destijds was plaatselijke opslag (op de computer zelf, op schijfjes in de bureaula) de standaard, en externe gegevensopslag via een netwerkverbinding een (nog tamelijk zeldzame) uitzondering. Externe gegevensopslag, vooral in de cloud, lijkt nu meer regel dan uitzondering. Zelfs zal de gebruiker niet eens altijd doorhebben waar gegevens zijn opgeslagen, op de harde schijf of extern, omdat de gegevens in beide gevallen even eenvoudig oproepbaar zijn. Met andere woorden: gegevensopslag ter plaatse en externe gegevensopslag zijn volstrekt functioneel equivalent geworden. En hoewel de opslag soms redundant gebeurt (zowel op de harde schijf als in de cloud), gaat het steeds vaker ook om communicerende vaten: wat in de cloud staat, hoeft niet meer op de harde schijf te worden opgeslagen. Voor de strafvordering betekent dit dat 'lokaal computeronderzoek' steeds minder betekenis krijgt: men zal de gegevens steeds meer uit externe opslagbronnen moeten binnenhalen. Dat is een van de redenen voor invoering van een doorzoeking op afstand. Maar het moet ook een reden zijn voor heroverweging van artikel 125j Nl.Sv: juist dat artikel zou een belangrijk hulpmiddel moeten zijn om gegevensverlies te voorkomen nu gegevens steeds vaker extern worden opgeslagen. Naar Belgisch recht is dit geen probleem. Uit de voorbereidende werken blijkt duidelijk dat de netwerk-

125 WIEMANS, *Ibid*.

126 CHR.H. VAN DIJK EN J.M.J. KELTJENS, *Computercriminaliteit*, Zwolle, Tjeenk Willink, 1995, 235.

127 *Kamerstukken 1991/92*, 21 551, nr. 11, 11.

zoeking kan volgen op eender welke '*informaticazoeking*' en ze dus niet noodzakelijk in het verlengde ligt van de huiszoeking.[128] De netwerkzoeking kan dus ook volgen op een doorzoeking van een informaticasysteem dat speurders tijdens een fouillering aantreffen, weliswaar enkel op bevel van de onderzoeksrechter.

CONSOLIDATIE WENSELIJK – In dat licht valt te overwegen om de netwerkzoeking niet alleen aan de doorzoeking te verbinden, maar aan alle vormen van computeronderzoek. Het discussiestuk in het kader van Modernisering Sv werpt deze vraag ook op, echter zonder nadere overwegingen pro of contra.[129] De veranderingen in het computerlandschap zijn dermate groot dat de vraag naar uitbreiding van 125j Nl.Sv met andere situaties zou moeten worden beantwoord met een voorzichtig '*ja*'. '*Ja*,' omdat computeronderzoek anders steeds inhoudslozer zal worden; voorzichtig, omdat de consequenties ervan wel nader in kaart moeten worden gebracht, en er ook nadere voorwaarden nodig zijn, vergelijkbaar met voorwaarden die nodig zijn voor onderzoek aan inbeslaggenomen computers (*infra*, 2.4). Ter gedachtebepaling wijzen we op de mogelijkheid die de federale Australische wetgeving biedt, als een voorbeeld van een regeling die wel erg ver gaat:

'*Operating seized electronic equipment*

(1) This section applies to electronic equipment seized under this Part (…).

(2) The electronic equipment may be operated at any location after it has been seized or moved, for the purpose of determining whether data that is evidential material is held on or accessible from the electronic equipment, and obtaining access to such data.

(3) The data referred to in subsection (2) includes, but is not limited to, the following:

---

128 Verslag namens de commissie, *Parl. St.* 2000-01, nr. 50K213/011, 8. Via een amendement werd de zinsnede '*in het kader van de huiszoeking*' uit het artikel weggelaten: '*Dit amendement strekt ertoe de bevoegdheid voor de uitbreiding van de zoeking in een informaticasysteem in lijn te brengen met de technologische realiteit. In netwerk verbonden computers worden immers niet enkel gehanteerd als in gebouwen opgestelde systemen, maar meer en meer worden vormen van mobiele telecommunicatie en – dataverkeer ontwikkeld. De realiteit van de draagbare computers moet derhalve in rekening worden gebracht ten einde te vermijden dat het ontwerp in dit opzicht nu reeds achterhaald is.*'

129 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 52-53.

> *(a) data held on the electronic equipment, including data held on the electronic equipment when operated under this section that was not held on the electronic equipment at the time the electronic equipment was seized;*
> *(b)* ***data not held on the electronic equipment but accessible by using it, including data that was not accessible at the time the electronic equipment was seized.***
> *(4) If the electronic equipment was seized under a warrant (…), the electronic equipment may be operated before or after the expiry of the warrant. (…)*'[130]

Het onderzoeken van gegevens die nog niet toegankelijk waren op het tijdstip van inbeslagneming (s. 3ZQV(3)(b)), lijkt duidelijk een stap te ver. Ook ontbreekt een beperking tot rechtmatig toegankelijke gegevens. De hoofdinsteek van de bepaling, namelijk dat het gaat om gegevens die toegankelijk zijn op of vanuit het apparaat, is echter wel interessant en het overwegen waard – en sluit verrassend goed aan op een van de uitgangspunten van de Commissie computercriminaliteit, die in 1987 het '*beschikbaarheidscriterium*' hanteerde.[131] Dat criterium is in de literatuur bekritiseerd als te ruim en onbepaald[132] en is door de wetgever ook niet overgenomen (die in plaats daarvan het dubbelebandcriterium introduceerde). Misschien is de tijd nu rijp om het beschikbaarheidscriterium alsnog te overwegen bij computeronderzoek, in meer gevallen dan alleen de doorzoeking. De wetgever kan de onbepaaldheid van het beschikbaarheidscriterium wegnemen door nadere voorwaarden te stellen aan de gevallen waarin gegevens voor de opsporingsautoriteiten vanuit onderzochte computers beschikbaar moeten worden geacht.

Discussiepunt: de netwerkzoeking moet mogelijk worden in alle gevallen waarin computers in het kader van de opsporing onderzocht worden, onder nader te bepalen voorwaarden.

BESCHERMING LOS VAN PLAATS AANTREFFEN – Naast beperkingen kent artikel 125j Nl.Sv echter ook een te ruim toepassingsbereik. Dit komt door

---

130 Section 3ZQV Crimes Act 1914 (Cth) (nadruk in (3)(b) toegevoegd).

131 COMMISSIE COMPUTERCRIMINALITEIT, *Informatietechniek en strafrecht*, 's-Gravenhage, Staatsuitgeverij, 1987, 88-89 (waarbij het ging om beschikbaarheid tijdens de huiszoeking, maar de argumentatie van de commissie laat zich ook toepassen op andere situaties waarin computers worden onderzocht).

132 F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 3; CHR.H. VAN DIJK EN J.M.J. KELTJENS, *Computercriminaliteit*, Zwolle, Tjeenk Willink, 1995, met verwijzingen.

de in 2000 geïntroduceerde systematiek van de doorzoeking. Waar artikel 125j Nl.Sv bij de introductie ervan gekoppeld was aan een *huis*zoeking, is deze in 2000 uitgebreid tot alle gevallen van een doorzoeking. Wat is nu de bescherming van een computer in een woning die rechtmatig van elders raadpleegbaar is via een netwerkzoeking? De plaats vanwaar de zoeking gebeurt, hoeft geen woning te zijn: een doorzoeking kan immers ook plaatsvinden op elke plaats met uitzondering van een woning door de (hulp)officier van justitie (art. 96c Nl.Sv), of in voertuigen door opsporingsambtenaren (art. 96b Nl.Sv). Met de komst van mobiele computers (waaronder smartphones) en draadloze verbindingen zal een in een auto of kantoor aangetroffen computer vaak een rechtmatige verbinding hebben met de 'huis-computer' van de gebruiker. Met de opkomst van domotica, zoals het via Internet regelen van de verwarming, zal dat alleen maar toenemen. Dat betekent dat een computer in een woning alleen onder relatief zware voorwaarden kan worden doorzocht als deze bij doorzoeking van de woning wordt onderzocht, maar onder lichte voorwaarden als deze via een netwerkzoeking vanuit een in een doorzochte auto aangetroffen smartphone plaatsvindt. Dat verschil in beschermingsniveau lijkt geen bewuste keuze van de wetgever, maar meer een neveneffect van de op verschillende tijdstippen geïntroduceerde regelingen voor de netwerkzoeking (in 1993) en de doorzoeking (in 2000), waarbij de samenhang tussen beide niet expliciet onder ogen is gezien. Als men immers de redenering van de wetgever bij de introductie van artikel 125j Nl.Sv volgt, dient het '*onderzoek in netwerken (…) aan dezelfde waarborgen te worden onderworpen als een huiszoeking*'.[133] Nu kan men betogen dat dat uitgangspunt is losgelaten in 2000, maar het lijkt toch niet de bedoeling dat het onderzoek in netwerken nu aan dezelfde waarborgen moet worden onderworpen als een doorzoeking van een vervoermiddel.[134] Artikel 125j Nl.Sv zou in dat licht in elk geval moeten worden aangepast. Of de waarborgen dan naar het niveau van de huiszoeking (art. 97/110 Nl.Sv) of naar dat van de doorzoeking van andere plaatsen (art. 96c Nl.Sv) wordt getild, lijkt een punt van nadere discussie. Opnieuw rijst dit probleem in het Belgische recht niet, omdat art. 88ter B.Sv hoe dan ook het bevel van de onderzoeksrechter voorop stelt voor de netwerkzoeking. De voor het najaar 2016 geplande wetswijziging kent echter ook een zekere netwerkzoekingsbevoegdheid toe aan de procureur des Konings, zodat

133 Zie noot 127.

134 Zie ook F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 5, betogend dat de grammaticale interpretatie van art. 125j Nl.Sv de ratio van het getrapte systeem van de doorzoekingsbevoegdheid geweld aandoet.

het probleem in de toekomst misschien wel zal opduiken. Hopelijk houdt de Belgische wetgever er rekening mee.

2.2. Heimelijke doorzoeking van computers op afstand

POLITIE-'HACK' – Onderzoek van computers kan niet alleen gebeuren bij een fysieke doorzoeking van een plaats, maar ook op afstand via een computernetwerk. Voor één specifieke vorm heeft de wetgever dat mogelijk gemaakt, wat we 'netwerkzoeking' noemen (*supra*, 2.1.3). Er is echter toenemende behoefte om ook zelfstandig, zeg maar vanaf het politiebureau (zij het best met enige maskering van die locatie), een onderzoek op afstand te kunnen doen in computers. Populair gezegd: de politie moet de computers van verdachten kunnen 'hacken'. In het Nederlandse debat duikt vaak de term 'terughacken' op[135], maar dat is ongelukkig, omdat het hoegenaamd niet hoeft te gaan om opsporing van hackers: het kan elk type misdrijf betreffen. Hoewel 'hacken' een voor de burger duidelijke omschrijving is van het type activiteit, past deze aanduiding niet echt bij opsporingsinstanties, omdat het – als er een wettelijke basis voor is – voor hen niet gaat om het *onrechtmatig* binnendringen in computers. Daarom is de term 'doorzoeking van computers op afstand', hoewel omslachtig, passender. Men kan ook de in Duitsland veelgebruikte term 'heimelijke online-doorzoeking' of 'heimelijke netwerkzoeking' (*verdeckte online Durchsuchung*) gebruiken. Momenteel kiest de Nederlandse wetgever voor de term 'onderzoek in een geautomatiseerd werk', die ons te ruim lijkt. België lijkt de term 'heimelijke zoeking in informaticasystemen' te gaan hanteren. Dat is een betere terminologie, omdat de heimelijkheid van het binnendringen en de bijhorende zoeking inderdaad wezenlijk zijn; de technische manier waarop is niet beslissend (behalve voor integriteit van het systeem en/of de gegevens bij onoordeelkundig binnendringen).

HUIDIG RECHT: GEEN DUIDELIJKE GRONDSLAG – Op dit moment bestaat er noch in Nederland, noch in België een wettelijke basis voor een heimelijke computerdoorzoeking op afstand, maar beide landen hebben concrete plannen om daar iets aan te veranderen. Men kan proberen de inkijkopera-

[135] In navolging van Merel Koning, die een veelbesproken scriptie publiceerde getiteld '*Terug-hacken als opsporingsmethode*' (https://merelkoning.nl/wp-content uploads/2012/06/Terughacken-als-opsporingsmethode-scriptie-Merel-Koning-september-2011-nn.pdf, geraadpleegd 1 maart 2016). Zie ook M.E. KONING, 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *P&I* 2012(2), 46-52.

tie (art. 126k/r/zd Nl.Sv, art. 46quinquies B.Sv) zodanig te interpreteren dat dit eronder zou vallen.[136] Dat is nogal gekunsteld, maar de wettekst van de inkijkoperatie lijkt het niet uit te sluiten. Het gaat daar om het betreden of met een technisch hulpmiddel benaderen van een 'besloten' (Nederland) of 'private' (België) plaats die geen woning is[137] om deze plaats op te nemen, sporen veilig te stellen of een peilbaken of bewegingsmelder[138] te plaatsen. De Nederlandse wetsgeschiedenis biedt echter geen enkel aanknopingspunt voor deze interpretatie: binnendringen in computers komt simpelweg nergens voor bij de voorbeelden van deze bevoegdheid. Daar komt bij dat de Nederlandse wetgever zich wel degelijk bewust was van de techniek en noodzaak van het binnendringen in computers door de overheid, nu tezelfdertijd als de Wet bijzondere opsporingsbevoegdheden (Wet BOB) ook de Wet op de inlichtingen- en veiligheidsdiensten 2002 werd behandeld. Daarin kregen de inlichtingen- en veiligheidsdiensten wel een expliciete bevoegdheid om in computers binnen te dringen (art. 24 Wiv 2002). Als de wetgever had gewild dat ook justitie dit zou mogen, dan had hij dat destijds met zoveel woorden moeten aangegeven, want expliciete vastlegging van bevoegdheden was net een belangrijke doelstelling van de Wet BOB.[139]. In België had de regering tijdens de parlementaire voorbereiding van de Wet Informaticacriminaliteit, en in het bijzonder bij toelichting over de openlijke netwerkzoeking, uitdrukkelijk gezegd dat het niet de bedoeling was dat de politie heimelijk computers zou kunnen hacken[140]. Omdat de Belgische wetgeving inzake Bijzondere Opsporingsmethoden, die de inkijkoperatie in België invoerde, van latere datum is[141], zou men

136 Zoals J.L.M. BOEK, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB* 2000, 589-593 betoogt. Zie ook C. CONINGS, 'Statusupdate: Belgische opsporing – voelt zich #verward bij het speuren in sociale media' in E. LIEVENS, E. WAUTERS, P. VALCKE (eds), *Sociale media anno 2015. Actuele juridische aspecten*, Antwerpen, Intersentia, 2015, 282-287; C. CONINGS en J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerr.* 2013, afl. 1, (23) 32.

137 In België ook geen '*aanhorigheid*' van de woning.

138 Een technisch hulpmiddel in de zin van het Belgische wetboek is een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert.

139 B.J. KOOPS & Y. BURUMA, 'Formeel strafrecht en ICT', in: B.J. KOOPS (red.), *Strafrecht en ICT*, 2e druk, Den Haag, Sdu 2007, 118.

140 In de parlementaire voorbereidingen lezen we in dat verband: '*Het is evenmin toegelaten dat de overheidsdiensten bijvoorbeeld via eigen informaticasystemen binnen zouden dringen in andere systemen die niet openstaan voor het publiek en die ervan verdacht worden aangewend te worden voor criminele doeleinden : « hacking » door de overheid als nieuwe, geheime bewakingsmaatregel is derhalve verboden.*' (MvT, *Parl. St. Kamer* 1999-2000, nr. 50K0213/001, 23.)

141 Art.6 wet 27 december 2005, in werking getreden op 30 december 2005.

kunnen zeggen die latere wet met enige goede wil zou kunnen worden gelezen als de introductie van de bevoegdheid tot het heimelijk betreden van '*digitale plaatsen*', die dan per definitie geen woning zijn. Niets wijst er echter op dat de wetgever een dergelijke evolutieve interpretatie van 'plaats' wenste. Bovendien krijgen ook in België de inlichtingendiensten wel uitdrukkelijk de bevoegdheid om zich heimelijk toegang te verschaffen tot informaticasystemen. De wet op de Bijzondere Inlichtingenmethoden voorzag dit in art. 18/16, waarbij de wetgever uitdrukkelijk verwees naar het Nederlandse art. 24 Wiv als inspiratiebron[142]. Naar aanleiding daarvan, bleek dat er plannen waren om ook de Bijzondere Opsporingsmethoden aan te passen[143]. Kerkhofs en Van Linthout lijken aan te geven dat het inbreken in sites of webaccounts zonder toegangscodes of met gebruik van hackertools bijgevolg verboden is. Het zou volgens hen echter wel mogelijk zijn op grond van een netwerkzoekingsbevel (*supra*, 2.1.3) en met behulp van een login en paswoord heimelijk toegang te nemen tot van een site of een account.[144] Die visie botst echter met de al aangehaalde zinsnede uit de voorbereidende werken dat '*"hacking" door de overheid als nieuwe,*

---

142 *'Deze bepaling is geïnspireerd op artikel 24 van de Nederlandse wet. Zij machtigt de inlichtingen- en veiligheidsdiensten om toegang te krijgen tot informaticasystemen met uitzondering van de informaticasystemen van de overheid. Een dergelijke toegang wordt momenteel bestraft door de artikelen 210bis, 504quater, 550bis en 550ter van het Strafwetboek, ingevoegd door de wet van 28 november 2000 inzake informaticacriminaliteit. Informaticasystemen vormen middelen tot communicatie en gegevensopslag die steeds vaker door de radicale en terroristische milieus worden gebruikt. Deze systemen kunnen ook het voornaamste doelwit zijn van spionage.*
(Wetsvoorstel betreffende de methoden voor het verzamelen van gegevens door de inlichtingen-en veiligheidsdiensten*, Parl.St. Senaat*, 2008-09, nr. 4-1053/1, 54.

143 Bijlage 1 bij document 52-2128/007: Hoorzitting over de evaluatie van de wetgeving betreffende terrorismemisdrijven – hierbij wordt ook de BOM-wet van 6 januari 2003, zoals gewijzigd bij wet van 27/12/2005 en van 16/01/2009 besproken: '*[Een werkgroep van magistraten bereidt met de Minister aanpassingen aan de bijzondere opsporingsmethoden voor]. Er wordt bijvoorbeeld gedacht aan:*
een wettelijke regeling van de opsporingsmethode waarbij de gerechtelijke autoriteiten de politiediensten kunnen machtigen buiten medeweten van de betrokkenen, al dan niet met behulp van technische middelen, valse signalen, valse sleutels of valse hoedanigheden: toegang te krijgen tot een informaticasysteem; er de beveiliging van op te heffen; er technische voorzieningen in aan te brengen teneinde de door het informaticasysteem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en de te decoderen; er de door het informaticasysteem relevante opgeslagen, verwerkte of doorgestuurde gegevens op eender welke manier van over te nemen'.

144 J. KERKHOFS en P. VAN LINTHOUT, 'Cybercriminaliteit doorgelicht*', T.Strafr.* 2008, afl. 4, (179) 199; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 267 en 275. Dat zou volgens de auteurs ook mogelijk zijn vanaf de computers van de overheid.

geheime bewakingsmaatregel" verboden is (*supra*, voetnoot 140). Of opsporingsinstanties de logingegevens al dan niet bezitten is echter geen criterium om uit te maken of er sprake is van strafbaar hacken (art. 550bis §1 Sw). Op grond van de netwerkzoeking zijn opsporingsinstanties onder bepaalde voorwaarden gerechtigd om toegang te nemen tot informaticasystemen op afstand die in verbinding staan met een systeem dat het voorwerp uitmaakt van een informaticazoeking. Onder die voorwaarden maken zij zich bijgevolg niet schuldig aan hacking, ook al wordt eventueel een beveiliging doorbroken. Bij de zinsnede in de voorbereidende werken lag de nadruk o.i. dan ook op het begrip '*geheime*'. Het was niet de bedoeling van de wetgever om via de netwerkzoeking het heimelijk binnendringen in informaticasystemen toe te laten. Bovendien moet de onderzoeksrechter de verantwoordelijke van het informaticasysteem op de hoogte brengen van de uitgevoerde maatregel (*supra*, 2.1.2.). Die informatieplicht is vergelijkbaar met de informatieplicht in het kader van het databeslag, waarbij de wetgever uitdrukkelijk stelt dat die duidelijk moet maken dat het niet gaat om een geheime maatregel.[145] Dat de netwerkzoeking heimelijk zou kunnen worden toegepast, lijkt ons om de hier opgesomde redenen dan ook moeilijk verdedigbaar. Volgens vaste rechtspraak van het EHRM is een duidelijke wettelijke grondslag met voldoende waarborgen een vereiste in het kader van heimelijke, indringende bewijsvergaring. Art. 88ter B.Sv vormt daarvoor dan ook geen afdoende basis.[146]

---

145 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 21; zie ook P. DE HERT en G. LICHTENSTEIN, 'Huiszoeking en beslag in geautomatiseerde omgevingen', in M. BOCKSTAELE (ed), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 66. J. KERKHOFS en P. VAN LINTHOUT stellen dat de notificatieplicht de heimelijke toepassing van de netwerkzoeking geenszins uitsluit. Ze wijzen daarbij op het feit dat de inkennisstelling enkel moet gebeuren indien de identiteit of woonplaats van de verantwoordelijke *redelijkerwijze* achterhaald kan worden, wat vaak niet het geval zal zijn omwille van de internationaliteit en anonimiteit die het Internet kenmerken. Verder halen de auteurs aan dat het voorschrift niet gepaard gaat met een termijn noch met een nietigheidssanctie. J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 267. O.i. wordt met deze argumenten geen aandacht besteed aan de wil van de wetgever die achter de vereiste inkenisstelling schuilgaat. Bovendien is de onmiddellijk inkennisstelling o.i. de regel en de uitgestelde inkennisstelling de uitzondering waarin de wetgever moet voorzien. Zie bv. art. 90 *novies* Sv m.b.t. de tapmaatregel.

146 C. CONINGS en J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerr.* 2013, afl. 1, (23) 31. Zie eveneens: D. DEWANDELEER, 'Misdrijven en strafonderzoek in de IT-context' in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2009-2010, 148.

(TELE)COMMUNICATIE – Ook in het kader van het onderzoek naar (tele)communicatie rijst de vraag naar de mogelijkheid tot het binnendringen in computers. In Nederland gelden afzonderlijke bevoegdheden voor het afluisteren van onmiddellijke (126l Nl.Sv) en middellijke communicatie (126m Nl. Sv). Beide bevoegdheden vallen naar Belgisch recht onder één en hetzelfde regime, namelijk dat van art. 90ter B.Sv. Bij direct afluisteren, gericht op het onderscheppen van onmiddellijke communicatie, mag justitie een besloten (of private) plaats of woning binnentreden om een technisch hulpmiddel te plaatsen om direct af te luisteren. Die bevoegdheid behelst naar onze mening ook de bevoegdheid om hardware-matig een technisch hulpmiddel op of in een computer te installeren. Het klassieke afluisteren van telefoongesprekken is natuurlijk vervangen door het legaal 'tappen' (meekijken, meeluisteren en registreren) van (tele)communicatie. Het technisch hulpmiddel kan er dus op gericht zijn zowel 'live gesprekken' als telecommunicatie die de computer in- of uitgaat te onderscheppen. Bij aftappen, gericht op het opnemen van middellijke communicatie[147], kan justitie niet alleen communicatie verkrijgen via de communicatieaanbieder, maar ook zelf met een technisch hulpmiddel middellijke communicatie opnemen. De wet sluit niet uit dat dit zou gebeuren door de computer van een verdachte te infecteren met een Trojaans paard of andere 'spyware', zodat justitie vervolgens via een netwerk rechtstreeks communicatie naar of van de computer kan opnemen. Volgens de Belgische preadviseurs rijst hier opnieuw de vraag naar de mogelijke evolutieve interpretatie van de bevoegdheid tot het binnendringen van private plaatsen uit art. 90ter B.Sv. Op grond van die interpretatie zou men inderdaad ook het private informaticasysteem kunnen binnendringen om er, al dan niet vanop afstand, software-matig een '*technisch hulpmiddel*' op te installeren. Het vergaren van gegevens moet zich alleszins beperken tot het opnemen van in- en uitgaande communicatie dan wel gesprekken in de nabijheid van de computer. De gegevens op de computer zelf mogen niet worden onderzocht, ook niet opgeslagen communicatie. Het gaat immers om 'opnemen' van communicatie, waarmee het onderscheppen tijdens het transport wordt bedoeld, en

147 De Nederlandse wet hanteert de term '*communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst*', waaronder zowel openbare als besloten communicatiediensten vallen en dus een ruimer begrip betreft dan de Telecommunicatiewet. We gebruiken hiervoor de term '*middellijke*' communicatie – communicatie die gebruikt maakt van een communicatiemiddel, ter onderscheiding van het '*live gesprek*', dat niet-middellijk oftewel onmiddellijk plaatsvindt. Ter vergelijking, de Belgische wet (art. 90ter, §1 B.Sv) heeft het over '*privé-communicatie*' voor de onmiddellijke en '*privételecommunicatie*' voor de middellijke.

niet het 'vastleggen' van communicatiegegevens. Ook art. 90ter B.Sv is ondubbelzinnig: '*privé-communicatie of -telecommunicatie, tijdens de overbrenging ervan, afluisteren, er kennis van nemen en opnemen*'. Deze vormen van het binnendringen in computers bieden dus geen basis voor een computer-doorzoeking op afstand. Onder het huidig recht valt het echter moeilijk te controleren of speurders die grens tussen communicatie die onderweg is en opgeslagen communicatie respecteren.

Daar de concrete Belgische tekstvoorstellen nog niet bekend waren op het moment van de redactie van dit preadvies, bestuderen we verder enkel het Nederlandse voorstel om te komen tot enkele tips voor de wetgevers in beide landen.

WETSVOORSTEL NEDERLAND.– Het in mei 2013 in consultatie gebrachte wetsontwerp computercriminaliteit III bevat een bevoegdheid om computers op afstand binnen te dringen. Eerst werd een nieuw artikel 125ja Nl.Sv ondergebracht in titel IV in de afdeling betreffende de doorzoeking ter vastlegging van gegevens, omdat het als vergelijkbaar werd gezien met een doorzoeking van plaatsen om gegevens vast te leggen.[148] De bevoegdheid was echter aanzienlijk ruimer dan een met een doorzoeking vergelijkbaar gegevensonderzoek: ze zou ook kunnen worden ingezet voor afluisteren en observatie, en bovendien heimelijk en voor een bepaalde periode. De Nederlandse Raad van State onderstreepte terecht dat de bevoegdheid veel meer het karakter heeft van de bijzondere opsporingsbevoegdheden (BOB), die heimelijk worden toegepast.

In het bij de Tweede Kamer ingediende wetsvoorstel computercriminaliteit III is de bevoegdheid (voorgesteld artikel 126nba) daarom ondergebracht bij de BOB in titel IVA (lees: vier-A).[149] Ook in diverse andere opzichten is het voorstel aangepast, dankzij de adviezen van vele instanties. In de kern gaat het wel nog steeds om een zeer ruime en ingrijpende bevoegdheid: het op afstand heimelijk binnendringen in computers om bepaalde onderzoekshandelingen te kunnen uitoefenen.

VOOR WELKE ONDERZOEKSHANDELINGEN? – Die doelhandelingen, limitatief opgesomd in lid 1, zijn de volgende.

---

148 Conceptwetsvoorstel computercriminaliteit III, mei 2013, http:// www. internetconsultatie.nl/computercriminaliteit.

149 Evenals in de andere BOB-titels V (georganiseerde misdaad, voorgesteld art. 126uba) en VB (terrorisme, voorgesteld art. 126zpa). We beperken ons hier verder tot de reguliere bevoegdheid van art. 126nba Nl.Sv.

a. De vaststelling van bepaalde kenmerken (vooral de identiteit of locatie) van de computer of gebruiker – een digitale variant van de inkijkoperatie.[150]
b. Het opnemen van zowel middellijke als onmiddellijke communicatie vertrouwelijke communicatie. Hier wordt het binnendringen van de computer ingezet als steunbevoegdheid voor aftappen (126m Nl.Sv), bijvoorbeeld door een functionaliteit die Skype-gesprekken onderschept, of direct afluisteren (126l Nl.Sv), bijvoorbeeld door een keylogger of het aanzetten van de microfoon van de computer of smartphone.
c. Stelselmatige observatie, waarbij het binnendringen als steunbevoegdheid dient voor observatie als geregeld in artikel 126g Nl.Sv Daarbij kan, in tegenstelling tot wat onder artikel 126g Nl.Sv mogelijk is, een technisch hulpmiddel ter observatie (in casu de op de binnengedrongen smartphone geïnstalleerde programmatuur) worden bevestigd op een persoon zonder diens toestemming. Daarbij kan het ook gaan om een heimelijk geïnstalleerde GPS-tracker, waarbij de bewegingen van de smartphone van de verdachte nauwkeurig in kaart kunnen worden gebracht.[151]
d. Het vastleggen van gegevens, zowel gegevens die in de computer zijn opgeslagen als gegevens die binnenkomen na het binnendringen tijdens de looptijd van het bevel.[152] Hoewel dit in eerste instantie enigszins lijkt op een functioneel equivalent van het inbeslagnemen of één-op-één kopiëren van de harde schijf bij een doorzoeking, gaat het om een veel ingrijpender bevoegdheid. Niet alleen vindt de gegevensvastlegging heimelijk plaats, maar ook gebeurt dit niet eenmalig maar over een bepaalde periode. De toelichting geeft daarbij ook voorbeelden van het volgen van het Internetgebruik of het meekijken met het e-mailverkeer van de gebruiker. Deze doelhandeling omvat dus zowel handelingen die vergelijkbaar zijn met de doorzoekingsbevoegdheden als handelingen die vergelijkbaar zijn met bijzondere opsporingsbevoegdheden als observatie en aftappen.
e. De ontoegankelijkmaking van gegevens. Hiermee kunnen onrechtmatige gegevens uit de computer van de verdachte worden verwijderd (gewist) of ontoegankelijk gemaakt (versleuteld), meestal na het kopiëren van de gegevens voor bewijsdoeleinden. De toelichting legt veel nadruk op de bestrijding van botnets (massale netwerken van geïnfecteerde

150 *Kamerstukken II* 2015/16, 34 372, nr. 3, 20.
151 *Kamerstukken II* 2015/16, 34 372, nr. 3, 26.
152 *Kamerstukken II* 2015/16, 34 372, nr. 3, 21.

> computers die, zonder dat de gebruikers het doorhebben, onder controle staan van de botnetbeheerder): met deze bevoegdheid kan de kwaadaardige programmatuur waarmee de computers binnen een botnet geïnfecteerd zijn, op afstand worden verwijderd. Dat gebeurde in de zgn. Bredolab-zaak, maar dat was omstreden omdat een bevoegdheid tot desinfectie op afstand ontbrak. De voorgestelde regeling biedt een expliciete wettelijke grondslag.[153]

DUUR – De inzet van de bevoegdheid is mogelijk voor een periode van vier weken, telkens verlengbaar met vier weken, en behoeft toestemming van de rechter-commissaris. Ook moet de beoogde inzet vooraf worden voorgelegd aan de Centrale Toetsingscommissie (CTC), een intern adviesorgaan van het OM.[154] De bevoegdheid kan worden toegepast bij ernstige misdrijven: voor de doelen a, b en c gaat het om voorlopige-hechtenismisdrijven die een ernstige inbreuk op de rechtsorde maken, voor de doelen d en e om misdrijven met een maximum gevangenisstraf van minstens acht jaar of speciaal aangewezen misdrijven[155].

WELKE COMPUTERS? – Alleen computers die in gebruik zijn bij de verdachte mogen op afstand worden onderzocht. Dat kan dus ook de laptop of smartphone van huisgenoten, vrienden of familie zijn, als de verdachte die (min of meer regulier, dus meer dan één- of tweemalig, nemen we aan) gebruikt. Het betekent dat de overheid ook een router kan binnendringen die door meerdere personen wordt gebruikt, als de verdachte er daar een van is. Vooral belangrijk is dat ook kan worden binnengeslopen in een server waarop de verdachte gegevens opslaat, zoals een cloud-server. Hoewel de toelichting vooral beschrijft dat na binnendringen in de computer van verdachte kan worden 'doorgestapt' naar het deel van een externe server dat verdachte gebruikt, sluit het niet expliciet uit dat speurders ook rechtstreeks in de server zouden binnendringen, mits de rechter-commissaris voor die server een specifiek bevel heeft gegeven.[156] Als dat

---

153 *Kamerstukken II* 2015/16, 34 372, nr. 3, 22. Over de Bredolab-zaak, zie M.E. KONING, 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *P&I* 2012(2), 46-52.

154 *Kamerstukken II* 2015/16, 34 372, nr. 3, 37.

155 Dat betreft vooral misdrijven waar '*vaak geen ander aangrijpingspunt voor de opsporing*' is dan deze bevoegdheid in te zetten, zoals botnetgebruik, kinderporno, grooming of andere computerdelicten. *Kamerstukken II* 2015/16, 34 372, nr. 3, 29.

156 Zie de tamelijk cryptische toelichting op p. 98-99 van *Kamerstukken II* 2015/16, 34 372, nr. 3.

inderdaad mogelijk zou zijn, rijst de grote vraag hoe dat onderzoek beperkt kan blijven tot het deel van de computer waarin gegevens staan die afkomstig zijn van de verdachte. Zeker in een cloud-omgeving zal de politie nauwelijks met precisie kunnen bepalen op welk gedeelte van welke server gegevens van de verdachte staan. Verder is, gezien het doel (onder e), het desinfecteren van bots, de ruime interpretatie van het begrip '*bij de verdachte in gebruik*' opmerkelijk. Daar vallen kennelijk ook de duizenden computers onder van onschuldige burgers die onrechtmatig onder de controle staan van een verdachte van botnetgebruik. We mogen hopen dat de rechter-commissaris het binnendringen in bot-computers alleen zal toestaan voor desinfectie en niet voor andere opsporingshandelingen.

WAARBORGEN – Het voorstel koppelt diverse waarborgen aan de uitoefening van de bevoegdheid. De rechter-commissaris moet het bevel schriftelijk geven en er de nodige specificaties voor de inzet in opnemen. Elke wijziging of verlenging van het bevel vergt hernieuwde toestemming van de rechter-commissaris. De ingezette software moet door een aangewezen keuringsdienst goedgekeurd worden conform technische eisen; het Besluit technische hulpmiddelen strafvordering wordt daartoe aangepast.[157] De uitvoering geschiedt door daartoe aangewezen opsporingsambtenaren, die de benodigde technische kennis hebben. Belangrijk is daarbij de functiescheiding: de technische rechercheurs zetten het middel in en vergaren data, die vervolgens worden geanalyseerd door de tactische rechercheurs die met de zaak belast zijn.[158] Na afloop van de inzet moeten de technische speurders het middel in beginsel verwijderen uit de geïnfecteerde computer, tenzij dat te moeilijk of riskant is. In het laatste geval moet de beheerder van de geïnfecteerde computer door politie of justitie worden geïnformeerd, zodat die zelf de software kan (pogen te) verwijderen (art. 126nba lid 6 Nl.Sv). Daarnaast moeten ook de relevante betrokkenen worden genotificeerd na afloop, tenzij het opsporingsbelang dat niet toelaat (art. 126bb Nl.Sv). Volgens de toelichting moeten ook derden worden genotificeerd als de speurders gegevens van anderen vastleggen. Uit de onduidelijke formulering[159] valt niet op te maken of dit slaat op notificatie van wie de gegevens heeft ingevoerd in de binnengedrongen computer, dan wel van de verantwoordelijke voor de verwerking van persoonsgegevens (als be-

157 *Kamerstukken II* 2015/16, 34 372, nr. 3, 31.

158 *Kamerstukken II* 2015/16, 34 372, nr. 3, 31.

159 '*Als de vastlegging van gegevens betrekking heeft op gegevens van een ander dan dient ook de verantwoordelijke voor die gegevens te worden genotificeerd.*' *Kamerstukken II* 2015/16, 34 372, nr. 3, 40.

doeld in de Wbp). Nuttig is tot slot dat de minister toezegt om, evenals bij aftappen gebeurt, jaarlijkse statistieken van de inzet van de bevoegdheid en de resultaten daarvan voor de strafvervolging te publiceren.[160]

BEDENKINGEN – Over de voorgestelde bevoegdheid valt veel meer te zeggen dan het bestek van dit preadvies toelaat. We gaan daarom niet in op vragen rond de noodzaak van deze bevoegdheid of de voorgestelde waarborgen als zodanig. Wel staan we stil bij de terminologie, de inbedding van de bevoegdheid in het bestaande systeem van opsporingsbevoegdheden en bij enkele aspecten die raken aan de aandachts- en discussiepunten elders in dit preadvies.

TERMINOLOGIE – Ten eerste de terminologie. De bevoegdheid heet (in de toelichting en in de titel van de nieuwe achtste afdeling van titel IVA) '*onderzoek in een geautomatiseerd werk*' en dat is geen goede benaming. Ze is te ruim, omdat vele andere bevoegdheden (zoals die uit de afdeling doorzoeking ter vastlegging van gegevens) ook onderzoek in computers regelen. Ze is ook onjuist, omdat het niet alleen gaat om onderzoek *in* een computer, maar ook om het onderzoeken van wat er gebeurt in de omgeving van de computer. De benaming zet dus burgers op het verkeerde been in de kenbaarheid van welke privacyinbreuken zij bij deze bevoegdheid kunnen verwachten. De doelhandelingen van direct afluisteren (via de microfoon van de pc, laptop of smartphone) en observatie (via de webcam of telefooncamera) slaan niet op onderzoek in de computer, maar op heel andere opsporingshandelingen. Het binnendringen in de computer voor deze doelhandelingen kan men bezwaarlijk als '*onderzoek*' in een computer aanduiden. Dit is één van de redenen waarom de wetgever de bevoegdheid beter zou opsplitsen: het gaat in feite om een aantal verschillende typen bevoegdheden, elk met een eigen dynamiek (zie ook *infra*).

Onder de terminologie valt ook het zeer ruime begrip '*geautomatiseerd werk*' (*supra*, hfd. 1). De toelichting erkent dat ook apparaten uit het Internet der Dingen, zoals navigatiesystemen van auto's en pacemakers onder de definitie vallen en sluit niet uit dat justitie ook in deze apparaten naar gegevens moet kunnen zoeken, '*afhankelijk van de ontwikkeling van zowel de techniek als de modus operandi van de misdaad*'.[161] We mogen hopen dat geen rechter-commissaris ooit toestemming zal geven om een pacemaker te infecteren met een Trojaans paard, maar het lijkt niet denkbeeldig dat navi-

160 *Kamerstukken II* 2015/16, 34 372, nr. 3, 40.
161 *Kamerstukken II* 2015/16, 34 372, nr. 3, 86.

gatiesystemen en andere apparaten zullen worden binnengedrongen om gegevens te verzamelen, af te luisteren of te observeren. Dat is niet per se onwenselijk, maar moet wel goed worden overdacht. Het infecteren van een computer tast de normale werking ervan aan. Dat is ook juist de bedoeling, maar onbedoelde en ongewenste neveneffecten op die normale werking vallen daarbij zeker niet uit te sluiten. Tekenend is dat de toelichting, na een wat optimistische verwijzing naar het feit dat de te gebruiken software aan technische eisen moet voldoen, zegt dat het onwaarschijnlijk is dat schade zal ontstaan, maar tegelijk erkent dat er '*onverhoopt*' schade kan ontstaan die door de burger zal kunnen worden verhaald.[162] Hoe goed kan men inschatten dat er alleen (onverhoopt) materiële schade zal ontstaan en geen letselschade of zelfs dodelijke ongelukken? Bij apparaten die op het Internet der Dingen zijn aangesloten, valt dat niet op voorhand met zekerheid uit te sluiten. Verder is relevant dat er gegevens kunnen worden verzameld over lichaamsfuncties, bijvoorbeeld bij het binnendringen in een smartphone die via Bluetooth doorlopend gegevens binnenkrijgt van een sporthorloge dat de hartslag meet of van andere gezondheidsapps die via sensoren het functioneren van het lichaam in kaart brengen.[163] Het verzamelen van dergelijke gezondheidsgegevens (niet alleen hartslag, maar ook bloeddruk, glucosespiegel, slaappatroon, stappentellers en (nachtelijke) bewegingsactiviteit) valt niet letterlijk onder artikel 11 Nl.Gw, maar vormt toch ook een soort van onderzoek aan (of zelfs in) het lichaam die inbreuk maakt op de lichamelijke integriteit,[164] en de noodzaak ervan zal dan ook expliciet door de wetgever moeten worden onderbouwd.

VERHOUDING TOT BESTAANDE BEVOEGDHEDEN NEDERLAND – Hoe verhoudt de voorgestelde bevoegdheid zich tot de bestaande bevoegdheden (met name bij toepassing in de woning, in verband met het huisrecht) en interceptie van communicatie? Bakent het voorstel het onderzoek in computers voldoende scherp af en zijn de waarborgen in lijn met de bestaande rechtsbescherming? De voorgestelde bevoegdheid is een hybride van verschillende typen onderzoek. Dat blijkt duidelijk uit het eerste lid (a t/m e), maar het lijstje van vijf doelbevoegdheden biedt geen scherpe classificatie. Zelf zouden we eerder de volgende drie typen onderscheiden: eenmalig

162 *Kamerstukken II* 2015/16, 34 372, nr. 3, 37.

163 Het voorbeeld is afkomstig van Simon Hania, tijdens een discussiebijeenkomst over het binnendringen in computers te Den Haag op 9 april 2014.

164 Zie B.J. KOOPS, H. VAN SCHOOTEN EN M. PRINSEN, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag, Sdu 2004, ITeR-reeks deel 70, 182-183.

onderzoek van de harde schijf, periodiek onderzoek van computergebruik en inzet als steunbevoegdheid voor andere opsporingsbevoegdheden.

1. *Eenmalig onderzoek van de harde schijf* – De bevoegdheid wordt als bijzondere opsporingsbevoegdheid geclassificeerd, wat wijst op periodieke inzet in plaats van eenmalig optreden. Toch is de classificering als BOB vooral gelegen in het heimelijke karakter van de bevoegdheid. Er bestaat echter ook behoefte aan het eenmalig onderzoeken van de harde schijf van verdachten. Daarbij denken we aan situaties waarin normaliter een doorzoeking zou plaatsvinden maar de te doorzoeken plaats onbekend is, vanwege het mobiele karakter van verdachte en zijn apparaten. Of aan gevallen waarin een doorzoeking ter vastlegging van gegevens naar verwachting niets zal opleveren omdat de computer te goed is beveiligd. Voor dergelijke situaties kan de voorgestelde bevoegdheid (met doelhandeling d, het vastleggen van reeds opgeslagen gegevens (maar niet van later binnenkomende gegevens)) een functioneel equivalent van de klassieke doorzoeking zijn.

Dit type bevoegdheid (en dan beperkt tot eenmalige inzet) zou in tweeën kunnen worden gesplitst. Aan de ene kant is er de niet-heimelijke bevoegdheid. Die zou passen in de afdeling doorzoeking ter vastlegging van gegevens, en wellicht als *sui generis*-lid aan artikel 125i kunnen worden toegevoegd. Het wetssystematische voordeel daarvan is dat dan voor de online doorzoeking ter vastlegging van (reeds opgeslagen) gegevens, naast rechterlijke toestemming, dezelfde waarborgen van toepassing zijn als voor de fysieke doorzoeking ter vastlegging van gegevens (art. 125l, 125la, 125m, 125n Nl. Sv) Dat zijn waarborgen die in belangrijke details afwijken van de BOB-waarborgen. Zo bepaalt de wet dat bij doorzoeking nietrelevante gegevens terstond worden verwijderd (art. 125n) terwijl zij bij BOB tot na afloop van de zaak moeten worden bewaard (art. 126cc). Aan de andere kant zou er ook een heimelijke variant zijn voor situaties waarin de overheid het computeronderzoek (nog) niet bekend kan maken aan de verdachte. Die past dan binnen de BOB, met bijbehorende BOB-voorwaarden. Daaronder zou eventueel ook de inkijkoperatie kunnen vallen (*infra*).

2. *Periodiek onderzoek van computergebruik* – Omdat de wetgever een systematisch onderscheid maakt tussen observatie en communicatieonderzoek, is het misschien aangewezen om ook bij het binnendringen in computers een onderscheid te maken tussen stelselmatige observatie van het computergebruik en interceptie van communicatie die met de computer plaatsvindt. Bij het eerste wordt heimelijk het gedrag van de verdachte

geobserveerd, dat zich uit via computergebruik. De overheid monitort bijvoorbeeld het surfgedrag: welke webpagina's bezoekt de verdachte, waar klikt hij op, welke informatie haalt hij binnen van Internet? Ook het monitoren van het op de computer maken van geschriften – denk aan dagboeken, administratie – valt hieronder. Daarnaast is er de interceptie van communicatie die met de computer plaatsvindt. Daarbij wordt heimelijk de communicatie van verdachte met andere personen onderschept: e-mailen, chatten, skypen en whatsappen, evenals het op Internet plaatsen van uitingen (twitteren, bloggen, reageren op webfora). In beide gevallen monitort de overheid toetsaanslagen (keylogger) en muisbewegingen, maar wetssystematisch gaat het om onderscheiden bevoegdheden (zie art. 126g lid 3 Nl.Sv, dat bepaalt dat bij observatie met een technisch hulpmiddel geen communicatie mag worden opgenomen). Technisch vallen die echter moeilijk te scheiden,[165] zodat het beter lijkt om beide vormen tezamen, in één bepaling, te regelen. De handelingen vallen onder doelhandeling d (vastleggen van gegevens) en lijken de kern van de voorgestelde bevoegdheid: dit zijn de voornaamste handelingen waarvoor het wenselijk kan zijn om een computer heimelijk binnen te dringen en voor een bepaalde periode te monitoren.

De stelselmatige observatie van computergebruik valt conceptueel het beste te vergelijken met stelselmatige observatie in de woning. Hoewel de computer zich niet per se in een woning hoeft te bevinden, gaat het om een vergelijkbare privacyinbreuk. Surfgedrag is vergelijkbaar met televisie kijken, boeken lezen en encyclopedieën raadplegen: handelingen die meestal niet voor derden zichtbaar zijn en die zich van oudsher vooral in de beslotenheid van de woning afspeelden. Met de rijkdom aan informatie op Internet, waaronder bronnen die samenhangen met de intieme persoonlijke levenssfeer, zoals seks, gezondheid, religie en politieke voorkeur, valt uit surfgedrag zelfs een scherper beeld van de persoonlijke levenssfeer van een verdachte te construeren dan observatie in de woning ooit zou kunnen. De interceptie van communicatie via de computer valt onder het bestaande begrip interceptie van vertrouwelijke communicatie. Het gaat per definitie om *vertrouwelijke* communicatie, ook waar openbare uitingen worden onderschept, omdat het onderscheppen plaatsheeft op een vertrouwelijk kanaal, dat wordt beschermd door het communicatiegeheim ongeacht de

[165] Bij gebruik van een keylogger is het tot op zekere hoogte mogelijk om te onderscheiden tussen computergebruik '*voor zichzelf*' en voor communicatie met anderen, omdat hiervoor vaak verschillende applicaties worden gebruikt. Er zijn echter zoveel applicaties in omloop, waarvan er dagelijks nieuwe bijkomen, dat het ondoenlijk lijkt om een lijst bij te houden van non-communicatie- en communicatie-applicaties.

inhoud.[166] Dit is dan ook een functioneel equivalent van de bevoegdheid tot direct afluisteren (art. 126l Nl.Sv).

3. *Steunbevoegdheid* – Het binnendringen in computers kan plaatsvinden als steunbevoegdheid voor stelselmatige observatie of interceptie van vertrouwelijke communicatie. Dit zijn de doelhandelingen genoemd onder b en c van lid 1 van de voorgestelde bevoegdheid. In tegenstelling tot het wetsvoorstel, zouden wij echter de inzet van keyloggers daar niet onder laten vallen. Als het de bedoeling is om uitsluitend vertrouwelijke communicatie te onderscheppen (zoals bedoeld in art. 126l Nl.Sv), dan zou de overheid daarbij geen andersoortige gegevensinvoer mogen vastleggen. Bij de inzet van een keylogger, of andere technische middelen waarmee de overheid het computergedrag van iemand kan monitoren, is het echter maar de vraag of communicatie voldoende kan worden onderscheiden van non-communicatie. Dat lijkt ons twijfelachtig.[167] De inzet van een keylogger hoort veeleer thuis onder het periodiek onderzoek van computergebruik uit de vorige alinea, waarbij de nadruk ligt op vastlegging van gegevens. Dat betekent dat de inzet van een keylogger moet voldoen aan de zwaardere voorwaarden van doelhandeling d van het wetsvoorstel (vastleggen van gegevens).[168] Het binnendringen van de computer om de microfoon van de computer of smartphone aan te zetten en daarmee de geluiden (met name communicatie) in de omgeving te onderscheppen is een equivalent van direct afluisteren. En software die een functionaliteit heeft om de signalen binnen bepaalde communicatieapplicaties, zoals Skype of WhatsApp, te onderscheppen (en niet meer dan die signalen) is een functioneel equivalent van het aftappen van communicatie als bedoeld in artikel 126m Nl.Sv. Als het binnendringen in een computer uitsluitend fungeert als steunbevoegdheid voor een andere bevoegdheid, plaatst de wetgever dit vanuit wetssystematisch oogpunt best gewoon bij die doelbevoegdheden. Lid 2 van artikel 126l Nl.Sv bepaalt dat de politie ter uitvoering van direct afluisteren een plaats kan betreden, waaronder een woning, onder aanvullende voorwaarden. Daar zou een nieuw lid op kunnen volgen dat aangeeft dat ze ter uit-

166 *Kamerstukken II* 2013/14, 33 989, nr. 3, 13.

167 Zie noot 165.

168 Men kan tegenwerpen dat bij direct afluisteren zelf (art. 126l) ook een keylogger kan worden ingezet en dat daarbij hetzelfde probleem speelt. Het binnendringen in een computer voor plaatsing van een keylogger lijkt echter qua privacyinbreuk equivalent aan het binnendringen in een woning ter plaatsing van een keylogger; dat is, volgens art. 126l lid 2, uitsluitend mogelijk bij misdrijven met een maximumgevangenisstraf van acht jaren of meer. De voorwaarden zijn in dat opzicht dus vergelijkbaar.

voering van het bevel ook in een computer mag binnendringen, waarbij dan de nodige waarborgen uit voorgesteld artikel 126nba Nl.Sv van overeenkomstige toepassing zijn. Een analoog onderdeel hoort dan in artikel 126m Nl.Sv en 90ter B.Sv voor het binnendringen in een computer ter uitoefening van een aftapbevel[169].

VIRTUELE INKIJKOPERATIE? – In deze classificering ontbreekt bewust de virtuele inkijkoperatie. Bij een inkijkoperatie in de fysieke wereld gaat de politie binnendringen '*om te kijken of bepaalde verboden voorwerpen of sporen aanwezig zijn*'. Daarbij mag alleen '*zoekend worden rondgekeken*' en niet doorzocht.[170] Zou een virtuele variant een zelfstandig type onderzoek moeten of kunnen zijn? De bedoeling van het voorstel is, bij de doelhandeling onder a in lid 1, dat wordt binnengedrongen in de computer voor een beperkter doel dan het onderzoek van de hele computer. Men wil namelijk bepaalde kenmerken van de computer vaststellen van computer of van de verdachte, bv. welk besturingssysteem die gebruikt, welke software of welke beveiliging. Met deze kennis in het achterhoofd kan de politie vervolgens andere bevoegdheden inzetten, zoals tappen of doorzoeking. Het zou dus gaan om een beperkte en voorbereidende bevoegdheid, vergelijkbaar met de inkijkoperatie van artikel 126k Nl.Sv. Het betreft een bijzondere opsporingsbevoegdheid, omdat het heimelijk plaatsvindt, maar zoals het eerste type binnendringen (eenmalig onderzoek) is de inkijkoperatie meestal eenmalig, binnen een beperkte periode. Verder zou het een minder ingrijpend karakter hebben dan het eenmalig of periodieke onderzoek van de computer, omdat niet alles mag worden onderzocht: '*Er is als het ware sprake van een virtuele plaatsopneming of inkijkoperatie, waarbij bepaalde kenmerken van het geautomatiseerde werk worden vastgesteld, ter voorbereiding van het binnendringen met het oog op het verrichten van bepaalde onderzoekshandelingen*'.[171] Voorbeelden van de vast te stellen kenmerken in wettekst en toelichting zijn de identiteit en de locatie van de gebruiker of de verdachte.[172] De wettekst gebruikt echter de term 'zoals'. Het gaat dus om een niet-uitputtende opsomming. De toelichting geeft deels voorbeelden van technisch-identificerende aard,

---

169 In België zitten direct afluisteren en telefoontap samen en inkijkoperatie ter plaatsing van de tap (art. 90ter, tweede lid B.Sv), enkel door de onderzoeksrechter, ook in woningen en bij beroepsgeheimhouders, apart van de andere inkijkoperatie op private plaatsen die geen woning of lokaal beroepsgeheimhouder zijn en tot de bevoegdheid OM behoren (art. 46quinquies B.Sv).

170 BLOM, T&C Strafvordering, 11e druk 2015, art. 126k Sv, aant. 6.

171 *Kamerstukken II* 2015/16, 34 372, nr. 3, 19.

172 *Kamerstukken II* 2015/16, 34 372, nr. 3, 20.

bijvoorbeeld het IP-adres, IMEI- of IMSI-nummer, of de locatie van het apparaat. Daarnaast gaat het echter ook om minder eenduidige kenmerken, waar het de '*identiteit*' van de verdachte betreft. Zo prijkt in de toelichting ook het voorbeeld: '*Het binnendringen van een smartphone van een persoon, die criminele contacten onderhoudt met een verdachte, om zijn identiteit vast te kunnen stellen.*'[173] Afgezien van de wat ongelukkige formulering,[174] is niet erg duidelijk welke identificerende kenmerken men bedoelt: zijn dat alleen technische kenmerken, zoals IP-adres of e-mailadres, of ook inhoudelijke kenmerken (bijvoorbeeld aliassen of roepnamen) die kunnen helpen om de verdachte te identificeren? Een ander voorbeeld is het '*in kaart brengen van de software die in het geautomatiseerde werk aanwezig is (o.a. welke versie het betreft)*'.[175] Dat gaat verder gaat dan technisch-identificerende kenmerken en heeft ook een inhoudelijke component. Daarmee bedoelen we niet zozeer dat er 'Apple-persoonlijkheden' zijn zoals er 'typische BMW-rijders' zijn. Veeleer dat dat de apps die iemand op de computer heeft, veel kunnen zeggen over zijn interessesfeer en gedrag. Dat is natuurlijk ook interessant voor speurders, maar gaat qua privacyinbreuk wel verder dan puur technisch-identificerende kenmerken.

AFGRENZINGSPROBLEMEN – Er zijn twee problemen met de vormgeving van de virtuele inkijkoperatie in voorgesteld artikel 126nba lid 1 onder a Nl.Sv. Ten eerste is de afgrenzing van het begrip '*bepaalde kenmerken*' onvoldoende duidelijk en daarmee mogelijk in strijd met de eis van voorzienbaarheid van wettelijk toegelaten inbreuken op art. 8, eerste lid EVRM. Ten tweede is het de vraag of kenmerken als identiteit en locatie te vinden zijn door alleen '*zoekend rondkijken*'. Kenmerkend voor computeronderzoek is dat niet op voorhand vast te stellen is welke gegevens waar te vinden zijn.[176] Voor technische kenmerken als IP-adres, IMEI-nummer en locatie van het apparaat kan dat wel, maar om de identiteit van de verdachte (die uit veel soorten gegevens af te leiden valt) te achterhalen, zal niet zelden de

---

173 *Kamerstukken II* 2015/16, 34 372, nr. 3, 20.

174 Iemand die 'criminele contacten' onderhoudt met de verdachte is zelf verdachte, dus bedoeld zal zijn het onderzoeken van de smartphone van een verdachte om de identiteit van andere verdachten vast te stellen. Mocht bedoeld worden dat ook de smartphone van niet-verdachten kan worden geïnfecteerd om de identiteit van de verdachte vast te stellen, dan gaat het om een wel erg vergaand middel dat niet in verhouding lijkt te staan tot het doel.

175 *Kamerstukken II* 2015/16, 34 372, nr. 3, 20.

176 O. KERR, 'Searches and Seizures in a Digital World', *Harvard Law Review* 2005, Vol. 119, No. 2, 531-585.

computerinhoud moeten worden doorzocht. Dat maakt het onderzoek ingrijpender en dus gaat het niet louter om een digitaal equivalent van de fysieke inkijkoperatie. Ook valt dit virtueel inkijken moeilijk te onderscheiden van het binnendringen ter vastlegging van gegevens, bedoeld in lid 1 onder d. De verantwoording van de virtuele inkijkoperatie steunt in zekere mate op een cirkelredenering. Het binnendringen ter vaststelling van bepaalde kenmerken vormt zoals gesteld slechts ter voorbereiding op de inzet van een andere (zwaardere) bevoegdheid, waaronder het binnendringen in computers voor andere doeleinden.[177] Doch als er al binnengedrongen is in de computer voor het vaststellen van identificerende kenmerken, veelal door bepaalde software te (doen) installeren, zal het binnendringen voor andere doeleinden niet een tweede keer met andere software geschieden. Daarvoor lijkt het doen infecteren van de computers van verdachten te complex. De te gebruiken software zal dus zowel functionaliteit voor het vaststellen van identificerende kenmerken of locatie moeten bevatten, als functionaliteiten voor het onderscheppen van communicatie of vastleggen van toetsaanslagen. Ook dat roept vragen op over de afbakening van doelbevoegdheid a (inkijken) ten opzichte van de andere doelbevoegdheden.

Al met al lijkt het Nederlandse voorstel voor de virtuele inkijkoperatie onvoldoende systematisch doordacht. Het hinkt op twee onverzoenbare gedachten. Ofwel is het een echte voorbereidingshandeling voor later onderzoek, die minder ingrijpend is dan de overige doelhandelingen. In dat geval moet ze beperkt blijven tot het nummer of de locatie van het apparaat. De vraag is of het doel het toch relatief zware middel van computerbinnendringing wel kan heiligen. Ofwel is het een bevoegdheid gericht op het vaststellen van de identiteit of locatie van de verdachte. In dat geval mogen meer types gegevens worden gezocht en vastgelegd, wat de bevoegdheid vrijwel even ingrijpend maakt als de doelbevoegdheid onder d (heimelijk vastleggen van gegevens). De vraag is daarbij of de bevoegdheid dan niet zou moeten samenvallen met de zwaardere bevoegdheid. Wellicht is het dus beter om de inkijkoperatie simpelweg te laten vallen onder het eenmalig onderzoek van de harde schijf. Daarbij kan immers ook worden gezocht naar de kenmerken die nodig zijn om het onderzoek verder te helpen, waaronder gegevens die nodig zijn om andere bevoegdheden in te zetten.

---

177 Zie de opmerking: '*Er is als het ware sprake van een virtuele plaatsopneming of inkijkoperatie, waarbij bepaalde kenmerken van het geautomatiseerde werk worden vastgesteld,* ***ter voorbereiding van het binnendringen*** *met het oog op het verrichten van bepaalde onderzoekshandelingen*', *Kamerstukken II* 2015/16, 34 372, nr. 3, 19 (nadruk toegevoegd).

COMPUTER EN COMPUTERGEBRUIK – Het Nederlandse voorstel benadert de bevoegdheid tot het heimelijk binnendringen in computers te veel als een soort Zwitsers zakmes. Dat is in de kern bedoeld als mes, maar laat zich ook voor allerlei andere doelen gebruiken door uitbreiding van het gereedschap met aanpalende werktuigen als blikopeners, schroevendraaiers of nagelvijlen. Doordat de voorgestelde wet te veel werktuigen (doelhandelingen) wil combineren, in een onvoldoende scherpe onderlinge afbakening, wordt waardoor het onoverzichtelijk en daarmee moeilijker te hanteren. Je kan brood smeren met het schroevendraaiertje, maar dat is niet de bedoeling en ook niet handig. De wetgever zou er beter aan doen om de bevoegdheid, als zelfstandige nieuwe bepaling, te schrijven in functie van waar ze eigenlijk voor is bedoeld: het onderzoeken van *een computer* en het onderzoeken van *computergebruik*. Deze twee functionaliteiten zijn te onderscheiden. Het op afstand onderzoeken van de *computer* mikt op het (eenmalig) vastleggen van reeds bestaande, opgeslagen gegevens. Het op afstand onderzoeken van *computergebruik* is gericht op het gedurende een zekere periode registreren van het computergedrag en dus ook op gegevens die worden gegenereerd nadat het bevel is gegeven. In België zou men het eerste meer een (door)zoeking noemen, het tweede veeleer een bewakingsmaatregel.[178] Dat sluit aan bij het bestaande wetssystematische onderscheid tussen onderzoek van opgeslagen gegevens en onderzoek van stromende gegevens. In de systematiek van de Nederlandse strafvordering valt dit onderscheid niet geheel samen met het onderscheid tussen doorzoekingsbevoegdheden en BOB, omdat ook het onderzoek van reeds opgeslagen gegevens onder omstandigheden heimelijk zou kunnen plaatsvinden. Verder zou, als het binnendringen in computers niet de kern is, maar een steunbevoegdheid voor een andere bevoegdheid, deze beter bij de doelbevoegdheden kunnen worden ondergebracht. Een en ander betekent dat de bevoegdheid in de volgende varianten ingepast zou kunnen worden in de systematiek van de opsporingsbevoegdheden.

DOORZOEKING, MET HEIMELIJKE VARIANT – Het binnendringen in een computer ter eenmalige vastlegging van reeds opgeslagen gegevens is een functioneel equivalent van de doorzoeking ter vastlegging van gegevens. Dit kan geschikt zijn in situaties waarin heimelijkheid niet nodig is (bij-

178 Zie voor het belang van het onderscheid tussen *real time* bewaking en doorzoeking van opgeslagen gegevens qua territoriale bevoegdheid om te zoeken ook het rechtsmachtsvoorstel, *infra*, 6.3.

voorbeeld omdat de verdachte reeds op de hoogte is van het feit dat een opsporingsonderzoek gaande is). In Nederland zouden daarbij de waarborgen van artikelen 125l t/m 125n Nl.Sv passen. Dit kan door een nieuw lid op te nemen in artikel 125i Nl.Sv. België zou er goed aan doen de informaticazoeking als zelfstandige onderzoeksbevoegdheid in de wet in te schrijven. Het plan van de regering om dat nog in 2016 te doen, valt dan ook toe te juichen.

Voor deze bevoegdheid zou er ook een heimelijke, aan strikte BOB-voorwaarden te onderwerpen, variant kunnen komen: de heimelijke eenmalige vastlegging van opgeslagen gegevens. Dit is een type dat hier en nu geen analogie uit de fysieke wereld kent: het komt neer op een heimelijke doorzoeking van een plaats, waaronder een woning. In België zou men spreken van een variant van een heimelijke huiszoeking, hoewel een heimelijke huiszoeking naar geldend recht niet mogelijk is en door de wetgever bij de invoering van de inkijkoperatie in de woning zelfs uitdrukkelijk van de hand is gewezen. Een belangrijk verschil met de in het Nederlandse wetsvoorstel opgenomen bepaling, is dat dit onderzoek niet gedurende een bepaalde periode zou mogen plaatsvinden, maar slecht eenmalig of kortstondig, d.w.z. slechts zolang als nodig is om de gegevens vast te leggen.

INTERCEPTIE EN OBSERVATIE – Daarnaast kan het binnendringen ook gebeuren met het oog op interceptie van communicatie die met de computer plaatsvindt. Dat is vergelijkbaar met interceptie van vertrouwelijke communicatie, het direct afluisteren van computer-gerelateerde communicatie. Om rechtszekerheid te bieden, kan de wetgever deze bevoegdheid best uitdrukkelijk in de wet opnemen. Het onderbrengen bij de doelbevoegdheid zorgt dat de bijhorende voorwaarden en waarborgen onverkort gelden en geeft duidelijker aan dat het binnendringen enkel de functionaliteit kan dienen om de doelbevoegdheid in te zetten. Voor direct afluisteren kan de politie wel software gebruiken die de microfoon van de computer aanzet, voor het vastleggen van communicatie uit de omgeving. Een keylogger die computercommunicatie vastlegt lijkt ons echter niet mogelijk als steunbevoegdheid, omdat het technisch moeilijk is om alleen communicatieve toetsaanslagen of muisklikken vast te leggen.

Het gebruik van een keylogger hoort bij een echt nieuwe bevoegdheid, die dus zeker een wettelijke basis behoeft: de *stelselmatige observatie van het computergebruik gedurende een bepaalde periode*. Die is vergelijkbaar met stelselmatige heimelijke observatie van gedrag in de woning. We kunnen echter niet genoeg onderstrepen dat, vanwege de grotere informatierijkdom van computergedrag, deze nieuwe maatregel veel indringender is dan de klas-

sieke onderschepping van communicatie en zelfs nog een stuk indringender dan heimelijke fysieke observatie in een woning. Bovendien legt de overheid alle gegevens ook nog eens vast. Een dermate verregaande bevoegdheid valt daarom slechts te verantwoorden voor de allerzwaarste feiten en met de allerstriktste waarborgen. Misschien moeten daar ook specifiek aangewezen andere – enkel digitaal opspoorbare – misdrijven bijkomen, maar op dat punt past toch zeer grote terughoudendheid. In de Belgische plannen komt er volgens de regering een 'fusie' tussen de heimelijke doorzoeking vanop afstand in informaticasystemen en onderschepping van telecommunicatie (de oude tapwet). Dat zou betekenen dat een gerechtelijk onderzoek onder leiding van een onderzoeksrechter nodig is. De tapwetgeving bevat weliswaar alle waarborgen, alleen heeft de wetgever de erbij horende nietigheidssanctie geschrapt in het begin van 2016[179]. De Belgische lijst van misdrijven waarvoor de tap mogelijk is, blijft aangroeien en de regering kondigde toevoeging van nieuwe misdrijven aan.[180]

ANDERE AANDACHTSPUNTEN – Nu de wetgevers in de Lage Landen een wettelijk kader gaan uitwerken, verliezen ze best een aantal andere aspecten niet uit het oog. Zullen bepaalde informaticasystemen als geheel worden uitgesloten van heimelijk binnendringen door politie en justitie? De Belgische inlichtingendiensten mogen (art. 18/16 Wet BIM) bv. geen systemen van politie en justitie hacken en voor andere overheidsnetwerken zijn er bijzondere toestemmingen vereist. Welke mate van BOM-afscherming van technische middelen blijft mogelijk en welke controle op de gehanteerde software door (experten van) de verdediging op de gegevens en de software is nodig in het kader van de tegenspraak en de controle op de betrouwbaarheid van het vergaarde digitaal bewijs? In welke mate mag de overheid, om de software binnen te loodsen bij het doelwit, misbruik maken van de identiteit van bestaande personen of bedrijven? Kan de overheid de privésector dwingen om overheidsspyware te laten zitten of geviseerde personen niet te waarschuwen, zoals de telecomsector moet meewerken en geheimhoudingsplicht heeft gekregen bij de klassieke onderschepping van telecommunicatie? Hoe zal dat in een grensoverschrijdende context werken? En, zoals gezegd: hoe regelen we de aansprakelijkheid van de overheid als

---

179 Art. 66 wet 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie, *BS* 19 februari 2016, 13141.

180 *Persbericht Verbetering van de bijzondere opsporingsmethoden en gegevensverzameling inzake internet en telecommunicaties* (sic!) – *tweede lezing*, http://www.koengeens.be /news /2016/06/29/verbetering-van-de-bijzondere-opsporingsmethoden-en-gegevensverzameling-inzake-internet-e.

het fout gaat? Normaal is de staat aansprakelijk voor schade die derden lijden door politieactiviteiten (art. 47 WPA), maar daartoe moet die burger natuurlijk weten dat de politie verantwoordelijk was en dat zal niet gemakkelijk aan te tonen zijn. De wettelijke uitsluiting van overheidsaansprakelijkheid die de inlichtingendiensten genieten als er iets fout gaat bij het heimelijk binnendringen van informaticasystemen (art. 18/16, §5 Wet BIM), lijkt niet veralgemeenbaar. Veeleer zal men inspiratie moeten halen uit art. 88quater, §5 B.Sv: '*De Staat is burgerrechtelijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt.*' Hier is de verantwoordelijkheid van de overheid immers nog directer.

Discussiepunten: De bevoegdheid tot binnendringen in computers moet anders worden vormgegeven dan in het Nederlandse wetsvoorstel. In plaats van een Zwitsers zakmes met te veel 'handige' functionaliteiten, moet het beter worden ingebed in de wetssystematiek. Bovenstaand voorstel geeft aan hoe dat zou kunnen.
Binnendringen voor zoeking is minder problematisch dan binnendringen voor vernietiging of ontoegankelijkmaking. Dat laatste zou best openlijk (en achteraf?) moeten gebeuren.

2.3. Doorzoeking van computers en opsporingsrechtsmacht

2.3.1. Inleiding: speuren in computers die zich buiten het eigen grondgebied bevinden

CONTRAST – Bij de doorzoeking van computers op afstand is een belangrijke vraag of en wanneer Nederlandse of Belgische onderzoekers op buitenlands grondgebied mogen onderzoeken. Die vraag is tot op zekere hoogte al beantwoord, bij de regeling van de netwerkzoeking (*supra*, 2.1.3). Daarbij is een vergelijking interessant, nu België zijn pragmatisch-flexibele aanpak contrasteert met de meer principieel-restrictieve Nederlandse benadering. We bekijken eerst de jurisdictievraag bij de Nederlandse netwerkzoeking en vervolgens hoe de wetgever de Nederlandse rechtsmacht voorstelt bij de doorzoeking van computers op afstand. Vervolgens stellen we vast dat België maximaal de mogelijkheden gebruikt die het Cybercrimeverdrag biedt en in de praktijk van onwetendheid een soort zegen maakt. Het gaat voor alle duidelijkheid dus niet om materiële rechtsmacht (is het feit of de persoon strafbaar onder Nederlands of Belgisch recht?) maar om

handhavingsrechtsmacht (mag een staat extraterritoriaal opsporingshandelingen verrichten?). De volgende vraag is echter of de klassieke onderliggende visie, namelijk dat de opsporingsactiviteit (ook) plaatsvindt in het land waar de gegevens zich bevinden, terecht is. We nodigen uit die benadering in vraag te stellen. De Belgische preadviseurs stellen in hoofdstuk 6 een alternatief voor, dat de zorg over soevereiniteit van staten en de rechtsbeschermingsverwachtingen van rechtsonderhorigen beter verzoent. Met rechtsonderhorigen bedoelen we dan zowel de door een zoeking mogelijks geviseerde individuen als politie en justitie. We hopen een beter evenwicht te bieden tussen de op het spel staande belangen, met een in een wereld van wereldwijd gegevensverkeer gemakkelijker hanteerbaar bevoegdheidsregime. Wie opsporingsactiviteiten wil reguleren, moet volgens ons immers ook nadenken en proberen coherente criteria uit te werken om te bepalen wanneer een opsporingsactiviteit (niet) als territoriaal mag worden beschouwd. Wie soevereine zeggenschap koppelt aan de plaats van de gegevens, benadert een ICT-omgeving nog te veel alsof het om een fysieke plaats gaat, terwijl de relativering van plaatsgebondenheid door snel wereldwijd gegevensverkeer net die moderne ICT-omgeving typeert. Dat lijkt noch voor politie en justitie, noch voor burgers een geschikte benadering. De plaats waar de onderzoekers en, vooral, de onderzochte persoon zich bevinden of normaal verblijven, hebben ook soevereine aanspraken. Alleen zal het nog wel even duren vooraleer de traditionele wereld van het internationaal publiekrecht van nut en noodzaak van deze benadering overtuigd geraakt.

2.3.2. De huidige benadering: territoriale begrenzing, met opmerkelijke Belgische uitzondering

PRINCIPE – Wanneer opsporingsinstanties zoeken naar bestaand fysiek bewijs, dan doen zij dat, logischerwijze, daar waar het bewijsmateriaal zich bevindt. Is het bewijsmateriaal gelegen in het buitenland, dan kunnen ze er, gelet op de staatssoevereiniteit en het territorialiteitsbeginsel, enkel toegang toe nemen via de wegen van internationale samenwerking. Een zoeking vanop afstand naar virtueel bewijsmateriaal[181], opgeslagen op een computer

[181] Het gaat hier bv. om de netwerkzoeking (*supra*, 2.1.3) of de heimelijke variant daarvan (*supra*, 2.2). Zie BVerfG 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07, *Mediaforum* 2008, afl. 5, 223, noot W.A.M. STEENBRUGGEN, *RTDI* 2009, afl. 34, 87, noot P. DE HERT, K. DE VRIES, S. GUTWIRTH; C. CONINGS, J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend', *Computerr.* 2013, afl.

in het buitenland, zou principieel dus ook uitsluitend via de wegen van internationale samenwerking moeten verlopen.[182] Dit standpunt vinden we niet enkel terug in de rechtsleer[183], maar ook de Raad van Europa en de nationale wetgevers van Nederland en België gaan daarvan uit. Art. 31 van het Cybercrime-verdrag handelt immers over wederzijdse rechtshulp ter verkrijging van data *opgeslagen op het territorium van een andere ondertekenende staat*. De Nederlandse justitie mag daarom slechts netwerkzoeken in computers die zich in Nederland bevinden.[184] Op een netwerk is het echter lang niet altijd duidelijk in welk land gegevens staan. Volgens de MvT bij de Wet computercriminaliteit mogen ambtenaren niet (althans niet zonder verdragsrechtelijke basis) netwerkzoeken als de gegevens op '*een kennelijk zich in het buitenland bevindend computersysteem*' staan.[185] Daarop bestaat slechts één verdragsrechtelijke uitzondering (Art. 32 Cybercrime-verdrag) en het valt niet te verwachten dat er binnen afzienbare tijd bijkomen.[186]

UITZONDERING GOEDE TROUW – Als de doorzoekende Nederlandse autoriteiten te goeder trouw aannemen dat gegevens in Nederland zijn opgeslagen, is er geen probleem. De beperking geldt alleen als het '*kennelijk*' zo is dat gegevens buitenslands staan. Indien vervolgens blijkt dat een netwerkzoeking plaatsvond buiten de landsgrenzen, zal gekeken moeten worden of zij redelijkerwijs mochten aannemen dat de computer zich wel in

---

1, 23-32. Er kan meer concreet gedacht worden aan het doorzoeken van een Dropbox-account, een account op sociale media of een webmail-account.

182 Ook in de Verenigde Staten wordt vandaag over het algemeen dit klassieke standpunt ingenomen: J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 371.

183 Zie: N. SEITZ, 'Transborder search: a new perspective in law enforcement?', *Yale Journal of Law and Technology* 2005, Vol. 7, 22 e.v.; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?,* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/ cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_ Computing_power_disposal_31Aug10a.pdf.

184 *Kamerstukken II* 1989/90, 21 551, nr. 3, 12 ('*De Nederlandse wet kan immers geen grondslag bieden voor een onderzoek in een geautomatiseerd werk dat onder de jurisdictie van een ander land valt*').

185 *Kamerstukken II* 1989/90, 21 551, nr. 3, 11.

186 Zie uitgebreid B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg, WODC/TILT, 2014, http://www.wodc.nl/onderzoeksdatabase/ 2326-de-gevolgen-van-cloudcomputing-voor-de-opsporing-en-vervolging.aspx.

het binnenland bevond. Als dat zo is, zal het bewijs in beginsel wel toelaatbaar zijn.[187]

UITZONDERING CYBERCRIME-VERDRAG – Art. 32 van het Cybercrimeverdrag voorziet daarnaast in enkele uitzonderingen waarin een rechtstreekse, grensoverschrijdende toegang mogelijk is. Rechtstreekse toegang tot buitenlandse gegevens kan ten eerste natuurlijk probleemloos als het gaat om publiek beschikbare (*open source*) gegevens. De tweede uitzondering is als men de rechtmatige en vrijwillige instemming heeft gekregen van '*the person who has the lawful authority to disclose the data to the Party through that computer system*'. Niet iedereen is het eens over hoe ver die uitzondering gaat. Gaat het bij die '*person*' om individuele gebruikers of kan ook een in een verdragsstaat gevestigde elektronischedienstenverlener met controle over de gegevens van talloze individuele computergebruikers hieronder vallen, als die via zijn algemene voorwaarden '*lawful authority to disclose*' heeft? De toelichting bij het Cybercrime-verdrag suggereert dat dit laatste mogelijk is op vrijwillige basis.[188] Het is echter in de praktijk vaak de vraag of een dienstenaanbieder juridisch bevoegd is om vrijwillig gegevens van eindgebruikers met derden, en in het bijzonder de overheid, te delen. Dat hangt doorgaans af van de contractuele relatie en van de gegevensbeschermingswetgeving die geldt voor de dienstenaanbieder.

BELGISCHE EXTRATERRITORIALE NETWERKZOEKING – De Belgische wetgeving inzake de netwerkzoeking voorziet in een meer verregaande bevoegdheid, wat door het Cybercrime-verdrag zelf niet wordt uitgesloten.[189] Art. 88*ter* §3 lid 2 B.Sv bepaalt immers het volgende: '*Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de*

---

187 Vgl. F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 6.1, die in dit geval verontschuldigbare dwaling aanneemt. Voor België geldt dit *a fortiori*, nu Belgische speurders zelfs wettelijke toelating hebben om gegevens die zich in het buitenland bevinden, te kopiëren in het kader van een Belgische netwerkzoeking (*infra*).

188 '*For example, a person's e-mail may be stored in another country by* ***a service provider****, or a person may intentionally store data in another country.* ***These persons*** *may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data (…)*' (nadruk toegevoegd). Toelichtend rapport bij het Cybercrime-verdrag van 23 november 2001, http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, §294.

189 *Ibid*., §294.

betrokken staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.' De voorbereidende werken verduidelijken dat de wetgever op die manier de unilaterale grensoverschrijdende netwerkzoeking onder strikte voorwaarden mogelijk wou maken om het hoofd te kunnen bieden aan het grote risico op verlies van bewijs. De wetgever stelt daarbij echter dat wanneer voldoende tijd[190] en kennis voorhanden is, de weg van de klassieke internationale rogatoire commissie moet worden gevolgd.[191] De Belgische wetgever blijft dus uitgaan van de lokalisatie van de opsporingshandeling op basis van de locatie van de data, maar voorziet toch in een unilaterale mogelijkheid om een *grensoverschrijdende zoeking* uit te voeren. In een datageoriënteerde visie, die ook de Belgische wetgever beweert voor te staan, is dit nochtans in principe in strijd met het verbod op het eenzijdig voorzien in extraterritoriale opsporingshandelingen.[192] Bij ons weten heeft echter nog geen enkel land hierover formeel geprotesteerd tegen België[193], maar dat landen als Rusland of China het niet eens zijn met de Belgische visie[194], lijdt weinig twijfel.

GEEN SANCTIE MISKENNING – Het is duidelijk dat alle speurders gretig gebruik zullen maken van mogelijke twijfel over de exacte locatie van data en zeker dat Belgische speurders graag gebruik zullen maken van hun doorzoekings- en vastleggingsmogelijkheid voor gegevens in het buitenland. Of ze zich veel inspanningen zullen getroosten om te zoeken in welke staat de gegevens zich bevonden en om dan achteraf de plaatselijke overheid in te lichten, valt te betwijfelen. Want als de territoriale beperkingsregels zijn geschonden, kan dat weliswaar als vormfout worden gekwalificeerd, maar

---

190 Doordat er gelet op het vluchtig karakter van gegevens vaak sprake zal zijn van tijdgebrek, dreigt die uitzondering eerder de regel te worden.

191 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 24.

192 PHIJ 7 september 1927, *SS Lotus* (Frankrijk/Turkije)*, C.P.J.I.Rec.* 1927, Serie A, nr. 10, overweging 45; zie hieromtrent eveneens C. CONINGS, J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend', *Computerr.* 2013, afl. 1, 27 e.v.; B. DE SMET, 'Registratie en lokalisatie van telecommunicatie', in *Comm. Straf.* 2008, 29.

193 Ook Finland, Portugal, Polen, Chili, Montenegro, Japan en V.S. hebben blijkbaar deze keuze gemaakt, zie CYBERCRIME CONVENTION COMMITTEE (T-CY) AD-HOC SUBGROUP ON JURISDICTION AND TRANSBORDER ACCESS TO DATA, *Transborder access and jurisdiction: What are the options? Report of the Transborder Group adopted by the T-CY on 6 December 2012*, 29, http://www.coe.int/en/web/cybercrime/tb.

194 Behalve Nederland, laten ook Tsjechië, Litouwen, Duitsland, Zweden, Turkije, Bosnië-Herzegovina, Japan, Hongarije en Estland het niet toe. In Cyprus hangt het van het type gegevens af. Voor sociale netwerken zou het mogen. (*Ibid.*)

zal een Nederlandse rechter de schending toch vaak eenvoudig '*wegschutznormen*'. Dat veronderstelt wel dat de rechter zou vinden dat de geschonden regel niet het belang van de verdachte beschermt, maar enkel het belang (soevereiniteit) van de andere staat.[195] Naar Belgische recht zijn er alleszins geen gevolgen: de schending valt normalerwijze niet onder een van de gevallen van de regeling voor bewijsuitsluiting in art. 32 V.T. B.Sv[196] en dus belet niets het gebruik van de onrechtmatig extraterritoriaal verkregen gegevens.

2.3.3. Territoriale begrenzing van de doorzoeking van computers op afstand

NEDERLANDSE BEGRENZING DOORZOEKING OP AFSTAND: BELGIË ACHTERNA?– Vanuit Nederland hoeft België niet onmiddellijk diplomatiek protest te verwachten. De consultatieversie van Computercriminaliteit III bevatte immers ook een bepaald ruime interpretatie van het internationaal recht:

'*Voor opsporingshandelingen in cyberspace met betrekking tot gegevens geldt in veel gevallen dat de feitelijke locatie van gegevens redelijkerwijs niet is te achterhalen. (…) In een dergelijk geval kunnen de gegevens die in het kader van het onderzoek zijn aangetroffen, worden vastgelegd of ontoegankelijk gemaakt, ongeacht de locatie waar de gegevens zich bevinden.*

Ook in het geval er bij de politie wel wetenschap bestaat van de feitelijke locatie van gegevens, kan – binnen de grenzen van artikel 539a Sv en onder de voorwaarde van (extra) territoriale rechtsmacht – zelfstandig worden opgetreden. Het zal sterk van de aard van de feitelijke handeling afhangen onder welke omstandigheden het volkenrecht zich verzet tegen zelfstandig optreden van de handhavende staat.'[197]

---

195 Voor een fijnmaziger antwoord, zie F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 6.2 en *infra*, hfd. 6.

196 Art. 32 V.T. B.Sv : '*Tot nietigheid van onregelmatig verkregen bewijselement wordt enkel besloten indien de naleving van de betrokken vormvoorwaarden wordt voorgeschreven op straffe van nietigheid, of de begane onregelmatigheid de betrouwbaarheid van het bewijs heeft aangetast, of het gebruik van het bewijs in strijd is met het recht op een eerlijk proces*.' Het Hof van Cassatie vond de miskenning van de territoriale bevoegdheidsregels (door de Franse politie, actief op Belgisch grondgebied na een grensoverschrijdende achtervolging) een louter formele onrechtmatigheid, die niet tot bewijsuitsluiting mocht leiden (Cass. 12 oktober 2005, AR P.05.0119.F., *T.Strafr.* 2006, 25 noot F. VERBRUGGEN).

197 Memorie van Toelichting bij Conceptwetsvoorstel in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), 34-35, http://www.internetconsultatie.nl/ computercriminaliteit.

TEGENWIND – De Nederlandse wetgever suggereert hier dus dat het internationaal recht het toelaat om eenzijdig gegevens vast te leggen wanneer de feitelijke locatie van gegevens redelijkerwijs niet te achterhalen is. Afhankelijk van welke mate van zekerheid je hanteert, kan dit in cyberspace al vlug om veel gegevens gaan. Het gaat verder dan België, want men zou de gegevens zelfs mogen verwijderen, wellicht vanuit de logica dat de strijd tegen botnets, kinderpornografisch materiaal of terreurwebsites moet worden opgedreven. Volgens de Nederlandse regering zouden er ook gevallen zijn waarin het internationaal recht eenzijdig optreden, dus zonder voorafgaande toestemming zou toestaan als de locatie van gegevens wel bekend is. De Adviesraad Internationale Vraagstukken noemde deze suggesties niet onderbouwd en aanvechtbaar; hij beschouwt het grensoverschrijdend doorzoeken van computers zonder toestemming van de staat waarin de gegevens zijn opgeslagen, niet geoorloofd naar het huidige internationaal recht.[198] Die conclusie is ook getrokken in een onderzoek van Koops en Goodwin.[199] Ook de Raad van State plaatste kritische kanttekeningen bij het concept en vroeg om betere onderbouwing en aanpassing van de wet.

GRENZEN AFTASTEN? – Naar aanleiding van het advies van de Raad van State zijn het bij de Tweede Kamer ingediende wetsvoorstel en de bijbehorende toelichting aangepast. Nu bevat het voorstel de eis dat het bevel tot doorzoeking van computers zou vermelden, '*indien bekend, dat de gegevens niet in Nederland zijn opgeslagen*' (art. 126nba lid 2 onder b Nl.Sv), zodat de rechter-commissaris deze omstandigheid bewust meeneemt in de beslissing. Hoewel de MvT nu minder lichtzinnig suggereert dat eenzijdige grensoverschrijdende doorzoekingen onder omstandigheden in overeenstemming zijn met het internationaal recht, gaat het voorstel tamelijk ver in het toelaten van extraterritoriale doorzoekingen. We vinden het zeker aangewezen om een voortrekkersrol in de internationale rechtsontwikkeling te spelen door een plausibel verhaal neer te zetten waarom bepaalde grensoverschrijdende handelingen toch in overeenstemming met het internationaal recht zijn.[200] De toelichting stelt dat door Nederlandse opsporingsdiensten '*met de grootste zorgvuldigheid*' zou worden geopereerd als de dienst '*een zekere inspanning verricht om de feitelijke locatie van gegevens te achterhalen*', en dat als bekend is (of later bekend wordt) dat gegevens zich in het buitenland

198 AIV (ADVIESRAAD INTERNATIONALE VRAAGSTUKKEN), *Het Internet. Een wereldwijde ruimte met begrensde staatsmacht*, Advies No. 92, Den Haag, november 2014, 60.

199 B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014.

200 Zoals gesuggereerd in *Ibid*., 73-76 en 90.

bevinden, een verzoek om rechtshulp moet worden gedaan '*op de kortst mogelijke termijn*'. Of '*een zekere inspanning*' voldoende is om '*met de grootste zorgvuldigheid*' te opereren, valt te betwijfelen in het licht van de internationale gevoeligheden; onzes inziens is op zijn minst een aanzienlijke inspanning nodig. Wanneer de onderzoekers niet kunnen vaststellen waar de gegevens zijn, mogen ze volgens de toelichting, in een '*stapsgewijze aanpak*', bepaalde kenmerken van de te onderzoeken computer bepalen, vervolgens gegevens overnemen en uiteindelijk zelfs ontoegankelijk maken. Voor het bepalen hoe ver men kan gaan, worden criteria gehanteerd (waaronder de vereiste inspanning om de locatie te achterhalen, de ernst van het misdrijf en de mate waarin dat Nederland raakt en de risico's voor de onderzochte computer); deze criteria worden nog uitgewerkt en zullen in een OM-Aanwijzing of AMvB komen.[201]

VOLDOENDE? – Of hiermee een 'plausibel verhaal' is neergezet, blijft de vraag. De pragmatische benadering van de toelichting strookt voor een goed deel met de visie van de Belgische preadviseurs (zie ook *infra*, hfd. 6). De Nederlandse preadviseur plaatst echter de volgende kritische kanttekeningen bij het wetsvoorstel in deze vorm.

Op zich maakt de toelichting goed duidelijk waarom het (dringend) wenselijk is om grensoverschrijdend te kunnen doorzoeken, en waarom in sommige situaties simpelweg niet kan worden bepaald waar gegevens zich bevinden en dus geen rechtshulpverzoek mogelijk is. De uitoefening van de bevoegdheid wordt echter niet aan strakke grenzen gebonden. In tegenstelling tot wat Koops en Goodwin suggereerden,[202] is de extraterritoriale doorzoeking niet beperkt tot enkele onomstreden ernstige misdrijven (zoals het verspreiden van kinderpornografie), maar tot een breder scala misdrijven (zeker voor de doelbevoegdheden van inkijkoperatie, interceptie en observatie). Zoals gezegd, beperkt het voorstel zich ook niet tot het kopiëren van gegevens, maar laat het ook verwijderen van gegevens toe. Daarenboven is de toelichting niet erg duidelijk welke mate van inspanning nodig is om te bepalen waar gegevens zich bevinden. Dat wordt overgelaten aan nog te schrijven lagere regelgeving. Dat opent meteen de deur voor Nederlandse opsporingsambtenaren om te zeggen – zoals hun Belgische collega's – dat ze echt hun best hebben gedaan en dat het helaas niet gelukt is, zonder dat ze het onderste uit de kan moeten halen om de (vermoedelij-

201 *Kamerstukken II* 2015/16, 34 372, nr. 3, 46–48.

202 B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 90.

ke) locatie vast te stellen. Evenmin geeft de toelichting duidelijk aan wat er gebeurt als de locatie later bekend geraakt en Nederland nog toestemming aan de buitenlandse staat zal vragen. Ze zegt alleen dat dan alsnog een verzoek om rechtshulp moet volgen.[203] Als alle gegevens al zijn gekopieerd, is niet duidelijk wat de consequenties zijn van non-respons of weigering van de achteraf aangezochte staat. Als die staat expliciet medewerking weigert, mag men aannemen dat Nederland reeds gekopieerde gegevens meteen moet vernietigen en ze niet mag gebruiken voor bewijs of verdere opsporing. Mag justitie, zolang de aangezochte staat nog niet heeft gereageerd, de reeds gekopieerde gegevens blijven gebruiken voor het opsporingsonderzoek? Of moeten deze worden bevroren? En als er helemaal geen reactie komt, kunnen de gegevens dan voor het bewijs worden gebruikt? Daarop geeft de toelichting geen antwoord.

Bovendien formuleert het wetsvoorstel het criterium te beperkt: het zou alleen gaan om situaties waarin *bekend* is *dat* gegevens buiten Nederland liggen (artikel 126nba lid 2 onder b Nl.Sv). Het moet ook, misschien zelfs vooral, situaties omvatten waarin *niet bekend* is *of* gegevens zich in Nederland of elders bevinden. In de situaties die de MvT aanhaalt (cloud computing, gebruik van Tor en andere verbergingstechnieken) zal de locatie meestal niet met (voldoende) zekerheid vast te stellen vallen, zodat het dus ook niet 'bekend' zal zijn dat de gegevens buiten Nederland liggen. Nu erkent de MvT wel dat '*ook voor het geval dat niet bekend is waar de gegevens zijn opgeslagen*' dit in het bevel moet worden vermeld,[204] maar dat hoort in de wettekst thuis.[205] Anders dreigt de praktijk zich te richten naar de letter van die wet en dus in situaties binnen het grijze gebied van onbekendheid van de locatie, dit niet per se aankaarten en in het (verzoek aan de rechter-commissaris tot een) bevel duidelijk maken.

Ten slotte voorziet ook het voorstel geen duidelijke sancties op onrechtmatige grensoverschrijdende doorzoekingen. Zoals bij de netwerkzoeking kunnen rechters de Schutznorm hanteren en oordelen dat de doorzoeking de soevereiniteit van een andere staat schendt, maar dat de geschonden norm niet de belangen van de verdachte beoogt te beschermen.[206] Hoewel dit staand recht is[207], geeft het geen prikkel voor opspo-

---

203 *Kamerstukken II* 2015/16, 34 372, nr. 3, 47.

204 *Kamerstukken II* 2015/16, 34 372, nr. 3, 48.

205 Het staat nu in één terloops zinnetje, terwijl de rest van de toelichting consequent spreekt over situaties waarin de buitenlandheid van gegevens *bekend* is. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3, 38, 48 (2x), 49.

206 *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 47.

207 Zie voor een pleidooi voor een alternatieve benadering: *infra*, hfd. 6.

ringsambtenaren om uiterst terughoudend te zijn bij netwerkzoekingen die de grenzen van het internationaal recht opzoeken. Hun zaak wordt er immers niet door geraakt, hooguit kan het (in vermoedelijk sporadische gevallen) leiden tot diplomatieke schermutselingen, maar dat is niet de primaire zorg van een opsporingsambtenaar of officier die een concreet ernstig misdrijf probeert aan te pakken.

Al met al laat de toelichting nog te veel open, en geeft deze daarmee te veel ruimte aan de praktijk, over de rechtmatigheid van extraterritoriale opsporing naar het internationaal recht. En de wettelijke regeling bevat navenant te weinig waarborgen om de soevereiniteit van andere staten te beschermen – de regeling lijkt de Nederlandse preadviseur, zeker met deze toelichting, geen plausibele interpretatie van het internationaal recht.

BAANBREKEND BELGIË – België lijkt op dit punt opmerkelijk minder terughoudend dan Nederland. Nooit heeft iemand getracht art. 88ter B.Sv terug te draaien. Bovendien heeft ook het Hof van Cassatie op basis van een extensieve interpretatie van de Belgisch-territoriale medewerkingsplicht, Belgische rechters bevoegd verklaard om niet in België gevestigde dienstverleners zonder rechtshulp te verplichten om gegevens naar België te brengen, onder bedreiging van strafsancties[208]. Nu de V.S. zelf niet vies is van ruime territoriale rechtsmacht-claims over buiten de V.S. opgeslagen gegevens[209], was er geen diplomatiek protest. Dat maakt het interessanter om te kijken hoe het Groothertogdom Luxemburg gaat reageren op de strafvervolging in België van het Luxemburgse bedrijf Skype wegens het niet voldoen aan de Belgische medewerkingsplicht.[210]

ACADEMISCH ALTERNATIEF VOORSTEL– Eenzijdige handelingen van staten en de reactie daarop van andere staten, zijn niet zonder belang in de vorming of interpretatie van het internationaal publiekrecht. De basis van dat recht ligt echter in vreedzame samenwerking tussen staten en voor de rechtszekerheid belanden afspraken soms best in formeel verbindende teksten. Staten doen om praktische of politieke redenen vrijwillig een (beperkte) afstand van soevereine aanspraken over buitenlandse vliegtuigen die hun luchtruim doorkruisen of schepen die voor hun kust varen, over kanalen of pijplijnen die over hun grondgebied lopen. Zo zouden ze in het

208 *Infra*, noot 496.

209 *Infra*, noot 374.

210 K. DE SCHEPPER, 'Cassatie bevestigt: Belgische gerecht kan rechtstreeks gegevens vorderen van Yahoo' (noot onder Cass. 1 december 2015), *RABG* 2016, 493.

kader van afspraken ook voor de soevereiniteit over gegevens die slechts over hun grondgebied passeren of er slechts zijn opgeslagen, afstand kunnen doen, dan wel minstens bepaalde inmenging door een staat met directere aanspraken op die gegevens kunnen dulden. De V.S. kan bv. dulden dat Nederland gegevens vordert van een Amerikaans sociaal netwerk (of zelfs toegang neemt), als de gegevens een duidelijke band vertonen met het Nederlandse grondgebied en/of in Nederland gevestigde personen en de locatie van de opslag de enige band is met de V.S. Wellicht zal dat in een eerste fase slechts tussen gelijkgezinde staten mogelijk zijn, op basis van een minimum aan onderling vertrouwen. De Belgische preadviseurs hebben in Leuven geprobeerd een samenhangende theorie uit te werken die als basis zou kunnen dienen voor dergelijke afspraken over rechtsmacht. Bij rechtsmacht gaat het om rechtszekerheid en aanknopingspunten moeten vastzitten aan iets dat enige stabiliteit vertoont. Dat is voor de plaatsen waar de per definitie hypermobiele gegevens zich bevinden, niet het geval. Daarom koppelen we de rechtsmacht over zoekingen aan de gemakkelijker vast te stellen band tussen personen en grondgebied, veeleer dan aan de plaats van de gegevens. De uitwerking hebben we grotendeels opgenomen in Deel 2, omdat ze zich wel leent tot debat onder de leden van de NVVS.

2.4. Onderzoek van in beslag genomen computers

RUIME BESLAGBEVOEGDHEID – In zowat alle situaties waarin ambtenaren misdrijven kunnen vaststellen of zoekingen kunnen uitvoeren, krijgen zij daarbij de bevoegdheid om voorwerpen in beslag te nemen. De inkijkoperatie is de uitzondering op die regel. Het beslag heeft (art. 35 B.Sv, art. 94 Nl.Sv) betrekking op alles wat kan dienen om de waarheid aan de dag te brengen en alles wat in aanmerking komt voor de bijzondere verbeurdverklaring. Dit laatste omvat illegale inhoud, zoals kinderpornografisch materiaal of vals geld. Beslag op bewijsmateriaal betreft alle zaken die kunnen dienen tot bewijs van onderzochte misdrijven, schuld of onschuld van personen die worden verdacht van die misdrijven.[211] Daar zullen natuurlijk ook dragers van digitale gegevens bij zijn, waaronder steeds vaker computers. Er zijn vele situaties waarbij computers in beslag kunnen worden genomen; vaak zijn de drempels om daartoe over te gaan redelijk laag.

LAAGDREMPELIGE DWANGBEVOEGDHEID – Zo heeft bij betrapping op heterdaad van om het even welk strafbaar feit iedere opsporingsambtenaar

[211] E. FRANCIS, 'Algemene principes van de bijzondere verbeurdverklaring en het beslag in strafzaken', *T.Strafr.* 2011, afl. 5, (306) 323.

beslagbevoegdheid (art. 96 lid 1 Nl.Sv, art. 49 B.Sv). Verder kan inbeslagneming tijdens het betreden van plaatsen.[212] Daarbij mag men alleen zoekend rondkijken en niet doorzoeken[213], wat betekent dat men een computer alleen in beslag kan nemen als hij het object was waarvoor werd binnengetreden ter inbeslagneming. De computer moet dan wel in het zicht staan en niet in een kast of lade liggen, of, in zeldzame gevallen in het kader van voortgezette toepassing, wanneer het beeldscherm van een in het zicht staande computer een strafbaar feit toont.[214] Hoewel de schouw (*descente*) (art. 151 Nl.Sv voor de officier van justitie, art. 192 Nl.Sv voor de rechter-commissaris) niet is bedoeld om sporen veilig te stellen, kunnen wel plaatsen worden betreden en ook in het zicht aangetroffen voorwerpen in beslag worden genomen.[215] Het onderscheid tussen louter betreden en doorzoeken kent het Belgisch recht enkel voor publiek toegankelijke plaatsen (*supra*, 2.1). Inbeslagneming kan in Nederland ook op basis van een bevel tot uitlevering van voorwerpen (art. 96a lid 1 Nl.Sv, voor opsporingsambtenaren bij verdenking van een voorlopigehechtenismisdrijf; art. 105 Nl.Sv, voor de rechter-commissaris in alle gevallen; art. 551 Nl.Sv voor opsporingsambtenaren bij specifieke delicten, vooral betreffende voorwerpen ter onttrekking aan het verkeer, zoals kinderpornovideo's). Bij staandehouding van de verdachte om diens identiteit vast te stellen (art. 52 j° 95, eerste lid Nl.Sv voor opsporingsambtenaren) kan inbeslagneming en natuurlijk bij aanhouding (art. 53 Nl.Sv, art. 1,2°-3° WVH) door eenieder (dus ook burgers) bij ontdekking op heterdaad van een strafbaar feit (art. 54 Nl.Sv), door het OM bij verdenking van een voorlopigehechtenismisdrijf (53-54 j° art. 95, eerste lid Nl.Sv[216], art. 2,1° WVH). Opsporingsambtenaren kun-

---

212 Dit is mogelijk als steunbevoegdheid voor diverse bevoegdheden, bv. betreden van plaatsen ter inbeslagneming door opsporingsambtenaren, ook buiten heterdaad, bij verdenking van een voorlopigehechtenismisdrijf (art. 96 lid 1 Nl.Sv).

213 Zie nader G.J.M. CORSTENS, *Het Nederlands strafprocesrecht*, bewerkt door M.J. BORGERS, 8e druk, Deventer, Kluwer, 546 en 585.

214 De Belgische regering is van plan om bij inkijken ook toe te laten dat de speurders kasten zouden open maken (het is nog niet duidelijk of ze die mogen openbreken) en stalen te nemen van aangetroffen verdachte inhoud. Dat lijkt zinvol voor chemische stoffen of drugs, maar niet op te gaan voor aangetroffen computermateriaal.

215 G.J.M. CORSTENS, *Het Nederlands strafprocesrecht*, bewerkt door M.J. BORGERS, 8e druk, Deventer, Kluwer, 582.

216 Momenteel kan, op basis van art. 95, eerste lid, iedereen die de verdachte aanhoudt of staande houdt, door deze met zich gevoerde voorwerpen in beslag nemen; wetsvoorstel 34 159 zal dit beperken tot opsporingsambtenaren. Burgers kunnen dan niet meer voorwerpen van aangehouden verdachten in beslag nemen. Niettemin blijft in dat wetsvoorstel art. 53 lid 3 stellen dat de niet-opsporingsambtenaar die een verdachte

nen, bij ernstige bezwaren (kort gezegd: een zware verdenking) tegen de verdachte, deze aan zijn kleding onderzoeken (art. 56, vierde lid Nl.Sv, art. 28 §2 WPA)[217]. De algemene beslagbevoegdheid krijgt in België concreet vorm in de artikelen 35 tot 39 B.Sv Buiten heterdaad ligt de bevoegdheid bij procureur des Konings (art. 28bis, §3, B.Sv)[218] en de onderzoeksrechter. Rechtsgeleerden verdedigen dat de beslagbevoegdheid uit de concrete zoekingsbevoegdheden voortvloeit. De instantie die bevoegd is om een zoeking uit te voeren, is meteen ook bevoegd voor het daarop volgende beslag.[219] Zo hebben ook agenten van gerechtelijke politie bijvoorbeeld beslagbevoegdheid wanneer zij optreden op grond van art. 15 WPA (bv. zoeking in een openbare plaats) of wanneer zij een huiszoeking met toestemming uitvoeren. De gerechtelijke fouillering en de beslagbevoegdheid in het verlengde daarvan, komen op grond van art. 28 WPA bijvoorbeeld ook toe aan politieambtenaren, onder de verantwoordelijkheid van een officier van gerechtelijke politie. In het kader van de uitoefening van hun gewone taken kunnen ze overgaan tot inbeslagname van overtuigingsstukken.[220] De Belgische wetgever zou dit in de toekomst best in de formele

---

aanhoudt, de aangehoudene onverwijld aan een opsporingsambtenaar overlevert, *onder afgifte aan deze van bij de verdachte aangetroffen voorwerpen*. De burger mag de voorwerpen dus niet in beslag nemen, maar kennelijk wel afpakken van de verdachte. Feitelijk zullen burgers dus nog steeds, waar dat relevant is bij de aanhouding, laptops of smartphones die de verdachte draagt kunnen afnemen en aan de politie ter inbeslagneming kunnen overdragen. Vgl. *Kamerstukken II* 2014/15, 34 159, nr. 3, 25-26.

217 Opsporingsambtenaren kunnen ook een aangehouden verdachte aan de kleding onderzoeken of voorwerpen die hij bij zich draagt of met zich voert onderzoeken om verdachtes identiteit vast te stellen (art. 55b Nl.Sv). In uitzonderingsgevallen zal daartoe bv. een smartphone of schootcomputer aangezet kunnen worden om te zien of er een naam op het inlogscherm verschijnt, of anderszins, als de computer niet beveiligd is, in de computer gezocht kunnen worden naar identiteitsgegevens. Inbeslagneming van de computer zal daarbij niet aan de orde zijn, maar het kan theoretisch voorkomen dat bij het openen of oppervlakkig doorzoeken van de computer bv. kinderporno (of een bestandsnaam die sterk daaraan doet denken) wordt aangetroffen, in welk geval inbeslagneming wel mogelijk is.

218 MvT, *Parl. St.* Kamer 1996-97, nr. 49K857/001, 23.

219 M. BOCKSTAELE, 'Huiszoeking, vaststellingen en beslag vanuit het perspectief van het plaatsbezoek' in M. BOCKSTAELE (ed.), *Huiszoeking en beslag*, Brussel, Politeia, 2004, 45-46; J. HOEFFLER, *Traité de l'instruction préparatoire en matière pénale,* Kortrijk, UGA, 1956, 238-240; R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2012, 343; R. VERSTRAETEN en L. DELBROUCK, 'Beslag in strafzaken', in *Comm. Straf.* 2014, 11-15; L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR,* Brussel, Larcier, 1962, 68, 70 en 71.

220 Zie eveneens Antwerpen 19 maart 2003, *RW* 2003-04, afl. 41, 1696.

wet verduidelijken.[221] Wanneer de opsporingsambtenaren zich tijdens een zoeking in de materiële onmogelijkheid bevinden om alle zaken die op het eerste gezicht verband kunnen houden met de onderzochte feiten, grondig te doorzoeken, kunnen zij die stukken in beslag nemen om ze op een later tijdstip grondiger te bestuderen.[222] Het beslag staat dan eerder in functie van de zoeking.

BESLAG COMPUTERHARDWARE – Niet altijd zullen computers in beeld komen als onderzoeksobject, maar toch zijn talloze scenario's denkbaar waarin dat wel zo zal zijn. Bijvoorbeeld als een politieagent iemand op heterdaad betrapt die heimelijk met zijn smartphone meisjes in een zwembad-verkleedhokje fotografeert, of als een politieagent een getuige van een busjeshokjesvernieling door voetbalvandalen (art. 141 Sr) beveelt de smartphone waarmee foto's van de vernieling zijn genomen, af te geven of uit te leveren. Of de politieagent die een loods betreedt ter inbeslagneming van gestolen spullen en daarbij een bestelbusje aantreft waarmee de spullen mogelijks vervoerd zijn en waarvan het (interactieve) navigatiesysteem sporen kan bevatten van ingevoerde bestemmingen. In al deze gevallen kan de computer (smartphone, navigatieapparaat) in beslag worden genomen. Vooral de inbeslagneming van smartphones bij aanhouding doet zich in de praktijk regelmatig voor. De vraag is dan onder welke voorwaarden onderzoek kan worden gedaan aan de inbeslaggenomen computers.

ONDERZOEK IN BESLAG GENOMEN VOORWERP – Het traditionele antwoord op die vraag is eenvoudig: de inbeslagnemingsbevoegdheid brengt met zich mee dat voor de waarheidsvinding onderzoek mag worden gedaan aan inbeslaggenomen voorwerpen.[223] Sporen op het voorwerp mogen worden veiliggesteld; de inhoud mag worden onderzocht op relevant bewijsmateriaal. Dat geldt, bij gebreke van een specifieke regeling die anders

---

221 Zie reeds: J. HOEFFLER, *Traité de l'instruction préparatoire en matière pénale,* Kortrijk, UGA, 1956, 240; zie in dit verband eveneens: P. TRAEST, G. VERMEULEN, W. DE BONDT, T. GOMBEER, S. RAATS en L. VAN PUYENBROECK, *Scenario's voor een nieuwe Belgische strafprocedure. Een praktijkgericht knelpuntenonderzoek,* Antwerpen, Maklu, 2015, 83. Er is een duidelijk draagvlak in de praktijk voor een uitdrukkelijke bevoegdheidsuitbreiding tot het leggen van bewarend onroerend beslag.

222 Cass. 10 maart 1998, AR P.96.0649.N, *RW* 1998-99, 644, noot A. VANDEPLAS; Cass. 20 november 2001, AR P.00.0548.N, *Arr.Cass.* 2001, afl. 9, 1968.

223 G.J.M. CORSTENS, *Het Nederlands strafprocesrecht*, bewerkt door M.J. BORGERS, 8e druk, Deventer, Kluwer, 541.

zou bepalen, ook voor computers.[224] Voor België volstaat het hier te verwijzen naar het reeds vermelde gebrek aan een specifiek juridisch regime voor de informaticazoeking en de daaruit voortvloeiende discussie in de rechtsleer. Die discussie speelt, onafhankelijk van het feit of speurders een informaticasysteem ter plaatse doorzoeken dan wel na de inbeslagname daarvan. Het Hof van Cassatie spreekt klare taal. Wanneer men een informaticasysteem in beslag kan nemen, kan men het ook doorzoeken. De voorgenomen wijzigingen op het vlak van doorzoekingen van informaticasystemen maken het gebrek aan voorafgaande rechterlijke controle alleen nog maar groter. Bovendien voorziet het, ondanks de vergelijkbare privacy-inmenging, vreemd genoeg wel in een onderscheid tussen het doorzoeken van een inbeslaggenomen systeem en een systeem dat (nog) niet in beslag is genomen. De eerste bevoegdheid komt toe aan de officier van gerechtelijke politie en de tweede aan de procureur des Konings (*supra*, 2.1.2.).

GROEIENDE TWIJFEL IN NEDERLAND – De Nederlandse wetgever erkende bij de totstandkoming van de wetten computercriminaliteit, computercriminaliteit II en bevoegdheden vorderen gegevens min of meer dat computers anders zijn, maar de consequenties ervan zijn daarbij niet onder ogen gezien.[225] Zoals Wiemans opmerkt '*verschaft de bevoegdheid om het computersysteem in beslag te nemen feitelijk dezelfde mogelijkheden om gericht en stelselmatig te zoeken naar relevante gegevens als de doorzoeking*.'[226] Anders dan bij het gericht en stelselmatig onderzoek van computers in het kader van de doorzoeking, heeft de wetgever het onderzoek van inbeslaggenomen computers niet nader genormeerd. Dat levert dus een discrepantie op in de rechtsbescherming, bijvoorbeeld ten aanzien van notificatie en vernietiging.[227] Ook los van de verschillen in toepasselijkheid van rechtsbeschermende bepalingen, verontrust het ongeregelde onderzoek aan inbeslaggenomen voorwerpen de lagere rechtspraak in toenemende mate. Vooral het onderzoek aan inbeslaggenomen smartphones roept vragen op over de subsidiariteit en proportionaliteit. Zo bepaalde het Hof Arnhem-Leeuwarden in april 2015

---

224 *Ibid*. HR 29 maart 1994, NJ 1994, 577 m.nt. Sch bepaalde reeds dat '*voor de waarheidsvinding onderzoek mag worden gedaan aan inbeslaggenomen voorwerpen ten einde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen en in computers opgeslagen gegevens daarvan niet zijn uitgezonderd*.'

225 F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125i-125o, aant. 6.

226 *Ibid*.

227 *Ibid*.

dat onderzoek van een inbeslaggenomen smartphone inmiddels strijdig is met artikel 8 EVRM:

'*De technische ontwikkelingen anno 2015 brengen met zich dat er via een smartphone niet alleen toegang wordt verkregen tot verkeersgegevens, maar ook tot de inhoud van communicatie en privé-informatie van de gebruiker van de smartphone. En dat zonder enige vorm van voorafgaande beoordeling van de subsidiariteit en/of proportionaliteit van de bevoegdheid. Dat brengt het hof tot het oordeel dat sprake is van een zodanig ingrijpende bevoegdheid dat, mede gelet op artikel 1 Sv, de algemene bevoegdheidsomschrijving van artikel 94 Sv heden ten dage niet meer kan worden aangemerkt als een wettelijk voorschrift dat als voldoende kenbaar en voorzienbaar kan worden aangemerkt bij de uitoefening van de verleende bevoegdheid. Het kan derhalve de toets van artikel 8 EVRM niet (meer) doorstaan.*'[228]

Het arrest doet denken aan de uitspraak in de Amerikaanse zaak-Riley, een mijlpaal-arrest waarin het Hooggerechtshof van de V.S. bepaalde dat voor inbeslagneming van een telefoon bij arrestatie een *warrant* (rechterlijke machtiging) nodig is:

'*The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. (…) That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. (…)*

In 1926, Learned Hand observed (…) that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." (…) If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form. (…) With all they contain and all they may reveal, they hold for many Americans "the privacies of life".'[229]

Het Leeuwardense arrest heeft navolging gekregen van de rechtbank Noord-Holland,[230] maar de rechtbanken Oost-Brabant,[231] Noord-Holland

---

228 Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954. De schending van art. 8 EVRM had overigens geen gevolgen omdat de inhoud van de smartphone geen onderdeel uitmaakte van de bewijsconstructie.

229 *Riley v. California*, 573 U.S. __ (2014), http://www.supremecourt.gov/opinions/ 13pdf/13-132_8l9c.pdf.

230 Rb. Noord-Holland 4 juni 2015, ECLI:NL:RBNHO:2015:4660.

231 Rb. Oost-Brabant 5 juni 2015, ECLI:NL:RBOBR:2015:3228.

(drie weken na de vorige uitspraak!)[232] en Limburg[233] houden vooralsnog vast aan de staande rechtspraak van de Hoge Raad en achten artikel 94 Nl.Sv wel een voldoende expliciete wettelijke basis voor de privacyinbreuk van onderzoek aan inbeslaggenomen smartphones. Het wachten is nu op de Hoge Raad (het OM is in cassatie gegaan van de Leeuwardense uitspraak) of het EHRM dan wel op de wetgever.

TERECHT – Wat ons betreft, snijdt de argumentatie van het Amerikaanse Hooggerechtshof en het Leeuwardense hof hout[234]: computers zijn inmiddels dermate belangrijke houders van privé-informatie geworden, met allerlei gegevens die vroeger in huis werden bewaard maar inmiddels de burger mobiel vergezellen (fotoalbums, muziek, boeken, dagboeken), dat onderzoek van computers vergelijkbaar is, of zelfs verder gaat, dan een doorzoeking van een woning. Het is dan ook dringend gewenst dat er een wettelijke regeling komt die beperkingen stelt en waarborgen treft voor het onderzoek aan inbeslaggenomen computers.

De Nederlandse wetgever is dat gelukkig ook van plan. De Contourennota erkent het probleem:

'*Ik ben van oordeel dat het vergaren van gegevens via de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken, zoals smartphones, hierbij onderbelicht is gebleven. Het valt niet goed te rechtvaardigen dat het onderzoek in een computer en het vastleggen van daarop opgeslagen gegevens tijdens een doorzoeking wel met specifieke waarborgen is omgegeven, terwijl wanneer diezelfde computer tijdens de doorzoeking in beslag zou zijn genomen, het onderzoek aan die inbeslaggenomen computer en het vastleggen van de daarop opgeslagen gegevens niet met vergelijkbare waarborgen is omgegeven. Daarbij komt dat op grond van de zelfstandige inbeslagnemingsbevoegdheden van opsporingsambtenaren, bijvoorbeeld bij staande houding en aanhouding, naar huidig recht geen betrokkenheid van een hogere autoriteit is voorzien voor het onderzoek aan bijvoorbeeld een inbeslaggenomen smartphone en de kennisneming en het gebruik van de daarop opgeslagen gegevens. (…) Tegen deze achtergrond acht ik nadere wettelijke normering (…) noodzakelijk. Ik denk daarbij aan het vereiste dat een hogere autoriteit beslist (…) alsmede waarborgen die vergelijkbaar zijn met die welke van toepassing zijn in het geval dat tijdens een doorzoeking onderzoek wordt gedaan aan een computer en de daarop opgeslagen gegevens ter plaatse worden vastgelegd (artikelen 125i e.v.[Nl.]Sv).*'[235]

---

232 Rb. Noord-Holland 26 juni 2015, ECLI:NL:RBNHO:2015:5447.

233 Rb. Limburg 28 oktober 2015, ECLI:NL:RBLIM:2015:9128.

234 Zie ook C. CONINGS, 'Het uitlezen van een gsm of ander privaat IT-systeem: This is not America' (noot onder Cass. 11 februari 2015), *RW* 2015, afl. 16, 622-626.

235 *Kamerstukken II* 2015/16, 29 279, nr. 278, 63-64.

Hierbij denkt de wetgever vooral aan een bevel van de officier van justitie voor het onderzoeken van inbeslaggenomen gegevensdragers of computers. De officier zou ook kunnen beoordelen of de rechter-commissaris moet worden ingeschakeld, als het verschoningsrecht of telecommunicatiegeheim kan worden geraakt door het computeronderzoek.[236] Is de officier van justitie in alle gevallen de juiste autoriteit is om toestemming te geven voor onderzoek aan inbeslaggenomen computers? Weliswaar neemt die belangrijke beslissingen waarbij de persoonlijke levenssfeer in het geding is, maar voor de zwaarste inbreuken is toestemming van de rechter-commissaris nodig. Zoals het citaat uit *Riley* laat zien, valt er veel voor te zeggen om het onderzoek aan een inbeslaggenomen smartphone aan (tenminste) hetzelfde waarborgniveau te verbinden als een doorzoeking van een woning. Ook het discussiestuk over Boek 2 in Modernisering Sv erkent de ingrijpendheid:

'*Het kennisnemen en vastleggen van op de gegevensdrager opgeslagen email-correspondentie, foto's en filmpjes, persoonlijke aantekeningen en internetzoekgeschiedenis kan, al dan niet in hun onderlinge samenhang, een ingrijpende inbreuk op de persoonlijke levenssfeer van de betrokkene opleveren. Men vergelijke de inbeslagneming van alle fotoboeken, alle videobanden, alle persoonlijke brieven, alle persoonlijke aantekeningen (dagboeken) bij een persoon die verdacht wordt van bijvoorbeeld handel in verdovende middelen. Een dergelijke inbeslagneming zou al gauw als disproportioneel worden aangemerkt.*'[237]

Deze argumentatie wordt in het discussiestuk echter niet voldoende doorgetrokken: als een computer inderdaad '*alle fotoboeken, alle videobanden, alle persoonlijke brieven, alle persoonlijke aantekeningen (dagboeken)*' van een verdachte bevat, moet het dan niet de rechter-commissaris zijn die toestemming geeft voor het onderzoek van de drager waarop al deze gegevens staan? De Belgische regering wil het vanaf de herfst van 2016 mogelijk maken dat de procureur een uitbreiding zou kunnen bevelen van een zoeking tot een informaticasysteem dat verbonden is aan het informaticasysteem dat het voorwerp is van de eerste maatregel voor '*zover de informatie toegankelijk is zonder code in te voeren. Elke andere niet-heimelijke zoeking in een informaticasysteem,* [moet worden] *bevolen door een onderzoeksrechter.*'[238]

---

236 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 52.

237 *Ibid*., 37.

238 *Persbericht Verbetering van de bijzondere opsporingsmethoden en gegevensverzameling inzake internet en telecommunicaties – tweede lezing*, http://www.koengeens.be/news/2016/06/29/verbetering-van-de-bijzondere-opsporingsmethoden-en-gegevensverzameling-inzake-internet-e.

Onzes inziens moet de normatieve bescherming van het huisrecht – de plaats waar vroeger al deze gegevens werden bewaard – hier worden doorgetrokken naar computers, althans naar de typen computers waarop burgers tegenwoordig hun persoonlijke leven bij zich dragen: smartphones, tablets en andere draagbare computers (nu in de beperkte zin van het woord 'computer'). We zouden daarbij een onderscheid willen maken tussen 'echte' computers (smartphones en andere persoonlijke computers) enerzijds (waarvoor het huisrecht naar analogie mutatis mutandis zou moeten gelden, en dus rechterlijke toestemming vereist is) en gegevensdragers (en mogelijk gegevensverwerkende apparaten, als een navigatiesysteem of koelkast, die wel een '*geautomatiseerd werk*' zijn maar geen functioneel equivalent van de 'echte' computer) anderzijds (waarvoor een bevel van de officier van justitie zou kunnen volstaan). Machtiging van de rechter-commissaris hoeft geen wezenlijke praktische bezwaren op te leveren: zoals een rechter-commissaris per mobiele telefoon toestemming kan geven voor een woningdoorzoeking, kan hij ook per mobiel toestemming geven voor een computerdoorzoeking.

Discussiepunt: Het onderzoek aan inbeslaggenomen smartphones, tablets en andere persoonlijke ('echte') computers behoeft een machtiging van de rechter-commissaris of onderzoeksrechter, omdat de privacyinbreuk vergelijkbaar is met die van een woningdoorzoeking.

Hoofdstuk 3. Aanpalende bevoegdheden

3.1. Bevel tot ongedaan maken van beveiliging ('ontsleutelbevel')

3.1.1. Analyse van de bevoegdheid

PLICHT OM OVERHEID TE HELPEN – Bij een doorzoeking zal het regelmatig voorkomen dat een computer beveiligd is. Door het conflict tussen het FBI en computergigant Apple over de toepasselijkheid van die medewerkingsplicht bij het opheffen van de beveiliging van de iPhone van een dode terrorist, kreeg het debat hierover wereldwijde media-aandacht.[239] In Nederland kan de doorzoekende autoriteit, in situaties waarin een doorzoeking ter vastlegging van gegevens (art. 125i Nl.Sv) of een netwerkzoeking (art. 125j Nl.Sv) heeft plaatsgevonden, de persoon van wie redelijkerwijs kan worden vermoed dat die kennis draagt van de wijze van beveiliging, bevelen toegang te verschaffen tot de desbetreffende computer (art. 125k lid 1 Nl.Sv). Hetzelfde geldt voor het meewerken aan de ontsleuteling van versleutelde bestanden (art. 125k lid 2 Nl.Sv). Gemakshalve duiden we beide vormen hierna ook wel aan als 'ontsleutelbevel'. Dit kan door zelf de computer te ontsluiten respectievelijk het bestand te ontsleutelen, of – desgevraagd – door de kennis (het wachtwoord, de sleutel) ter beschikking te stellen. Naar Belgisch recht kan een ontsleutelbevel steunen op art. 88quater B.Sv. Ook dat bevat twee soorten medewerkingsplichten in het kader van digitaal speurwerk, waarvoor de onderzoeksrechter bevoegd is: een informatieplicht en een actieve medewerkingsplicht. De informatieplicht kan het verstrekken van login-gegevens tot voorwerp hebben. De actieve medewerkingsplicht kan betrekking hebben op het actief zoeken naar de door de overheid gevraagde data en de ontsleuteling van de eventueel versleutelde systemen, bestanden of gegevens. De personen die worden vermoed bijzondere kennis te hebben over het systeem of de versleutelingsdienst kunnen er dus toe worden verplicht inlichtingen te verstrekken over de werking van het systeem of de diensten en over de mogelijkheid tot toegang tot gezochte data in verstaanbare vorm (bv. het meedelen van de encryptiesleutel of het verschaffen van informatie over de configuratie of beveiliging van het informaticasysteem). De Belgische overheid kan daarnaast ieder geschikt persoon ertoe verplichten, in de mate dat dit in zijn mogelijkheden ligt – dat is het twistpunt bij Apple –, zelf het informatica-

[239] Het heeft zelfs zijn eigen Wikipediapagina: FBI–Apple encryption dispute.

systeem te bedienen of relevante gegevens te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de gevorderde vorm (art. 88quater §2 B.Sv). Met deze medewerkingsplichten wilde de wetgever tegemoetkomen aan het gebrek aan expertise bij de overheid m.b.t. hoogtechnologische evoluties en het tekort aan beschikbare deskundigen. Voorbeelden van medewerkingsplichtigen zijn importeurs/verdelers van computers of software, Trusted Third Parties, dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt en beveiligingsspecialisten.

Opzettelijke weigering mee te werken is in Nederland strafbaar met maximaal drie maanden gevangenisstraf (art. 184 Sr), in België met een gevangenisstraf van zes maanden tot één jaar en met geldboete van (zes maal[240]) zesentwintig tot (zes maal) twintigduizend euro of met een van die straffen alleen. Anders dan in Nederland, is in België voorts iedereen die vanwege zijn bediening dan wel zijn medewerking kennis krijgt van de uitgevoerde maatregel, tot geheimhouding verplicht. Iedere schending van die plicht is strafbaar (art. 88quater § 4 B.Sv). In het kader van de tap formuleert de wetgever vergelijkbare medewerkingsplichten (art. 90quater, §4 B.Sv). De Nederlandse wet kent ook zo een medewerkingsplicht in het kader van de telecommunicatietap, die ook voor communicatieaanbieders geldt, behalve als deze zelf verdachte zijn (art. 126m lid 6-9 Nl.Sv). De Belgische tapregelgeving bevat verder nog een specifieke medewerkingsplicht voor de operator van een communicatienetwerk en de verstrekker van een telecommunicatiedienst tot het verlenen van technische bijstand. De strafmaat bij die medewerkingsplicht is beduidend lichter.[241] Dit verschil is ingegeven door de gedachte dat de operatoren en dienstenaanbieders in het kader van interceptie van telecommunicatie institutionele medespelers zijn van de overheid waarvan meer goodwill kan worden verwacht.[242] Het risico op onwil tot medewerking zou bij anderen dan operatoren en dienstenaanbieders groter zijn. In de praktijk bleek dat niet helemaal te kloppen; het OM vervolgt nu het Luxemburgse bedrijf Skype voor de correctionele

240 De nominale boetebedragen in het Sw moeten worden vermeerderd met opdeciemen, wat neerkomt op een verzesvoudiging.

241 Het Wetboek van Strafvordering voorziet in een gevangenisstraf van zes maanden tot een jaar en een geldboete van 26 euro tot 20 000 euro of een van die straffen alleen voor 'personen met een bijzondere kennis' en een geldboete van 26 euro tot 10 000 euro voor operatoren van een communicatienetwerk en verstrekkers van een telecommunicatiedienst.

242 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 29.

rechtbank van Antwerpen, afdeling Mechelen.[243] Deze zaak zal wellicht verduidelijking brengen over de reikwijdte van de medewerkingsplicht en de toepassing naar de plaats van deze Belgische bevoegdheid.

NIET AAN VERDACHTEN EN VERSCHONINGSGERECHTIGDEN – Het bevel kan in Nederland niet worden gegeven aan verdachten; verschoningsgerechtigden (beroepsgeheimhouders of familieleden) mogen wel het bevel krijgen maar hoeven er niet aan te voldoen (art. 125k lid 3 j° art. 96a lid 3 j° 217-219 Nl.Sv).[244] Voor de medewerkingsplicht uit art. 88quater §2 B.Sv sluit de wetgever de verdachte en de personen bedoeld in art. 156 B.Sv (familieleden die niet moeten getuigen) uit het toepassingsgebied. Voor art. 88quater §1 B.Sv doet hij dat niet. Het Hof van Beroep te Gent besliste nochtans dat de ontsleutelplicht ten aanzien van de verdachte, op grond van art. 88*quater* §1 B.Sv, in strijd is met het *nemo tenetur*-beginsel.[245] Ook naar Belgisch recht verandert de medewerkingsplicht ten aanzien van de beroepsgeheimhouder in een recht. De beperking van het toepassingsgebied is aanzienlijk. Het bewijsmateriaal zal veelal op de computer van de verdachte zelf staan (of in diens cloud) en met de toenemende personalisering van computers zullen ook huisgenoten (als hen al geen verschoningsrecht toekomt) meestal het wachtwoord niet kennen. De bepaling zal daarom vooral relevant kunnen zijn in bedrijfsmatige contexten waarin een (niet-verdachte) systeembeheerder in staat zal zijn de beveiliging ongedaan te maken. We gaan hieronder dieper in op het ontsleutelbevel ten aanzien van de verdachte (*infra*, 3.1.2).

NEDERLAND: BEPERKING TOEPASSINGSGEBIED – Oorspronkelijk – bij de invoering in 1993 – kon het Nederlandse ontsleutelbevel worden gegeven bij een doorzoeking of bij een netwerkzoeking. '*Bij een doorzoeking*' betekende dat het bevel alleen zou kunnen worden gegeven tijdens de doorzoeking, terwijl in de praktijk veelal computers in beslag genomen worden om later te worden onderzocht in alle rust en zorgvuldigheid. Daarom heeft de wetgever bij de Wet computercriminaliteit II de bepaling aangepast: de bevoegdheid is nu mogelijk '*indien toepassing is gegeven aan artikel*

243 *Supra*, noot 210.

244 Voor België, zie: D. DEWANDELEER, 'Misdrijven en strafonderzoek in de IT-context' in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2009-2010, (125) 162-163.

245 Gent 23 juni 2015, *NJW* 2016, afl. 336, 134, noot C. CONINGS.

125i of artikel 125j'.[246] Dat betekent dat bij een doorzoeking *ter inbeslagneming* (dus niet ter vastlegging van gegevens) – waar evengoed beveiligde computers en gegevensdragers zullen worden aangetroffen, die niet zelden in beslag worden genomen – de bevoegdheid nu niet meer kan worden toegepast. Vermoedelijk heeft de wetgever dit niet zo bedoeld of voorzien, maar de wettekst laat moeilijk een andere lezing toe. Teleologisch valt te verdedigen dat het de bedoeling is dat het bevel ook mogelijk is bij een doorzoeking ter inbeslagneming, maar bij een zo expliciete wettekst moet de grammaticale interpretatie overheersen. Dit lijkt een manco in de wetgeving dat in elk geval om aanpassing vraagt.

Ook voor 2006 was de reikwijdte van artikel 125k Nl.Sv echter al beperkt, namelijk tot situaties van computeronderzoek in het kader van een doorzoeking. In de andere gevallen waarin computers of gegevensdragers in beslag kunnen worden genomen (zie par. 2.4) kon, en kan, geen ontsleutelbevel worden gegeven. De logica daarvan valt moeilijk in te zien. Zeker nu beveiliging van computers gemeengoed is geworden en versleuteling van bestanden ook gebruikelijker, lijkt het raadzaam om artikel 125k Nl.Sv uit te breiden tot elk computeronderzoek.[247] De inbeslagname van computers heeft immers (buiten gevallen waarin dat gebeurt om dure computers te verkopen ter ontneming van wederrechtelijk verkregen voordeel) alleen zin als de inhoud kan worden onderzocht, en artikel 125k Nl.Sv is juist bedoeld voor situaties waarin de opsporingsinstanties de beveiliging van de computer of van bestanden niet zelf kunnen doorbreken. Evenals artikel 125l Nl.Sv (over verschoningsgerechtigden) algemeen geredigeerd is (het betreft elk 'onderzoek in een geautomatiseerd werk'), zou ook artikel 125k Nl.Sv van toepassing moeten zijn op elk onderzoek in een computer.

3.1.2. Het ontsleutelbevel aan verdachten

NEDERLAND – Zoals gezegd, is het uitgangspunt vandaag dat een ontsleutelbevel vanwege het *nemo tenetur*-beginsel (dat een verdachte niet hoeft

---

246 *Stb.* 2006, 300, i.w.tr. 1 september 2006. De wetgever koos voor deze formulering in plaats van het eerder voorgestelde '*bij of terstond na een doorzoeking*', dat hij alsnog te beperkend vond. Dat is weinig systematisch, nu het vergelijkbare art. 126nh/uh/zp Sv wel de clausule '*bij of terstond na*' hanteert. Met een contextafhankelijke interpretatie van het begrip '*terstond*' (zo snel als mogelijk is, maar wat mogelijk is hangt van de situatie af, bv. of er een expert beschikbaar is, en om hoeveel gegevens het gaat) hoeft een dergelijke formulering niet te beperkend te zijn.

247 De Tweede Kamer heeft dit punt voorgelegd aan de minister, *Kamerstukken II* 2000/01, 26 671, nr. 6, 11 en 24, maar daarop is deze in de Memorie van Antwoord, *Kamerstukken II* 2004/05, 26 671, nr. 10, niet ingegaan.

mee te werken aan zijn eigen veroordeling) niet kan worden gegeven aan verdachten.[248] In de praktijk zal het niet vaak voorkomen dat iemand anders dan de verdachte kennis heeft van de versleuteling (lees: de sleutel heeft of het wachtwoord kent dat de sleutel beveiligt). Een systeembeheerder kan vaak wel toegang tot een netwerk verschaffen, maar zal meestal niet de cryptosleutels van gebruikers kennen. Dit betekent dus een zware beperking. Het is dan ook niet verwonderlijk dat regelmatig de vraag rijst of het bevel niet toch aan verdachten moet mogen worden gegeven.[249]

Zo werd in het concept-wetsvoorstel Computercriminaliteit II van januari 1998 voorgesteld om het decryptiebevel ook aan verdachten te geven '*indien uit feiten en omstandigheden blijkt van ernstige bezwaren tegen de verdachte en indien het onderzoek dringend noodzakelijk is voor het aan de dag brengen van de waarheid*'. Volgens de Memorie van Toelichting bij dat wetsontwerp was deze inbreuk op het *nemo tenetur*-beginsel gerechtvaardigd.
'*Het blijkt namelijk in de praktijk dat het bij het toenemend gebruik door criminelen van informatietechnologie voor de politie soms zeer moeilijk, zo niet onmogelijk is om het overtuigend bewijs van het strafbaar feit te leveren, aangezien dit letterlijk ligt opgesloten in een computer. Het gaat dan om strafbare feiten die geen andere sporen achterlaten dan in de vorm van gegevensbestanden, zodat het voor de politie ook niet mogelijk is om langs andere weg achter de benodigde gegevens te komen.*'[250]

Het concept achtte deze benadering in overeenstemming met artikel 6 lid 1 EVRM. Dat bleek omstreden. Na diverse protesten uit de juridische wereld die deze inbreuk op het *nemo tenetur*-beginsel onaanvaardbaar achtten, verdween het voorstel uit het wetsontwerp en kwam het ook niet meer terug in de discussie rond Computercriminaliteit II.[251]

---

248 Van 1 januari tot 1 september 2006 is het overigens wel mogelijk geweest een ontsleutelbevel aan de verdachte te geven. De wetgever had in de Wet bevoegdheden vorderen gegevens (i.w.tr. 1 januari 2006) art. 125m-oud Nl.Sv vervangen door een heel andere tekst, zonder de nemo-teneturbepaling voor het ontsleutelbevel die in dat artikel stond elders op te nemen. Dit is gerepareerd in de Wet computercriminaliteit II (i.w.tr. 1 september 2006) door invoering van het huidige art. 125k lid 3 Nl.Sv.

249 Zie reeds COMMISSIE COMPUTERCRIMINALITEIT, *Informatietechniek en strafrecht*, 's-Gravenhage, Staatsuitgeverij, 1987, 87-88, die een ontsleutelbevel aan verdachten niet passend vond, maar tegelijk stelde dat '*een heroverweging omtrent de verdeling van de rechten en plichten in het strafproces pas op zijn plaats [is] indien zou blijken dat de wetshandhaving ernstig in de knel komt. Vooralsnog is dat niet evident*', daarmee implicerend dat wanneer wel empirisch bewijs zou voorliggen dat de wetshandhaving ernstig wordt geblokkeerd door encryptie, heroverweging nodig is.

250 Memorie van Toelichting, Concept Computercriminaliteit II, januari 1998.

251 Zie B.J. KOOPS, 'Cryptografie en strafvordering', in: B.J. KOOPS (red.), *Strafrecht en ICT*, 2e druk, Den Haag, Sdu, 2007, 128, en B.J. KOOPS, *Het decryptiebevel en het nemo-*

De geschiedenis herhaalt zich. Hetzelfde patroon zien we in de discussie over Computercriminaliteit III. Mede naar aanleiding van de zedenzaak rond Robert M. en zijn netwerk, werden Kamervragen gesteld of niet alsnog een ontsleutelplicht voor verdachten moest worden ingevoerd. De minister antwoordde wat terughoudend, maar zegde toe een onderzoek te laten uitvoeren naar de behoefte en juridische haalbaarheid hiervan.[252] Dit onderzoek concludeerde '*dat er enige ruimte is binnen de grenzen van het nemo-teneturbeginsel om een onder strafdreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. De regeling moet dan wel zeer zorgvuldig en afgewogen zijn en rekening houden met alle criteria die het Europees Hof aanlegt. (…) De effectiviteit van een strafrechtelijk gesanctioneerd decryptiebevel dat binnen de nemo-teneturgrenzen blijft, zal gezien de zware eisen niet groot zijn maar zou in incidentele gevallen wel aanwezig kunnen zijn.*'[253] De minister stelde naar aanleiding hiervan, met een wat ruimhartige interpretatie van de conclusie van het onderzoek, voor om een decryptiebevel aan verdachten van terrorisme of van stelselmatige kinderporno (art. 240b lid 2 Sr) te kunnen geven, onder dreiging van (maar liefst) drie jaar gevangenisstraf.[254] Dat riep evenals in 1998 kritiek op in de juridische literatuur[255] en van verschillende instanties in de Internetconsultatie.[256] Naar aanleiding van het advies van de Raad van State de noodzaak en effectiviteit van het voorstel '*dragend te motiveren*' of anders het voorstel te schrappen, mede vanwege spanning met EHRM-rechtspraak,[257] heeft de minister besloten het decryptiebevel aan verdachten uit het wetsvoorstel computercriminaliteit III te halen.[258] De situatie blijft dus bij het oude, althans tot een volgende episode in de decryptiebevelsaga.

BELGIË – De Belgische wetgever sloot de verdachte en diens familieleden,

---

teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?, Meppel/Den Haag, Boom Lemma uitgevers/WODC, serie Onderzoek & Beleid 305, 2012, 68-70, met verwijzingen.

252 *Kamerstukken II* 2010/11, 32 500 VI, nr. 106, 3-4.

253 B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 175.

254 Voorgesteld art. 125k lid 4-7 Sv jo art. 184b Sr. Conceptwetsvoorstel in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), http://www.internetconsultatie.nl/ computercriminaliteit.

255 D.A.G. VAN TOOR, 'Het decryptiebevel en het nemo-teneturbeginsel', *NJB* 2013, 477-479; B.J. KOOPS, 'Cybercriminaliteit', in: S. VAN DER HOF, A.R. LODDER en G.J. ZWENNE (red.), *Recht en computer*, 6e druk, Deventer, Kluwer, 2014, 234.

256 *Kamerstukken II* 2015/16, 34 372, nr. 3, 5.

257 *Kamerstukken II* 2015/16, 34 372, nr. 4, 25-32.

258 *Kamerstukken II* 2015/16, 34 372, nr. 3, 6.

zoals opgesomd in art. 156 B.Sv, enkel uit van het toepassingsgebied van de actieve medewerkingsplicht. Die gedeeltelijke uitsluiting motiveerde hij als volgt: '*De verplichting om bepaalde data te zoeken kan evenwel niet worden opgelegd aan de verdachte, gezien de bescherming tegen zelf-incriminatie. De verdachte moet hier immers, zoals in de context van de getuigenverklaring, zijn zwijgrecht kunnen laten gelden. De andere verplichtingen zijn in dit opzicht evenwel niet onverenigbaar met de vereisten die worden gesteld door het EVRM (zie bijvoorbeeld het arrest Saunders tegen het Verenigd Koninkrijk van 17 december 1996).*'[259] Verschillende rechtsgeleerden stellen zich vragen bij deze summiere motivering van de wetgever en de slechts gedeeltelijke uitsluiting van de verdachte en zijn familieleden van het toepassingsgebied van art. 88quater B.Sv.[260] Het Hof van Beroep te Gent besliste bovendien reeds dat de ontsleutelplicht ten aanzien van de verdachte, op grond van art. 88quater §1 Sv, in strijd is met het *nemo tenetur*-beginsel.[261]

VERZOENBAARHEID MET EVRM – Is de ontsleutelplicht t.a.v. de verdachte inderdaad onverzoenbaar met het zwijgrecht en *nemo tenetur*-beginsel, zoals uitgelegd door het EHRM? Op basis van een analyse van de Belgische preadviseurs,[262] beantwoorden wij deze vraag aan de hand van vier vragen die in de rechtspraak van het Hof aan bod komen. (1) Is er sprake van dwang?; (2) komt het *nemo tenetur*-beginsel in het gedrang: (a) is die dwang voldoende direct gericht op het verkrijgen van zelfincriminerend bewijsmateriaal of (b) tast het de verklaringsvrijheid aan?; (3) raakt de ontsleutelplicht het beginsel in zijn kern?; en als dat niet het geval is, (4) kan de aantasting van het beginsel worden gerechtvaardigd?

VRAAG 1: DWANG? Het *nemo tenetur*-beginsel komt slechts in het gedrang

259 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 27-28.

260 D. DEWANDELEER, 'Misdrijven en strafonderzoek in de IT-context', in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2009-2010, 159-160, noot nr. 126; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 369.

261 Gent 23 juni 2015, *NJW* 2016, afl. 336, 134, noot C. CONINGS.

262 Dit vormt een nuancering van de analyse in: C. CONINGS, 'Statusupdate: Belgische opsporing – voelt zich #verward bij het speuren in sociale media' in E. LIEVENS, E. WAUTERS, P. VALCKE (eds), *Sociale media anno 2015. Actuele juridische aspecten*, Antwerpen, Intersentia, 2015, 288-304. Zie voor een volledige analyse met uitgebreide bespreking van de EHRM-rechtspraak: C. CONINGS, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld,* o.l.v. prof. F. VERBRUGGEN en prof. R. VERSTRAETEN (verwacht: juli 2016) en B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012.

wanneer er sprake is van dwang. Een werkelijke plicht tot ontsleuteling kan maar bestaan door een strafsanctie te koppelen aan de niet-naleving ervan. Er is in dat geval duidelijk sprake van dwang. Ook het EHRM nam al meerdere malen aan dat strafdreiging een vorm van dwang is.[263]

VRAAG 2A: BEWIJSMATERIAAL? – We onderscheiden twee toepassingsgevallen van het *nemo tenetur*-beginsel: het bekomen van zelf-incriminerend bewijsmateriaal onder dwang en het aantasten van de verklaringsvrijheid onder dwang. We gaan eerst dieper in op de vraag of het ontsleutelbevel in aanmerking komt als "*het onder dwang bekomen van zelf-incriminerend bewijsmateriaal*". Het Hof geeft in zijn rechtspraak hieromtrent weinig houvast wat betreft criteria die bepalen of het *nemo tenetur*-beginsel toepassing vindt, wat deze beoordeling moeilijk maakt. We menen uit de rechtspraak te mogen concluderen dat het voornamelijk draait om de vraag in welke mate de overheid haar opsporings- en bewijstaak op de verdachte afschuift.[264] Hier komt onzes inziens de nauwe verbondenheid met het vermoeden van onschuld het meest naar voren.[265] Het *nemo tenetur*-beginsel treedt in werking wanneer opsporingsinstanties niet zeker zijn van het bestaan van een bepaald bewijsstuk, niet weten waar zij het moeten gaan zoeken en daarom het bewijsstuk trachten te bekomen via een informatie- of medewerkingsplicht t.a.v. de mogelijke verdachte. Voor de ontsleutelplicht valt vooreerst te verdedigen dat de plicht enkel is gericht op het verkrijgen van de IT-sleutel (de logingegevens, de code). Opsporingsinstanties bekomen enkel de IT-sleutel onder dwang, niet het mogelijks incriminerende materiaal waartoe de IT-sleutel toegang verleent. We zouden echter ook kunnen stellen

263 EHRM 25 februari 1993, nr. 10828/84, Funke/Frankrijk; EHRM 17 december 1996, nr. 19187/91, Saunders/Verenigd Koninkrijk; EHRM 21 december 2000, nr. 34720/97, Heaney en McGuinness/Ierland; EHRM 21 december 2000, nr. 36887/97, Quinn/Ierland; EHRM 3 mei 2001, nr. 31827/96, J.B./Zwitserland; EHRM 8 april 2004, nr. 38544/97, Weh/Oostenrijk; EHRM 4 oktober 2005, nr. 6563/03, Shannon/Verenigd Koninkrijk; EHRM 29 juni 2007, nrs. 15809/02 en 25624/02, O'Halloran en Francis/Verenigd Koninkrijk; EHRM 14 oktober 2010, nr. 1466/07, Brusco/Frankrijk; EHRM 5 april 2012, nr. 11663/04, Chambaz/Zwitserland.

264 Zie in die zin eveneens: B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 57.

265 Zie bijvoorbeeld EHRM 20 maart 2001, nr. 33501/96, Telfner/Oostenrijk: '*In requiring the applicant to provide an explanation although they had not been able to establish a convincing prima facie case against him, the courts shifted the burden of proof from the prosecution to the defence*.' Het Hof stelt in deze zaak een schending van het vermoeden van onschuld vast.

dat het overhandigen van de sleutel neerkomt op het overhandigen van het mogelijks zelf-incriminerende bewijsmateriaal dat de sleutel onthult. In die zin valt te verdedigen dat de opsporingsinstanties door middel van de plicht niet enkel de IT-sleutel, maar ook het bewijsmateriaal zelf door toedoen van de verdachte verkrijgen. Hier valt over te discussiëren. Opsporingsinstanties komen zelf het versleutelde IT-systeem of de versleutelde gegevens op het spoor. Ze zoeken zelf naar de mogelijks relevante informatie. Net zoals bij klassieke vormen van opsporing ligt de drager van het bewijsmateriaal in sommige gevallen voor het grijpen, maar vergen ze in andere gevallen heel wat speurwerk. Een vaste computer is doorgaans goed zichtbaar, maar een USB-stick neemt tegenwoordig verscheidene vormen aan (bijvoorbeeld een sleutelhanger, een nagemaakte autosleutel, een balpen). Hetzelfde geldt voor het concrete IT-bewijs. Eens het aangetroffen IT-systeem, eventueel met behulp van een ontsleutelplicht, toegankelijk is voor de opsporingsinstanties, is het goed mogelijk dat het bewijsmateriaal direct wordt aangetroffen, bijvoorbeeld op het bureaublad van de computer. Zeker in die situatie zal de verdachte het gevoel hebben met de sleutel ook het bewijsmateriaal zelf te overhandigen; datzelfde gevoel zal echter de verdachte hebben die aan een blaastest meewerkt en door het uitademen direct bewijs levert alcohol te hebben gedronken. Men zou kunnen stellen dat in beide gevallen de verdachte niet het bewijsmateriaal aanlevert, maar een handeling uitvoert die de opsporingsinstantie in staat stelt bewijsmateriaal te verkrijgen. De opsporingstaak wordt daarmee niet per se *verschoven* naar de verdachte. Het is bovendien mogelijk, zeker bij computers en geheugendragers met grote opslagcapaciteit, dat de verdachte het bewijsmateriaal verdoken heeft opgeslagen, zodat de speurders nog steeds zelf actief naar incriminerend bewijs moeten zoeken. Hoe gemakkelijk of moeilijk het speurwerk in de concrete zaak ook is, de overheid spoort het incriminerend materiaal zelf op. De onder dwang verkregen sleutel maakt enkel toegankelijk of leesbaar wat de overheid zelf opspoort. Dat er bij een ontsleutelplicht sprake zou zijn van een werkelijk afschuiven van de opsporings- en bewijstaak, het risico waartegen het EHRM lijkt te willen beschermen, ligt daarom minder voor de hand dan in de door het Hof beoordeelde zaken over de plicht tot overhandiging van bepaalde stukken, zoals *Funke*.

Dat ligt anders bij de ruime medewerkingsplicht uit art. 88*quater* §2 B.Sv, waar de Belgische wetgever de verdachte volgens ons alleszins terecht uitsluit van het toepassingsgebied. Dit artikel behelst immers ook de plicht om zelf actief te *zoeken* naar gegevens (zoals documenten of bestandsmappen) en ze te overhandigen, wat dus ook betrekking zou kunnen hebben

op het zoeken naar en overhandigen van zelf-incriminerende gegevens.[266] Met zo een plicht zou de overheid haar opsporingstaak immers afschuiven op de verdediging, wat in het licht van het *nemo tenetur*-beginsel inderdaad problematisch is. Een uitzondering daarop kan bestaan in het uitzonderlijke geval waarin de overheid weet dat het specifieke bewijsmateriaal bestaat en waar het precies ligt opgeslagen.[267]

Hoewel het problematische karakter van de loutere ontsleutelplicht (het overhandigen van een sleutel of het zelf ontsleutelen van een door opsporingsinstanties gevonden bestand of drager) minder vanzelfsprekend is dan bij de ruime medewerkingsplicht, kan het ontsleutelen en dus toegankelijk en leesbaar maken van wat speurders vinden echter wel als een aspect van de opsporingstaak ten aanzien van het versleutelde worden gezien. Het zoeken door opsporingsinstanties omvat immers ook het doorbreken van barrières (bijvoorbeeld een auto of kluis openbreken). Toegangsverschaffing is in dat licht ook een opsporingstaak; de verdachte kan worden *gevraagd* iets te ontsluiten (en daarmee schade aan auto of kluis te voorkomen) maar niet *gedwongen*. In die zin raakt de ontsleutelplicht, zowel in de vorm van een informatieplicht als actieve medewerkingsplicht, het *nemo tenetur*-beginsel wel, zij het in beperkte mate.

VRAAG 2B: VERKLARING? – We zouden de ontsleutelplicht (zowel via een informatieplicht als actieve medewerkingsplicht) ook kunnen beschouwen als een plicht tot het afleggen van een (impliciete) verklaring. De IT-sleutel is op zichzelf niet direct incriminerend. Het gaat louter om een combinatie van cijfers, letters en tekens. In dat opzicht valt ook te verdedigen dat het meedelen van de IT-sleutel geen verklaring inhoudt, maar een mededeling van een simpel feit; de verdachte kan immers de inhoud van de IT-sleutel niet met een intellectuele inspanning wijzigen. Opsporingsinstanties kunnen de accuraatheid van de IT-sleutel onmiddellijk controleren. Er is dan ook geen risico op een aantasting van de betrouwbaarheid van de verkre-

---

266 Zie in dit licht eveneens: GwH 17 december 2015, nr. 178/2015, 49-52 (m.b.t. het strafuitvoeringsonderzoek).

267 Vgl. de Amerikaanse zaak-*Boucher*, waarin een douaneambtenaar bij een grenscontrole had gezien hoe verdachte desgevraagd een schijfdeel liet zien waarin kinderpornobestanden stonden. Toen later dit schijfdeel versleuteld bleek, kon verdachte wel worden gedwongen de sleutel te geven of zelf de bestanden te ontsluiten; het bestaan van en verdachtes beschikkingsmacht over de kinderpornobestanden was immers een 'uitgemaakte zaak' (*foregone conclusion*). In re Boucher, 2009 WL 424718 (D.Vt. 2009); zie B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 113-116.

gen informatie door de uitoefening van dwang, een belangrijk risico waar het *nemo tenetur*-beginsel en meer specifiek het zwijgrecht aan willen tegemoetkomen. Het meedelen of ingeven van de IT-sleutel kan echter wel indirect incriminerend zijn. De kennis van de code geeft immers aan dat de betrokkene toegang had tot het versleutelde IT-systeem of de versleutelde gegevens. Het kan bijgevolg een belangrijke indicatie zijn dat incriminerend bewijsmateriaal, dat na de decryptie wordt aangetroffen, aan de betrokkene toebehoort.[268] Ook kan het eventueel de gedeeltelijke vervulling van het subjectief delictsbestanddeel aantonen, bv. de wetens-component van het algemeen opzet bij het bezit van kinderpornografie.[269] Hier komt de verklaringsvrijheid wel mogelijks in het gedrang, aangezien de betrokkene door het meedelen of ingeven van de IT-sleutel als het ware verklaart toegang te hebben tot het versleutelde systeem of de gegevens.

VRAAG 3: DE MATE VAN AANTASTING? – Wanneer het EHRM vaststelt dat het *nemo tenetur*-beginsel in het gedrang komt, gaat het na of de kern van dat beginsel wordt geraakt. Het neemt daarbij drie elementen in overweging: de aard en mate van de dwang (1), de waarborgen (2) en het type bevraging en het gebruik van het verkregen bewijs (3). Enkel indien het Hof op grond van die criteria besluit dat de ontsleutelplicht geen schending uitmaakt van de kern van het *nemo tenetur*-beginsel, is een rechtvaardiging van de aantasting van het beginsel mogelijk. (1) Wanneer de plicht wordt afgedwongen met een strafsanctie is de dwang direct. Afhankelijk van het type sanctie en de zwaarte van de mogelijke sanctie is de dwang al dan niet ernstig. Gelet op de huidige mogelijkheid tot vrijheidsberoving in geval van de niet-naleving van art. 88quater B.Sv, is de dwang naar Belgisch recht vandaag ernstig. (2) Op grond van het tweede criterium is het van belang voldoende waarborgen in de procedure in te bouwen. In dit kader rijst o.i. de vraag in welke mate de verdachte de mogelijkheid krijgt om in zijn verdediging te verklaren dat hij de IT-sleutel niet meer kent of dat hij die nooit gekend heeft aangezien het IT-systeem of het concrete bestand niet aan hem toebehoort.[270] Art. 88quater §1 Sv voorziet in de mogelijkheid om een bevel te geven ten aanzien van iedere persoon waarvan de onderzoeksrechter vermoedt dat hij een bijzondere kennis heeft van het betrokken

---

268 B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 137-138.

269 Zie S. MASON, 'Electronic evidence: dealing with encrypted data and understanding software, logic and proof', *Era Forum* 2014, vol. 15, afl. 1, 30.

270 Vgl. EHRM 29 juni 2007, nrs. 15809/02 en 25624/02, O'Halloran en Francis/Verenigd Koninkrijk.

informaticasysteem of van gebruikte beveiligings- of versleuteldienst. Of er sprake is van een aantasting van het *nemo tenetur*-beginsel zal o.i. afhangen van de manier waarop dat vermoeden concreet vorm krijgt. In de voorbereidende werken lezen we in dat verband het volgende: '*Het openbaar ministerie moet het bewijs van de kennis leveren, aangezien het vermoeden niet tot doel heeft de bewijslast om te keren*.'[271] Dat lijkt ons vanuit het *nemo tenetur*-beginsel een belangrijke waarborg. Een andere belangrijke waarborg is rechterlijke toetsing. Aangezien het bevel van art. 88quater §1 B.Sv door of in opdracht van de onderzoeksrechter gebeurt, voldoet de Belgische wet ook daaraan. Verder is het belangrijk dat de verdachte bijstand heeft van een raadsman, zodat hij weloverwogen zijn proceshouding kan bepalen t.a.v. het al dan niet meewerken. De Belgische wet voorziet daar echter niet in. (3) In het licht van het derde criterium is van belang dat de bevraging beperkt is. Het gaat slechts om de mededeling van één of enkele zeer concrete gegevens, die zelf bovendien niet direct incriminerend zijn. De onder dwang verkregen IT-sleutel speelt op zich nauwelijks een rol als bewijsmateriaal, tenzij het afgeven van de sleutel of het ontsleutelen zelf verklarende waarde heeft (zie vraag 2B) en dit een significant onderdeel uitmaakt van de bewijsvoering. Aangezien zoals gezegd de overheid moet bewijzen dat verdachte kennis heeft van de sleutel, zal het meewerken echter geen (aanvullende) verklarende waarde hebben. De afgedwongen informatie is dus enkel de code – een feitelijke mededeling; de opsporingsinstanties zoeken het incriminerend bewijsmateriaal zelf. De overheidstaak blijft in essentie dus bij de opsporingsinstanties.

VRAAG 4: RECHTVAARDIGING? – Op grond van het voorgaande achten we de kans reëel dat het Hof aanvaardt dat er slechts sprake is van een relatief beperkte aantasting van het *nemo tenetur*-beginsel. Alleen de zwaarte van de huidige sanctie zal er waarschijnlijk toe kunnen leiden dat het Hof toch concludeert tot een aantasting in de kern van het recht. Zou de straf echter lager zijn en het Hof een relatief beperkte aantasting vaststellen, dan betrekt het het publiek belang en de nood aan een ontsleutelplicht in zijn overweging om een mogelijke rechtvaardiging te beoordelen. Hoe ernstiger het misdrijf waarvoor de overheid de ontsleutelplicht inzet, en hoe moeilijker het is om met andere middelen bewijsmateriaal te verzamelen, des te groter zal het publiek belang van een ontsleutelplicht zijn. Tegenwoordig bestaan zeer gebruiksvriendelijke versleutelprogramma's die toelaten gesofisticeerde en onkraakbare sleutels te produceren en bovendien gratis beschikbaar zijn

[271] Verslag namens de commissie, *Parl. St.* Senaat 1999-2000, nr. 2-392/3, 69.

op het Internet.[272] Bij gebrek aan een ontsleutelplicht zijn opsporingsinstanties al snel aangewezen op het gebruik van zeer indringende onderzoeksmaatregelen die het heimelijk onderscheppen van paswoorden toelaten, maar vaak disproportioneel zijn. Een effectief onderzoek in informaticasystemen dreigt dan al snel onmogelijk te worden.[273] De nood aan de invoering van een ontsleutelplicht in de wet om rechtshandhaving effectief mogelijk te maken, neemt het Hof mee in overweging.[274] Ook de pertinentie van de plicht speelt een rol bij de beoordeling.

Het blijft echter bij dat alles wel maar de vraag of een ontsleutelplicht voor de verdachte, die doorgaans zal opteren voor de minst zware sanctie, werkelijk kan bijdragen tot efficiëntere criminaliteitsbestrijding.[275] Ook gelaagde versleuteling, waarbij de verdachte kan kiezen om de sleutel te gebruiken die enkel de onschuldige bestanden onthult, tast de pertinentie van de plicht mogelijks aan.[276] Verder denken we aan de wellicht moeilijke weerlegbaarheid van het argument dat de verdachte de code is vergeten. Hoewel de beschikbaarheid van onkraakbare encryptie om ernstige misdrijven te verhullen dus een belangrijk argument oplevert ter rechtvaardiging van een ontsleutelplicht voor verdachten, zijn er ook de nodige vraagtekens te plaatsen bij de te verwachten effectiviteit ervan.

CONCLUDEREND – Op grond van het voorgaande menen we dat een ontsleutelplicht (zowel via een informatieplicht als actieve medewerkingsplicht) ten aanzien van de verdachte, afhankelijk van de concrete vormgeving en waarborgen, in beginsel de *nemo tenetur*-toets van het EHRM kan doorstaan. Wel moet die voldoende pertinent zijn in de praktijk, en dat valt nu te betwijfelen. De kern van het probleem is dit: de (op zich relatief beperkte) inbreuk op het *nemo tenetur*-beginsel is te rechtvaardigen als de ontsleutelplicht een wezenlijke bijdrage kan leveren aan de opsporing van ernstige misdrijven die anderszins moeilijk op te sporen zijn; daarvoor is

---

272 Bijvoorbeeld Veracrypt; zie memorie van toelichting bij het Nederlandse concept wetsvoorstel computercriminaliteit III, mei 2013, 48, https://www.internetconsultatie.nl/computercriminaliteit; B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 37 en 42.

273 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 26-27; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 364-365.

274 EHRM 29 juni 2007, nrs. 15809/02 en 25624/02, O'Halloran en Francis/Verenigd Koninkrijk; B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 52.

275 Zie hierover: KOOPS, *ibid*., 141-144.

276 Advies RvS bij het wetsvoorstel computercriminaliteit III, *Kamerstukken II,* nr. 34372/4, 26-27.

echter een substantiële strafdreiging nodig (anders zullen verdachten niet meewerken), wat de inbreuk waarschijnlijk onaanvaardbaar maakt. En omgekeerd: een inbreuk is aanvaardbaar bij een beperkte mate van dwang (een relatief lichte sanctie), maar dat doet afbreuk aan de pertinentie van de ontsleutelplicht. Het is sterk de vraag of een middenweg (een niet te zware maar ook niet te lichte sanctie) een uitweg uit dit dilemma zou kunnen bieden. Een gevangenisstraf van zes maanden of meer zal al snel een te grote mate van dwang opleveren; een gevangenisstraf van minder dan twee jaar zal al snel niet effectief zijn; er is dus geen enkele ruimte (zelfs een negatieve ruimte) voor een middenweg. In dat licht lijkt het verstandiger om de discussie over een ontsleutelplicht voor verdachten achter ons te laten, en in plaats daarvan alternatieve mogelijkheden te onderzoeken, zoals het verbinden van belastende gevolgtrekkingen of strafmaatoverwegingen aan een decryptieweigering of het beloven van immuniteit bij een ontsleutelbevel aan een mede-verdachte.[277]

3.2. Ontoegankelijkmaking van gegevens

GEGEVENS ALS VOORWERP OF MIDDEL – Volledigheidshalve vermelden we kort nog een aanpalende bevoegdheid. Als bij een doorzoeking gegevens worden aangetroffen die voorwerp uitmaken van een strafbaar feit (bijvoorbeeld kinderporno of bedrijfsgeheimen) of met behulp waarvan een strafbaar feit is gepleegd (een computervirus), kan de officier van justitie of de rechter-commissaris bevelen die gegevens ontoegankelijk te maken als dit '*noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten*' (art. 125o Nl.Sv). Dit is een functioneel equivalent van het in beslag nemen van voorwerpen ter onttrekking aan het verkeer. Voor conservatoir beslag van gegevens met geldwaarde is ontoegankelijkmaking dus niet mogelijk.[278] De bevoegdheid is beperkt tot situaties van een *doorzoeking* in een computer; bij onderzoek aan inbeslaggenomen computers buiten situaties van een doorzoeking (*supra*, 2.4) is ontoegankelijkmaking dus niet mogelijk – wederom een voorbeeld van het niet volledig systematisch invoeren van gegevensequivalenten van de klassieke bevoegdheden die op goederen zien.[279]

---

277 Zie B.J. KOOPS, *Het decryptiebevel en het nemo-teneturbeginsel*, Meppel/Den Haag, Boom Lemma uitgevers/WODC, 2012, 172-173.

278 Zie F.P.E. WIEMANS, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen, Wolf Legal Publishers 2004, 225.

279 In wetsvoorstel computercriminaliteit III wordt voorgesteld art. 126cc uit te breiden met een ontoegankelijkmakingsbevel voor situaties van '*onderzoek in een geautomatiseerd*

VERGELIJKBAAR BELGIË – In België is het ontoegankelijk maken een onderdeel van het gegevensbeslag in art. 39bis B.Sv (*supra*, 2.1.2). Het artikel voorziet in de bevoegdheid om de toegang tot de originele gegevens en kopies daarvan te verhinderen en in de plicht om bepaalde specifiek in de wet omschreven gegevens ontoegankelijk te maken.

Het gaat naast de gegevens die het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf, ook om '*gegevens die strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen*'. Inhoudelijk lijkt dat grotendeels hetzelfde bereik te hebben als de Nederlandse bepaling. Ook op grond van art. 88quater §2 B.Sv kan verder ieder geschikt persoon ertoe worden verplicht, in de mate dat dit in zijn mogelijkheden ligt, zelf het informaticasysteem te bedienen of relevante gegevens ontoegankelijk te maken of te verwijderen, in de gevorderde vorm. Volgens het – door Schoefs bekritiseerd – arrest van het Hof van Cassatie mag een Belgische onderzoeksrechter het gegevensbeslag gebruiken (in zijn functie van stopzetting van het illegaal gedrag) om Belgische ISP's te dwingen om de toegang van Belgische Internetgebruikers tot buitenlandse websites met illegale inhoud af te sluiten.[280] Vanwege het grondwettelijke verbod op preventieve censuur[281] is dat een opmerkelijke beslissing.

---

werk'. Dat vult de lacune niet op, aangezien art. 126cc alleen van toepassing is op bijzondere opsporingsbevoegdheden (blijkens het opschrift van titel VD waar art. 126cc in staat), niet op situaties van bv. inbeslagneming bij aanhouding.

280 Cass. 22 oktober 2013, AR P.13.0550.N, *Computerr.* 2014, afl. 2, 106, noot K. VANDERHAUWAERT, *T.Strafr.* 2014, afl. 2, 126, noot R. SCHOEFS.

281 Art. 25 B.Gw: '*De drukpers is vrij; de censuur kan nooit worden ingevoerd; geen borgstelling kan worden geëist van de schrijvers, uitgevers of drukkers. Wanneer de schrijver bekend is en zijn woonplaats in België heeft, kan de uitgever, de drukker of de verspreider niet worden vervolgd.*'

Hoofdstuk 4. Rechtsbescherming voor bepaalde typen gegevens

Bij onderzoek in computers bestaan diverse vormen van rechtsbescherming. Om de omvang van het preadvies binnen de perken te houden, diepen we bepaalde waarborgen hier niet uit (zoals notificatie of bijstand door de raadsman).[282] We staan wel stil bij rechtsbescherming ten aanzien van bepaalde typen gegevens, omdat dit het meest interessante licht werpt op de systematische inbedding (of lacunes daarin) van computers in het opsporingsonderzoek.

4.1. Beroepsgeheim

BESCHERMING BIJ KLASSIEKE DOORZOEKING – Bij de klassieke doorzoekingsbevoegdheden biedt artikel 98 Nl.Sv bescherming aan het beroepsgeheim van professionele geheimhouders, als bedoeld in artikel 218.[283] Dit artikel bepaalt in lid 5 dat een doorzoeking bij zulke personen (buiten gevallen waarin zij daarvoor toestemming geven) alleen plaatsvindt '*voor zover het zonder schending van het stands-, beroeps- of ambtsgeheim kan geschieden*', en dat deze zich niet uitstrekt '*tot andere brieven of geschriften dan die welke het voorwerp van het strafbare feit uitmaken of tot het begaan daarvan gediend hebben*'. Buiten gevallen van een doorzoeking mogen evenmin (behoudens met toestemming) brieven of andere geschriften die onder het beroepsgeheim vallen in beslag worden genomen, tenzij de rechter-commissaris bepaalt dat van de inhoud kennis mag worden genomen en tot inbeslagneming mag worden overgegaan, een beslissing waartegen beklag openstaat (art. 98 lid 1-4 Nl.Sv).

In de Belgische praktijk gelden voor de klassieke huiszoeking in de wo-

---

282 Zie B.J. KOOPS & Y. BURUMA, 'Formeel strafrecht en ICT', in: B.J. KOOPS (red.), *Strafrecht en ICT*, 2e druk, Den Haag, Sdu 2007 en F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, voor een bespreking van deze waarborgen in Nederland.

283 Professionele verschoningsgerechtigden (art. 218 Nl.Sv) zijn het 'klassieke kwartet' van advocaten (en in het verlengde daarvan medewerkers van een bureau voor rechtshulp), geneeskundigen (inclusief apothekers en verloskundigen), geestelijken en notarissen; journalisten kennen slechts een beperkt verschoningsrecht in de vorm van journalistieke bronbescherming. Zie G.J.M. CORSTENS, *Het Nederlands strafprocesrecht*, bewerkt door M.J. BORGERS, 8e druk, Deventer, Kluwer, 139, en *Kamerstukken II* 2014/15, 34 032, nrs. 1-3 betreffende bronbescherming van journalisten.

ning of het kantoor van een beroepsgeheimhouder[284] ook bijzondere regels. Die liggen opmerkelijk genoeg niet vast bij wet. Vooreerst moeten er ernstige aanwijzingen voorhanden zijn dat er zich bij de beroepsgeheimhouder relevante stukken bevinden die niet (langer) gedekt zijn door het beroepsgeheim.[285] Verder moet, vanwege het delicate karakter van deze zoeking, de onderzoeksrechter haar in principe zelf uitvoeren.[286] Die onderzoeksrechter beoordeelt of een document al dan niet onder het beroepsgeheim valt.[287] Zo mogelijk vindt de huiszoeking plaats in aanwezigheid van een afgevaardigde van de disciplinaire overheid van de geheimhouder.[288] Die moet erop toezien dat geen stukken die onder de bescherming van het beroepsgeheim vallen, het voorwerp uitmaken van een beslag en in het strafdossier belanden. Hij bekijkt de te onderzoeken stukken die op het eerste gezicht een verband vertonen met de uitoefening van het beroep en vormt een oordeel over het beschermde karakter ervan.[289] Dat oordeel is echter niet bindend voor de onderzoeksrechter.[290] Bij omvangrijke dossiers

---

284 Artikel 458 Sw geeft zelf een aantal voorbeelden: geneesheren, heelkundigen, officieren van gezondheid, apothekers en vroedvrouwen. Hieraan kunnen bij wijze van voorbeeld de volgende beroepsgroepen nog worden toegevoegd: bedienaren van de eredienst, advocaten, notarissen en bedrijfsrevisoren. L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR*, Brussel, Larcier, 1962, 237.

285 L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR*, Brussel, Larcier, 1962, 248.

286 Omzendbrief nr. 2011/5 van 25 mei 2011 van het College van Procureurs-generaal betreffende het instituut van de Bedrijfsrevisoren, http://www.om-mp.be/extern/getfile.php?p_name=3979795.PDF&pid=4713163, 8; T. BAUWENS, 'De stafhouder als adviseur en onafhankelijke en onpartijdige rechter' (noot onder Cass. 18 mei 2006), *RW* 2007-08, afl. 11 (436) 437; T. OPGENHAFFEN, 'De huiszoeking en inbeslagname bij advocaten. Voldoet België aan het Europees Verdrag voor de Rechten van de Mens?', *T.Strafr.* 2014, afl. 6, (346) 347.

287 Cass. 2 november 2011, AR P.10.1692.F, *NC* 2012, afl. 4, 303, *RDPC* 2012, afl. 2, 208, concl. D. VANDERMEERSCH; Concl. D. VANDERMEERSCH bij Cass. 2 november 2011, *RDPC* 2012, afl. 2, (208) 210; D. VAN GERVEN, 'Het beroepsgeheim van de advocaat', *TPR* 2012, afl. 4, (1413) 1483.

288 Dat is bv. het geval bij de huiszoeking bij bedrijfsrevisoren (zie omzendbrief nr. 2011/5 van 25 mei 2011 van het College van Procureurs-generaal betreffende het instituut van de Bedrijfsrevisoren, http://www.om-mp.be/extern/getfile.php?p_name=3979795.PDF&pid=4713163, 7). In de rechtspraak en rechtsleer komen doorgaans de huiszoekingen bij de arts en advocaat aan bod.

289 A. JACOBS, 'Les perquisitions dans les cabinets d'avocats. Les usages à l'épreuve de la jurisprudence de la Cour Européenne des Droits de l'Homme', in *Het strafrecht bedreven. Liber Amicorum Alain De Nauw,* Brugge, Die Keure, 2011, (415) 424-426; D. VAN GERVEN, 'Het beroepsgeheim van de advocaat', *TPR* 2012, afl. 4, (1413) 1484; L. VIAENE, *Huiszoeking en beslag in strafzaken,* in *APR*, Brussel, Larcier, 1962, 251.

290 Cass. 18 mei 2006, AR D.05.0015.N, *Arr.Cass.* 2006, afl. 5, 1128, concl. G. DU-

kan de onderzoeksrechter ook het geheel in beslag nemen en in verzegelde omslag bewaren om op een later tijdstip in samenspraak met de afgevaardigde van de disciplinaire overheid tot selectie over te gaan.[291] Verder is er nauwelijks aandacht voor de bescherming van het beroepsgeheim in geval van zoekingen bij derden. België is te zeer afhankelijk van de gewoonten in de praktijk.

BELGIË: COMPUTERS – Anders dan de tapwet (art. 90octies B.Sv[292]) bevat art. 88ter B.Sv, dat de netwerkzoeking regelt, geen bijzonder regime ter bescherming van het beroepsgeheim. De voorbereidende werken stellen in dit verband enkel dat '*dezelfde regels gelden inzake personen die onderworpen zijn aan een beroepsgeheim als in het geval van een klassieke huiszoeking*'.[293] Steeds meer informatie zit vandaag in elektronische informatiesystemen, ook in de woning en zeker in de werkomgeving van de beroepsgeheimhouders. Het

---

BRULLE, *RW* 2007-08, afl. 11, 435, noot T. BAUWENS; Cass. 24 april 2012, AR P.12.0064.N, *Pas.* 2012, afl. 4, 888; F. BLOCKX, 'Zwijgrecht en spreekplicht in het licht van het beroepsgeheim en de discretieplicht' in J. ROZIE, S. RUTTEN, A. VAN OEVELEN, *Zwijgrecht versus spreekplicht,* Antwerpen, Intersentia, 2013, (73) 104; E. BREWAEYS, 'Huiszoeking bij advocaten: de onderzoeksrechter is de baas', *Juristenkrant* 2012, afl. 252, 8. De afgevaardigde van de disciplinaire overheid kan zijn bezwaren hooguit laten acteren in het proces-verbaal van de huiszoeking. In de praktijk verzegelen verschillende onderzoeksrechters de betwiste stukken. Dit laat toe om het stuk achteraf opnieuw te bekijken. Ook het onderzoeksgerecht of de vonnisrechter kan achteraf de relevantie van het beroepsgeheim beoordelen en zo nodig het verzegelde stuk uit het strafdossier of uit de debatten houden. (T. OPGENHAFFEN, 'De huiszoeking en inbeslagname bij advocaten. Voldoet België aan het Europees Verdrag voor de Rechten van de Mens?', *T.Strafr.* 2014, afl. 6, (346) 347 en 353).

291 T. BAUWENS, 'De "Zaak Alzheimer Bis": over geheugenverlies tijdens het gerechtelijk onderzoek. Het beroepsgeheim en de onderzoekshandelingen ten aanzien van advocatenkantoren', *T.Strafr.* 2011, (99) 103.

292 Dat geldt weliswaar enkel voor de woonplaats of de (tele)communicatiemiddelen van een advocaat of arts en voor lokalen, aangewend voor hun beroepsdoeleinden. Een tapmaatregel kan alleen als de beroepsuitoefenaar zelf wordt verdacht van één van de misdrijven die een tapmaatregel kunnen wettigen of als precieze feiten erop wijzen dat een derde, verdacht van één van die misdrijven, gebruik maakt van die lokalen, woonplaats of (tele)communicatiemiddelen. Enkel na een inkennisstelling van de stafhouder of de vertegenwoordiger van de provinciale orde der artsen kunnen de bevoegde overheidsinstanties overgaan tot de uitvoering van de tapmaatregel. De tuchtoverheid heeft volgens de wettekst geen enkele inspraak hoewel de voorbereidende werken spreken van '*samenwerking met de tuchtoverheden'* en het betrekken van de tuchtoverheid in de beoordeling van de onderzoeksmaatregel door de onderzoeksrechter. (Verslag namens de commissie, *Parl. St.* Senaat 1992-93, nr. 843/2, 159 en 188.)

293 MvT, *Parl. St.* Kamer 1999-2000, nr. 50K0213/001, 23.

zal vaak niet mogelijk zijn om de grote hoeveelheid informatie ter plaatse te doorzoeken om onmiddellijk te beslissen welke bestanden wel of niet zijn gedekt door het beroepsgeheim. Vandaar dat bovenvermelde praktijk bij omvangrijke dossiers (gehele inbeslagneming, bewaring in verzegelde omslag om op een later tijdstip in samenspraak met de afgevaardigde van de disciplinaire overheid te selecteren) een digitale tegenhanger heeft gekregen. D. Van Gerven verwijst voor zoekingen bij advocaten naar een aanbeveling van de *Ordre des barreaux francophones et germanophones*.[294] Die laat een ruim databeslag toe, mits dat gepaard gaat met een verzegeling, zodat de informatie achteraf samen met de stafhouder of diens vertegenwoordiger kan worden doorzocht.[295] Dat doorzoeken van de bestanden zou dan gebeuren aan de hand van onderling overeengekomen trefwoorden. Een beslag op het informaticasysteem zou niet toegelaten zijn omdat daardoor de rechten van verdediging van de cliënten in het gedrang komen. De advocaat zou daarom steeds in de mogelijkheid moeten worden gesteld zijn informaticasysteem verder te gebruiken.

NEDERLAND COMPUTERS – Naar analogie met de regeling van de fysieke huiszoeking heeft de Nederlandse wetgever met de Wet computercriminaliteit een bepaling ingevoerd die generieke bescherming biedt bij onderzoek in computers aan gegevens die onder het beroepsgeheim vallen. Artikel 125l Nl.Sv luidt:
'*Naar gegevens die zijn ingevoerd door of vanwege personen met bevoegdheid tot verschoning als bedoeld in artikel 218,*[296] *vindt, tenzij met hun toestemming, geen onderzoek plaats voor zover daartoe hun plicht tot geheimhouding zich uitstrekt. Een onderzoek in een geautomatiseerd werk waarin zodanige gegevens zijn opgeslagen, vindt, tenzij met hun toestemming, slechts plaats, voor zover dit zonder schending van het stands-, beroeps- of ambtsgeheim kan geschieden*.'

294 Aanbeveling van 12 februari 2007 van de OBFG en matière de saisie par un juge d'instruction du matériel informatique d'un avocat,à l'occasion d'une perquisition dans son cabinet ou dans dáutres circonstances, http://obfg.be, 50; D. VAN GERVEN, 'Het beroepsgeheim van de advocaat', *TPR* 2012, afl. 4, (1413) 1485.

295 Eenzelfde benadering vinden we terug in de omzendbrief betreffende het Instituut van de Bedrijfsrevisoren: omzendbrief nr. 2011/5 van 25 mei 2011 van het College van Procureurs-generaal betreffende het Instituut van de Bedrijfsrevisoren, http://www.om-mp.be/extern/getfile.php?p_name=3979795.PDF&pid=4713163, 8.

296 Het wetsvoorstel bronbescherming in strafzaken stelt voor hier een verwijzing in te voegen naar een nieuw artikel 218a, waarin bronbescherming voor journalisten wordt gewaarborgd, zie *Kamerstukken II* 2014/15, 34 032, nrs. 1-3.

De toelichting hierbij is summier – kennelijk betreft het een vanzelfsprekende bepaling: '*In deze bepaling zijn de waarborgen van artikel 98 overgenomen en aangepast aan de situatie van gegevensopslag in een geautomatiseerd werk.*'[297] De aansluiting bij artikel 98 Nl.Sv maakt de daarop ziende jurisprudentie ook naar analogie van toepassing. Dat betekent dat gegevens alleen mogen worden vastgelegd (net zoals brieven en geschriften alleen in beslag mogen worden genomen) als deze *voorwerp van het strafbare feit uitmaken of tot het begaan daarvan gediend hebben*.[298] De bescherming is evenwel, naar de letter, niet volstrekt gelijk: art. 125l Nl.Sv beperkt zich tot onderzoek van gegevens, en zou dus niet van toepassing zijn op voor de hand aangetroffen gegevens (dus op een beeldscherm). Naar de geest moet de bepaling echter worden geïnterpreteerd als gelijkwaardig, zodat justitie voor de hand aangetroffen gegevens niet mag vastleggen (en dus ook niet gebruiken voor nader onderzoek).[299] Door de generieke formulering is art. 125l Nl.Sv van toepassing op alle situaties waarin computers worden onderzocht, dus niet alleen in het kader van een doorzoeking, maar ook alle andere gevallen waarin computers in beslag zijn genomen en worden onderzocht. Het geldt bovendien zowel voor doorzoekingen en inbeslagnemingen bij de geheimhouders zelf als elders. De Hoge Raad neemt daarbij een gelijkaardig standpunt in als de Belgische praktijk: onderzoek in een bij een geheimhouder inbeslaggenomen computer hoeft niet op voorhand beperkt te worden tot bestanden die volgens de geheimhouder niet onder zijn verschoningsrecht vallen, mede omdat '*computerbestanden zich naar hun aard niet eenvoudig lenen voor afzonderlijk onderzoek*'. Hij vindt dat de gehele computer dus mag worden onderzocht, maar wel '*op een wijze waarbij het verschoningsrecht (…) niet in het gedrang komt.*'[300]

DETECTIE BEROEPSGEHEIM-GEGEVENS – Bij de huidige regeling doen zich twee problemen voor, zoals ook in het Discussiestuk in het kader van Herziening Sv opgemerkt. Het eerste is dat het bij onderzoek in computers die bij geheimhouders in beslag worden genomen of onderzocht, duidelijk zal zijn dat er waarschijnlijk gegevens in zitten die onder het verschoningsrecht vallen, zodat de opsporingsambtenaar daarop bij voorbaat alert zal zijn. Dat is echter anders bij onderzoek van de computer van of via derden: de on-

297 *Kamerstukken II* 1989/90, 21 551, nr. 3, 28. (De hieropvolgende zin is weggelaten, die sinds de Wet herziening gerechtelijk vooronderzoek uit 2000 achterhaald is.)

298 F. VELLINGA-SCHOOTSTRA, 'De doorzoeking ter vastlegging van gegevens', in J. BOKSEM E.A. (red.), *Handboek Strafzaken*, Kluwer, 2014, hfd. 14.13, §14.3.4.

299 *Ibid*., §14.3.4.

300 HR 20 februari 2007, LJN-nr. AZ3564.

derzoekende ambtenaar zal dan veelal niet verdacht zijn op de aanwezigheid van geheimhoudergegevens, waardoor deze gegevens als '*bijvangst*' ter kennis kunnen komen van de politie. Dat probleem is moeilijk op te lossen, maar kan tot op zekere hoogte worden ondervangen door een regeling zoals bestaat bij taps (art. 126aa lid 2 Nl.Sv en Besluit bewaren en vernietigen niet gevoegde stukken).[301] Ook in België geldt in de tapwetgeving wel een bijkomende bescherming wanneer die tap gericht is op een niet-beroepsgeheimhouder maar toch toevallig informatie oplevert die door het beroepsgeheim is gedekt. Communicatie beschermd door het beroepsgeheim kan geen onderdeel uitmaken van het proces-verbaal en bijgevolg ook niet van het strafdossier. De politie legt haar in een bestand onder verzegelde omslag neer ter griffie.[302] Indien het gaat om het beroepsgeheim van een arts of advocaat stelt de onderzoeksrechter de vertegenwoordiger van de provinciale orde der artsen respectievelijk de stafhouder in kennis van wat hij beschouwt als (tele)communicatie beschermd door het beroepsgeheim, die de verbalisanten bijgevolg niet in het proces-verbaal mogen opnemen.[303] De achilleshiel van deze wet is dat zij de onderzoeksrechter echter in elk scenario niet dwingt om de betrokken tuchtoverheid in kennis te stellen van de communicatie die volgens die onderzoekrechter niet onder het beroepsgeheim valt. Dat roept de vraag naar het nut van dit procedurevoorschrift op.[304] De voorbereidende werken lijken wel aan te geven dat de tuchtoverheden ook kennis krijgen van wat de onderzoeksrechter in het proces-verbaal opneemt. De opmerkingen die zij daarbij formuleren kan de onderzoeksrechter dan aan het proces-verbaal toevoegen.[305]

ANDERE GEGEVENSDRAGERS – In Nederland is er nog een tweede, wetstechnisch probleem. Artikel 125i Nl.Sv, dat artikel 98 Nl.Sv van overeen-

---

301 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 47. De regeling behelst, kort gezegd, dat processen-verbaal of voorwerpen waarin mededelingen staan die onder het professionele verschoningsrecht vallen, worden vernietigd; wanneer zij echter daarnaast ook mededelingen bevatten die niet onder het verschoningsrecht vallen, kunnen zij eventueel aan het dossier worden toegevoegd met machtiging van de rechter-commissaris.

302 Art. 90sexies §3 B.Sv.

303 Art. 90octies B.Sv. De tuchtoverheid heeft daarbij geen enkele inspraak. L. ARNOU, 'Afluisteren tijdens het gerechtelijk onderzoek', in *Comm. Straf.* 2008, 37.

304 H. BOSLY en D. VANDERMEERSCH, 'La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées', *RDPC* 1995, (301) 316-317.

305 Verslag namens de commissie, *Parl. St.* Senaat 1992-93, nr. 843/2, 188.

komstige toepassing verklaart,[306] omvat onderzoek ter vastlegging van gegevens op papier, op elektronische gegevensdragers en in computers. Artikel 125l Nl.Sv daarentegen, blijft beperkt tot computers en ziet niet op andere gegevensdragers. Vellinga-Schootstra pleit daarom voor herziening, en mogelijk afschaffing, van art. 125l Nl.Sv, omdat het beperkter is dan art. 125i Nl.Sv.[307] Zij gaat daarbij echter voorbij aan het feit dat in ander opzicht art. 125i Nl.Sv juist beperkter is, omdat het alleen gevallen van doorzoeking betreft, en niet van toepassing is op situaties waarin computers in beslag worden genomen buiten de doorzoeking. Opnieuw lijkt er een lacune te bestaan voor geheimhouderbescherming in situaties waarin digitale gegevensdragers in beslag worden genomen bij niet-geheimhouders, bijvoorbeeld een usb-staafje dat in beslag wordt genomen bij aanhouding van een verdachte. Het Discussiestuk stelt dan ook voor om art. 125l Nl.Sv uit te breiden tot alle gegevensdragers,[308] waarbij wellicht enkel dragers van digitale gegevens, niet (ook) papieren gegevensdragers worden bedoeld. Anders zou te veel overlap met artikel 98 Nl.Sv ontstaan. Het zou een verbetering zijn, hoewel we ook wel voelen voor het pleidooi van Vellinga-Schootstra '*voor [integrale] herziening van de doorzoekingswetgeving, waarbij het onzalige onderscheid tussen gegevens en voorwerpen als rechtvaardiging voor de regeling van de materie op twee verschillende plaatsen in het wetboek wordt losgelaten.*'[309] Het is immers de vraag wat nog het verschil zou zijn tussen art. 98 Nl.Sv (brieven en geschriften) en art. 125l Nl.Sv (gegevensdragers en com-

306 Waar beter had kunnen worden verwezen naar artikel 125l Nl.Sv, zie noot 80 en bijbehorende tekst.

307 F. VELLINGA-SCHOOTSTRA, 'Het medisch verschoningsrecht in strafzaken', *DD* 2009/60.

308 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 47. Het discussiestuk suggereert dat dit een codificatie van rechtspraak zou zijn, verwijzend naar Hoge Raad 4 juni 2013, ECLI: NL:HR:2013:BZ0004, waarin bepaald is: '*In aanmerking genomen dat computerbestanden zich naar hun aard niet gemakkelijk lenen voor afzonderlijk onderzoek dient gewaarborgd te zijn dat de inbeslaggenomen gegevensdragers op de voet van art. 125l Nl Sv zullen worden onderzocht op een wijze waarbij het verschoningsrecht van de advocaat niet in het gedrang komt.*' Die uitspraak is echter dubbelzinnig, omdat deze zin wordt voorafgegaan door de zinnen: '*Voor de waarheidsvinding mag onderzoek worden gedaan aan inbeslaggenomen voorwerpen teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen.* ***In computers opgeslagen*** *gegevens zijn daarvan niet uitgezonderd*' (nadruk toegevoegd). Dat maakt het onduidelijk of de term 'gegevensdragers' echt bedoelt te verwijzen naar alle soorten gegevensdragers waarin computerbestanden zijn opgeslagen, of toch alleen naar computers.

309 F. VELLINGA-SCHOOTSTRA, 'Het medisch verschoningsrecht in strafzaken', *DD* 2009/60.

puters), nu het in beide gevallen zou gaan om gegevens die zijn vastgelegd op gegevensdragers, ongeacht de precieze vorm van de gegevens of de gegevensdrager. Hoewel we, anders dan Vellinga-Schootstra,[310] het onderscheid tussen gegevens en voorwerpen niet zouden willen loslaten, omdat gegevens, anders dan voorwerpen, multipel zijn en dus gekopieerd kunnen worden, lijkt een integratie van de klassieke papieren en de nieuwere digitale rechtsbeschermingsbepalingen wel nodig. Daarbij geldt de rechtsbescherming ongeacht de vorm van de gegevensdrager, en is deze (zoals in art. 125l Nl.Sv, maar anders dan in art. 98 Nl.Sv) van toepassing ook buiten gevallen van doorzoeking waarbij gegevensdragers worden onderzocht.

Discussiepunt: Kunnen we de regels van de tapwetgeving ten aanzien van geheimhoudergegevens wel veralgemenen tot alle zoekingen? Talloze personen van wie politie en justitie de computer onderzoekt, gaan communicatie met talloze mensen opslaan, waaronder die met advocaten en artsen. Het is maar de vraag of de disciplinaire overheden van advocaten en artsen bereid zijn om quasi-permanent ter beschikking te staan om, telkens als de computer van een patiënt of cliënt wordt doorzocht, bij te springen om het beroepsgeheim te beschermen. Als advocatuur en medische wereld nog in het beroepsgeheim geloven, zouden ze er goed aan doen om met de ICT-wereld na te denken over technische manieren (elektronische watermerken, bijzondere codes, ...) om binnen grote hoeveelheden gegevens gemakkelijker detecteerbaar te maken welke daarvan door het beroepsgeheim zijn gedekt.

4.2. Inhoud van communicatie

EXTRA BESCHERMING – Communicatie geniet een bijzondere bescherming tegen kennisneming in verband met het communicatiegeheim, maar de reikwijdte daarvan is afhankelijk van de precieze vormgeving in de grondwetten en de manier waarop de wetgever de grondwettelijke bescherming in de loop der jaren heeft geïnterpreteerd bij de vormgeving van opsporingswetgeving. De Belgische Grondwet bevat alleen de historische bescherming van de het briefgeheim (art. 29 B.Gw[311]) en heeft geen specifieke bescherming voor communicatie via andere middelen. Die bekijkt men gewoon als onderdeel van het door art. 22 B.Gw gewaarborgde '*recht*

310 *Ibid*.

311 Art. 29 B.Gw: '*Het briefgeheim is onschendbaar. De wet bepaalt welke agenten verantwoordelijk zijn voor de schending van het geheim der aan de post toevertrouwde brieven*.'

op eerbiediging van het privé-leven', dat geldt '*behoudens in de gevallen en onder de voorwaarden door de wet bepaald*'. In België is art. 8 EVRM de centrale norm in het debat over indringende opsporingsmethoden. In Nederland maakt art. 13 Nl.Gw een onderscheid tussen brieven (waarbij altijd rechterlijke toestemming nodig is voor kennisneming van inhoud) en telefoongesprekken en telegrammen (waarvoor kennisneming mogelijk is door bij wet aangewezen autoriteiten). E-mail en andere nieuwe communicatievormen zullen pas onder de reikwijdte van artikel 13 Nl.Gw vallen als het huidige wetsvoorstel ter actualisering[312] wordt aangenomen en in werking treedt. Dat kan nog vele jaren kan duren.

INCONSISTENTIES NEDERLAND – De Nederlandse strafvorderlijke wetgeving maakt dienovereenkomstig een onderscheid tussen (gesloten) brieven en andere vormen van communicatie. De wetgever heeft de niet-grondwettelijk beschermde elektronische communicatie over het algemeen hetzelfde geregeld als de wel grondwettelijk beschermde telefonische communicatie. Geheel consistent is de regeling echter niet, en evenmin geeft de wetgeving blijk van een eenduidige visie op wat nu precies beschermwaardig is in communicatie-inhoud. Een grondige bespreking hiervan is te complex voor dit rapport,[313] maar de belangrijkste inconsistenties komen kort gezegd op het volgende neer.

Ten eerste geldt de grondwettelijke bescherming alleen tijdens transport, dus voor zover een bericht in de beschikkingsmacht is van een communicatieaanbieder.[314] Brieven kennen echter ook aanvullende bescherming buiten de transportfase (bijvoorbeeld als ze bij verzender of ontvanger thuis liggen), mits ze gesloten zijn. Kennisneming is dan namelijk alleen mogelijk met toestemming van de rechter-commissaris en er geldt een geheimhoudingsplicht (art. 102a j° 101 en 102 Nl.Sv). Die aanvullende bescherming geldt echter niet voor andere vormen van (beveiligde) communicatie, zoals (ongelezen of beveiligde) e-mailberichten die bij een doorzoeking bij de verdachte in diens computer worden aangetroffen. Deze discrepantie kent geen duidelijke ratio, al is de achtergrond van de wettelijke regeling wel enigszins te begrijpen vanuit de historische ontwikkeling, waarbij artikel 102a Nl.Sv een laatste overblijfsel is van de veel oudere ge-

312 *Kamerstukken II* 2013/14, 33 989, nrs. 1-3.

313 Zie voor uitgebreide analyses en kritiek B.J. KOOPS, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer, 2002 en B.J. KOOPS, 'Van brieven, geschriften en onbegrijpelijke wetgeving', *DD 33* (8), 850-878.

314 Zie *Kamerstukken II* 2013/14, 33 989, nr. 3, hfd. 2, met verwijzingen.

schriftenbescherming die bij de regeling van de doorzoeking in de 19e en 20e eeuw bestond, waarbij aanvankelijk '*geschriften, boeken en andere papieren*' (art. 107 Nl.Sv-1838, art. 111 Nl.Sv-1886) en later '*brieven en andere geschriften*' (art. 113 Nl.Sv-1926) bij een huiszoeking alleen onderzocht mochten worden met uitdrukkelijk verlof van de rechtbank. In 2000 is deze bescherming verder ingeperkt tot brieven (door afschaffing van art. 113 en invoering van art. 102a Nl.Sv), in de kennelijke (maar onjuiste) veronderstelling dat deze vorm van bescherming tijdens een doorzoeking samenhing met het briefgeheim, terwijl de oorsprong lag in een sui generis-bescherming van papieren en geschriften.

Het discussiestuk in het kader van Modernisering Sv wijst terecht op de hierdoor ontstane inconsistente regeling en stelt voor om de bescherming van brieven te beperken tot het grondwettelijk vereiste, namelijk de transportfase.[315] Dat is wat België doet (*infra*). Een alternatief is om ook andere communicatie te gaan beschermen op dezelfde manier als brieven onder artikel 102a Nl.Sv, maar dat zou op '*grote praktische bezwaren*' stuiten en wordt daarom afgewezen.[316] Hoewel dat laatste geen sterk argument is – rechtsbescherming moet worden vormgegeven op inhoudelijke gronden, en niet primair worden beïnvloed door praktische bezwaren – valt het voorstel uit het discussiestuk om artikel 102a Nl.Sv af te schaffen wel te billijken. Het maakt de wetgeving beter in lijn met de ratio van de grondwettelijke communicatiebescherming, die immers beperkt is tot de transportfase. Buiten de beschikkingsmacht van een communicatieaanbieder is er immers geen dwingende reden om communicatie anders te behandelen dan andere vormen van gegevens, die evenzeer (of even weinig, afhankelijk van het geval) privacygevoelig kunnen zijn (denk aan dagboeken, naaktfoto's, financiële administratie). Tegelijkertijd valt wel te betreuren dat met de invoering van artikel 102a Nl.Sv en de aankomende afschaffing ervan het historische besef van de geschriftenbescherming geheel dreigt te verdwijnen. De wetgever was in de 19e en het grootste deel van de 20e eeuw veel terughoudender om opsporende ambtenaren die een huis doorzoeken de aldaar opgeslagen papieren en geschriften te laten lezen. Die zijn immers veelal privacygevoeliger en bovendien relevanter voor de vrijheid van meningsuiting dan de meeste (niet-gegevensdragende) objecten. Nu willen we niet pleiten voor herinvoering van de geschriftenbescherming, maar wel aandacht vragen voor het feit dat gegevensdragers, *doordat* zij gegevens dra-

315 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 36.

316 *Ibid*., 49.

gen, een bijzonder inzicht kunnen geven in de persoonlijke levenssfeer. Kennisneming van die gegevens vergt adequate bescherming; de teloorgang van de geschriftenbescherming en de voorgestelde afschaffing van artikel 102a Nl.Sv onderstrepen het onverminderde belang om computeronderzoek (maar ook het onderzoek van andere gegevensdragers) een hoog beschermingsniveau te geven.

Verdere inconsistenties treffen we aan in de regeling van onderzoek van communicatie dat plaatsvindt bij of via communicatieaanbieders. Voor doorzoeking bij aanbieders van openbare telecommunicatie is in 2006 een specifieke bepaling ingevoerd met een vergelijkbare strekking als artikel 114 Nl.Sv dat voor post geldt: van bij telecomaanbieders opgeslagen berichten (zoals webmail of stempost) mag slechts met machtiging van de rechtercommissaris worden kennisgenomen, en alleen voor zover de berichten van of voor de verdachte zijn, op de verdachte betrekking hebben, of voorwerp uitmaken van het strafbare feit (art. 125la Nl.Sv).[317] De bepaling geldt volgens de wettekst echter alleen voor berichten aangetroffen bij een doorzoeking *ter vastlegging van gegevens*, niet bij een reguliere doorzoeking ter inbeslagneming, waarbij immers ook computers doorzocht en gegevens gekopieerd mogen worden. Verder lijkt het alleen te gelden voor onderzoek tijdens de doorzoeking, niet voor onderzoek aan een gegevensdrager die bij een doorzoeking in beslag is genomen en later wordt onderzocht. Het discussiestuk stelt dan ook terecht voor de bescherming generieker te maken tot onderzoek aan gegevensdragers en in geautomatiseerde werken die in gebruik zijn bij een aanbieder van een communicatiedienst.[318] Dat laatste zou ook de inconsistentie herstellen dat deze bepaling nog de oude formulering '*aanbieders van openbare telecommunicatienetwerken of -diensten*' gebruikt, terwijl het wetboek bij de interceptiebepalingen sinds de Wet computercriminaliteit II spreekt van '*aanbieders van communicatiediensten*', waar ook besloten telecommunicatie onder valt.

Tot slot ziet het discussiestuk Modernisering Sv '*enige inconsistentie*' in de verdenkingsvoorwaarden voor onderzoek van communicatie, uiteenlopend van verdenking van elk strafbaar feit (bij doorzoeking door rechtercommissaris) tot verdenking van een voorlopigehechtenismisdrijf met ernstige inbreuk op de rechtsorde (bij vorderen van inhoud van e-mail bij

317 Ingevoerd bij de Wet bevoegdheden vorderen gegevens, *Stb.* 2005, 390.

318 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 48. We nemen aan dat dit dan ook gaat gelden voor het binnendringen op afstand in een computer van een communicatieaanbieder (voorgesteld art. 126nba Nl.Sv), hetzij direct in de serverruimte hetzij als verlengstuk het binnendringen in de computer van de verdachte.

communicatieaanbieders). Voorgesteld wordt dit te uniformeren, bijvoorbeeld tot '*verdenking van een misdrijf waarop vier jaren of meer is gesteld*'.[319] Ook hier verdient het streven naar consistentie steun, en de voorgestelde maatstaf lijkt niet onredelijk. Toch betekent het weer een significante verruiming van het vorderen van communicatie-inhoud bij communicatieaanbieders. Daar bestaat nu de zwaarste voorwaarde voor, opmerkelijk genoeg zwaarder dan voor de vordering tot uitlevering van brieven aan de postvervoerder, terwijl dit juist in het huidige tijdperk de meest voorkomende vorm van het bemachtigen van communicatie-inhoud bij aanbieders is.

BELGIË – In België bevat art. 29 B.Gw de mogelijkheid om bij wet '*schending van het geheim der aan de post toevertrouwde brieven*' toe te laten. Het in 2003 ingevoerde art. 46ter §1 B.Sv gaat specifiek over brieven: '*Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings aan een postoperator toevertrouwde post, bestemd voor of afkomstig van een verdachte of die op hem betrekking heeft, onderscheppen en in beslag nemen, wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben.*'[320] De drempel ligt op voorlopigehechtenismisdrijven (dat is in België immers vanaf één jaar gevangenisstraf) en de nadruk ligt op het beslag. Voor de eigenlijke doorzoeking geldt art. 88sexies B.Sv: alleen de onderzoeksrechter is gemachtigd onderschepte en in beslag genomen post te openen en kennis te nemen van de inhoud ervan, maar bij ontdekking op heterdaad kan de procureur des Konings deze bevoegdheid ook uitoefenen. Een bijzondere bescherming voor brieven van advocaten en artsen geldt. Hun brieven kunnen slecht worden geopend wanneer zij zelf verdacht zijn van een voorlopigehechtenismisdrijf. De disciplinaire overheid wordt bovendien ingelicht, maar er is geen echte wettelijk voorgeschreven filterbijstand.[321] De voorschriften van art. 46ter en 88sexies B.Sv gelden enkel voor brieven *in de periode waarin zij*

---

319 *Ibid*., 49-50.

320 Het kan ook proactief (art. 46ter §1, tweede lid B.Sv) en (derde lid): '*indien de procureur des Konings van oordeel is de inbeslagneming niet te moeten handhaven, geeft hij de stukken onverwijld aan de postoperator voor verdere verzending terug.*' Voor de briefwisseling van gedetineerden en de controle op de inhoud bestaat er een specifieke wettelijke regeling in art. 55, 56, 57 en 66 basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden.

321 Art. 88sexies, derde lid B.Sv: '*Deze maatregel kan slechts betrekking hebben op de post van een advocaat of een arts, wanneer deze er zelf van verdacht worden één van de strafbare feiten bedoeld in artikel 46ter, § 1, eerste lid, gepleegd te hebben. Deze maatregel kan niet ten uitvoer worden gelegd zonder dat de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is.*'

aan de post zijn toevertrouwd. De Belgische wetgeving heeft nooit een ruimere geschriftenbescherming gekend. Bovendien valt een belangrijk verschil op tussen traditionele en elektronische post. De kennisneming van de inhoud van privécommunicatie en telecommunicatie tijdens de overbrenging ervan (de tap), kan in België alleen als het onderzochte misdrijf prijkt op de uitdrukkelijke lijst van '*tapbare*' (zeer ernstige) misdrijven in art. 90ter §2 B.Sv. Voor de kennisname van de inhoud van onderschepte post is er geen beperkende lijst van misdrijven. Waarom de Belgische wetgever vindt dat, ondanks art. 29 Gw, klassieke brieven minder bescherming verdienen dan elektronische communicatie, is niet duidelijk. Misschien vond men toen de brievenopening er kwam in 2003, de tapwet uit 1994 te streng, misschien had men veeleer de (minder strenge) regels van het beslag in het achterhoofd[322], maar echt consistent is het niet. Terwijl in Nederland de inhoud van (gesloten) brieven meer bescherming lijkt te krijgen dan de inhoud van elektronische communicatie, is het in België dus net wat minder. De Belgische wetgever heeft alleszins zowel voor papieren als voor elektronische post de bescherming[323] beperkt tot de fase waarin de communicatie onderweg is, met de woorden '*aan de post toevertrouwd*' respectievelijk '*tijdens de overbrenging ervan*'. Buiten de overbrenging gelden de algemene regels, zoals die van de huiszoeking, informaticazoeking en netwerkzoeking en de medewerkingsplichten uit art. 88quater B.Sv. De opkomst van webmail en cloudservices heeft natuurlijk gezorgde voor debatten over wanneer e-mails of andere berichten nu wel of niet '*in overbrenging zijn*'. Het debat gaat o.m. over '*aangekomen, maar nog niet door de bestemmeling geopende email op servers*'[324], over verzonden mails, waarvan men bij doorzoeking van het sys-

322 Het artikel heeft het immers over in het kader van art. 46ter B.Sv '*onderschepte en in beslag genomen post*'. '*Indien de onderzoeksrechter van oordeel is de inbeslagneming niet te moeten handhaven*' kan die kiezen om het poststuk alsnog terug te sluiten en toch naar de geadresseerde laten verzenden (88sexies §2 B.Sv).

323 Toch voor zover het gaat over bescherming tegen politie en justitie. Opmerkelijk genoeg is voor de bescherming tegen de inlichtingen- en veiligheidsdiensten de regeling anders. De wetteksten (art. 18/1, §2, 4°, 18/6. §1 en 18/14. §1 Wet BIM) hebben het daar over '*al dan niet aan een postoperator toevertrouwde post*'.

324 Corr. Leuven 4 december 2007, *T.Strafr.* 2008, afl. 3, 223, noot L. Ceulemans; L. CEULEMANS, 'De kennisname van e-mails "tijdens de overbrenging ervan", een verduidelijking van het telecommunicatiegeheim' (noot onder corr. Leuven 4 december 2007), *T.Strafr.* 2008, afl. 3, 226-231; D. DEWANDELEER, 'Misdrijven en strafonderzoek in de IT-context' in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2009-2010, 153-158; P. VAN LINTHOUT, J. KERKHOFS, 'Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel', *T.Strafr.* 2008, 79-94.

teem van de verzender niet zeker kan weten of die de bestemmeling al heeft bereikt en dus '*in overdracht*' was, over groepsberichten (WhatsApp, beperkte Twitteraccount, ...) die door sommige bestemmelingen zijn bekeken, maar door andere niet, of over ontwerp-mailberichten die nooit zijn verstuurd (dus nooit '*in overdracht*'), maar wel gelezen zijn door verschillende personen die inloggegevens delen[325]. De rechtsleer geeft uiteenlopende interpretaties[326]. Onderzoeksrechters trachten, als er onduidelijkheid is of men communicatie in overdracht zal aantreffen, problemen te voorkomen door voor alle zekerheid naast de tap ook de netwerkzoeking te bevelen[327]. Omdat de netwerkzoeking en het databeslag echter nog niet heimelijk mogen gebeuren, is dit geen echte oplossing. Vandaar dat de geplande hervorming van de regering, die de (heimelijke) zoeking in informaticasystemen en de toegang tot de inhoud van privé(tele)communicatie in een geïntegreerd systeem wil samenbrengen, de juiste keuze lijkt. Het valt wel af te wachten welke drempels en waarborgen dan zullen gelden. Met haar plannen voor het najaar van 2016, lijkt de Belgische regering het idee uit de analoge tijd, dat tijdens de overbrenging – en alleen dan – de overheid kennis kon nemen van de inhoud van de communicatie, omdat die daarna '*vervlogen*' is, wel los te laten. Ze lijkt dus van plan de bevoegdheid tot het heimelijk doorzoeken van informaticasystemen (en dus onder meer communicatie voor en na de overbrenging) en de telecommunicatieonder-

325 C. CONINGS, P. VAN LINTHOUT, 'Sociale media: een nieuwe uitdaging voor politie en justitie', *Panopticon* 2012, afl. 3, (205) 222-223; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 245-246.

326 L. ARNOU, 'Afluisteren tijdens het gerechtelijk onderzoek' in X, *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer,* Mechelen, Kluwer, afl. 59, 12-18; L. CEULEMANS, 'De kennisname van e-mails "tijdens de overbrenging ervan", een verduidelijking van het telecommunicatiegeheim' (noot onder corr. Leuven 4 december 2007), *T.Strafr.* 2008, afl. 3, 226-231; P. DE HERT, 'Internetrechten in het bedrijf. Controle op *e-mail* en Internetgebruik in Belgisch en Europees perspectief', *AM* 2001, afl. 1, (110) 124-125; D. DEWANDELEER, 'Misdrijven en strafonderzoek in de IT-context' in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2009-2010, 153-158; J. DUMORTIER, R. VANHECKE, S. MISSOTTEN, 'Laat de Belgische wetgeving gerechtelijk aftappen van privécommunicatie via gsm of internet toe', *Computerr.* 1997, afl. 4, (145) 149; P. VAN LINTHOUT, J. KERKHOFS, 'Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel', *T.Strafr.* 2008, 79-94; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 276-290. Zie eveneens: Corr. Leuven 4 december 2007, *T.Strafr.* 2008, afl. 3, 223, noot L. CEULEMANS.

327 P. VAN LINTHOUT, J. KERKHOFS, 'Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel', *T.Strafr.* 2008, 93; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 290-295.

schepping (tijdens de overbrenging) in een gefuseerde bevoegdheid te brengen. Bij gebrek aan tekstvoorstellen kunnen we op de details nog niet ingaan.

4.3. Gevoelige persoonsgegevens

BIJZONDERE PERSOONSGEGEVENS – De wetgeving ter bescherming van persoonsgegevens maakt een onderscheid tussen '*gewone*' en '*bijzondere*' persoonsgegevens. De laatste zijn bepaalde categorieën gevoelige persoonsgegevens, waarbij een hoger risico van discriminatie bestaat, zoals gegevens betreffende ras, religie of gezondheid. De verwerking van 'gevoelige' persoonsgegevens is aan zwaardere voorwaarden gebonden (art. 16 e.v. Wbp, art. 6 en 7 Privacywet). Dat geldt ook voor verwerking van '*gevoelige*' persoonsgegevens in de politiële sector (art. 5 Wpg, art. 8 Privacywet en art. 44/1 §2 WPA).

BIJZONDERE BEPALING IN NEDERLAND – In de Nederlandse strafvorderingswetgeving komt het onderscheid tussen 'gewone' en 'gevoelige' gegevens bij één type bevoegdheid voor: het vorderen van gegevens. Bij de invoering van de Wet bevoegdheden vorderen gegevens[328] is een onderscheid gemaakt tussen het vorderen van identificerende (126nc Nl.Sv), 'gewone' (126nd Nl.Sv) en 'gevoelige' (126nf Nl.Sv) gegevens. Voor het laatste is toestemming van de rechter-commissaris nodig.[329] Het onderscheid is niet doorgevoerd bij de gelijktijdig ingevoerde bevoegdheid tot doorzoeking ter vastlegging van gegevens:
'*Het onderscheid naar categorieën gegevens (identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens) is bij de doorzoeking moeilijk hanteerbaar omdat de met opsporing belaste instantie bij de doorzoeking vooraf niet weet wat hij aan zal treffen. Dat is ook nu het geval bij toepassing van de bevoegdheid tot doorzoeking ter inbeslagneming van een voorwerp.*'[330]
AFSCHAFFEN? – De Contourennota Modernisering Sv stelt voor het onderscheid te laten vervallen, omdat het inconsistent en onpraktisch zou zijn:
'*In de tweede plaats wil ik het expliciete onderscheid tussen identificerende gegevens, gevoelige gegevens en andere gegevens, met de daaraan gekoppelde gedifferentieerde*

328 *Stb.* 2005, 390.

329 Hetzelfde geldt voor het vorderen van inzage in bescheiden of gegevens bij een strafrechtelijk financieel onderzoek, waarbij 'gevoelige' gegevens zijn uitgezonderd van de bevoegdheid van de opsporingsambtenaar inzage te vorderen (art. 126a lid 1 onder a jo 126nd).

330 *Kamerstukken II* 2003/04, 29 441, nr. 3, 11.

verdenkingscriteria, laten vervallen. Dit onderscheid naar de aard van de te vergaren gegevens kent de wet niet ten aanzien van de andere vormen van gegevensvergaring. Bovendien leidt de huidige, zeer strenge wettelijke normering van de bevoegdheid om gevoelige gegevens te vorderen, tot problemen waaraan men in de praktijk het hoofd tracht te bieden door andere bevoegdheden tot het vergaren van gegevens toe te passen, zoals het bevel tot uitlevering van de gegevensdrager waarop de gewenste gegevens zijn opgeslagen. Ook in deze zin is betere afstemming tussen de bestaande bevoegdheden gewenst.'[331]

De praktijkproblemen ontstaan onder andere door de kwalificatie van persoonsgegevens als gevoelig. Zo zijn foto's van personen haast per definitie gevoelig omdat het ras (en mogelijk de gezondheidsstatus) van personen eruit is af te leiden, wat betekent dat voor het vorderen van foto's van personen altijd rechterlijke toestemming nodig is.[332] De opkomst van Big Data Analytics versterkt deze problematiek nog, omdat uit de combinatie van willekeurig welke gegevens in potentie ook vaak gegevens over bijvoorbeeld gezondheid, religie, politieke of seksuele voorkeur zijn af te leiden. In dat licht lijkt het voor de hand te liggen het onderscheid op te heffen.[333]

BEHOUDEN? – Het lijkt echter wat vroeg om de aanvullende bescherming voor 'gevoelige' gegevens simpelweg te laten vervallen. Ook de nieuwe generatie persoonsgegevensbeschermingswetgeving handhaaft immers het onderscheid: '*Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden verdienen specifieke bescherming aangezien de context van de verwerking ervan aanzienlijke risico's voor de grondrechten en fundamentele vrijheden kan meebrengen.*'[334] De vraag is of voor de bescherming van gevoelige gegevens kan worden volstaan met bepalingen in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Aangezien het vergaren van gegevens ook een belangrijke vorm van verwerking is, ligt het voor de hand om ook in de regeling van strafvordering bepalingen op te nemen om te voorkomen dat gevoelige persoonsgegevens zonder aanvullende waarborgen worden verzameld.

---

331 *Kamerstukken II* 2015/16, 29 279, nr. 278, 64.

332 Zie over deze problematiek G.J. ZWENNE en L. MOMMERS, 'Zijn foto's en beeldopnamen "rasgegevens" in de zin van artikel 126nd Sv en artikel 18 Wbp?', *P&I* 2010(5), 237-247.

333 Zie ook E.M.L. MOEREL en J.E.J. PRINS, 'Privacy voor de homo digitalis', in: *Homo digitalis. Handelingen Nederlandse Juristen-Vereniging 2016-I*, 1-136 op p. 82-90.

334 Overweging 37, Richtlijn 2016/680/EU (bescherming persoonsgegevens bij opsporing en vervolging).

Hoewel de praktische en wetssystematische argumenten uit de Contourennota op het eerste gezicht aannemelijk lijken, zijn zij niet volstrekt overtuigend. Weliswaar zit er een asymmetrie tussen de regeling van doorzoeking en die van gegevensvordering in de bescherming van persoonsgegevens, maar dat komt vooral door de manier waarop de wetgever de vorderingsbevoegdheden heeft geformuleerd. In plaats van een onderscheid naar type persoonsgegevens, had het meer voor de hand gelegen om een onderscheid te maken naar type geadresseerde. De toelichting bij de wet maakt immers duidelijk dat art. 126nf Nl.Sv moet worden ingezet wanneer vooraf duidelijk is dat (naar verwachting, waarschijnlijk) gevoelige gegevens bij de gevorderde gegevens zullen zitten. Dit blijkt vooral afhankelijk van de aard van de bevraagde gegevensverwerker: '*Dit betekent bijvoorbeeld dat van een kerkgenootschap, een vakvereniging of een vereniging van personen die een bepaalde aandoening hebben alleen op basis van de bevoegdheid tot het vorderen van gevoelige gegevens, gegevens gevorderd kunnen worden*.'[335] Bij andere geadresseerden, waar men niet op voorhand hoeft te verwachten dat deze gevoelige gegevens verwerkt, kan de 'gewone' bevoegdheid van art. 126nd Nl.Sv worden ingezet; als achteraf blijkt dat er gevoelige gegevens bij de gevorderde gegevens zitten, kunnen deze gewoon (als bijvangst) worden gebruikt.[336]

AANKNOPINGSPUNT – De redenering is vergelijkbaar met de ratio van het onderscheid tussen plaatsen bij de regeling van doorzoeking. Daar bestaat weliswaar geen expliciete bescherming van gevoelige gegevens, maar indirect is dat wel het geval. Sommige plaatsen zijn uit de aard der zaak 'gevoelig', in de zin dat het waarschijnlijk is dat er gevoelige gegevens worden aangetroffen. Daarom worden geheimhouderkantoren (evenals woningen) apart behandeld, met de waarborg van een rechterlijke machtiging voor doorzoeking. De doorzoekingsregeling maakt aldus een onderscheid tussen situaties waarin het vooraf meer of minder waarschijnlijk is dat een zware inbreuk zal worden gemaakt op grondrechten. De plaats van doorzoeking, en niet het type gegevens dat gezocht wordt op deze plaats, fungeert hierbij als een aanknopingspunt voor de verwachte grondrechteninbreuk. Vergelijkbaar hiermee zou de gegevensvorderingsbevoegdheid ook de geadresseerde hebben kunnen gebruiken als aanknopingspunt, in plaats van het type gevorderde gegevens.

Dit betekent dat, hoewel het onderscheid tussen 'gewone' en 'gevoelige' gegevens moeilijk valt te maken, de wetgeving wel een indirecte be-

335 *Kamerstukken II* 2003/04, 29 441, nr. 3, 10.
336 *Kamerstukken II* 2003/04, 29 441, nr. 3, 10-11.

scherming kan bieden aan gevoelige gegevens, door een geschikt aanknopingspunt te vinden om situaties te beschrijven waarin het op voorhand te verwachten valt dat er gevoelige gegevens zullen worden vergaard. De doorzoekingsregeling doet dat door voor geheimhouderkantoren en woningen een rechterlijke machtiging te eisen. De gegevensvorderingsbevoegdheid zou het kunnen doen door een rechterlijke machtiging te eisen voor vorderingen aan verwerkers van gevoelige persoonsgegevens, zoals kerkgenootschappen of ziekenhuizen. Voor andere gevallen waarin computers worden onderzocht, kan nagedacht worden over een analoge regeling, met de strekking dat het onderzoek in situaties waarin vooraf te verwachten valt dat de computer gevoelige gegevens bevat, een rechterlijke machtiging nodig is. Te denken valt aan het onderzoek aan de inbeslaggenomen smartphone van een vakbondsbestuurder, of het onderzoek van computers bij een doorzoeking van een webwinkel die medicijnen of porno verkoopt.

BELGIË – Met uitzondering van de bepalingen over het beroepsgeheim, maakt de Belgische regeling voor doorzoeking geen bijzonder onderscheid in functie van de gegevens. Voor identificatie- en verkeersgegevens inzake telecommunicatie en het gebruik van elektronische diensten, zijn er met art. 46bis en 88bis B.Sv specifieke bepalingen[337], net als voor klassieke post. Ten aanzien van banken of de kredietinstellingen bestaat er het specifieke 46quater B.Sv. De wetgever lijkt vreemd genoeg financiële informatie, die indirect toch leidt tot vele andere informatie over het privé- en beroepsleven, als niet zo gevoelig te beschouwen. De procureur kan die immers vorderen zonder enige rechterlijke machtiging, zodra '*er ernstige aanwijzingen zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben*'. Dat is des te opmerkelijker, nu het niet alleen gaat over rekeningstanden of transacties uit het verleden, maar ook (art. 46quater §2 a) B.Sv) om een (heimelijk) toezicht gedurende ver-

337 Met een ruime definitie van de '*elektronische dienstverleners*' die zijn onderworpen aan de Belgische medewerkingsplichten, bv. een wijziging in 2011 definieert in art. 1.5. van het koninklijk besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, §2, eerste lid, 88bis, §2, eerste en derde lid, en 90quater, §2, derde lid van het Wetboek van strafvordering en van artikel 109ter, E, §2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven de '*internetsector*': '*het geheel van operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten : – die aan gebruikers toegang tot het internet aanbieden, – die aan eindgebruikers via een netwerkaansluitpunt elektronische communicatiediensten over het internet aanbieden, – die activiteiten op het internet aanbieden, of – die faciliteiten hiervoor ter beschikking stellen zoals bijvoorbeeld netwerkonderdelen, lokalen, eindapparatuur of bijbehorende faciliteiten.*'

lengbare periodes van twee maanden op bankverrichtingen. Dat lijkt nochtans een behoorlijk indringende vorm van overheidsinmenging in het privéleven van het doelwit. Het lijkt ons wenselijk dat het opvorderen van gegevens bij andere dienstverleners, zoals hotels, reisbureaus, bewakingsfirma's e.d. een uitdrukkelijke rechtsbasis krijgt. Zoals gezegd, zouden strengere regels gelden als de overheid kan verwachten dat de vordering gevoelige gegevens zal opleveren. Hier en nu rekent België voor de bescherming van gevoelige gegevens op de algemene Privacywet en op de specifieke bepalingen in de Wet op het Politieambt. Tegen deze in 2014 in de WPA ingevoegde bepalingen over het politioneel informatiebeheer hebben mensenrechtenorganisaties een vernietigingsberoep ingesteld bij het Grondwettelijk Hof, dat daar waarschijnlijk in de zomer van 2016 uitspraak over zal doen.[338]

Discussiepunt: De aanvullende bescherming van 'gevoelige' persoonsgegevens moet niet worden afgeschaft bij de Nederlandse regeling van gegevensvordering, maar anders worden vormgegeven. Bovendien moet deze bescherming systematisch worden doorgevoerd bij andere opsporingsbevoegdheden. Gezocht moet worden naar een geschikt aanknopingspunt om situaties te definiëren waarin op voorhand te verwachten valt dat 'gevoelige' persoonsgegevens zullen worden vergaard en onderzocht.

4.4. 'Relevante' gegevens en vernietiging van niet-relevante gegevens

ENKEL BIJ NEDERLANDSE NETWERKZOEKING? – Bij onderzoek in computers kunnen grote hoeveelheden gegevens worden onderzocht; meestal zal het merendeel ervan niet relevant zijn voor het onderzoek. Het Nederlandse recht kent één expliciete beperking bij onderzoek in computers tot voor het onderzoek relevante gegevens: bij de netwerkzoeking, in artikel 125j Nl.Sv, is het onderzoek beperkt tot '*gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen*'. Bij andere vormen van onderzoek in computers komt een dergelijke beperking niet voor, ook niet bij de doorzoeking ter vastlegging van gegevens (art. 125i Nl.Sv). De ratio van dit verschil in behandeling is niet helemaal duidelijk.

338 Persbericht Liga voor Mensenrechten 10 oktober 2014, 'Liga eist beteugeling van nagenoeg grenzeloze macht politie om gegevens te verzamelen', http://www.mensenrechten.be/index.php/site/nieuwsberichten/1576.

In het oorspronkelijke wetsvoorstel was de netwerkzoeking bestemd om onderzoek te doen naar '*gegevens die kunnen dienen om de waarheid aan de dag te brengen*'. De summiere toelichting hierbij luidde: '*Hier ligt een parallel met artikel 94*',[339] dat vatbaarheid voor inbeslagneming definieert (namelijk '*alle voorwerpen die kunnen dienen om de waarheid aan de dag te brengen (…)*'). In het wetgevingstraject is de clausule '*kunnen dienen*' vervolgens aangescherpt tot '*redelijkerwijs nodig zijn*',[340] wat een (marginale) subsidiariteits- en proportionaliteitstoets impliceert bij het doen van het onderzoek.[341] De parallel met artikel 94 Nl.Sv is daarmee echter niet gegeven: bij voorwerpen wordt de beperking immers gesteld bij de inbeslagneming, niet bij de zoektocht om relevante voorwerpen te vinden. Het had, als een parallel moet worden getrokken, meer voor de hand gelegen om de beperking tot relevante (dat wil zeggen voor het onderzoek redelijkerwijs nodige) gegevens te stellen bij de *vastlegging van* aangetroffen gegevens, niet bij het *onderzoek naar* gegevens.

RATIO?- Wat daar ook van zij, duidelijk is dat er een verschil is tussen de netwerkzoeking en andere vormen van onderzoek in computers. Mogelijk is de ratio daarvan dat de netwerkzoeking een onderzoek betreft in computers van derden, terwijl het onderzoek van computers bij een doorzoeking veelal slaat op de computer van de verdachte.[342] Dat laatste hoeft echter niet het geval te zijn: een doorzoeking kan ook bij niet-verdachten plaatsvinden en bij een huiszoeking bij verdachten kunnen computers van huisgenoten worden onderzocht. Waar de beperking tot relevante gegevens bij de netwerkzoeking op zich een nuttige waarborg lijkt tegen visexpedities, om te voorkomen dat een computer op afstand wordt 'leeggetrokken' om vervolgens nader onderzoek te doen naar alle vastgelegde gegevens, rijst de vraag of die waarborg dan niet ook zou moeten worden ingevoerd bij alle vormen van computeronderzoek. Omgekeerd kan men zich afvragen of de subsidiariteits- en proportionaliteitstoets die impliciet in de doorzoekingsbevoegdheden besloten ligt, en die dus ook geldt voor onderzoek in computers bij doorzoeking en inbeslagneming, niet evenzeer geldt voor de netwerkzoeking, zodat de explicitering ervan in art. 125j Nl.Sv overbodig is, en daarmee onsystematisch omdat het onterecht een verschillende be-

339 *Kamerstukken II* 1989/90, 21 551, nr. 3, 27.

340 *Kamerstukken II* 1991/92, 21 551, nr. 22 (amendement).

341 Zie hierover F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 4.3.

342 Vgl. F.P.E. WIEMANS, in: MELAI/GROENHUIJSEN E.A., *Het wetboek van strafvordering*, 2006, art. 125j, aant. 4.3.

handeling suggereert. In de meeste gevallen is het moeilijk om onderzoek in computers op voorhand te beperken tot onderzoek naar bepaalde gegevens of op bepaalde 'plaatsen' in de computer. De onderzoekers kunnen moeilijk op voorhand inschatten wat ze waar zullen aantreffen in een computer. Daarom heeft een uitdrukkelijke eis om op voorhand het onderzoek te beperken tot redelijkerwijs nodige gegevens weinig zin. Ze heeft nauwelijks normerende werking. Ook een beperking bij de *vastlegging* van aangetroffen gegevens tot relevante gegevens zou weinig uitmaken, omdat in veel gevallen de volledige harde schijf wordt gekopieerd om later onderzoek aan te doen.

ACHTERAF – Voor de beperking van het onderzoek tot relevante gegevens is het daarom belangrijker om te kijken naar ex post-waarborgen dan naar ex ante-waarborgen.[343] Art. 125n Nl.Sv bepaalt dat bij een doorzoeking vastgelegde gegevens moeten worden vernietigd zodra ze niet meer van belang zijn voor het onderzoek. Ze kunnen wel worden bewaard voor een ander strafrechtelijk onderzoek of in een register zware criminaliteit. In dit opzicht wijkt de vernietigingsplicht bij de doorzoeking substantieel af van die bij bijzondere opsporingsbevoegdheden: veel via BOB vergaarde gegevens moeten namelijk worden bewaard tot twee maanden na afloop van de zaak (art. 126cc Nl.Sv). Nu moet een vernietigingsplicht, vanuit het oogpunt van rechtsbescherming, een precaire balans slaan tussen twee botsende belangen. Enerzijds is het wenselijk dat gegevens die niet verder worden gebruikt voor de opsporing of het bewijs, zo spoedig mogelijk worden vernietigd. Dat verkleint het risico van misbruik, lekken of hacken van de gegevens. Anderzijds is het wenselijk dat vergaarde gegevens bewaard blijven, zodat de verdediging (en daarmee de rechter) kan controleren wat opsporingsdiensten precies hebben verzameld en daar ook mogelijk ontlastende gegevens uit kan lichten. Kennelijk heeft de Nederlandse wetgever geoordeeld dat deze balans anders uitvalt bij de doorzoeking dan bij bijzondere opsporingsbevoegdheden, wellicht in de veronderstelling dat bij doorzoekingen de verdachte meestal zelf nog een kopie zal hebben van vastgelegde gegevens en daarom zelf ontlastende gegevens kan aanvoeren. Maar aangezien de doorzoeking ook in computers van derden kan plaatsvinden, en bovendien de computer van de verdachte zelf in beslag kan zijn genomen waardoor hij geen kopie van de gegevens heeft, houdt die veronderstelling weinig steek.

343 O. KERR, 'Searches and Seizures in a Digital World', *Harvard Law Review* 2005, Vol. 119, No. 2, 531-585.

In elk geval is er een opvallende discrepantie nu de regeling van doorzoeking ter vastlegging van gegevens en die van de vordering van gegevens uiteenlopen, terwijl deze bevoegdheden alternatieve mogelijkheden zijn om gegevens te verkrijgen. De laatste bevoegdheid is gedefinieerd als een bijzondere opsporingsbevoegdheid (art. 126nc e.v. Nl.Sv), zodat gevorderde gegevens, ook de niet-relevante, bewaard moeten blijven, terwijl door de politie zelf vastgelegde gegevens volgens art. 125n Nl.Sv vernietigd moeten worden zodra ze niet meer van belang zijn. Een andere inconsistentie is dat art. 125n Nl.Sv zich beperkt tot gegevens vastgelegd bij een doorzoeking, en dus niet ziet op gegevens die zijn overgenomen uit bijvoorbeeld een bij aanhouding inbeslaggenomen computer; ook daar valt het verschil in benadering moeilijk te verklaren.[344]

Het wetsvoorstel computercriminaliteit III maakt de situatie nog gecompliceerder door voor te stellen aan artikel 126cc Nl.Sv een lid toe te voegen: '*6. Zodra blijkt dat gegevens die zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk van geen betekenis zijn voor het onderzoek, worden zij vernietigd. Artikel 125n, tweede lid, is van toepassing.*'[345] Hiermee wordt voor de doorzoeking van een computer op afstand (voorgesteld art. 126nba Nl.Sv, een bijzondere opsporingsbevoegdheid)[346] een vernietigingsplicht ingevoerd die vergelijkbaar is met die bij de doorzoeking van plaatsen, en dus afwijkt van de andere bijzondere opsporingsbevoegdheden. Dit wordt echter niet toegelicht in de Memorie van Toelichting (die merkwaardigerwijs suggereert dat 126cc lid 6 Nl.Sv te maken heeft met de regeling van ontoegankelijkmaking[347]) en is in strijd met de opmerking dat '*[d]e plaatsing in deze afdeling impliceert dat de rechtswaarborgen [uit de regeling van bijzondere opsporingsbevoegdheden, bjk] ook van toepassing zijn op het onderzoek in een geautomatiseerd werk.*'[348] Wellicht is er hier iets misgegaan in de redactie van het wetsvoorstel. In elk geval wordt de situatie er niet duidelijker of consistenter op.

Ondertussen is de wetgever zich er wel van bewust dat er geen eenduidig regime bestaat voor de bewaring en vernietiging van gegevens, maar hij stelt eventuele wijzigingen uit tot bij de voorgenomen herziening van de

344 F.P.E. WIEMANS, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen, Wolf Legal Publishers 2004, 249.

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

346 Hoewel de wetsbepaling generiek spreekt van '*een onderzoek in een geautomatiseerd werk*', is de reikwijdte beperkt tot de bijzondere opsporingsbevoegdheden, blijkens het opschrift van titel VD.

347 *Kamerstukken II* 2015/16, 34 372, nr. 3, 56.

348 *Kamerstukken II* 2015/16, 34 372, nr. 3, 16.

Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens.[349] Voorals-nog blijft de regeling van vernietiging van niet-relevante gegevens dus onsystematisch. Onzes inziens zou in elk geval de reikwijdte van art. 125n Nl.Sv uitgebreid moeten worden tot alle situaties van doorzoeking, inbeslagneming en onderzoek aan inbeslaggenomen voorwerpen waarbij gegevens worden vastgelegd.

BELGIË: OORVERDOVENDE STILTE – Dat voorafgaande filtering bij de vergaring van gegevens zo moeilijk is, maakt de vraag naar bewaring en hergebruik dan wel vernietiging van gegevens dus steeds prangender. Daardoor valt het des te meer op dat de Belgische wetgever op dat punt helemaal geen beleid lijkt te hebben. De tapwetgeving schrijft bewaring voor van alle opnamen, met het oog op latere tegenspraak door de verdediging of controle door de rechter. Als de verdediging beweert dat de selectie van het bewijs oneerlijk is verlopen of dat gegevens uit hun context zijn gehaald, kan het immers – zeker, maar niet alleen (*supra*, Nederland) bij heimelijke zoekingen – van belang zijn de volledige informatie bij te houden voor eventuele controle achteraf.[350] De enige uitdrukkelijke vernietigingsplicht slaat op aantekeningen van de politie over de tap, meer bepaald over wat niet in het proces-verbaal komt.[351] Gelet op het zwaarwichtig karakter

---

349 *Discussiestuk. Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2)*, versie 4 juni 2014, 52.

350 De vrees voor suggestief knip- en plakwerk door de politie bracht de Belgische wetgever ertoe om aanvankelijk (in 1994) alle afgetapte conversaties, ook de niet-relevante, volledig door politiemensen te laten overschrijven (zo nodig met beëdigde vertaling). Dat viel financieel en logistiek niet te verantwoorden (wie vermoedde dat hij werd afgeluisterd, legde de telefoon soms naast de radio met een buitenlands praatprogramma) en in al 1998 greep de wetgever in. Het blijft wel nodig alle opnames te bewaren, de door de politie van belang geachte gedeelten over te schrijven en voor de niet van belang geachte loutere de aangehaalde onderwerpen en van de identificatiegegevens van de gebruikte communicatiemiddelen te vermelden. De onderzoeksrechter krijgt uitdrukkelijk de mogelijkheid bijkomende gedeelten van de opnamen te laten overschrijven (art. 90sexies B.Sv).

351 Art. 90septies, tweede lid B.Sv: '*Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in het voorgaande lid door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van de overschrijving van [1 de van belang geachte gedeelten van de opgenomen communicaties of telecommunicaties]1 van de opname, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties. De voor de uitvoering van de maatregel aangewezen officier van gerechtelijke politie gaat over tot deze vernietiging en vermeldt dit in een proces-verbaal*.'

van de feiten en de mogelijkheid om een herziening van de uitspraak te vragen, werd ervoor gekozen de dossiers, de processen-verbaal en de opnames niet te vernietigen.[352] Het verbod tot vernietiging geldt ook in geval van een buitenvervolgingstelling aangezien nieuwe bezwaren een heropening van de zaak kunnen verantwoorden.[353] Voor het overige gelden de algemene regels over beslag, die nauwelijks aandacht besteden aan de beëindiging daarvan. Een aanpassing uit 2014[354], die vernietiging mogelijk maakt in de loop van het onderzoek bij een beslag dat te omvangrijk, onpraktisch of te duur is, lijkt enkel mogelijk voor (fysieke) goederen, niet voor gegevens.[355] Zeker zijn we echter niet want '*de goederen die, indien ze opnieuw in omloop worden gebracht, een inbreuk inhouden op de openbare orde, de goede zeden of een wettelijke bepaling*', zullen, bv. als het gaat over kinderpornografisch materiaal of computervirussen, mogelijks '*digitale goederen*' zijn. Een van de belangrijkste argumenten in het vernietigingsberoep tegen de Wet op het politioneel informatiebeheer, is precies de kwestie van de lange bewaring en de archivering. Vooral het gebrek aan duidelijke voorschriften inzake de verwijdering van gegevens na een uitdrukkelijke vrijspraak zal moeilijk te verzoenen vallen met de rechtspraak van het EHRM. Dat koppelt de bewaring aan het doelbindingssbeginsel[356], d.w.z. de bewaring van persoonsgegevens kan slechts zolang dat noodzakelijk is voor het nagestreefde doel. Een regelmatige controle kan verzekeren dat de bewaring

352 MvT, *Parl. St.* Senaat 1992-93, nr. 843/1, 17; De stukken bewaard bij de griffie, het dossier en het bijzonder register blijven bewaard onder de regeling van de Archiefwet van 24 juni 1955.

353 Verslag namens de commissie, *Parl. St.* Senaat 1992-93, nr. 843/2, 203.

354 Wet 25 april 2014 houdende diverse bepalingen betreffende Justitie, *BS* 14 mei 2014.

355 Art. 28novies §2.B.Sv: '*De procureur des Konings kan de vernietiging bevelen van goederen die tot één van de volgende categorieën behoren:1° de goederen die uit hun aard een ernstig gevaar opleveren voor de openbare veiligheid of de volksgezondheid; 2° de goederen die bij de opheffing van het beslag de fysieke integriteit of de goederen van personen in ernstige mate kunnen aantasten;3° de goederen die, indien ze opnieuw in omloop worden gebracht, een inbreuk inhouden op de openbare orde, de goede zeden of een wettelijke bepaling;4° de goederen waarvan de kosten van de bewaring in natura wegens de aard of hoeveelheid van de goederen, kennelijk niet evenredig zijn met de verkoopwaarde ervan.*'

356 Zie EHRM 26 maart 1987, nr. 9248/81, Leander/Zweden; EHRM 4 december 2008, nrs. 30562/04 en 30566/04, S. en Marper/Verenigd Koninkrijk; EHRM 18 mei 2010, nr. 26839/05, Kennedy/Verenigd Koninkrijk; EHRM 18 april 2013, nr. 19522/09, M.K/Frankrijk; EHRM 4 juni 2013, nr. 7841/08, 57900/12, Peruzzo en Martens/Duitsland. Zie eveneens EHRM 17 december 2009, nr. 16428/05, Gardel/Frankrijk en EHRM 17 december 2009, nr. 22115/06, M.B./Frankrijk (m.b.t. de opstelling van een register met gegevens over plegers van seksuele misdrijven).

effectief daartoe beperkt blijft.[357] Te lange bewaring zonder duidelijke selectiecriteria[358] en een gebrek aan een bepaling over de verwijdering van afgetapte communicatie, zeker in geval van vrijspraak, houden volgens het EHRM een tekortkoming in het licht van art. 8 EVRM[359] in, net zoals een volledig discretionaire bevoegdheid voor de rechter om na veroordeling de onderschepte gegevens te bewaren dan wel te verwijderen[360]. Het valt te vrezen dat de Belgische wetgeving niet voldoet, zelfs niet als er in de praktijk, zoals het EHRM eist, beperking is van het aantal toegangsgerechtigden tot de gegevens en de bewaring voldoende beveiligd is tegen verlies, verkeerdelijk gebruik en werkelijke vormen van misbruik.[361] De ervaringen van de Federale Overheidsdienst Justitie met informatisering zijn trouwens niet van aard om op dat punt al te veel vertrouwen in te boezemen.

---

357 Zie voor een voorbeeld van hoe het moet: EHRM 4 juni 2013, nr. 7841/08, 57900/12, Peruzzo en Martens/Duitsland.

358 EHRM 18 april 2013, nr. 19522/09, M.K./Frankrijk.

359 EHRM 24 april 1990, nr. 11801/85, Kruslin/Frankrijk; EHRM 24 april 1990, nr. 11105/84, Huvig/Frankrijk; EHRM 26 april 2007, nr. 71525/01, Dumitru Popescu/Roemenië; EHRM 1 juli 2008, nr. 42250/02, Calmanovici/Roemenië.

360 EHRM 4 december 2015, nr. 47143/06, Roman Zakharov/Rusland.

361 Zie voetnoot 356. EHRM 4 december 2015, nr. 47143/06, Roman Zakharov/Rusland: '*Russian law stipulates that data collected as a result of secret surveillance measures constitute a State secret and are to be sealed and stored under conditions excluding any risk of unauthorised access. They may be disclosed to those State officials who genuinely need the data for the performance of their duties and have the appropriate level of security clearance. Steps must be taken to ensure that only the amount of information needed by the recipient to perform his or her duties is disclosed, and no more. The official responsible for ensuring that the data are securely stored and inaccessible to those without the necessary security clearance is clearly defined […]. Domestic law also sets out the conditions and procedures for communicating intercepted data containing information about a criminal offence to the prosecuting authorities. It describes, in particular, the requirements for their secure storage and the conditions for their use as evidence in criminal proceedings […]. The Court is satisfied that Russian law contains clear rules governing the storage, use and communication of intercepted data, making it possible to minimize the risk of unauthorised access or disclosure.*'

Deel 2. Reflectie

In Deel 1 is op diverse onderdelen aangegeven waarom en hoe de huidige en voorgestelde wetgeving in Nederland en België verbeterd zou kunnen worden. In Deel 2 gaan we een stap verder en proberen wij de contouren te schetsen van een toekomstbestendige regeling van het onderzoek in computers. Onzes inziens vergt dit een fundamentele visie op de plaats van computers in het systeem van opsporingsbevoegdheden. Wat is, in het wettelijke systeem, de verhouding tussen onderzoek van computers en onderzoek van gegevens, en hoe verhoudt zich hierbij de computer ten opzichte van andere typen gegevensdragers? Is het zinvol computers, als houder van gegevens, als aparte categorie onderzoeksobject te hanteren (en niet gegevens zelf als object)? Zo ja, wat is daar de ratio van, en hoe kan het concept (rechtsgoed) van computers worden geduid en afgebakend? Deze vragen worden opgepakt in hoofdstuk 5, waarin de Nederlandse preadviseur zijn visie uiteenzet. De Vlaamse preadviseurs werken vervolgens in hoofdstuk 6 de internationale vraagstukken uit. Wat zijn de meest aangewezen criteria om een zoeking met betrekking tot gegevens territoriaal te lokaliseren in een context van wereldwijd gegevensverkeer? Welke criteria verzoenen praktische werkbaarheid voor politie en justitie het best met respect voor de soevereine zeggenschap van staten over hun grondgebied en bevolking?

Hoofdstuk 5. Een normatief kader voor onderzoek in computers

5.1 Computers als gegevensdrager, object of omgeving?

FUNCTIONALITEITEN VAN DE COMPUTER – Dit preadvies richt zich op de rol van computers in de opsporing, vanuit de gedachte dat computers een bijzonder 'iets' vormen ten opzichte van andere dingen die speurders tegenkomen. Maar wat maakt de computer nu bijzonder? En ten opzichte van welke andere dingen uit zich die bijzonderheid?

De definitie van '*geautomatiseerd werk*' en '*informaticasysteem*' wijst op drie basisfunctionaliteiten van computers: het opslaan van gegevens, het verwerken van gegevens en het overdragen van gegevens. Een fundamenteel verschil tussen Nederland en België is dat in de Nederlandse definitie de drie functionaliteiten cumulatief zijn, terwijl ze in de Belgische wetgeving alternatief zijn. Een digitale gegevensdrager als een usb-staafje of een geheugenkaart is dus geen geautomatiseerd werk, maar wel een informaticasysteem. Dat heeft belangrijke systematische gevolgen, omdat Nederland gegevensdragers (voor zover ze geen computers zijn) apart moet noemen als deze ook worden bedoeld als opsporingsobject. Als dat gebeurt (zoals in art. 125i Nl.Sv, de doorzoeking ter vastlegging van gegevens) worden dan zowel digitale als papieren gegevensdragers bedoeld; die zijn in België dan weer uitgesloten van het bereik van de informaticabepalingen. Het verschil in definitie betekent dat de reikwijdte van de diverse computer- en gegevensgerelateerde bepalingen uiteenloopt tussen beide landen. Het is niet duidelijk of de wetgever altijd even bewust heeft gekozen voor die verschillen in reikwijdte.

In Nederland ligt bij de begripsbepaling de nadruk op de functionaliteit van het geautomatiseerd *verwerken* van gegevens, zoals ook blijkt uit de voorgestelde definitie in Computercriminaliteit III: daarin verschilt de computer van de gegevensdrager. Maar is dat nu het meest relevante aspect van computers in de context van opsporing? De speurders zijn niet geïnteresseerd in hoe gegevens worden verwerkt, maar in de gegevens zelf. Het belangrijkste aspect van een computer voor de opsporing is dat het een opslagplaats is van gegevens. Met de opkomst van de cloud verandert dat enigszins, omdat de gegevens veelal niet meer op de computer zelf opgeslagen liggen, maar in de cloud. In die zin is de functionaliteit van overdracht van gegevens belangrijk. Maar overdracht als zodanig is niet het doorslaggevende element van computers – de wetgever maakt immers een systema-

tisch onderscheid tussen onderzoek in geautomatiseerde werken en onderzoek van (tele)communicatie. Het feit dat elektronische communicatie in Nederland inmiddels gedefinieerd is (art. 126la Nl.Sv) als communicatie met behulp van geautomatiseerde werken, waardoor het onderzoek van communicatie feitelijk een deelverzameling lijkt van het onderzoek van computers, doet daar niet aan af: nog steeds is in de wetgeving het onderzoek van opgeslagen gegevens en van stromende gegevens een belangrijk systematisch onderscheid. Nu in het huidige computerlandschap opslag en communicatie steeds meer in elkaar overlopen, moet het onderscheid tussen opslag en overdracht misschien wel geheel worden losgelaten, maar dat vergt een ingrijpende en fundamentele herziening van de wetgeving (niet alleen het Wetboek van Strafvordering maar ook de Grondwet, gezien de zelfstandige rol van art. 13 Nl.Gw in de Nederlandse catalogus van grondrechten), waar de wetgever nog niet aan toe lijkt. Ervan uitgaande dat het onderscheid tussen opslag en communicatie blijft gehandhaafd, waarbij computers vooral geassocieerd worden met (onderzoek van) opgeslagen gegevens en communicatie met (onderzoek van) gegevens in overdracht, blijft de vraag staan wat nu de kern uitmaakt van computers in de context van opsporing. Onzes inziens is dat dan toch vooral het element van opslag, waarbij de secundaire functionaliteiten van overdracht en verwerking gevolgen hebben voor de manier waarop opgeslagen gegevens onderzocht kunnen worden (vandaar de invoering van steunbevoegdheden als ontsleutelbevel en netwerkzoeking).[362]

DE COMPUTER ALS GEGEVENSDRAGER – Wat maakt computers nu anders dan niet-elektronische gegevensdragers, in de zin dat het een aparte regeling in strafvordering zou rechtvaardigen? België lijkt de nadruk te leggen op de digitale component: de gegevens worden opgeslagen met behulp van informatica. Dat suggereert dat digitaal opgeslagen of verwerkte gegevens anders zijn dan analoog opgeslagen of verwerkte gegevens. Maar gegevens zijn gegevens: een papieren boek bevat dezelfde gegevens als een e-boek;

362 Binnen het materiële strafrecht ligt dit misschien anders. Voor strafbaarstellingen is de functionaliteit van verwerking van gegevens waarschijnlijk minstens zo belangrijk als die van opslag: hacken en malware leveren niet alleen het gevaar op van kennisneming van gegevens, maar tasten ook de integriteit van de verwerkingsfunctionaliteit van de computer aan. In die zin is de (materieelrechtelijke) definitie van '*geautomatiseerd werk*', met de nadruk op verwerking, goed te begrijpen. Dit roept de vraag op of de definitie (of het gebruik van terminologie) in het strafprocesrecht wel de definitie uit het materiële recht zou moeten volgen. Computers spelen in zeker opzicht een verschillende rol in beide rechtsgebieden.

een papieren afdruk van een digitale foto, een tekstdocument of een rekenblad-bestand geeft dezelfde gegevens weer als de digitaal opgeslagen variant.[363] Kennelijk is er toch iets wat een verschil in behandeling rechtvaardigt. Mogelijk is dat het feit dat digitale gegevens geautomatiseerd kunnen worden onderzocht, terwijl analoge gegevens handmatig moeten worden geanalyseerd. Dat lijkt echter niet een goede verklaring te geven waarom bij doorzoeking en inbeslagneming (soms) een onderscheid wordt gemaakt, omdat het alleen betrekking heeft op het onderzoek achteraf. Meer plausibel is de verklaring dat computers en digitale gegevensdragers een grote hoeveelheid gegevens bevatten, op een relatief kleine drager, en dat het verschil tussen digitale opslag en analoge opslag, gezien de wet van Moore,[364] steeds groter is geworden. Een verzameling encyclopedieën past inmiddels op een geheugenkaart van twee vierkante centimeter (en dan is er nog ruimte over voor de complete administratie van een gemiddelde verdachte). Dit heeft tot gevolg dat de praktijk van doorzoeking en inbeslagneming is veranderd: er zijn natuurlijke grenzen aan het inbeslagnemen en handmatig doorzoeken van analoge gegevensdragers, die zijn weggevallen bij de transitie naar digitale gegevensdragers. Bij een doorzoeking is het, anders dan bij een boekenkast of stellingkast met ordners, nauwelijks mogelijk om snel een (grove) selectie te maken van de papieren of mappen die het meest relevant lijken voor het onderzoek; daarom wordt de hele digitale gegevensdrager in beslag genomen of gekopieerd, en pas achteraf – gefaciliteerd door automatische zoekfuncties – onderzocht. Ook het feit dat digitaal opgeslagen gegevens eenvoudig en snel gekopieerd kunnen worden, maakt het praktisch mogelijk om alles mee te nemen voor later onderzoek, zonder afbreuk te doen aan de beschikkingsmacht van de rechthebbende over de gegevens, wat met papier (althans als het gaat om veel gegevens) nauwelijks mogelijk is.

---

363 Er zijn wel verschillen in termen van metadata: een digitaal bestand bevat bepaalde metadata die de papieren afdruk niet bevat, en omgekeerd (papier bevat bijvoorbeeld indicaties van de printer waarmee het is afgedrukt, en wellicht vingerafdrukken of vlekken). Dat kan echter niet een fundamenteel verschil in behandeling rechtvaardigen: de wetgever heeft immers niet uitgelegd dat de computer/informatica-criminaliteitswetgeving vooral is ingevoerd om onderzoek naar metadata mogelijk te maken – het gaat primair om de gegevens zelf.

364 De wet van Moore zegt dat de opslagcapaciteit (preciezer: het aantal transistors op een chip) elke twee jaar verdubbelt. Inmiddels is het tempo vertraagd vanwege natuurkundige drempels waar de voortgaande miniaturisatie tegenaan loopt, maar de opslagcapaciteit van chips neemt nog wel steeds toe. Zie https://nl.wikipedia.org/wiki/Wet_van_Moore (geraadpleegd 1 juli 2016).

De computer kan dus worden gezien als een bijzonder type gegevensdrager, vanwege de enorme hoeveelheid gegevens erop die (als kopie of met de gegevensdrager zelf) veelal integraal worden meegenomen voor later onderzoek. Op dit punt toont zich een discrepantie in de wetgeving: de computer (en digitale gegevensdragers in België) worden wel als een bijzonder object beschouwd in de regeling van doorzoeking en inbeslagneming, maar niet in de regeling van uitlevering van voorwerpen. Die maakt geen onderscheid tussen voorwerpen: de wettelijke regeling behandelt gereedschappen, kleding, papier en computers hetzelfde. De nu ontstane discussie over onderzoek aan inbeslaggenomen voorwerpen (*supra*, 2.4) en de Nederlandse praktijk dat speurders soms uitlevering van de gegevensdrager bevelen in plaats van gegevens te vorderen om de zware drempel voor vordering van gevoelige gegevens te omzeilen (*supra*, noot 331), tonen een lacune in de wet aan: ook bij de uitleveringsbevoegdheid zouden computers en digitale gegevensdragers een bijzondere positie moeten krijgen, nu zij dat ook bij de doorzoekingsbevoegdheden hebben.

DE COMPUTER ALS OMGEVING – Terug naar de ratio van de bijzondere positie van computers. Los van de enorme opslagcapaciteit zijn computers ook bijzonder omdat zij externe toegang, zonder fysieke nabijheid, faciliteren. De overdrachtsfunctionaliteit faciliteert niet alleen communicatie (in de zin van uitwisseling van berichten met anderen) maar ook externe opslag en externe toegang. Dat werkt twee kanten op. Ten eerste kunnen vanuit een computer gegevens extern worden opgeslagen – dat is de reden waarom de netwerkzoeking is ingevoerd. Ten tweede kan de computer van afstand worden doorzocht – daarom wordt nu gediscussieerd over de heimelijke doorzoeking van computers op afstand. Anders dan papieren gegevensdragers, zijn computers als opslagmiddel onderdeel van een netwerk. Niet voor niets spreekt de Belgische wetgeving van een informatica*systeem*, waar de in Nederland voorgestelde nieuwe definitie ('*apparaat of groep van onderling verbonden of samenhangende apparaten*') bij aan lijkt te sluiten. Het betekent dat de band tussen gegevens en gegevensdrager losser is dan bij papieren of andere analoge gegevensdragers: de gegevens kunnen eenvoudig van het ene naar het andere knooppunt in het netwerk worden overgedragen. Dat maakt de computer als opslagplaats van gegevens ook minder tot een object in de zin van een voorwerp: de grenzen ervan zijn niet eenvoudig vast te stellen, omdat ze niet samenvallen met de fysieke grenzen

van het enkele apparaat. De computer als onderzoeksobject is in dat opzicht meer een sfeer of een omgeving dan een ding.[365]

Deze conceptualisering – de computer als omgeving met een enorme opslagcapaciteit – heeft belangrijke gevolgen voor rechtsbescherming. Omdat onderzoek van computers veelal leidt tot het overnemen van alle gegevens voor later onderzoek, komen veel meer gegevens, waaronder meer niet-relevante gegevens, in bezit van de opsporingsinstantie dan voorheen het geval was met analoge gegevensdragers. Bovendien schept de overdrachtsfunctionaliteit mogelijkheden voor toegang op afstand, waardoor nieuwe onderzoeksmethoden (zoals een heimelijke doorzoeking) in beeld komen. Nu heeft de wetgever het onderzoek van computers met de nodige waarborgen omkleed, maar dat is niet gebeurd vanuit een systematische visie op de rol van computers in de opsporing, getuige de diverse discrepanties en enkele lacunes die we in Deel 1 hebben beschreven. Volgens ons is de tijd rijp voor een nieuw normatief kader waarbinnen computers kunnen worden gepositioneerd. Dat kader heeft tijd nodig om uit te kristalliseren, maar de hoofdlijnen ervan staan ons wel voor ogen, zoals beschreven in de volgende paragraaf.

5.2 Naar een digitaal huisrecht

HET TE BESCHERMEN BELANG – Met de toenemende digitalisering levert een onderzoek van computers, gezien de hoeveelheid en aard van de daarin of daarmee opgeslagen gegevens, een diep inzicht in de persoonlijke levenssfeer van burgers – dieper dan vrijwel elke andere opsporingsmethode zou kunnen opleveren, en dieper dan in het analoge tijdperk menselijkerwijs mogelijk was. Het onderzoek in computers moet daarom worden genormeerd en beperkt tot wat noodzakelijk is in een democratische samenleving. Het rechtsgoed dat beschermd moet worden is daarbij vooral de ver-

365 Vgl. C. CONINGS, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld,* o.l.v. prof. F. VERBRUGGEN en prof. R. VERSTRAETEN (verwacht: juli 2016), met nieuwe criteria voor de inschatting of een indringende onderzoeksmaatregel is toegelaten en, zo ja, onder welke voorwaarden. Ze pleit ervoor om het onderscheid op basis van fysieke 'plaatsen' zoals de woning of de computer, in te ruilen voor een beoordeling met een centrale rol voor het aan de persoon gekoppelde concept '*private omgeving*'. Die omgeving omvat zowel opgeslagen informatie, privécommunicatie in een context met redelijke privacyverwachting als alle dienstverlening die gebeurt met een privacyverwachting voor de dienstengebruiker. In deze visie is de computer dus niet zelf een omgeving, maar kan deze wel deel uitmaken van iemands private omgeving.

trouwelijkheid van de opgeslagen gegevens tegen onbevoegde kennisneming: het gaat primair om een privacybelang. Daarnaast is er het rechtsgoed van de integriteit van opgeslagen gegevens en van de programmatuur (ofwel van de computer als gegevensverwerkingsapparaat). Dat speelt vooral een rol bij heimelijke toegang op afstand; het is minder prominent aan de orde als te beschermen belang bij de meeste andere vormen van computeronderzoek. Ook het derde aspect van informatiebeveiliging, de beschikbaarheid van gegevens, is een te beschermen rechtsgoed; dat uit zich in subsidiariteitsvragen of de computer in beslag mag worden genomen (waarmee de gegevens niet meer beschikbaar zijn voor de computerbezitter) dan wel de gegevens kunnen worden gekopieerd. Hoewel de drie aspecten van vertrouwelijkheid, integriteit en beschikbaarheid niet geheel te scheiden zijn, concentreren wij ons verder op het belangrijkste aspect, de vertrouwelijkheid.

De vertrouwelijkheid van computergegevens wordt in de huidige wettelijke regeling vooral beschermd vanuit de plaats waar ze zijn opgeslagen. Dat volgt uit de systematiek van de doorzoekingsbevoegdheden, die onderscheid maken tussen de plaatsen waar mag worden gezocht, waarbij de ter plaatse aanwezige computers en digitale gegevensdragers evenzeer mogen worden onderzocht als andere aanwezige objecten. Het betekent dat een computer in een woning een hogere bescherming kent dan een laptop in een auto of een smartphone in de jaszak of handtas. Met het mobiel worden van gegevensopslag (via laptops, tablets, smartphones en cloud) is de plaats van een doorzoeking echter niet langer een geschikt aanknopingspunt voor rechtsbescherming. Ten tijde van de Wet computercriminaliteit (1993) dacht men bij computers nog vooral aan vaste bureaucomputers, en de opslagcapaciteit van de toenmalige 'floppies' (wie kent ze nog?) was beperkt, zodat de meeste computergegevens thuis lagen opgeslagen. In die context was het geen onlogische keuze om computergegevens grotendeels vanuit het huisrecht te beschermen. Nu het computerlandschap drastisch is veranderd, is de woning echter niet langer geschikt als kapstok om de rechtsbescherming van computergegevens aan op te hangen. Er is een nieuwe kapstok nodig.

AANKNOPINGSPUNT – De computer zou zelf zo'n nieuwe kapstok kunnen zijn. In Duitsland heeft het constitutionele hof een nieuw grondrecht in de Duitse grondwet ingelezen: het grondrecht op de vertrouwelijkheid en

integriteit van computersystemen.[366] Volgens het hof bieden de bestaande grondrechten van huisrecht en bescherming van communicatie onvoldoende bescherming tegen het op afstand binnendringen in computers door de overheid; het gat in rechtsbescherming wordt gevuld door dit nieuwe grondrecht, als onderdeel van de open norm van het persoonlijkheidsrecht.[367] De Nederlandse en Belgische (grond)wetgevers doen er goed aan te onderzoeken of en hoe een soortgelijk grondrecht in de bestaande grondrechtencatalogus kan worden ingelezen dan wel als nieuw grondrecht kan worden ingevoerd.

Is nu de computer (het geautomatiseerd werk of informaticasysteem) de meest geëigende kapstok voor een nieuw grondrecht? Aangezien de computer niet alleen een ding is, maar ook een omgeving vanwege de verknooptheid in een netwerk, is de grens van de computer niet eenvoudig af te bakenen. De wettelijke definities geven geen duidelijke begrenzing aan, door de uitbreiding tot een '*groep van apparaten*' (Nederland) of '*netwerken en delen daarvan*' (België). Tegelijk geldt de behoefte aan rechtsbescherming evenzeer voor digitale gegevensdragers die zelf geen computer zijn (zoals een usb-staafje of geheugenkaart) en voor gegevens die extern – ergens 'in de cloud' – opgeslagen liggen. Daarentegen geldt de behoefte aan sterke rechtsbescherming minder (hoewel deze niet geheel afwezig is) voor apparaten die wel onder de wettelijke definitie van geautomatiseerd werk of informaticasysteem vallen, maar die niet hetzelfde karakter hebben als computers in de zin van een omgeving voor grootschalige gegevensopslag. Een slimme koelkast of autonavigatiesysteem is niet hetzelfde als een smartphone of laptop waar het gaat om privacybescherming. Om al deze redenen zou het aanknopingspunt voor bescherming onzes inziens iets abstracter moeten zijn dan de computer zoals die in de huidige wetgeving wordt geconceptualiseerd.

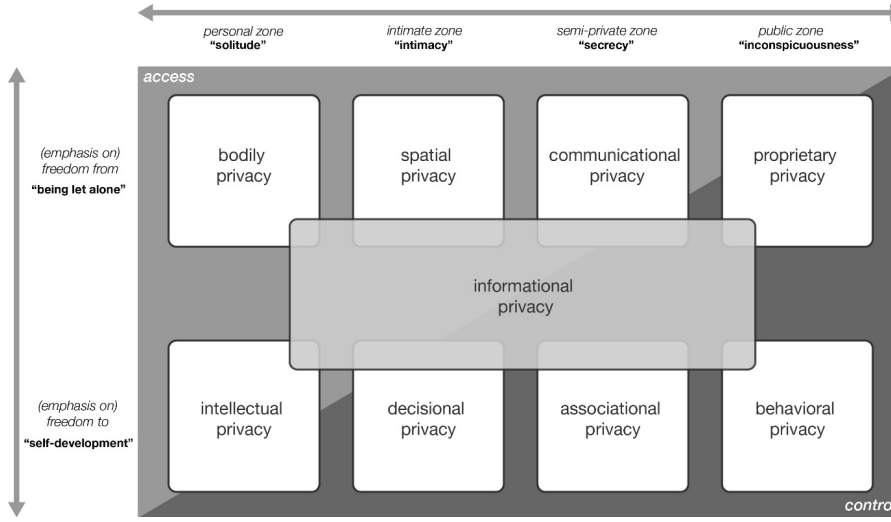
HERCONCEPTUALISERING VAN RUIMTELIJKE PRIVACY – Waar zouden we een grondrechtelijke bescherming van opgeslagen computergegevens moeten situeren? Het is behulpzaam om hier de typologie van privacy te gebruiken die Koops met collega's heeft ontwikkeld,[368] waarin privacyty-

366 BverfG 27 februari 2008, 1 BvR 370/07, ECLI:DE:BverfG:2008: rs2008 0227 .1bvr037007.

367 *Ibid*., §§166–206.

368 B.J. KOOPS, B.C. NEWELL, T. TIMAN, I. ŠKORVÁNEK, T. CHOKREVSKI & M. GALIČ, 'A Typology of Privacy', 38 *University of Pennsylvania Journal of International Law* Vol. 38 nr. 2 (te verschijnen 2016).

pen zijn gegroepeerd langs een spectrum van interactie met de omgeving, van een strikt persoonlijke sfeer tot aan een publieke sfeer (figuur 1).



Figuur 1. Typologie van privacy.
Bron: B.J. Koops e.a., 'A Typology of Privacy', 38 U. Pa. J. Int'l L. __ (2016)

Tussen de persoonlijke en de publieke sfeer staan de intieme sfeer, waarbij de interactie met de omgeving beperkt is tot familie en vrienden, en de semi-private sfeer, waarin iemand communiceert met een bredere cirkel van mensen (maar zonder in de publieke sfeer te treden). Het prototype van privacy in de intieme sfeer is de ruimtelijke privacy, die met name wordt beschermd door het huisrecht; het prototype in de semi-private sfeer is de communicatieve privacy, die wordt beschermd door het recht op vertrouwelijkheid van communicatie.

De lacune in rechtsbescherming voor opgeslagen computergegevens is vooral ontstaan doordat gegevens uit de intieme sfeer (denk aan boeken, foto's, muziek, dagboeken, administratie, bewaarde brieven) die voorheen grotendeels thuis werden bewaard (en dus werden beschermd door het huisrecht) nu mobiel zijn geworden. De manier waarop de ruimtelijke privacy rechtens wordt beschermd – het huisrecht – is daarmee deels achterhaald geraakt: vanzelfsprekend is er nog steeds behoefte aan het huisrecht om burgers te beschermen tegen binnentreden in de woning, maar de bescherming tegen kennisneming van gegevens uit de intieme sfeer wordt

niet langer afdoende gedekt vanuit de ruimtelijke privacy in de huidige vormgeving.

Tegen die achtergrond wordt duidelijk dat de nieuwe bescherming te situeren valt in de intieme sfeer, via een nieuwe conceptualisering van de ruimtelijke privacy. Er is behoefte aan een huisrecht 2.0: bescherming van de ruimte waarin gegevens uit de intieme sfeer opgeslagen liggen. Dat is geen fysieke ruimte zoals de woning dat is, maar een abstracte ruimte (zoals cyberspace een abstracte ruimte is). De kern van het huisrecht is het *ius excludendi*: het recht te bepalen wie je in je eigen ruimte (de woning) wilt binnenlaten. Evenzo zou de kern van het digitale huisrecht het *ius excludendi* met betrekking tot gegevens uit de intieme sfeer moeten zijn: het recht te bepalen wie je toegang geeft tot dat deel van cyberspace waarover je zelf kunt beschikken. Lorenzo Picotti omschrijft dit, in zijn conceptualisering van het rechtsgoed dat de Italiaanse computercriminaliteitswetgeving beoogt te beschermen, als volgt:

'Het gaat om een bijzondere sfeer van bescherming, waarop iedere persoon recht heeft in Cyberspace, die zich vertaalt in de macht om derden uit te sluiten en om gevrijwaard te blijven tegen ongewenste inbreuken en mogelijk schadelijke of althans niet-consensuele inmengingen, om een vrije, autonome en veilige eigen "informaticaruimte" te waarborgen, waarin de eigen persoonlijkheid zich zonder belemmeringen kan ontwikkelen, die functioneert door plaatsongebonden relaties en activiteiten op het net.'[369]

Picotti noemt dit een 'cybernetische ruimte' (en bewust geen 'virtuele ruimte', omdat het om een reële ruimte gaat). Deze valt niet samen met een specifiek informaticasysteem, maar wordt gevormd door het geheel aan computer- en server-ruimte (inclusief servers van dienstaanbieders), met inbegrip van de daarin opgeslagen gegevens, waarover een persoon het *ius excludendi* kan uitoefenen: '*de essentie is dat het een veilige ruimte is, gereserveerd voor de exclusieve beschikkingsmacht van de gerechtigde, en beschermd tegen inmengingen van buiten die ongewenst zijn of waarvoor althans niet uitdrukkelijk toestemming is gegeven*.'[370]

DIGITAAL HUISRECHT – De tijd is rijp om een digitaal huisrecht in te voeren, dat de digitale ruimte beschermt waarover een burger de exclusieve beschikkingsmacht kan uitoefenen. Het afbakenen en operationaliseren van

369 L. PICOTTI, 'La tutela penale della persona e le nuove tecnologie dell'informazione', in: L. PICOTTI (ed.), *Tutela penale della persona e nuove tecnologie*, s.l., CEDAM, 2013, 29-75 op p. 59-60 (nadruk weggelaten; mijn vertaling, BJK).

370 *Ibid*., 60 (nadruk weggelaten).

die exclusieve digitale ruimte zal geen sinecure zijn, maar dat betekent niet dat het geen vruchtbaar concept kan zijn in de rechtsontwikkeling. Het huisrecht heeft per slot van rekening ook geen statisch, eenduidig concept van 'huis' opgeleverd, maar een veelzijdig en context-afhankelijke notie die ook caravans, tenten en zelfs afgesloten kuilen in een veld kan omvatten.[371] Het feit dat een deel van de digitale ruimte niet volledig exclusief aan een persoon toebehoort, zoals bij in de cloud opgeslagen gegevens het geval is, is evenmin een doorslaggevend bezwaar: een hotelkamer wordt beschermd door het huisrecht, ondanks het feit dat een hotelgast de beschikkingsmacht over de hotelkamer deelt met de hoteleigenaar. In de cloud opgeslagen gegevens kunnen daarom evenzeer door een digitaal huisrecht worden beschermd, mits het aan derden voldoende duidelijk is dat de rechthebbende exclusieve beschikkingsmacht wil uitoefenen, bijvoorbeeld door beveiliging met een wachtwoord. Ook het feit dat de eigen digitale ruimte soms wordt gedeeld met anderen (zoals een laptop die door huisgenoten gezamenlijk wordt gebruikt, of een cloud-account waar iemand anderen toegang toe verleent) is niet per se een reden om digitaal huisrecht te ontzeggen: een woning wordt immers ook vaak gedeeld, en iemand die een (reserve)sleutel geeft aan de AirBNB-gasten die tijdelijk in de woning zullen verblijven, verliest ook niet aanspraak op zijn huisrecht.

Het zal nog het nodige onderzoek en veel discussie vergen voordat een dergelijk digitaal huisrecht kan worden ingevoerd. Wat behoort wel en niet tot de exclusieve eigen digitale ruimte? Hoe sterk moet deze ruimte worden beschermd tegen inmenging door opsporingsdiensten? Welke inbreuken op het digitale huisrecht zijn onder welke voorwaarden aanvaardbaar? Zou het digitaal huisrecht een sui generis-recht moeten zijn, of kan het worden geïntegreerd met het huisrecht tot een generieke bescherming van de intieme ruimte?[372]

Dit zijn geen eenvoudige vragen, maar het concept van een digitaal huisrecht biedt wel een stevige basis om deze vragen te bediscussiëren, vanuit een visie op privacybescherming die niet blijft steken in 20e-eeuwse grondrechten, maar vooruitkijkt en rekening houdt met wat beschermwaardig is in het 21e-eeuwse computerlandschap.

Discussiepunten: Om burgers adequaat te beschermen tegen overheidsonderzoek in computers, waarbij het persoonlijke leven indringender in

371 B.J. KOOPS, H. VAN SCHOOTEN EN M. PRINSEN, *Recht naar binnen kijken*, Den Haag, Sdu, 2004, 43.

372 Vgl. CONINGS' concept van de 'private omgeving', *supra*, noot 365.

beeld komt dan bij vrijwel elke andere opsporingsbevoegdheid, is een zware, grondrechtelijke vorm van rechtsbescherming nodig. Die rechtsbescherming kan worden gestoeld op het concept van 'digitaal huisrecht', dat de digitale ruimte beschermt waarover een burger het *ius excludendi* kan uitoefenen.

Moet de wetgever bij de regeling van de opsporingsmethoden de eigenheid van het 'digitale huis' als aparte omgeving erkennen en beschermen, zodat naast de fysieke woning ook het digitale huis bescherming zou bieden aan zijn 'bewoner'? Of is het veeleer wenselijk om geen apart regime te voorzien voor de digitale omgeving, maar te werken met de bescherming van de persoonlijke omgeving als zodanig? Die omvat dan zowel fysieke plaatsen met een grote privacyverwachting (zoals de woning) als de 'digitale privéwereld' en alle dienstverlening waarbij de gebruiker redelijke privacyverwachting heeft.

Hoofdstuk 6. De territoriale opsporingsbevoegdheid t.a.v. 'digitale plaatsen'[373]

6.1. Inleiding

LOKALISATIEVRAAGSTUK – Een grondwettelijk systeem dat de opsporingsbevoegdheden in computers hun juiste plaats geeft, moet natuurlijk kunnen fungeren in de geglobaliseerde ICT-wereld. In par. 2.3 hebben we al stilgestaan bij de moeilijke vraag waar opsporingsinstanties hun onderzoekshandelingen stellen als bewijs vergaren in de virtuele wereld (bv. het bekijken van een Facebook-account, een Google-agenda, een Dropbox-account of een YaHoo!-webmailaccount).[374] Voeren zij een zoeking uit op de server waar de gezochte gegevens staan opgeslagen of stellen zij hun onderzoekshandelingen op de plaats waar de onderzochte persoon handelt? Opereren zij op de plaats waar ze zelf toegang nemen tot de gegevens? Speelt de locatie van de betrokken dienstenaanbieder een rol? Elk criterium vormt een link tussen het gezochte digitaal bewijs en de fysieke realiteit. Elk criterium kan bijgevolg de opsporingshandeling op een bepaald territorium lokaliseren. De vraag is echter welk criterium doorslaggevend moet zijn.

SOEVEREINITEIT VAN STRUIKELBLOK TOT BOUWSTEEN?– We stelden in par. 2.3 vast dat de traditionele visie in het internationaal publiekrecht in toenemende spanning komt te staan met voorstellen om nationale speurders meer armslag te geven bij het speuren in de gemondialiseerde computerwe-

---

373 Dit onderdeel van het preadvies is een slechts licht bewerkte (ingekorte) versie van het eerder gepubliceerde: C. CONINGS, 'De lokalisatie van opsporing in een virtuele omgeving: Wie zoekt waar in cyberspace?', *NC* 2014, 1-25. Ook vormt dit een belangrijk onderdeel van C. CONINGS, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld,* o.l.v. prof. F. VERBRUGGEN en prof. R. VERSTRAETEN (verwacht: juli 2016).

374 Die vraag ligt ook voor in de Amerikaanse Microsoft-zaak voor het Hof van Beroep van het 2de circuit (Microsoft Corporation v. United States of America), specifiek m.b.t. medewerkingsplichten: wanneer de Amerikaanse overheid de in de Verenigde Staten gelokaliseerde dienstenaanbieder Microsoft beveelt tot het overhandigen van e-mails die staan opgeslagen op servers in Ierland, vindt de overheidshandeling dan plaats in de Verenigde Staten of in Ierland? Is m.a.w. de locatie van de medewerkingsplichtige of de locatie van de gezochte data doorslaggevend? Zie J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 328-329 en 389-397. J. DASKAL verwijst naar het lokalisatievraagstuk als '*defining the relevant here and there*', *ibid.*, 326. De auteur behandelt uitvoerig de Amerikaanse benadering van de lokalisatieproblematiek.

reld. In wat volgt, trachten we, op basis van een visie op soevereiniteit die niet alleen slaat op zeggenschap over grondgebied maar over mensen op dat grondgebied[375], een voorstel te doen voor een nieuw, beter regime voor lokalisering van zoekingen. Het gaat bij zoekingen immers niet over toegestane inbreuken op de rechten of plichten van gegevens of van servers, maar die van mensen en bedrijven.

6.2. Soevereiniteit: interne en externe beschermingsfunctie

LEGITIMATIE STAATSSOEVEREINITEIT – Staatssoevereiniteit kan worden gelegitimeerd door een oorspronkelijke behoefte aan organisatie van de samenleving en de gedachte dat die ordenende opdracht best rust op de schouders van een hogere instantie, die in staat is bescherming te bieden aan haar onderdanen.[376] Opdat die hogere instantie haar ordenende en beschermende taak zou kunnen vervullen, behelst de staatssoevereiniteit verschillende bevoegdheden die de hogere instantie in staat moeten stellen effectieve controle uit te oefenen. Zo omvat staatssoevereiniteit o.a. de bevoegdheid om wetten te schrijven en de naleving daarvan af te dwingen.[377] De idee dat een hogere instantie het best geplaatst is voor de bescherming van de belangen van haar onderhorigen in hun onderlinge relatie (*interne bescherming*) vormt een belangrijk fundament van de staatssoevereini-

375 Dit concept van soevereiniteit past trouwens in de Belgische constitutionele traditie. Na de onafhankelijkheid in 1830 kreeg het nieuwe staatshoofd Leopold I (1831) niet de territoriaal geformuleerde titel '*Koning van België*', maar die van '*Koning der Belgen*'. De nieuwe constitutionele monarchie steunde immers op het idee van volkssoevereiniteit, als basis en grens voor de macht van het nieuwe staatshoofd. (F. DELPEREE en B. DUPRET, 'Le roi des Belges', *Pouvoirs, Revue français d'études constitutionnelles et politiques* 1990, nr.54, 15). De twintigste eeuw heeft ons echter geleerd hoe belangrijk het is het negentiende-eeuwse concept van volkssoevereiniteit in toom te houden met een plicht om de territoriale integriteit van andere staten te respecteren, een kwestie die in de eenentwintigste eeuw brandend actueel blijft. *Infra*, 6.2.

376 Die gedachte vinden we o.a. terug bij sociaal-contractdenkers als THOMAS HOBBES, JOHN LOCKE, JEAN-JACQUES ROUSSEAU en JOHN RAWLS. Zie eveneens: S. CHESTERMAN, *One Nation Under Surveillance. A New Social Contract to Defend Freedom Without Sacrificing Liberty,* Oxford, Oxford University Press, 2011, 249-250. Vergelijk art. 1 EVRM, waarin elke staat zich heeft verbonden '*de rechten en vrijheden te verzekeren [van] een ieder die ressorteert onder [zijn] rechtsmacht*'.

377 A. CASSESE, *International Law,* Oxford, Oxford University Press, 2005, 49-50.

teit.[378] Enkel een voldoende grote erkenning hiervan door de personen die onder de staatsmacht ressorteren, maakt soevereine bevoegdheid mogelijk (bottom-up erkenning). Wanneer onvoldoende onderdanen in de ordenende en beschermende capaciteit van de staat geloven, loopt die het risico dat zijn soevereiniteit zal worden ondermijnd. Soevereiniteit steunt bijgevolg op een zekere mate van *interne erkenning* door de 'onderdanen'.

NOODZAKELIJKE (TERRITORIALE) BEGRENZING – Het territorialiteitsbeginsel beperkt de staatssoevereiniteit en de daarmee gepaard gaande bevoegdheden tot een nationaal territorium. De ordende, controlerende en beschermende taak van de staat geldt zo in verhouding tot een bepaald grondgebied.[379] Enkel een begrenzing van de soevereiniteit maakt interstatelijke en dus *externe erkenning* mogelijk. Dit maakt een tweede vorm van erkenning uit, die eveneens een noodzakelijke bestaansvoorwaarde vormt van de staatssoevereiniteit.[380] Staten erkennen de begrenzing van hun eigen bevoegdheidssfeer ten aanzien van de bevoegdheidssfeer van andere staten. Zij mogen het grondgebied van een andere staat niet betreden noch zich mengen in de interne aangelegenheden van die staat zonder diens toestemming.[381] De begrenzing is gericht op de bescherming van de soevereiniteit zelf en het mogelijk maken van een vreedzame co-existentie op internationaal niveau.[382] Het VN-Handvest spreekt in dit verband van de soevereine gelijkheid van staten.[383] De begrenzing veruitwendigt zich in de bevoegdheid om handelingen van andere staten binnen de eigen bevoegdheidssfeer uit te sluiten.[384] De soevereine staat kan op die manier ook een bescherming garanderen van de personen en zaken op zijn territorium tegen onge-

---

378 E. LANCKSWEERDT, 'Soevereiniteit, angst en leiderschap', *TBP* 2012, 472. De auteur verwijst daarbij naar THOMAS HOBBES, één van de voornaamste grondleggers van de soevereiniteitsleer.

379 B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 33.

380 I. WALLERSTEIN, *World-Systems Analysis: An Introduction*, Durham, Duke University Press, 2004, 44: *'Sovereignty is more than anything else a matter of legitimacy […that] requires reciprocal recognition. Sovereignty is a hypothetical trade, in which two potentially conflicting sides, respecting de facto realities of power, exchange such recognitions as their least costly strategy.'*

381 B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 19.

382 W.H. VON HEINEGG, 'Legal implications of Territorial Sovereignty in Cyberspace', in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (EDS), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 8.

383 Art. 2 Handvest van de Verenigde Naties.

384 A. CASSESE, *International Law,* Oxford, Oxford University Press, 2005, 51.

oorloofde inmengingen door andere soevereine staten (*externe bescherming*).[385] Bescherming tegen aantastingen door personen die zich bevinden op het territorium van een andere staat wordt geboden door internationale samenwerking tussen de betrokken soevereine staten. Enkel zo kunnen soevereine staten hun beschermende taak ten volle vervullen. De externe erkenning van de soevereiniteit brengt bovendien een verplichting met zich mee om het gebruik van het eigen territorium voor handelingen die een inbreuk uitmaken op rechten van andere staten, niet toe te laten en tegen een dergelijk gebruik op te treden.[386] Die verplichting veronderstelt dat de staat zijn verantwoordelijkheid opneemt voor wat er zich op zijn eigen territorium afspeelt.[387] Ook daartoe moet ze over de nodige controlebevoegdheid beschikken over wat er gebeurt op het eigen territorium. Territorialiteit bleek het meest werkbare en vanzelfsprekende criterium ter afbakening van het staatsgezag.[388] Het staatsgezag strekt zich zo op de eerste plaats uit tot het nationale grondgebied, de territoriale wateren en het luchtruim daarboven.[389] De open zee (*mare liberum*) en de ruimte (*outer space*) zijn vrij van soevereiniteitsaanspraken gelet op hun algemeen belang.[390] Geen enkele staat heeft een recht op uitsluiting van andere staten uit delen van de ruimte of de open zee. Het gebruik ervan staat open voor eenieder.[391] Toch is er ook een zekere '*territoriale*' afbakening terug te vinden in de ruimte en in de open zee. De schepen en in de ruimte gelanceerde objecten vallen immers onder de rechtsmacht van de staat waarvan zij de

385 W.H. VON HEINEGG, 'Legal implications of Territorial Sovereignty in Cyberspace', in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 8.

386 IGH, 9 april 1949, *The Korfu Channel Case*, http://www.icj-cij.org/docket/files/1/1645.pdf; VON HEINEGG, *ibid.*, 15 e.v.

387 B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 66.

388 Zie hierover uitgebreid: A. CASSESE, *International Law,* Oxford, Oxford University Press, 2005, 81 e.v.; KOOPS en GOODWIN, *ibid.*, 31-32.

389 Zie hieromtrent meer concreet: C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht en internationaal strafrecht,* Antwerpen, Maklu, 2006, 1205 e.v.; W. DEREZE, 'De grens tussen luchtvaart en ruimtevaart'*, Jura Falconis* 2007-08, 100-104.

390 DEREZE, *ibid.*, 102-104; zie ook M. HILDEBRANDT, 'Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace', *University of Toronto Law Journal* 2013, afl. 63, 196-224.

391 Zie het VN-ruimteverdrag van 27 januari 1967 en het VN-Zeerechtverdrag van 10 December 1982.

vlag dragen of waar zij werden geregistreerd.[392] Hoewel de ruimte en open zee op zichzelf vrij zijn van individuele rechtsmacht, kunnen staten bijgevolg toch soevereine bevoegdheden hebben over gebeurtenissen die zich daar afspelen.

INTERNE ERKENNING TERRITORIALE BEGRENZING – Net zoals een interne erkenning (door onderdanen) geldt ten aanzien van de staatssoevereiniteit, is er ook een vorm van interne erkenning van de territoriale begrenzing van die soevereiniteit. Rechtsonderhorigen erkennen dat er verschillende samenlevingen naast elkaar bestaan die elk soevereine bevoegdheden toekennen aan een hogere instantie om organisatie en bescherming van die samenleving mogelijk te maken. Ze aanvaarden dan ook dat de soevereiniteit van de eigen staat, gericht op hun rechtsbescherming, noodzakelijk moet worden begrensd. Zij aanvaarden zo de gevolgen van een grensoverschrijding. Ze erkennen immers dat zij zich begeven onder de soevereine bevoegdheid van een andere staat telkens wanneer zij de grens oversteken. Zij verliezen op dat moment in zekere zin de rechtsbescherming van hun eigen staat. Evenzeer aanvaarden zij dat de zaken die zij mee de grens overnemen, onder de soevereine bevoegdheid van de bezochte staat vallen.[393] Die staat dient zijn beschermende taak te vervullen ten aanzien van alle personen die zich op zijn territorium begeven. De personen moeten zich aan de lokale regelgeving houden. De betrokken staat kan die gedraging afdwingen en kan de nodige dwangbevoegdheden uitoefenen ten aanzien van de personen die zich op zijn territorium begeven en de zaken die zich daar bevinden. Wil men zichzelf of zijn zaken (bv. laptop, boekhouding, medisch dossier) bijgevolg niet onder de bevoegdheid brengen van een buitenlandse staat, dan dient men binnen de eigen landsgrenzen te blijven of deze zaken daar achter te laten. De erkenning van de territoriale begrenzing van soevereiniteit brengt rechtszekerheid. Het rechtssysteem dat op een persoon of zaak van toepassing is, is op de eerste plaats het rechtssysteem van de staat waar die persoon of zaak zich bevindt. Nederlanders weten dat in Nederland voor hen het Nederlandse recht geldt, d.w.z. de Nederlandse rechtsbescherming en de in Nederland toegelaten overheidsinmenging. Ze rekenen er bv. op dat Nederland hen zal beschermen tegen inbreuken op hun rechten door bv. de Belgische of Iraanse overheid, maar

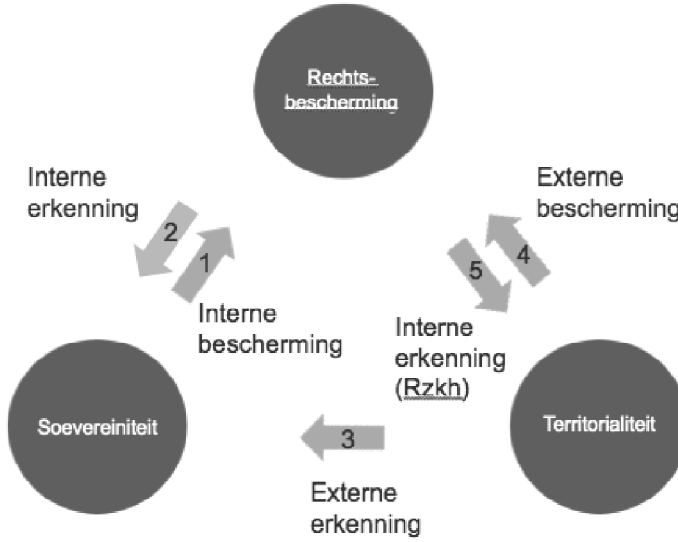
---

392 C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht en internationaal strafrecht,* Antwerpen, Maklu, 2006, 1206 e.v.; W. DEREZE, 'De grens tussen luchtvaart en ruimtevaart', *Jura Falconis* 2007-08, 102-104.

393 Zie eveneens: J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 367-368.

ze weten ook dat ze bij een bezoek aan Antwerpen wel onder de Belgische wetten vallen en bij een reis naar Teheran onder de Iraanse.

RECHTSBESCHERMING – SOEVEREINITEIT – TERRITORIALITEIT – Wanneer we nadenken over de toepasbaarheid van het soevereiniteitsprincipe en het territorialiteitsbeginsel in de huidige gedigitaliseerde samenleving, moeten we het hierboven geschetste samenspel tussen rechtsbescherming, soevereiniteit en territorialiteit duidelijk in het achterhoofd houden. We vatten het daarom nog even kort samen. (1) De staatssoevereiniteit is erop gericht de primaire nood aan ordening en bescherming binnen een samenleving te beantwoorden. (2) De erkenning dat een hogere instantie het best geplaatst is om aan die oorspronkelijke behoefte te voldoen vormt één van de belangrijkste fundamenten van de staatssoevereiniteit (interne erkenning). Die soevereiniteit wordt op haar beurt beschermd door de territoriale begrenzing ervan. (3) Die begrenzing maakt een erkenning van de soevereiniteit door andere soevereine staten mogelijk (externe erkenning). (4) Bovendien zorgt zij ervoor dat de soevereine staat zijn beschermende functie kan vervolledigen door binnen zijn territorium eveneens bescherming te bieden tegen het optreden van andere soevereine staten (externe bescherming). (5) Ook rechtsonderhorigen erkennen tot slot de noodzakelijke territoriale begrenzing van soevereine bevoegdheden.



Figuur 2. Samenspel rechtsbescherming, soevereiniteit en territorialiteit

CENTRALE VRAAG – In Deel 1, en in het bijzonder waar we het over grensoverschrijdende netwerkzoeking en beslag hadden (2.3), bleek hoe het fenomeen '*cyberspace*' het traditionele denkpatroon inzake opsporing en territorialiteit uitdaagt. De uiteindelijke vraag is: kunnen we de huidige (digitale) opsporingsmogelijkheden op zo een manier *territoriaal begrenzen* dat de (interne en externe) *soevereiniteit* en zo de (interne en externe) *bescherming van grondrechten* van individuen worden gewaarborgd? Kunnen we met andere woorden het territorialiteitsbeginsel zodanig opvatten dat dit het hierboven geschetste samenspel niet verstoort?

6.3. Van het huidige naar een nieuw systeem: plaats van het object, maar ook van de persoon

6.3.1. Inleiding

TWEE SOORTEN ZOEKING – In par. 2.2 hebben we gezien dat we bij zoekingen naar bewijs in cyberspace doorzoeking van bestaand bewijs, van opgeslagen gegevens, kunnen onderscheiden van (heimelijke) bewakingsmaatregelen. Opsporingsinstanties kunnen dus een persoon in reële tijd virtueel in de gaten houden (*virtuele opsporing in real time*) of kunnen een zoeking uitvoeren naar opgeslagen data los van een gelijklopende handeling

door het onderzochte subject (*zoeking naar opgeslagen data*). Met virtuele opsporing in real time bedoelen we het observeren van virtuele handelingen zoals het openen van websites, communicaties of bestanden, op het moment dat het onderzochte subject die handelingen stelt.[394] Ook het bekijken van de geopende websites, communicaties en bestanden zelf maakt opsporing in real time uit. Het kan daarbij eveneens gaan om communicaties uit het verleden die door de onderzochte persoon worden herbekeken. Het gebruik van keyloggers[395], die toetsaanslagen en muisbewegingen registreren, is een voorbeeld van virtuele opsporing in real time, net zoals het bekijken of beluisteren van communicatie op het moment dat die door het onderzochte subject wordt gevoerd (bv. Skype-gesprek, chatgesprek, het typen en verzenden van een e-mail). De zoeking naar opgeslagen data staat daarentegen los van gelijktijdige handelingen door het onderzochte subject m.b.t. de onderzochte gegevens. Het gaat dan om het, al dan niet heimelijk, doorzoeken van profielen op sociale media of accounts die toegang verlenen tot cloud-diensten (bv. Dropbox of iCloud) of webmaildiensten (bv Yahoo!, Hotmail of Gmail). Het onderscheid wordt bepaald door de vraag: krijgen opsporingsinstanties zicht op wat de onderzochte persoon op het moment van de zoeking doet (bekijken zij wat wordt geopend, bekijken of beluisteren zij een live gesprek) of bekijken ze gegevens los van een gelijklopende handeling door het subject? Zoals gezegd, hanteert België momenteel nog een technisch onderscheidingscriterium tussen opsporing in real time en de zoeking naar bestaand bewijs, nl. de vraag of de onderzochte gegevens in overdracht zijn of niet. We hebben aangestipt dat dit criterium van overdracht erg moeilijk werkbaar is in een digitale omgeving[396] en de Belgische regering het lijkt te zullen loslaten (*supra*, 4.2, *in fine*). Volgens ons is dat terecht, want het is niet pertinent: niet alleen als onderscheidingscriterium tussen soorten zoekingen[397], maar ook voor het vraagstuk over de lokalisatie van de opsporingshandelingen.

---

394 Dit is technisch mogelijk door bv. het gebruik van spyware (*supra*, 2.2).

395 We behandelen de vraag naar de toelaatbaarheid van de inzet van keyloggers door opsporingsinstanties niet. We gaan enkel in op de vraag waar eventuele opsporingshandelingen dienen te worden gelokaliseerd.

396 Zie hierover ook uitgebreid: P. VAN LINTHOUT, J. KERKHOFS, 'Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel', *T.Strafr.* 2008, 79-94.

397 Het Belgische recht kent strenge toepassingsvoorwaarden voor een zoeking naar communicatie '*in de fase van overbrenging*' (art. 90ter e.v. Sv (tapwetgeving)). Dat was logisch aangezien men op het ogenblik van de invoering van de tapwetgeving in 1994 de focus richtte op telefoonconversaties waarbij men enkel kennis kon krijgen van de *inhoud* van communicatie tijdens de overbrenging ervan. Voor of na de overbrenging

NU EN (?) STRAKS – We gaan hieronder per soort zoeking na waar zij vandaag worden gelokaliseerd en onderzoeken of die lokalisatie het geschetste samenspel tussen rechtsbescherming, soevereiniteit en territorialiteit in stand houdt. Waar dat niet het geval lijkt, zoeken we naar alternatieve criteria ter lokalisering van virtuele opsporingshandelingen. Zo proberen we zowel voor virtuele opsporing in real time (6.3.2) als voor de zoeking naar opgeslagen gegevens (6.3.3) tot een hoofdcriterium voor lokalisatie van de opsporing te komen. Vervolgens stellen we ons de vraag of, in het kader van virtuele zoekingen in het algemeen, de territoriale bevoegdheid op grond van het gewenste hoofdcriterium verder moet worden aangevuld met bevoegdheden van andere staten die eveneens een link vertonen met de gezochte gegevens (6.3.4). Tot slot bekijken we of de voorgestelde benadering ook praktisch bruikbaar is. We hebben immers niets aan een mooie theorie als die onwerkbaar blijkt in de praktijk (6.3.5).

6.3.2. Opsporing in real time: van huidige tegenstrijdige benadering naar alternatieve subject-gebonden lokalisatiemethode

TELEFOONTAP – De klassieke telefoontap maakte het natuurlijk al lang mogelijk conversaties af te luisteren tussen personen die zich in verschillende landen bevinden. De communicatie wordt van de verzender naar de ontvanger verzonden via allerlei technische tussenstations (bv. zendmasten) die zich op hun beurt ook op het territorium van een andere staat kunnen bevinden. Nationale wetgevers en de Europese Unie lijken de vraag naar de lokalisatie van het bewijsmateriaal (de conversatie) uit de weg te gaan.[398] De telefoontap wordt naar Belgisch recht bijvoorbeeld eenvoudigweg bevolen ten aanzien van een bepaalde persoon, een telecommunicatiemiddel of een plaats. Waar die persoon, dat telecommunicatiemiddel of die plaats zich bevindt, bepaalt bijgevolg waar de tap moet worden gelokaliseerd en tot wiens territorium de conversatie als het ware behoort. De Europese Unie benadert deze problematiek op dezelfde wijze in de overeenkomst

kon men enkel het *bestaan* van de communicatie vaststellen. Kennisname van de inhoud vormt uiteraard een veel grotere inmenging in het recht op privacy en moest daarom aan strengere vereisten worden verbonden. Die logica gaat in de digitale wereld echter niet langer op. Ook voor en na de overbrenging van communicatie kan men kennis nemen van de inhoud ervan.

398 Zie art. 90ter §1, lid 3 B.Sv; art. 126m Nl.Sv; §100a (Duitse) Strafprozeβordnung (StPo); art. 18-20 van de overeenkomst van 29 mei 2000 betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, www.eclan.eu (Hierna EU-overeenkomst inzake wederzijdse rechtshulp.)

inzake wederzijdse rechtshulp. Buiten de situaties waarin technische bijstand vanuit het buitenland vereist is[399], treden de Europese regels inzake samenwerking in strafzaken pas in werking wanneer de *af te tappen persoon* zich niet (langer) op het nationale territorium van de aftappende staat bevindt.[400] In de richtlijn inzake het Europese Onderzoeksbevel (hierna EOB) blijft diezelfde logica overeind.[401] De conversatie vindt dus plaats daar waar de deelnemers aan de conversatie zich bevinden.[402] Zodoende kan eenzelfde conversatie op verschillende territoria worden gelokaliseerd en onder de soevereine bevoegdheid vallen van verschillende overheden (nl. indien de gesprekspartners zich in verschillende landen bevinden). Zij hebben elkaars toestemming niet nodig om de conversatie, die hen beiden toebehoort, te onderscheppen. Iedere staat heeft zo de zeggenschap over de mogelijkheid tot rechtstreekse inmenging in het recht op private communicatie van de personen die zich op zijn territorium bevinden. Iedere staat bepaalt soeve-

399 Zie hierover toelichtend rapport bij de Overeenkomst van 29 mei 2000 betreffende wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, *Pb.C.* 29 december 2000, afl. 379, 20-21: De situatie waarin technische bijstand vanuit het buitenland vereist is voor het aftappen van een persoon op het eigen grondgebied valt buiten het traditionele kader van wederzijdse rechtshulp. De staat dient in deze situatie in de mogelijkheid te worden gesteld '*op het eigen grondgebied*' een maatregel te nemen terwijl wederzijdse rechtshulp er klassiek op is gericht een maatregel op het grondgebied van een andere lidstaat te laten uitvoeren.

400 Zie art. 18-20 EU-overeenkomst betreffende de wederzijdse rechtshulp in strafzaken. Zie eveneens het toelichtend rapport bij de Overeenkomst van 29 mei 2000 betreffende wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, *Pb.C.* 29 december 2000, afl. 379, 20-21. Het toelichtend rapport vermeldt uitdrukkelijk dat het aftappen door een staat van communicatie van of naar zijn grondgebied, een maatregel inhoudt op het eigen grondgebied.

401 Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, *Pb.L.* 1 mei 2014, afl. 130 (hierna: EOB). De lidstaten moeten de richtlijn op uiterlijk 22 mei 2017 hebben omgezet. Tot die datum vallen de verzoeken om wederzijdse rechtshulp onder de reeds bestaande regelgeving betreffende wederzijdse rechtshulp in strafzaken. Zie i.v.m. de interceptie van telecommunicatie: art. 30 (over technische bijstand (indien van toepassing, dient bij voorkeur de technische bijstand verkregen te worden van de staat op wiens territorium de af te tappen persoon zich bevindt)) en art. 31 EOB (over de situatie waarin de af te tappen persoon zich in het buitenland bevindt, maar geen technische bijstand vereist is).

402 P. DE HERT, 'Cybercrime and jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty Is at Stake?' in KOOPS en BRENNER (eds), *Cybercrime and Jurisdiction. A Global Survey*, Den Haag, T.M.C. Asser Press, 2006, 82.

rein[403] wanneer een tapmaatregel mogelijk is ten aanzien van personen op zijn territorium en staat in voor de bescherming tegen ongeoorloofde rechtstreekse inmengingen door andere Staten in grondrechten van diezelfde personen (externe bescherming).[404] België en Nederland spelen het in theorie zeer streng en kennen hun rechters steeds een controle- en vetorecht toe als het tapdoelwit van een andere staat[405] zich op hun grondgebied bevindt (art. 90ter §6-7 B.Sv[406], vgl. art. 552oc Nl.Sv). De Belgische wet

403 Weliswaar met inachtneming van de beperkingen die voortvloeien uit internationale verplichtingen waartoe de betrokken staat zich heeft verbonden, zoals art. 8 EVRM.

404 Zie art. 18 lid 5 a) EU-overeenkomst betreffende de wederzijdse rechtshulp in strafzaken en het toelichtend rapport daarbij. Een lidstaat waarvan enkel technische bijstand vereist is, mag de inwilliging van een verzoek tot aftappen en rechtstreeks doorsluizen van de afgetapte informatie niet afhankelijk stellen van de vraag of dat verzoek in overeenstemming is met zijn nationale wetgeving. Die situatie doet zich bv. voor indien de af te tappen persoon zich op het territorium van de aftappende staat bevindt en gebruik maakt van een satelliettelefoon. Gelet op art. 18 lid 5 b) en art. 20, lid 4 b) kan een lidstaat het aftappen van een persoon op zijn grondgebied door een andere lidstaat bv. belemmeren indien het aftappen niet toelaatbaar zou zijn onder het eigen recht. Zie eveneens art. 30 en 31 EOB en de Belgische rechtsregel in de volgende voetnoten.

405 De Belgische wet spreekt over '*de persoon op wie deze maatregel betrekking heeft*'. Dat moet o.i. strikt worden geïnterpreteerd: bv. een Nederlandse rechter beveelt onderschepping van de communicatie van een concrete persoon en die reist naar België, maar de Nederlandse tap duurt voort. Het lijkt dus niet de bedoeling dat, als die persoon vanuit Nederland systematisch naar een contactpersoon in België belt of mailt, laatstgenoemde ook zou worden beschouwd als '*een persoon op wie deze maatregel betrekking heeft*'. Een van de zorgen in de jaren 1990 was bv. dat in de grenszones de politie van het buurland telecommunicatie aan de andere kant van de grens zouden kunnen onderscheppen, waarbij geen enkele van de deelnemers zich op het grondgebied van de onderscheppende staat zou bevinden. Hoe deze regel moet worden toegepast als de maatregel (nog) geen persoon viseert, maar enkel een bepaald toestel, is niet duidelijk. Vaak valt het gemakkelijk te bepalen of een mobiele telefoon of computer zich op dat moment in België bevindt en is dat ook element dat voor de onderzoekers van belang kan zijn.

406 Art. 90ter B.Sv: '*§ 6. Een bevoegde buitenlandse overheid mag, in het raam van een strafrechtelijk onderzoek, tijdelijk privé-telecommunicatie afluisteren, er kennis van nemen en opnemen tijdens de overbrenging ervan, ingeval de persoon op wie deze maatregel betrekking heeft, zich op het Belgische grondgebied bevindt en indien voldaan is aan de volgende voorwaarden: 1° deze maatregel vereist geen technische tussenkomst van een instantie die in België is gevestigd; 2° de betrokken buitenlandse overheid heeft kennis gegeven van deze maatregel aan een Belgische rechterlijke overheid; 3° in deze mogelijkheid is voorzien in een internationaal rechtsinstrument tussen België en de verzoekende Staat; 4° de in § 7 bedoelde beslissing van de onderzoeksrechter is nog niet meegedeeld aan de betrokken buitenlandse overheid. De gegevens die op grond van deze paragraaf zijn verzameld, kunnen alleen worden gebruikt op voorwaarde dat de bevoegde Belgische rechterlijke overheid instemt met de maatregel.*

zegt overigens niet waarop de Belgische onderzoeksrechter moet steunen om de buitenlandse tap van iemand die in België is te machtigen of af te wijzen. Logischerwijze zal die aan de vereisten van de Belgische wet moeten toetsen. [407] Het misdrijf (of beter, de Belgische tegenhanger van het buitenlandse misdrijf) zal dus op de Belgische '*taplijst*' moeten staan. De vraag is natuurlijk of in een wereld met zoveel grensoverschrijdende telecommunicatie de buitenlandse overheden België steeds zullen waarschuwen en of België al die buitenlandse meldingen wel degelijk kan en wil verwerken.[408] Evenmin is het duidelijk hoe België een eventueel door een Belgisch onderzoeksrechter uitgevaardigd gebruiksverbod in het buitenland moet afdwingen, als de tap naar plaatselijk recht rechtmatig was. Het Europees Onderzoeksbevel zwakt het principe overigens wel enigszins af door ook de staat die louter technische bijstand moet verlenen (en dus geen territoriale band met de betrokken subjecten vertoont), toch de mogelijkheid te geven om medewerking te weigeren.[409] Voor de tap kent het formeel strafrecht kent dus ook wel zijn lokalisatiemethodes, al staat men er minder uitdrukkelijk bij stil dan in het materieel strafrecht. Voor het lokali-

---

§ 7. Zodra de procureur des Konings de in paragraaf 6, eerste lid, 2°, bedoelde kennisgeving ontvangt, maakt hij ze onverwijld aanhangig bij de onderzoeksrechter. De onderzoeksrechter bij wie een kennisgeving als bedoeld in § 6, eerste lid, 2°, aanhangig is gemaakt, stemt in met de betrokken maatregel indien deze toelaatbaar is overeenkomstig het bepaalde in dit artikel. Hij stelt de betrokken buitenlandse overheid in kennis van zijn beslissing binnen zesennegentig uur vanaf de ontvangst ervan door de Belgische gerechtelijke overheid. Ingeval een bijkomende termijn noodzakelijk is, kan de onderzoeksrechter zijn beslissing en de kennisgeving ervan aan de bevoegde buitenlandse overheid maximum acht dagen uitstellen. Hij verwittigt hiervan onverwijld de bevoegde buitenlandse overheid met opgave van de redenen. Ingeval de onderzoeksrechter de in § 6 bedoelde maatregel niet toestaat, deelt hij de buitenlandse overheid eveneens mee dat de verkregen gegevens moeten worden vernietigd zonder te kunnen worden gebruikt.'

407 Art. 552oc, 3° Nl.Sv zegt dat de rechter-commissaris een beslissing neemt '*met inachtneming van het bepaalde in het toepasselijke verdrag en het bepaalde bij of krachtens artikel 126m of 126t.*'

408 Als er in België een formele machtiging van een onderzoeksrechter nodig is, zal bv. de Belgische wetgeving inzake taalgebruik in rechtszaken gelden (art. 12 wet van 15 juni 1935 op het gebruik der talen in rechtszaken), zodat buitenlandse stukken officieel moeten vertaald zijn en de Belgische beslissingen op hun beurt opnieuw naar de taal van het land dat de melding deed.

409 Art. 30 EOB: '*An EIO may be issued for the interception of telecommunications in the Member State from which technical assistance is needed. …] In addition to the grounds for non-recognition or non-execution referred to in Article 11, the execution of an EIO referred to in paragraph 1 may also be refused where the investigative measure would not have been authorised in a similar domestic case. The executing State may make its consent subject to any conditions which would be observed in a similar domestic case.*'

seren van de tap verschuift de focus van het gezochte object, d.i. het bewijsmateriaal (*object-georiënteerde benadering*) naar het onderzochte subject, d.i. de onderzochte persoon (*subject-georiënteerde benadering*).[410]

OOK TELECOMTAP – Deze subject-georiënteerde benadering van de klassieke tapbevoegdheid in de EU-overeenkomst inzake wederzijdse rechtshulp, geldt ook voor het aftappen van nieuwe vormen van telecommunicatie. Het toelichtend rapport bij de overeenkomst verwijst uitdrukkelijk naar de bedoeling om de bepalingen over het aftappen van communicatie toe te passen op alle communicatievormen die zullen voortvloeien uit de bestaande en toekomstige technologie.[411] Het verdrag heeft zowel betrekking op het bekomen van verkeersgegevens (wie communiceert met wie, tijdstip, duur…) als inhoudelijke gegevens.[412] De informaticatap vindt volgens de Overeenkomst dus plaats daar waar de afgetapte persoon zich bevindt.[413]

LOKALISATIEMETHODE OBSERVATIE – Voor de visuele observatie in de fysieke wereld valt er echter geen lokalisatiemethode terug te vinden in supra- of internationale overeenkomsten. Ook het nationale recht bepaalt niet uitdrukkelijk wanneer een observatie al dan niet grensoverschrijdend is. Is de plaats van het geobserveerde (subject of object) of de plaats van de observeerder doorslaggevend? De locatie van waaruit de observatie plaatsvindt, kan o.i. niet zonder meer bepalend zijn. De mate van rechtsbescherming van de geobserveerde wordt in die visie immers volledig afhankelijk gesteld van de technische mogelijkheden van de observerende staat. Zo is het bijvoorbeeld, minstens in de toekomst, wellicht technisch mogelijk om infraroodtechnologie te combineren met satelliettechnologie om zo warm-

410 Zie bij lokalisering toestel onbekend persoon: *infra*, 6.3.4.

411 Toelichtend rapport bij de Overeenkomst van 29 mei 2000 betreffende wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, *Pb.C.* 29 december 2000, afl. 379, 20 en 22.

412 Toelichtend rapport bij de Overeenkomst van 29 mei 2000 betreffende wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, *Pb.C.* 29 december 2000, afl. 379, 22.

413 België heeft deze regel zoals gezegd geïmplementeerd in art. 90ter, §6-7 B.Sv, *supra*, noot 406. Dat betekent dus dat telkens een buitenlandse overheid, waar ook ter wereld, elektronische communicatie (email, SMS, WhatsApp, chatgesprekken, ...) onderschept van een doelwit dat in België zit, zij België moet waarschuwen en van de Belgische rechters toestemming moet krijgen om de resultaten te mogen gebruiken. Omgekeerd zal België bij iemand die vanuit België met de auto naar Albanië reist en onderweg boodschappen blijft sturen, dus al snel de Duitse, Oostenrijkse, Sloveense, Kroatische, Bosnische, Montenegrijnse en Albanese instemmingen moeten verkrijgen.

tebronnen in woningen over de hele wereld te detecteren. Indien de locatie van de observeerder beslissend is dan zou een dergelijke observatie onder de plaatselijke nationale wetgeving mogelijk zijn, ook al bevindt het geobserveerde zich elders in de wereld. Door daarentegen te focussen op de locatie van het geobserveerde, behouden staten de mogelijkheid om hun soevereine controlebevoegdheden overeenkomstig het nationale recht uit te oefenen t.a.v. alle handelingen die op hun territorium worden gesteld. Enkel in die visie kunnen ze op het eigen grondgebied hun ordenende en beschermende taak vervullen. Bovendien stelt die benadering staten in de mogelijkheid om, via hun recht op uitsluiting, personen en zaken op het eigen territorium te beschermen tegen ongeoorloofde grondrechtenschendingen door buitenlandse overheden. Focussen op de plaats van waaruit wordt geobserveerd brengt daarenboven een onlogisch onderscheid met zich mee tussen observaties vanuit het luchtruim (bv. via drones), dat tot het territorium behoort van de onderliggende staat, en observaties vanuit de ruimte via satellieten.[414] We menen bijgevolg te mogen stellen dat de locatie van het onderzochte subject (d.i. de afgetapte persoon of de geobserveerde persoon/zaak) de locatie van klassieke opsporingshandelingen *in real time*, zoals de telefoontap en de visuele observatie, hoort te bepalen. Wensen staten satellieten of andere systemen in te zetten om controles op elkaars territoria uit te voeren, dan kan dit o.i. enkel op grond van internationale (eventueel stilzwijgende) overeenstemming.[415]

CYBERCRIME-VERDRAG – Art. 20 en 21 Cybercrime-verdrag[416] verplichten de ondertekenende staten in de bevoegdheid te voorzien om verkeers-

414 Zie m.b.t. het moeilijke onderscheid tussen luchtruim en ruimte: W. DEREZE, 'De grens tussen luchtvaart en ruimtevaart', *Jura. Falc.* 2007-08, afl. 1, 99-129.

415 Zie bv. beginselen met betrekking tot remote-sensing van de aarde vanuit de ruimte, zoals vastgesteld door de Algemene Vergadering van de Verenigde Naties op 11 december 1986, http://www.un.org/documents/ga/res/41/a41r065.htm: Overeenkomstig die beginselen mag *remote-sensing* (afstandswaarneming) enkel uitgevoerd worden ten behoeve van alle landen, zoals voor milieubescherming, bescherming van natuurlijke grondstoffen en bescherming t.a.v. natuurrampen.

416 Verdrag van Boedapest inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van 23 november 2001, *European Treaty Series No. 185,* http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm (hierna: Cybercrime-verdrag); België ratificeerde dit verdrag op 20 augustus 2012 (inwerkingtreding: 1 december 2012). Zie wet van 3 augustus 2012 houdende instemming met het verdrag betreffende de computercriminaliteit, gedaan te Boedapest op 23 november 2001, *BS* 21 november 2012.

gegevens[417] en gegevens die betrekking hebben op de inhoud van *communicatie op het eigen grondgebied* te onderscheppen. Enerzijds dienen de staten te voorzien in een mogelijkheid voor bevoegde ambtenaren om zelf de data te verzamelen of te onderscheppen via technische hulpmiddelen op hun grondgebied.[418] Anderzijds verplicht het verdrag de staten om in een medewerkingsplicht in hoofde van serviceproviders te voorzien. Dit kan de vorm aannemen van een verplichting om zelf de data te onderscheppen via technische hulpmiddelen op het grondgebied van die staat of om de overheid hierin bij te staan. Gelet op het toelichtend rapport bij het Cybercrime-verdrag is, '*praktisch gezien*', de medewerkingsplicht '*in principe toepasselijk*' op service providers die over een fysieke infrastructuur of uitrusting beschikken op het territorium van de bevelende staat waardoor zij in de mogelijkheid verkeren om de maatregel ten uitvoer te leggen.[419] Net zoals dat het geval is bij de telefoontap, lijken internationale regels tot wederzijdse rechtshulp dus nodig wanneer (technische) bijstand vanuit het buitenland noodzakelijk is.[420] Art. 20 en 21 gaan enkel over een bevoegdheid met betrekking tot communicatie op het eigen grondgebied. Volgens het toelichtend rapport vindt communicatie plaats op het grondgebied van een lidstaat indien één van de communicerende partijen zich daar bevindt of

---

417 Dit zijn overeenkomstig art. 1, d Cybercrime-verdrag '*computergegevens die verband houden met een met behulp van een computersysteem gevoerde communicatie, en worden voortgebracht door een computersysteem dat een onderdeel vormt van de communicatieketen, en de herkomst, de bestemming, de route, de tijd, de datum, de omvang, de duur of de aard van de betrokken dienst aanduiden*'.

418 Indien de beginselen uit het nationale rechtsstelsel dit niet toelaten, dient het real-time onderscheppen van verkeersgegevens en inhoudelijke gegevens via andere wegen te worden verzekerd (art. 20,2 en 21,2 Cybercrime-verdrag).

419 Toelichtend rapport bij het Cybercrime-verdrag van 23 november 2001, http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, §222 en 230 (hierna toelichtend rapport bij het Cybercrime-verdrag).

420 Het Cybercrime-verdrag geeft zelf echter geen uitsluitsel gelet op de vage bewoordingen en het feit dat het verdrag slechts gericht is op het harmoniseren van minimale bevoegdheden inzake opsporing in een digitale omgeving. (Zie art. 39 Cybercrime-verdrag en het toelichtend rapport bij het Cybercrime-verdrag, §131.) Het verdrag lijkt, afhankelijk van het type medewerkingsplicht, nu eens de locatie van de medewerkingsplichtige als criterium voor de lokalisering van opsporingshandelingen naar voor te schuiven (zie art. 18, a Cybercrime-verdrag inzake het verstrekkingsbevel) en dan weer de locatie van de data (zie art. 16 *juncto* 29 Cybercrime-verdrag inzake het bevriezingsbevel). Wat betreft het verkrijgen van abonnee-informatie verwijst het verdrag naar de plaats waar een Internetdienst wordt aangeboden (art. 18, b Cybercrime-verdrag). Omtrent de lokalisering van vorderingen tot medewerking zijn verschillende visies terug te vinden.

indien het informaticasysteem of de telecommunicatieapparatuur waarmee de communicatie wordt overgezonden, daar kan worden gelokaliseerd.[421] Communicerende partijen kunnen zowel personen als computers zijn.[422] Dit wijst op de ruime betekenis van het begrip '*communicatie*' in het Cybercrime-verdrag, wat ook bijvoorbeeld het openen van een website inhoudt.[423]

DISCREPANTIE RAAD VAN EUROPA EN EU – In het Cybercrime-verdrag vinden we dus eveneens een lokalisatiemethode terug die bovendien deels gelijkt op de lokalisatiemethode uit de EU-overeenkomst inzake wederzijdse rechtshulp. Door de verwijzing naar de locatie van de communicatiepartijen bevestigt het Cybercrime-verdrag de subject-georiënteerde benadering uit de EU-overeenkomst. Toch is er een belangrijk verschil. Het Cybercrime-verdrag lijkt, zonder bijkomende uitleg, immers te vereisen dat eveneens in een tapbevoegdheid wordt voorzien ten aanzien van het informaticasysteem of de telecommunicatieapparatuur die de communicatie doorzendt. Het verdrag combineert zo de subject- en object-georiënteerde benadering ter lokalisering van real time opsporingshandelingen. Wanneer een staat immers tapt op een tussenstation op zijn territorium dat enkel instaat voor het doorzenden van de communicatie dan vindt die tap, volgens het Cybercrime-verdrag, plaats op het territorium van die aftappende staat. Het feit dat de communicatiepartners zich elders bevinden is irrelevant. Dit staat in schril contrast met de zienswijze in de Europese Unie. Art. 20 van de EU-overeenkomst inzake wederzijdse rechtshulp handelt over de mogelijkheid om personen in het buitenland af te tappen zonder dat daartoe grensoverschrijdende technische bijstand vereist is. Hoewel er geen recht*shulp* nodig is, vereist het artikel wel een kennisgeving aan en instemming van de staat waar de af te tappen persoon zich bevindt. [424] Met het oog op rechtszekerheid is een gelijkschakeling van de lokalisatiemethode van de Raad van Europa en die van de Europese Unie aanbevolen.

---

421 Toelichtend rapport bij het Cybercrime-verdrag, §222 en §230.

422 Toelichtend rapport bij het Cybercrime-verdrag, §222 en 230.

423 M. GERCKE, *Understanding cybercrime: Phenomena, challenges and legal response*, Genève, International Telecommunication Union (ITU), 2012, 260.

424 Die kennisgeving dient te gebeuren vóór het aftappen indien bij het geven van het tapbevel bekend is dat de persoon zich op het grondgebied van de in kennis te stellen lidstaat bevindt. In andere gevallen dient de kennisgeving plaats te vinden onmiddellijk nadat bekend wordt dat de persoon zich op het grondgebied van de in kennis te stellen lidstaat bevindt. Cf. Art. 31 EOB.

NATIONALE REGELGEVING – Net zoals in verschillende andere rechtssystemen[425], geldt in België de regelgeving inzake de telefoontap eveneens voor de informaticatap.[426] De locatie van het afgetapte subject bepaalt bijgevolg waar de informaticatap plaatsvindt. Dit blijkt ook uit het vermelde artikel 90ter §6-7 B.Sv of 126ma Nl.Sv[427] (*supra*).

SUBJECT: AANVAARD – Zowel het Cybercrime-verdrag als de EU-overeenkomst inzake wederzijdse rechtshulp hanteren een subject-georiënteerd uitgangspunt: de staat op wiens territorium het onderzochte subject zich bevindt, is territoriaal bevoegd voor het opsporen in real time. Dit lijkt logisch vanuit de soevereiniteitsgedachte en de daarmee beoogde rechtsbescherming. De soevereine bevoegdheid van de staat waar het subject zich bevindt (hierna: subject-staat) behelst de mogelijkheid tot controle van handelingen gesteld op en communicatie gevoerd vanuit of naar diens grondgebied, onder de voorwaarden omschreven in diens nationale recht en met respect voor de rechten en vrijheden waartoe die zich op internationaal vlak heeft verbonden. De subject-staat behoudt zo de controle over wat zich afspeelt op zijn territorium. Een volledig subject-georiënteerde benadering stelt bovendien een duidelijke territoriale grens aan de soevereine bevoegdheid. Wanneer het subject de grens overschrijdt, vervalt ook de mogelijkheid om unilateraal het real-time onderzoek verder te zetten. Immers, telkens wanneer het af te tappen subject zich in het buitenland bevindt is internationale samenwerking vereist, zelfs indien geen technische bijstand vanuit het buitenland nodig is. Verder biedt deze zienswijze voldoende rechtszekerheid. Rechtsbescherming, in het bijzonder de bescherming van het recht op privacy[428], vindt plaats overeenkomstig het recht van het land waarin de rechtsonderhorige zich bevindt en waar hij handelingen stelt en communicatie voert. De staat waar het subject zich bevindt heeft het recht op uitsluiting van andere staten en kan zo externe bescherming bieden aan zijn onderdanen tegen inmengingen in hun grondrechten die volgens het plaatselijke recht ongeoorloofd zijn. Het hierboven geschetste samenspel (*supra*, 6.2) blijft bijgevolg in stand.

---

425 Zie bv. Art. 126 m Nl.Sv; §100a Strafprozeβordnung (StPo).

426 Zie art. 90ter B.Sv.

427 Deze Nederlandse wet vereist kennisgeving aan en instemming van de staat waar het doelwit zich bevindt, maar wel slechts 'voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag'. Als er geen verdrag is, zal Nederland dus blijkbaar autonoom kunnen handelen.

428 Art. 8 EVRM.

AANVULLING MET OBJECT (CYBERCRIME-VERDRAG)? – Een aanvulling van de subject-georiënteerde bevoegdheid met een object-georiënteerde bevoegdheid, waarbij de locatie van de data zonder meer bepalend is, lijkt niet wenselijk. In het Cybercrime-verdrag vinden we een criterium terug dat louter gebaseerd is op de technische aanwezigheid van de gegevens. Zodra gegevens technisch aanwezig zijn op het territorium van een staat, kan die staat de gegevens overeenkomstig zijn nationale regelgeving in real time opsporen. Dat vinden we een bedenkelijke, zelfs onvoorzichtige keuze. De overheid van 'gegevenstransitlanden' kan er op steunen voor het doelbewust opsporen van gegevens met betrekking tot communicatie gevoerd tussen personen in het buitenland, zonder enige vorm van internationale samenwerking en zonder dat er een aantoonbare link bestaat tussen de onderzochte gegevens en de opsporende staat (bv. via het monitoren van een Internet Exchange Point[429]). Via welke informaticasystemen (routers) de data passeren is tot op zekere hoogte immers ingegeven door willekeur.[430] Als een Belg en een Nederlander chatten en de gegevens passeren langs Duitsland, zou Duitsland theoretisch gezien het gesprek tussen de Belg en Nederlander unilateraal overeenkomstig Duitse regelgeving kunnen aftappen. De soevereiniteit van het land waar de onderzochte persoon zich bevindt, lijkt hier in haar externe dimensie moeilijk mee te rijmen. Zelfs indien alle communicatiepartners en de aanbieder van de communicatiedienst zich op zijn territorium bevinden is het mogelijk dat andere staten er onder hun nationale regelgeving toegang toe kunnen nemen louter omwille van de technische opbouw en werking van het Internet. Dan kan Duitsland unilateraal de communicatie van een Nederlander in Rotterdam via de diensten van een Nederlands bedrijf met een andere Nederlander in Gouda aftappen, louter omdat gegevens via een kabel over Duits grondge-

429 D.i. een soort knooppunt van het Internet waarop netwerken van verschillende dienstenaanbieders zijn aangesloten en via dewelke zij onderling hun communicatie uitwisselen. Zie i.v.m. de mogelijkheid tot het monitoren van een Internet Exchange Point: F. BHATTI, J. SOUTER, 'ExSERT: Enabling Distributed Monitoring at Internet Exchange Points', 2005, http://saleem.host.cs.st-andrews.ac.uk/ publications/2005/lcs2005/lcs2005-hbs2005.pdf; zie ook: G.L. HERRERA, 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space', 2005, *kms2.isn.ethz.ch, 21-23.*

430 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 329-330 en 367-368; J. GULDENTOPS, *Geschiedenis en het internet: een historische, methodologische en heuristische benadering van de informatiesnelweg,* Leuven, Acco, 1996, 9; G.L. HERRERA, 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space', 2005, *kms2.isn.ethz.ch, 4*; zie eveneens: Verslag namens de commissie, Parl. St. Senaat 1999-2000, nr. 2-392/3, 22.

bied passeren. Het territorialiteitsbeginsel speelt dan nog maar een beperkte rol. De Internetinfrastructuur holt de rechtsmacht- en rechtsbeschermingsaanspraken van de staat waar de communicatie wordt gevoerd of de virtuele handelingen worden gesteld (in ons voorbeeld: Nederland) volledig uit. Die staat verliest dus de controle over de externe rechtsbescherming van personen die zich op zijn territorium bevinden en van daaruit virtueel handelen of communiceren. Zo is er ook geen sprake meer van rechtszekerheid voor de rechtsonderhorigen, die doorgaans niet weten en bovendien niet kunnen weten via welke weg data naar hun bestemming reizen.[431] Het standpunt dat rechtsonderhorigen de territoriale begrenzing van de soevereiniteit van de staat waar zij verblijven ook in die omstandigheden moeten erkennen, lijkt ons absurd en onhoudbaar gelet op de arbitraire weg die de gegevens afleggen en de onmogelijkheid voor de rechtsonderhorige om die weg te kennen.[432] Wil het land waar de data op een gegeven moment toevallig technisch aanwezig zijn, die data onderscheppen dan vereisen de staatssoevereiniteit en de loyaliteit in het internationaal recht o.i. nauwere regels tot samenwerking.[433] Voor dataverkeer dat geen band vertoont met het eigen grondgebied, zouden staten dus een soort verbod op inmenging moeten erkennen, vergelijkbaar met het recht van vrije vreedzame doorvaart van buitenlandse schepen.

6.3.3. De zoeking naar opgeslagen data: huidige object-georiënteerde benadering en herdachte virtuele zoeking

HUIDIG UITGANGSPUNT: LOCATIE DATA – Wanneer opsporingsinstanties zoeken naar bestaand fysiek bewijs, dan doen zij dat, logischerwijze, daar waar het bewijsmateriaal zich bevindt. Is het bewijsmateriaal gelegen in het buitenland, dan kunnen ze er, gelet op de staatssoevereiniteit en het territorialiteitsbeginsel, enkel toegang toe nemen via de wegen van internationale samenwerking. We zouden bijgevolg kunnen stellen dat een zoeking vanop afstand naar virtueel bewijsmateriaal[434], opgeslagen op een informaticasysteem in het buitenland, principieel eveneens enkel via de wegen van inter-

431 DASKAL, *ibid.,* 330.

432 Zie ook *ibid.,* 366-368.

433 Ter vergelijking: B. DE SMET, 'Registratie en lokalisatie van telecommunicatie', in *Comm. Straf.* 2008, 29.

434 Het gaat hier bv. om de netwerkzoeking (*supra*, 2.1.3) of de heimelijke variant daarvan (*supra*, 2.2).

nationale samenwerking kan worden verkregen.[435] Dit standpunt vinden we niet enkel terug in de rechtsleer[436], maar ook de Raad van Europa en de nationale wetgever blijken hiervan uit te gaan. Art. 31 Cybercrime-verdrag handelt immers over wederzijdse rechtshulp ter verkrijging van data *opgeslagen op het territorium van een andere ondertekenende staat*. Art.32 Cybercrime-verdrag voorziet daarnaast in enkele uitzonderingen waarin een rechtstreekse, grensoverschrijdende toegang mogelijk is. De Belgische wetgeving inzake de netwerkzoeking (art. 88ter §3, lid 2 Sv) voorziet in een verregaandere bevoegdheid, wat door het Cybercrime-verdrag zelf niet wordt uitgesloten (*supra*, 2.3.2).[437] Waar de nationale wetgever dus eveneens lijkt uit te gaan van de lokalisatie van de opsporingshandeling op basis van de locatie van de data, voorziet hij toch in een unilaterale mogelijkheid om een *grensoverschrijdende zoeking* uit te voeren. In een data-georiënteerde visie, zoals die van de wetgever vandaag, is dit nochtans in principe in strijd met het verbod op het eenzijdig voorzien in extraterritoriale opsporingshandelingen (*supra*, 2.3).

INEFFICIËNT CRITERIUM – Zoals de Belgische pragmatische benadering aangeeft, levert de huidige object-georiënteerde benadering in de praktijk heel wat problemen op. We hebben gezien dat een steeds groter gedeelte van het menselijke leven verhuist naar de digitale omgeving. Communicatie verloopt steeds meer via virtuele wegen (e-mail, Skype, WhatsApp, sociale media) en allerhande gegevens zoals foto's en video's worden opgeslagen met behulp van Dropbox of soortgelijke clouddiensten om het uitwisselen ervan te vergemakkelijken, de duurzaamheid ervan te verzekeren of de toegankelijkheid ervan te verbeteren. Die via het Internet aangeboden en gebruikte diensten, zijn niet gebonden aan territoriale grenzen en de gezochte data zijn uiterst vaak in het buitenland opgeslagen. Zelfs de data gerelateerd aan het gebruik van een nationale dienst, bevinden zij zich niet noodzakelijk op het eigen territorium. Steeds meer zaken krijgen zo plots

---

435 Ook in de Verenigde Staten wordt vandaag over het algemeen dit klassieke standpunt ingenomen: J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 371.

436 Zie: N. SEITZ, 'Transborder search: a new perspective in law enforcement?', *Yale Journal of Law and Technology* 2005, Vol. 7, 22 e.v.; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?,* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/ cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_ Computing_power_disposal_31Aug10a.pdf.

437 Toelichtend rapport bij het Cybercrime-verdrag, §294.

een internationaal karakter, louter omwille van de plaats van opslag van de gezochte gegevens. Internationale rechtshulp is noodzakelijk telkens wanneer de gezochte data op servers in het buitenland staan. Data van eenzelfde bestand kunnen bovendien op uiteenlopende territoria worden opgeslagen.[438] In de object-georiënteerde visie bestaat er dan ook een disproportionele nood aan samenwerking over de grenzen heen, wat de nodige vertraging met zich meebrengt. Dergelijke vertragingen kunnen politie en justitie zich moeilijk veroorloven, ook omdat de data met grote snelheid van locatie kunnen veranderen. Het risico op verlies van het volatiele bewijsmateriaal en op eindeloze en vruchteloze inspanningen om met steeds weer andere staten samen te werken, is daardoor erg groot. Staten met veel dienstenaanbieders en een grote opslagcapaciteit worden in de object-georiënteerde benadering dan weer geconfronteerd met een overload aan rechtshulpvragen, die zij vermoedelijk steeds moeilijker verwerkt krijgen. Zoals gezegd (*supra*, 2.3.2), voorziet art. 32 van het Cybercrime-verdrag slechts in twee beperkte uitzonderingen voor de ondertekenende lidstaten. Rechtstreekse grensoverschrijdende toegang is op de eerste plaats mogelijk als de data voor iedereen toegankelijk zijn (Internet als open bron). Dit vormt een bevestiging van de bestaande praktijk en geldt bijgevolg ook buiten het territoriaal toepassingsgebied van het Cybercrime-verdrag.[439] Verder is rechtstreekse grensoverschrijdende toegang toegelaten indien een persoon met rechtmatige controle over de gezochte data toestemt in toegang door opsporingsinstanties.[440] Die tweede uitzondering geldt enkel binnen het territoriale toepassingsgebied van het Cybercrime-verdrag. Als de plaats van opslag niet gekend is, kunnen de opsporende instanties ook niet weten of de uitzondering van toepassing is.[441] De kans bestaat dan dat de data zich bevinden op het territorium van een niet-verdragsluitende staat. Bovendien is de kans groot dat opsporingsinstanties er niet in slagen de vereiste toestemming in een concrete zaak te verkrijgen. Beide uitzon-

438 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 368-369 (m.b.t. *partitioned databases*).

439 N. SEITZ, 'Transborder search: a new perspective in law enforcement?', *Yale Journal of Law and Technology* 2005, Vol. 7, 38.

440 Bv. de legale gebruiker van de onderzochte gegevens. De dienstenaanbieders kunnen in principe niet wettelijk instemmen met de grensoverschrijdende toegang tot gegevens van de gebruikers van hun diensten. Zij houden de gegevens normaal enkel bij en hebben er geen controle over noch vormt het hun eigendom. Zie CYBERCRIME CONVENTION COMMITTEE, 'Guidance Note # 3, Transborder access to data (article 32)', 2013, www.coe.int/TCY.

441 CYBERCRIME CONVENTION COMMITTEE, 'Report: Transborder access and jurisdiction: What are the options?', *T-CY* 2012, nr. 3, 21.

deringen lossen weinig op. Binnen het Comité van het Cybercrime-verdrag wordt daarom verwoed gedebatteerd over verregaandere mogelijkheden tot unilaterale grensoverschrijdende zoekingen.[442] Daarnaast probeert het Cybercrime-verdrag de samenwerking op verschillende manieren te versnellen.[443] De vertaling van theorie naar praktijk verloopt moeizaam.[444] Ondertussen hebben de ministers van Justitie van de Europese Unie de kwestie van snellere rechtshulp en jurisdictie uitdrukkelijk op de agenda gezet. Op de Raad van 9 juni 2016 hebben ze '*een oriënterend debat gehouden over (…) de mogelijke fundamenten voor handhavingsjurisdictie in de cyberruimte, d.w.z. de gronden waarop bevoegde autoriteiten kunnen overgaan tot onderzoeksmaatregelen in de cyberruimte wanneer bestaande kaders onvoldoende houvast bieden, bijvoorbeeld gevallen waarin relevant digitaal bewijsmateriaal verborgen is of zich met hoge snelheid tussen jurisdicties verplaatst*.' In hun conclusies hebben ze de Commissie gevraagd '*een denkproces over mogelijke aanknopingspunten voor het onderbouwen van handhavingsjurisdictie [op gang te brengen]*'.[445]

LOSS OF OBJECT-LOCATION – Niet alleen gebrek aan tijd tast de efficiëntie van het huidige systeem aan, ook gebrek aan kennis is een ernstige struikelblok. De hedendaagse virtuele realiteit confronteert opsporingsinstanties er steeds vaker mee dat de precieze locatie van data moeilijk of niet valt te achterhalen.[446] *Cloud computing* draagt hier in belangrijke mate toe bij.[447] De

442 Zie *ibid*.

443 Art. 25 Cybercrime-verdrag voorziet zo in de mogelijkheid om '*snelle communicatiemiddelen, zoals fax of e-mail*' te gebruiken voor verzoeken tot wederzijdse rechtshulp; Art. 29 Cybercrime-verdrag omschrijft de mogelijkheid tot het verzoeken van een staat om de bevriezing van gegevens, opgeslagen via een informaticasysteem op diens territorium, te bevelen. Dat verzoek kent een minimum aan formaliteiten en wordt gebruikt in afwachting van een meer gefundeerde vraag om verstrekking van de gegevens (zie in dit verband ook art. 30); Art. 35 Cybercrime-verdrag voorziet in de oprichting van 24/7 contactpunten.

444 M. GERCKE, *Understanding cybercrime: Phenomena, challenges and legal response*, Genève, International Telecommunication Union (ITU), 2012, 280 (over de oprichting en het gebruik van 24/7 contactpunten).

445 RAAD VAN DE EU 9 juni 2016, Persmededeling 321/16, 'Strijd tegen criminaliteit in de cyberruimte: Raad bereikt akkoord over praktische maatregelen en volgende stappen', http://www.consilium.europa.eu/press-releases-pdf/2016/6/47244642380_nl.pdf.

446 Zie in dit verband ook: HvJ C-131/12, *Google Spain*, 2014, overweging 43 i.v.m. Google Search: '*The information indexed […] is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition*.' In dit verband wordt vaak gesproken over de '*loss of location*'. KOOPS en GOODWIN verwijzen meer precies naar de '*loss of knowledge of location*'. B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the*

cloud bestaat uit verschillende servers die met elkaar in verbinding staan via het Internet. Data, opgeslagen in de *cloud*, worden om financiële redenen en omwille van het optimale gebruik van opslagcapaciteit vaak verplaatst.[448] De lokalisatie van de data op een gegeven moment in de tijd blijkt daarbij moeilijk. Bestanden in de *cloud* kunnen bovendien worden opgesplitst in kleine deeltjes die mogelijks elk ergens anders worden opgeslagen.[449] Ook worden kopies van data op verschillende plaatsen opgeslagen om verlies tegen te gaan.[450] De Belgische[451] en Nederlandse wetgevers schuiven in dat verband een beperkte oplossing naar voren door een grensoverschrijdende zoeking onder andere mogelijk te maken wanneer speurders er redelijkerwijze niet in slagen de betrokken staat te identificeren. Met het toenemend belang van *cloud computing* dreigt de uitzondering echter eerder de regel te worden. Opdat een criterium voor procedurele bevoegdheid werkbaar zou zijn, is het net van groot belang dat opsporingsinstanties de vervulling ervan op voorhand gemakkelijk kunnen inschatten.[452] Verder mag het criterium eveneens niet te zeer aan verandering onderhevig zijn. De locatie van de gegevens lijkt daarom geen goed criterium.[453]

---

cloud, and cross-border criminal investigation, The Hague/Tilburg, WODC/TILT, 2014, 42.

447 J.J. SCHWERHA, *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers",* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations, 9. Al zou het probleem in de rechtsleer soms te zeer worden uitvergroot: KOOPS en GOODWIN, *ibid*., 44. Zo zouden cloud-providers de data vaak dicht bij de gebruiker opslaan om de snelheid van de dienst te maximaliseren en zouden cloud-providers meer en meer de verwerking en opslag van data beperken tot bepaalde regio's, zoals de Europese zone, teneinde aan dataprotectievoorschriften te kunnen voldoen.

448 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 373; B.J. KOOPS, R. LEENES, P. DE HERT, S. OLISLAEGERS, *Misdaad en opsporing in de wolken, knelpunten en kansen van cloud computing voor de Nederlandse opsporing* in *WODC,* Tilburg, Universiteit van Tilburg, 2012, 12; KOOPS en GOODWIN, *ibid*., 22; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. The power of disposal?,* Project on Cybercrime Council of Europe, 2010.

449 KOOPS, LEENES, DE HERT, OLISLAEGERS, *ibid*., 36; KOOPS en GOODWIN, *ibid*., 22.

450 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 368; KOOPS en GOODWIN, *ibid*., 22.

451 MvT, *Parl. St*. Kamer 1999/2000, nr. 50K0213/001, 24-25.

452 J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?,* Project on Cybercrime Council of Europe, 2010.

453 Zie eveneens: J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 329.

VOORLOPIG STANDPUNT? – Het is niet bepaald een overtuigde keuze van de Raad van Europa om de zoeking naar opgeslagen data te lokaliseren daar waar de gegevens staan opgeslagen. Al in 1995 stelde het Comité van Ministers van de Raad van Europa in aanbeveling R(95)13 dat een unilaterale zoeking naar data in het buitenland *mogelijks* een schending van de soevereiniteit van dat land inhield.[454] Tijdens de totstandkoming van het Cybercrime-verdrag bleek het onmogelijk om eensgezindheid te bereiken over de vraag of de zoeking in een buitenlands computersysteem al dan niet een soevereiniteitsschending tot gevolg heeft.[455] Gelet op de zeer beperkte mogelijkheden tot grensoverschrijdende zoekingen onder het internationale publiekrecht achtten de staten concrete afspraken voor een dergelijke zoeking noodzakelijk.[456] Het soevereiniteitsvraagstuk kreeg binnen de Raad van Europa dus geen afdoend antwoord. Uit het toelichtend rapport bij het Cybercrime-verdrag blijkt daarenboven dat de verdragsluitende staten in art. 32 voorlopig slechts de mogelijkheden wensten vast te leggen waarover eensgezindheid kon worden bereikt. Dit artikel geeft geen fiat voor verregaandere bevoegdheden, maar sluit ze anderzijds ook niet uit.[457] Digitale opsporing stond nog te zeer in de kinderschoenen om de problematiek al op definitieve wijze te kunnen beslechten.[458] De vraag naar de lokalisering van de zoeking, die nauw samenhangt met het soevereiniteitsvraagstuk, werd echter jammer genoeg niet uitdrukkelijk aangehaald. Noch voor de medewerkingsverplichtingen, noch voor de opsporingshandelingen wordt echt aandacht besteed aan het criterium voor de lokalisering. Een zoeking naar data, opgeslagen in het buitenland, bestempelt het Cybercrime-verdrag zonder veel uitleg als een grensoverschrijdende zoeking.

---

454 Aanbeveling R(95)13 betreffende problemen in verband met het strafproces die gelieerd zijn met informatietechnologie, http://www.coe.int/t/dghl/ standardsetting/media/Doc/CM/Rec%281995%29013_en.asp; zie eveneens: MvT, *Parl. St.* Kamer 1999/2000, nr. 50K0213/001, 45-46.

455 CYBERCRIME CONVENTION COMMITTEE, 'Report: Transborder access and jurisdiction: What are the options?', *T-CY,* 2012, nr. 3, 27; H.W.K. KASPERSEN, 'Jurisdiction in the Cybercrime Convention', in B.J. KOOPS en S.W. BRENNER (eds), *Cybercrime and Jurisdiction, A Global Survey*, Den Haag, T.M.C. Asser Press, 2006, 20; zie eveneens: W.H. VON HEINEGG, 'Legal implications of Territorial Sovereignty in Cyberspace', in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 11-12.

456 H.W.K. KASPERSEN, 'Jurisdiction in the Cybercrime Convention', in B.J. KOOPS en S.W. BRENNER (eds), *Cybercrime and Jurisdiction, A Global Survey*, Den Haag, T.M.C. Asser Press, 2006, 20.

457 Toelichtend rapport bij het Cybercrime-verdrag, §294.

458 *Ibid*.

NOOD ONDERBOUWDE KEUZE – Buiten het Cybercrime-verdrag en de EU regelgeving omtrent het aftappen van telecommunicatie komt de strafprocedurele lokalisatieproblematiek op internationaal niveau helaas nergens uitdrukkelijk aan bod. Het internationale publiekrecht biedt geen pasklare oplossing. De traditionele logica dat de zoeking naar fysiek bewijs plaatsvindt op de plaats waar het bewijsmateriaal zich bevindt, kan echter niet zomaar worden doorgetrokken naar zoekingen naar virtueel bewijs. Die logica gaat immers enkel op voor de rechtstreekse doorzoeking van een informaticasysteem (de informaticazoeking), zoals het uitlezen van een computer of een mobiele telefoon. Die situatie is immers perfect vergelijkbaar met andere zoekingen, zoals de huiszoeking of doorzoeking van andere plaatsen. De plaats waar het bewijs zich bevindt en de plaats waar het bewijs toegankelijk is (voor de gebruiker en voor opsporingsinstanties) vallen samen waardoor de klassieke lokalisatie van zoekingen naar bestaand fysiek bewijs kan worden toegepast. Een belangrijk verschilpunt doet zich echter voor bij zoekingen naar opgeslagen data op afstand, zoals de netwerkzoeking en de online doorzoeking van een online account (bv. Dropbox, webmail, sociale media) (*supra*, 2.1.3, 2.2). De plaats waar het bewijsmateriaal zich bevindt en de plaats(en) van toegang tot en gebruik van het bewijsmateriaal vallen dan immers niet meer samen.[459] Een persoon kan gegevens opslaan over de grenzen heen, maar ze oproepen en gebruiken waar hij wil en wanneer hij wil. Er doet zich bijgevolg een nieuwe situatie voor die niet geheel vergelijkbaar is met zoekingen naar fysiek bewijs in de fysieke wereld. We overlopen daarom enkele andere mogelijkheden ter lokalisering van de virtuele zoeking op afstand om vervolgens het huidig object-georiënteerde standpunt met de naar onze mening meest geschikte alternatieven te vergelijken.

LOCATIE OPSPORINGSINSTANTIES – Een eerste optie ter lokalisering van de openlijke of heimelijke zoeking naar opgeslagen data op afstand (hierna: de virtuele zoeking op afstand) is de locatie van opsporingsinstanties. In deze visie is de plaats waar de opsporingsambtenaar data oproept eveneens de plaats waar de virtuele zoeking plaatsvindt. Enkel wanneer er nood is aan fysieke overschrijding van grenzen, zoals bij een huiszoeking, dringen internationale regels tot samenwerking zich op. Deze visie lijkt ons echter te verregaand. Via het Internet is immers een zeer grote hoeveelheid informatie, al dan niet openlijk, rechtstreeks beschikbaar in België. Die informatie

[459] Zie eveneens: J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 329 en 373-375.

zal vaak betrekking hebben op buitenlandse aangelegenheden, personen en zaken. De locatie van opsporingsinstanties als criterium zou dan ook een duidelijke aantasting van de soevereiniteit van andere staten met zich meebrengen. Personen en gebeurtenissen op hun territorium zouden immers kunnen worden onttrokken aan hun externe rechtsbescherming, enkel en alleen omwille van een aanwezigheid in het virtuele landschap. Bovendien tast deze visie de rechtszekerheid van rechtsonderhorigen aan. Die hebben in dat geval geen enkel zicht op wanneer informatie over hen, bereikbaar vanop afstand, ondanks afscherming kan worden bekeken en gecontroleerd door buitenlandse overheden. Opsporingsinstanties die naar nationaal recht over een hackingsbevoegdheid beschikken zouden die bevoegdheid bijvoorbeeld geheel eenzijdig kunnen aanwenden om toegang te nemen tot een beveiligde Dropbox-account van een rechtsonderhorige in het buitenland. De computers van de overheid zonder meer vergelijken met virtuele ramen die het mogelijk maken vanop het eigen grondgebied op te sporen in het buitenland (te kijken in de tuin van de buren, bij wijze van spreken) is o.i. een brug te ver.

LOCATIE ONDERZOCHTE PERSOON – We zouden de virtuele zoeking op afstand eveneens kunnen kwalificeren als een onderzoeksdaad ten aanzien van een persoon, net zoals dat het geval is bij de telefoon- en informaticatap. Het zoeken naar bestaand digitaal bewijs kan vergeleken worden met een zoeking naar (een aspect van) *iemands* virtueel verleden. De nadruk komt dan meer te liggen bij de persoon die wordt onderzocht dan bij de gegevens die worden gezocht. Er is in dat geval geen sprake van extraterritoriale opsporing als de onderzochte persoon zich op het nationale territorium bevindt. De legale virtuele beweegruimte van de betrokkene (dit zijn alle digitale gegevens waar de betrokkene vanop afstand toegang toe heeft, zoals online profielen op allerhande websites, met uitzondering van de door de betrokkene gehackte profielen, geeft zo mee vorm aan de bevoegdheidssfeer van de staat op wiens territorium de betrokkene zich bevindt. Het simpelweg doortrekken van de lokalisatiemethode die we al tegenkwamen bij opsporing in real time is ook hier echter te ongenuanceerd. Opsporing in real time zegt iets over het doen en laten van de onderzochte persoon op het moment dat het onderzoek wordt gevoerd. Door die onderzoekshandelingen te lokaliseren op de plaats waar de onderzochte persoon zich bevindt, worden staten in de mogelijkheid gesteld om de communicatie en handelingen op hun territorium gevoerd of gesteld, in *real time* te controleren. De locatie van de onderzochte persoon als criterium hanteren voor het lokaliseren van de virtuele zoeking op afstand zou daarentegen het volgen-

de betekenen: het betreden van een territorium voor een vakantie, zakenreis of doorreis zou een virtueel verleden, opgeslagen via allerhande online accounts, onder puur nationale regelgeving zichtbaar maken voor de plaatselijke overheid. Een persoon zou in deze visie dus noodzakelijkerwijze zijn digitaal hebben en houden, voor zover dat vanop een afstand toegankelijk is, steeds mee de grens overnemen wanneer hij die zelf oversteekt. Een virtueel verleden thuislaten is dan geen optie meer. Dit zou o.i. een ernstige aantasting inhouden van de vrijheid van personen en zelfbeschikking van onderdanen om zaken niet aan het rechtstreeks gezag van een buitenlandse overheid te onderwerpen (*supra*, 6.2). Gelet op de territoriale begrenzing van de soevereiniteit begeeft een individu zich onder de rechtsmacht van een buitenlandse overheid telkens wanneer hij de grens oversteekt. Zijn doen en laten komt onder de controlebevoegdheid van de buitenlandse overheid, net zoals de zaken die hij met zich meeneemt. Wil de persoon zaken, die een bewijs van communicatie of handelingen uit het verleden kunnen inhouden (zoals brieven, documenten, foto's, een laptop of een smartphone), niet aan die soevereine bevoegdheid onderwerpen, dan dient hij ze niet mee de grens over te nemen en laat hij ze beter thuis. Personen die keuze aan ontnemen, louter omwille van de virtuele bereikbaarheid van gegevens, is ongenuanceerd en o.i. niet wenselijk.

GEWOONLIJKE VERBLIJFPLAATS – Ook de gewoonlijke verblijfplaats van het onderzochte subject is een mogelijk criterium ter invulling van het territorialiteitsbeginsel. Dit uitgangspunt lokaliseert de virtuele leefwereld van een persoon op zijn gewoonlijke verblijfplaats. Het verenigt als het ware het zwaartepunt van iemands virtuele leven met dat van zijn fysieke leven. Wanneer opsporingsinstanties bijvoorbeeld toegang wensen te nemen tot de Dropbox-account van een verdachte zouden er geen internationaalrechtelijke problemen meer rijzen, indien de gewoonlijke verblijfplaats van de verdachte is gesitueerd op het nationale territorium. Een verplaatsing van de gewoonlijke verblijfplaats houdt eveneens een verhuis van de virtuele leefwereld in. Bij een occasionele fysieke overschrijding van grenzen wordt de persoon geacht zijn virtuele verleden thuis te laten. De buitenlandse overheid kan wel unilateraal toegang nemen tot het virtuele heden van de betrokkene, gelet op de lokaliseringsmethode bij opsporing in real time (*supra*, 6.3.2, bv. observeren welke data de betrokkene tijdens zijn verblijf consulteert), en tot de data die de betrokkene effectief de grens mee overneemt (bv. data opgeslagen op de smartphone die de betrokkene op zak heeft). Toegang tot het virtueel verleden, los van een gelijklopend gebruik van de data door de onderzochte persoon, zoals een online door-

zoeking van een Hotmail- of Dropbox-account of een Google-agenda, kan daarentegen enkel via samenwerking met het land waar de onderzochte persoon zijn gewoonlijke verblijfplaats heeft. Net zoals in het fiscaal recht kan worden gewerkt met vermoedens.[460] De gewoonlijke verblijfplaats is dan vermoedelijk de plaats waar de betrokkene is ingeschreven in het rijksregister. Dat vermoeden is echter weerlegbaar.

LOCATIE GECONSULTEERDE DIENSTENAANBIEDER – Tot slot zou ook de locatie van de dienstenaanbieder via wiens diensten de gezochte gegevens worden opgeslagen de opsporingshandeling kunnen lokaliseren. Een onderzoek naar gegevens op Facebook zou in dat geval bijvoorbeeld plaatsvinden in de Verenigde Staten, onafhankelijk van waar Facebook de gezochte gegevens heeft opgeslagen of aan wie die gegevens in feite toekomen. Dit zou in ieder geval praktischer zijn dan het huidige criterium aangezien de opsporing niet langer wordt verhinderd door *loss of object-location*. Ook dit criterium nemen we bijgevolg mee in de confrontatie om uit te maken welk hoofdcriterium in acht moet worden genomen ter bepaling van de territoriale bevoegdheid.

CRITERIUM OBJECT/DIENST: SCHENDING EXTERNE SOEVEREINITEIT VERBLIJF-STAAT?[461] – Tijdens de voorbereidende werken van het Cybercrime-verdrag bleek dat het onduidelijk was of een rechtstreekse zoeking naar in het buitenland opgeslagen data, een schending van de soevereiniteit van de staat van opslag vormt (*supra*). Of een meer subject-georiënteerde bevoegdheid dus de soevereiniteit van de staat van opslag (object-staat) wel schendt, is dus een legitieme, vooralsnog onbeantwoorde vraag.[462] De om-

460 Zie art. 2§1, 1° Wetboek van inkomstenbelastingen, *BS* 30 juli 1992.

461 Ter opfrissing: de staatssoevereiniteit in haar externe dimensie heeft betrekking op haar (horizontale) werking tussen staten onderling. De staten dienen elkaars soevereiniteit te erkennen (externe erkenning). Dit maakt een vreedzame co-existentie van soeverein gelijke staten mogelijk. De externe soevereiniteit van een staat houdt een recht op uitsluiting van andere staten van het eigen territorium in, waardoor de staat in de mogelijkheid wordt gesteld om eigen onderdanen te beschermen tegen ongeoorloofde buitenlandse overheidsinmengingen (externe bescherming) (*supra*, 6.2).

462 Zie hierover J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 379: '*The location independence betweteen the data and the government agent accessing the data in State B without any readily apparent violation of State B's territorial integrity. From the perspective of State B, however, this is arguably a violation of sovereignty since State A is determining when, and according to what procedures and substantive standards, data located in State B can be seized. Such unilateral seizure of data ignores longstanding efforts of nations – including the United States – to establish sovereign control and regulation over data within one's own territory.*'

gekeerde vraag duikt daarentegen niet op in de voorbereidende werken, hoewel zij zeker even belangrijk is: vormt de huidige object-georiënteerde benadering geen schending van de soevereiniteit van de staat waar de onderzochte persoon zich gewoonlijk bevindt (verblijf-staat)? In de object-georiënteerde benadering trekken de staten met de grootste opslagcapaciteit als het ware de soevereine bevoegdheid over en het recht op uitsluiting van zeggenschap van andere staten m.b.t. gegevens van personen, verspreid over de hele wereld, naar zich toe. Die gegevens vormen echter vaak een soort veruitwendiging van activiteiten gesteld op het territorium van een andere staat. Waar een virtueel leven effectief wordt geleid, is dan irrelevant. Hetzelfde geldt wanneer de bevoegdheid dient te worden gelokaliseerd in de staat van de dienstenaanbieder. De staat van waaruit personen hun virtuele handelingen gewoonlijk stellen of hun virtuele communicatie gewoonlijk voeren (d.i. de verblijf-staat) beschikt, buiten real time opsporing, over geen enkele bevoegdheid om die handelingen en communicatie autonoom te controleren. Nochtans verwachten we wel dat een staat de verantwoordelijkheid neemt voor wat er op zijn territorium gebeurt (*supra*, 6.2). In de huidige visie heeft de staat echter geen autonome toegangsbevoegdheid tot de data, terwijl die wel consulteerbaar en bruikbaar zijn voor de betrokken persoon op zijn territorium. Om controle mogelijk te maken zou de staat van gewoonlijk verblijf steeds moeten samenwerken met de staat waar de gegevens staan opgeslagen respectievelijk de staat vanwaar de dienst wordt aangeboden. Een schending van de soevereiniteit van de verblijf-staat in een object- of dienstengeoriënteerde benadering lijkt ons bijgevolg meer voor de hand liggend dan een schending van de soevereiniteit van de object-staat in een subject-georiënteerde benadering. De plaats waar de gegevens staan opgeslagen is bovendien zeker niet altijd gelijk aan de locatie van de geconsulteerde dienstenaanbieder. In dat geval kent de object-georiënteerde benadering de soevereine bevoegdheid over de gegevens toe aan een staat die nauwelijks nog een link vertoont met de onderzochte activiteit of persoon. Het juridisch kader vervreemdt op die manier volledig van de realiteit die het beoogt te regelen. Wanneer bijvoorbeeld een Belgische onderzoeksrechter tijdens een huiszoeking een kijkje wenst te nemen in de Google-agenda van de bewoner dan zou hij daarvoor moeten samenwerken met de staat op wiens territorium de agendagegevens worden opgeslagen. Hoewel Google Inc. een Amerikaans bedrijf is, slaat het zijn gegevens niet noodzakelijk op in de Verenigde Staten. Google Inc. beschikt immers over verschillende datacenters in Noord- en Zuid-Amerika, Azië

en Europa.[463] Zij vormen als het ware de '*Google-cloud*'. Enkel indien de gezochte gegevens toevallig staan opgeslagen in het Belgische data-center zou de onderzoeksrechter onder nationale regelgeving toegang kunnen nemen. Zo niet dient hij medewerking te bekomen van de staat van opslag. Daarvoor dient hij echter eerst de plaats van opslag te kennen, wat zeker geen eenvoudige opdracht is.

OBJECT-CRITERIUM CYBERCRIME-VERDRAG: RECHT UITSLUITING? – Aangezien de verdragsluitende staten meenden dat een unilaterale zoeking naar data opgeslagen in het buitenland mogelijks de soevereiniteit van de staat van opslag schendt, hanteert het Cybercrime-verdrag een object-georiënteerd uitgangspunt. Art. 32 Cybercrime-verdrag voorziet daarbij dus in twee mogelijkheden tot rechtstreekse grensoverschrijdende zoekingen. Staten bereikten blijkbaar voldoende eensgezindheid over de mogelijkheid tot rechtstreekse grensoverschrijdende zoeking met toestemming van de persoon met controle over de gezochte data (art. 32, b Cybercrime-verdrag).[464] Het gaat hier bijvoorbeeld om de toestemming van een persoon aan opsporingsinstanties om toegang te nemen tot zijn e-mailgegevens of andere gegevens die hij over de grenzen heen heeft opgeslagen. Volgens sommigen (*supra*, 2.3.2) kan ook de ISP kan die toestemming verlenen indien de contractvoorwaarden dit bepalen.[465] Toestemming van de staat van opslag is dan niet langer nodig. Bepaalde private (rechts)personen kunnen vandaag dus mee vorm geven aan de eventuele soevereiniteitsaanspraken van de staat van opslag. Dit is eigenaardig nu nationale soevereiniteit niet enkel een zekere bescherming aan individuen garandeert, maar ook raakt aan de belangen van de staat.[466] Op basis van een criterium van controle of individuele beschikkingsmacht over de gegevens, krijgt een individu hier dus de mogelijkheid om het uitsluitingsrecht[467] van de staat van

---

463 http://www.google.com/about/datacenters/inside/locations/index.html.

464 Zie CYBERCRIME CONVENTION COMMITTEE, 'Guidance Note # 3, Transborder access to data (article 32)', 2013, www.coe.int/TCY.

465 De Guidance Note bij art. 32 getuigt nochtans van enige terughoudendheid voor wat betreft de mogelijkhied van de dienstenaanbieder. CYBERCRIME CONVENTION COMMITTEE, *ibid*.: *'Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent*.' Zie eveneens: B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 54.

466 M. GERCKE, *Understanding cybercrime: Phenomena, challenges and legal response*, Genève, International Telecommunication Union (ITU), 2012, 277-278.

467 D.i. het recht om andere staten van het eigen territorium uit te sluiten.

opslag opzij te schuiven. De toestemming van de bezitter van een e-mailaccount tot toegang tot dat account door de plaatselijke opsporingsinstanties zet zo bijvoorbeeld de (mogelijke) belangen van de staat op wiens territorium de e-mails staan opgeslagen, buiten spel. Dit wijst er o.i. op dat de verdragsluitende staten niet zozeer staan op een recht op uitsluiting van de subject-staat of de staat van de dienstenaanbieder door de object-staat. Vermeldenswaardig is dat art. 32, b Cybercrime-verdrag één van de belangrijkste redenen vormt waarom Rusland niet toetreedt tot het verdrag. Ook Slovakije vindt de toestemming van een private partij onvoldoende als grondslag voor een zoeking naar data het in buitenland.[468]

SUBJECT CRITERIUM: SCHENDING SOEVEREINITEIT STAAT OPSLAG – In een *uitsluitend* subject-georiënteerde benadering zou de staat waar het subject zijn gewoonlijke verblijfplaats heeft, de staat van het object (d.i. de staat van opslag) kunnen uitsluiten. De staat van opslag kan een beperking van zijn bevoegdheid ten aanzien van data die op zijn territorium zijn opgeslagen als een inbreuk op zijn soevereiniteit ervaren. Die staat beschikt dan immers niet langer over autonome bevoegdheden met betrekking tot alle zaken die zich op zijn territorium bevinden.

OBJECT/DIENST CRITERIUM: CRIMINELE FORUMSHOPPING – In de huidige object-georiënteerde benadering kunnen overheden slechts via trage internationale wegen data bekomen die opgeslagen staan in het buitenland. Criminelen kunnen daar gemakkelijk misbruik van maken door clouddiensten slim te gebruiken of door hun gegevens op te slaan in landen die bekend staan om hun moeizame internationale samenwerking of de plaats van opslag geregeld te wijzigen.[469] Ook kunnen zij de op hun toepasselijke wet in zekere mate omzeilen door illegale inhouden op te slaan op servers in het buitenland waar diezelfde inhouden niet verboden zijn. Te denken valt aan pseudo-kinderpornografie (in Nederland 'virtuele kinderpornografie' genoemd), waarbij geen echte kinderen worden gebruikt en die vandaag niet overal op dezelfde wijze is strafbaar gesteld.[470] Doordat dubbele straf-

---

468 B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 57.

469 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 390; KOOPS en GOODWIN, *ibid*., 26-27; G. VACIAGO, 'Remote forensics and cloud computing: an Italian and European legal overview', *Digital Evidence and Electronic Signature Law Review,* 2011, vol. 8, 124.

470 In de Verenigde Staten wordt zo enkel virtuele kinderpornografie strafbaar gesteld in de mate dat zij niet van echte kinderpornografie te onderscheiden valt. Zie Prosecuto-

baarstelling bepalend kan zijn voor de bereidheid van staten om rechtshulp te bieden, kan de misdadiger op die manier de opsporing lam leggen.[471] Zo doet de object-georiënteerde benadering o.i. afbreuk aan de interne werking van staatssoevereiniteit.[472] Door zich op het territorium van een staat te begeven onderwerpt men zichzelf aan het gezag van die staat. De zaken die men op dat territorium in zijn bezit heeft en de handelingen die men er stelt vallen evenzeer onder dat gezag. Door data in het buitenland op te slaan, onttrekt men die data aan het gezag van de eigen overheid. Voor de betrokkene blijven die data in principe echter wel perfect toegankelijk op om het even welk moment en vanop eender welke plaats. Het volle genot blijft, maar individuen worden in de gelegenheid gesteld om zelf te beslissen of ze bepaalde zaken al dan niet wensen te onttrekken aan de staatssoevereiniteit van de plaatselijke overheid. Dit doet afbreuk aan de interne erkenning van de soevereiniteit die één van de voornaamste bestaansvoorwaarden daarvan vormt. De territoriale bevoegdheid uitsluitend toekennen aan de staat van waar de door het subject geconsulteerde dienst wordt aangeboden zou een gelijkaardig probleem met zich meebrengen.

SUBJECT CRITERIUM: HERSTEL INTERNE ERKENNING – Het Internet mag niet ontaarden in een medium waarmee een persoon op zoek kan gaan naar

---

rial Remedies and Other Tools to end the Exploitation of Child Pornography Today Act (PROTECT Act), *Pub. L.* No. 108-21, 117 Stat. 650 (2003); M.J. HENZEY, 'Going on the offensive: a comprehensive overview of internet child pornography distribution and aggressive legal action', *Appalachian Journal of Law* 2011-12, vol. 11, afl.1, 23-24. Een verregaandere bestraffing van virtuele kinderpornografie werd er in het verleden reeds als ongrondwettig bestempeld. Zie *Ashcroft v. Free Speech Coalition,* 535 U.S. 234 (2002). Art. 383bis van het Belgische Strafwetboek stelt pseudo-kinderpornografie daarentegen in meer algemene bewoordingen strafbaar: '*[…] zinnebeelden, voorwerpen, films, foto's, dia's of andere beelddragers die houdingen of seksuele handelingen met pornografisch karakter voorstellen waarbij minderjarigen betrokken zijn of worden voorgesteld […]*'. Ook het louter toegang nemen tot de kinderpornografie, zonder het te bezitten, is strafbaar overeenkomstig art. 383bis §2 Sw.

471 Zo bepaalt art. 5 Europees verdrag van 20 april 1959 aangaande de wederzijdse rechtshulp in strafzaken: '*Any Contracting Party may […] reserve the right to make the exeaution of letters rogatory for search or seizure of property dependent on one or more of the following conditions: (a) that the offence motivating the letters rogatory is punishable under both the law of the requesting Party and the law of the requested Party*'; zie eveneens art. 14 Kaderbesluit van 18 december 2008 van de Raad betreffende het Europees bewijsverkrijgingsbevel.

472 Zie eveneens: P. DE HERT, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty Is at Stake?' in KOOPS en BRENNER (eds), *Cybercrime and Jurisdiction. A Global Survey,* Den Haag, T.M.C. Asser Press, 2006, 109.

de door hem gewenste bescherming om vervolgens daar zijn gegevens op te slaan. De subject-georiënteerde benadering zou het evenwicht tussen individu en overheid op dit vlak kunnen herstellen. De focus op de gewoonlijke verblijfplaats zorgt ervoor dat de voornaamste controlebevoegdheid over het virtuele en fysieke leven bij dezelfde overheid komt te liggen. Individuen kunnen niet langer aan het plaatselijke recht ontsnappen door gegevens in het buitenland op te slaan terwijl die voor de betrokkene perfect raadpleegbaar blijven. Enkel zo wordt de noodzakelijk interne erkenning van de soevereiniteit van de betrokken staat hersteld en kan de overheid de aan haar toevertrouwde taak tot controle en bescherming op een efficiënte wijze vervullen.

RESULTAAT: VOORKEUR STAAT VERBLIJF – Uit voorgaande vergelijking blijkt dat, voor de virtuele zoeking op afstand, de staat waar het onderzochte subject zijn gewoonlijke verblijfplaats heeft een autonome opsporingsbevoegdheid hoort te krijgen. De autonome opsporingsbevoegdheid heeft dan betrekking op de legale virtuele beweegruimte van het onderzochte subject. Het lijkt ons onwenselijk die bevoegdheid afhankelijk te stellen van de wil van de staat van opslag of de staat van de dienstenaanbieder. Net zoals bij de virtuele opsporing in real time, verdient de focus op het subject o.i. dus de voorkeur, met dien verstande dat de locatie van het subject zelf hier niet doorslaggevend is, maar wel de locatie van diens gebruikelijke verblijfplaats. In een subject-georiënteerde benadering krijgen rechtssubjecten bovendien de bescherming die ze mogen verwachten.[473] Onafhankelijk van waar de data zich bevinden, geniet een persoon met betrekking tot bestaande data immers een bescherming van zijn mensenrechten op grond van de wetgeving van het land waar hij zijn gewoonlijke verblijfplaats heeft en dus zijn data over het algemeen gewoonlijk consulteert. Zo kadert ieder virtueel handelen binnen een coherent en voor de betrokkene kenbaar regime van bescherming van de privacy en andere mensenrechten. Ook de rechtszekerheid is zodoende gediend met een subject-georiënteerde benadering waarbij de focus ligt op de gewoonlijke verblijfplaats van het subject.

473 Zie over de vraag naar een verschuiving van de focus van de plaats van opslag van de data naar de plaats van inmenging op fundamentele rechten en vrijheden eveneens: F. CAJANI, *Technologies and Business vs Law – Cloud computing transborder access and data retention*, 2012, 16-17, www.coe.int.

6.3.4. Virtuele opsporingen: aanvulling bij hoofdcriterium?

OVERIGE STATEN MET GEFUNDEERDE LINK – De locaties van het subject en diens gewoonlijke verblijfplaats moeten dus als hoofdcriteria gelden voor de lokalisering van virtuele opsporingshandelingen. Rest nog de vraag of we de bevoegdheid van de subject-staat respectievelijk verblijf-staat verder moeten aanvullen met een territoriale bevoegdheid voor andere staten. Net zoals bij de klassieke telefoontap is het denkbaar dat meerdere staten soevereine bevoegdheden kunnen laten gelden m.b.t. dezelfde virtuele communicatie of handeling. Aangezien virtuele handelingen meer linken vertonen met het fysieke territorium dan de vluchtige klassieke telefoonconversaties, moeten we nagaan of die bijkomende aanknopingspunten bevoegdheden in hoofde van de betrokken staten opleveren. In een volledig subject-georiënteerde benadering (met de focus op het onderzochte subject dan wel zijn verblijfplaats) komt geen autonome opsporingsbevoegdheid toe aan de staat van de door het subject geconsulteerde dienstenaanbieder (hierna: dienstenstaat), via wiens diensten de te onderzoeken gegevens bijvoorbeeld zijn verzonden of ontvangen (bv. Facebook, Yahoo!, Microsoft (Hotmail, Skype)). Die buitenlandse dienstenaanbieder beschikt echter over een heel aantal gegevens, zoals verkeersgegevens en identificatiegegevens. De staat waar de dienstenaanbieder zich bevindt, vertoont in tegenstelling tot andere staten geen willekeurige, technische link, maar een gefundeerde link met deze data. Die gefundeerde link kan een territoriale bevoegdheid in hoofde van de dienstenstaat verantwoorden. Hetzelfde geldt voor de staat waar het subject of de door het subject geconsulteerde dienstenaanbieder gegevens opslaat.

DIENSTENSTAAT: SOEVEREINITEIT – De dienstenstaat de bevoegdheid ontzeggen om autonoom de met die dienst verbonden gegevens op te sporen, zou diens soevereiniteit o.i. kunnen schenden. Indien de gezochte gegevens toegankelijk zijn voor de dienstenaanbieder en verbonden zijn met zijn dienst, die door het subject wordt geconsulteerd, vertoont de dienstenstaat een gefundeerde link met de gezochte gegevens en kan zijn soevereiniteitsaanspraak niet zomaar van tafel worden geveegd. Data die passeren over de kanalen van een dienstenaanbieder vertonen daarom nog geen gefundeerde link met de dienstenstaat. Er moeten o.i. dan ook ernstige aanwijzingen voorhanden zijn dat de dienst door het onderzochte subject werd geconsulteerd en dat de gezochte gegevens daar betrekking op hebben.

DIENSTENSTAAT: RECHTSBESCHERMING EN RECHTSZEKERHEID – Doordat een rechtsonderhorige bewust gebruik maakt van diensten aangeboden door een buitenlandse dienstaanbieder kan hij ook verwachten dat zijn gegevens onder het aldaar toepasselijke recht opspoorbaar zijn. Door gebruik te maken van een vanuit het buitenland aangeboden dienst overschrijdt de rechtsonderhorige, weliswaar op een virtuele wijze, zelf de grenzen van het territorium waar hij zich fysiek bevindt. Het onderzochte subject bevindt zich niet enkel fysiek in één staat, maar begeeft zich virtueel op het territorium van een andere staat van waaruit hij diensten consulteert. De rechtsonderhorige dient de gevolgen van zo een grensoverschrijding te aanvaarden. Hij onderwerpt zijn gegevens zelf aan de soevereine bevoegdheid van de staat (bv. de Verenigde Staten) van waaruit de dienst (bv. Facebook) wordt aangeboden. Rechtszekerheid staat aan deze autonome opsporingsbevoegdheid bijgevolg niet in de weg. We stellen daarom voor de subject-georiënteerde benadering aan te vullen met een bevoegdheid op basis van de plaats van waaruit de door het onderzochte subject geconsulteerde dienst wordt aangeboden. De concrete criteria ter bepaling van die plaats moeten blijk geven van de focus op het subject. Op wiens virtuele territorium kan het subject worden geacht zich te begeven? Dit moet in ieder geval een voor het subject kenbare plaats zijn. De door het subject geconsulteerde dienstenaanbieder kan voor de uitoefening van zijn diensten beroep doen op andere dienstenaanbieders, die zich in het buitenland kunnen bevinden.[474] Het subject kan o.i. daarbij niet worden geacht zich te begeven op het territorium van de (derde) staat van waaruit die laatste dienstenaanbieders hun dienst verstrekken. Het is dan immers niet het subject dat de grenzen virtueel overschrijdt, maar de door het subject geconsulteerde dienstenaanbieder.[475] Het is evenwel van belang dat de logica van de virtuele aanwezigheid op territorium van een staat ook wordt doorgetrokken naar de grondwettelijke bescherming. Wanneer de grondwettelijke bescherming in een staat een zekere link tussen de betrokken onderdaan en de staat vereist, moet ook de legale virtuele aanwezigheid van een persoon op het territorium van die staat als een voldoende band worden beschouwd om de grondwettelijke bescherming te activeren. Dus als de EU het be-

474 Zie bv. B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 23.

475 Vandaag geniet het subject op dit niveau een bijkomende bescherming doordat de Europese dataprotectieregelgeving in een beperking voorziet van de mogelijkheid voor dienstenaanbieders om gegevens naar derde landen, buiten de Europese Unie, door te geven, afhankelijk van het niveau van bescherming dat daar geldt. Zie art. 25 en 26 richtlijn 95/46/EG; art. 45-50 algemene verordening gegevensbescherming.

langrijk vindt om de gegevens van Europese burgers en bedrijven onder de bescherming van het EU-recht (bv. gegevens- of consumentenbescherming) te laten vallen, dan moet het nadenken wanneer het dienstverleners wil verplichten een op het grondgebied van een EU-lidstaat gevestigde tak te scheppen om diensten te mogen aanbieden op de hele Europese markt. Die vestigingsplicht kan de plicht om data in EU-lidstaten op te slaan, dan vervangen. De Europese mensenrechtenbescherming blijft verzekerd[476] en snelle samenwerking binnen de EU is mogelijk.

SOEVEREINITEIT OPSLAGSTAAT – We zagen reeds dat het gebrek aan een autonome bevoegdheid in hoofde van de staat van opslag een schending kan uitmaken van diens soevereiniteit. Ook hier benaderen we de problematiek verder vanuit de rechtsbescherming en rechtszekerheid. Een onderscheid dringt zich hier op. Het antwoord op de vraag naar een aanvullende bevoegdheid hangt o.i. immers af van wie beslist de onderzochte gegevens over de grenzen heen op te slaan.

OPSLAG DOOR DIENSTENAANBIEDER – Stel dat een Amerikaanse dienstenaanbieder de gegevens van een Europees subject opslaat in Argentinië. De staat waar een dienstenaanbieder gegevens van een subject opslaat (Argentinië), zou geen autonome bevoegdheid aan die opslag mogen ontlenen t.a.v. de gegevens van dat Europese subject. In die situatie loopt het immers mank op het niveau van de interne erkenning van de territoriale begrenzing van de soevereiniteit. Een persoon dient te erkennen dat de soevereiniteit van zijn eigen staat begrensd is en dat er andere soevereine staten zijn die eveneens over autonome bevoegdheden beschikken om hun ordenende en beschermende taak binnen hun territorium te kunnen vervullen. De rechtsonderhorige dient bijgevolg te erkennen dat wanneer hij beslist de grenzen van zijn eigen staat te overschrijden, hij daarmee de soevereiniteit aanvaardt van de staat op wiens territorium hij beslist te vertoeven. De beslissing tot het overschrijden van grenzen en tot het zich onderwerpen aan een buitenlandse soevereine instantie dient evenwel op de eerste plaats in zijn eigen handen te

476 De nieuwe algemene verordening gegevensbescherming verzekert de toepassing van het Europese dataprotectierecht voor verwerkingen van gegevens van betrokkenen in de Unie voor zover die verwerkingen vallen onder het materiële toepassingsgebied van de algemene verordening. Zo moeten dienstenaanbieders uit derde landen de bepalingen van de verordening naleven wanneer ze gegevens verwerken in het kader van hun dienstverlening in de Europese Unie, voor zover die activiteiten niet buiten de werkingssfeer van het Unierecht vallen. Zie art. 3, 2 a) algemene verordening gegevensbescherming.

liggen. Dat is in een Internetcontext echter doorgaans niet het geval. Doorgaans bepalen de dienstenaanbieders waar de data van hun gebruikers worden opgeslagen en blijven de gebruikers zelf onwetend over de plaats van opslag.[477] De dienstenaanbieders zullen hun keuze van de plaats van opslag vaak maken op grond van economische overwegingen. Indien de plaats van opslag bepalend is voor rechtsmacht dan gaat het transparant karakter van de indeling van rechtsmacht volledig verloren en wordt iedere rechtszekerheid in een virtuele omgeving onderuit gehaald. Indien een rechtsonderhorige er bijvoorbeeld voor kiest enkel nationale dienstenaanbieders (bv. Telenet, Proximus of Twoo voor een Belgische rechtsonderhorige) te consulteren om zich op die manier niet onder de soevereine bevoegdheid van een buitenlandse staat te onderwerpen, dan zou de dienstenaanbieder aan die keuze afbreuk kunnen doen door de gegevens over de grenzen heen op te slaan. Bovendien wordt de mate van mensenrechtenbescherming dan volledig afhankelijk gesteld van keuze van de plaats van opslag door de dienstenaanbieder. Cloud computing zou deze problematiek alleen maar vergroten doordat daarbij gegevens op verschillende plaatsen worden opgeslagen en constant worden verplaatst. In deze context is voor de bepaling van procedurele rechtsmacht het criterium van de locatie van de gegevens o.i. te arbitrair. In het licht van de rechtszekerheid en de mensenrechtenbescherming dient de bevoegdheid van de staat van opslag in dit geval afhankelijk te worden gesteld van de medewerking van de subject-staat/de staat van gewoonlijk verblijf (afhankelijk van het type onderzoek) of de staat van waaruit de door het subject geconsulteerde dienst wordt aangeboden.

OPSLAG DOOR ONDERZOCHTE SUBJECT – De dienstenaanbieder zelf plaatst zich daarentegen wel onder de bevoegdheid van de staat waar hij zijn gegevens opslaat. Met betrekking tot die opslag, dient die dienstenaanbieder zich dan ook aan de aldaar geldende regels te onderwerpen. De staat van opslag beschikt zo wel over een autonome opsporingsbevoegdheid ten aanzien van de gegevens op zijn territorium die betrekking hebben op de dienstenaanbieder zelf. We kunnen die redenering verder doortrekken: telkens wanneer een rechtssubject zijn gegevens zelf gericht, bewust over de grenzen heen opslaat op een specifieke server, dan brengt dit een bevoegdheid van de staat van opslag met zich mee. Dit is bijvoorbeeld het geval wanneer een persoon die in België zijn gewoonlijke verblijfplaats heeft, maar werkt in Nederland, zijn gegevens opslaat op servers op zijn kantoor. Zowel België als Nederland hebben in dit voorbeeld een autono-

477 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 373.

me opsporingsbevoegdheid ten aanzien van de gegevens, opgeslagen in Nederland. België is bevoegd tot een virtuele zoeking vanop afstand op grond van het hoofdcriterium (gewoonlijke verblijfplaats) en Nederland op grond van het bijkomende criterium (de plaats van opslag door het subject). De focus ligt in alle gevallen op het onderzochte subject en de vraag of hij virtueel grenzen overschrijdt en zich daardoor virtueel op het territorium van een buitenlandse staat begeeft en zich zonder de bevoegdheid van die buitenlandse staat plaatst. Die benadering verzekert dat de autonoom onderzoekende staat steeds een gefundeerde link vertoont met het onderzochte subject op wie de gegevens betrekking hebben of aan wie zij in feite toebehoren. Ook hier is het van belang dat de logica van de virtuele aanwezigheid op een bepaald territorium eveneens speelt bij de bepaling van de toepasselijke grondwettelijke bescherming.

NOOD INTERNATIONALE OVEREENKOMST – Deze benadering is evenwel een ideaalbeeld. In de praktijk zal het moeilijk, zo niet onmogelijk blijken om staten te verbieden in het kader van een strafrechtelijk onderzoek toegang te nemen tot gegevens op hun eigen territorium die in feite toebehoren aan een rechtssubject waar ze geen gefundeerde link mee vertonen. Dit geldt bovendien t.a.v. iedere staat voor wie de gegevens technisch bereikbaar zijn vanop diens territorium.[478] Enkel via internationale afspraken kunnen landen elkaar effectief tot op zekere hoogte beperken in de mogelijkheid van toegang tot gegevens die op het eigen territorium kunnen worden gelokaliseerd.[479] Zolang dat niet gebeurt, kunnen staten pogen zo veel mogelijk in een bescherming te voorzien door eigen dienstenaanbieders te beperken in hun mogelijkheid om gegevens over de grenzen heen op te slaan. Zo een benadering vinden we vandaag terug in de EU-wetgeving inzake gegevensbescherming.[480] In het kader van de doorgifte van persoonsgegevens naar derde landen schrijft die wetgeving een getrapt systeem voor afhankelijk van het door het derde land geboden beschermingsniveau t.a.v. de persoonlijke levenssfeer en de fundamentele vrijheden en rechten

478 Staten kunnen wel aangeven dat zij zich in hun soevereiniteit geschonden voelen wanneer andere staten gegevens opsporen waarmee zij enkel een louter technische band vertonen. Of dit enig resultaat oplevert valt evenwel te betwijfelen.

479 Vgl. Art. 20 EU-overeenkomst betreffende de wederzijdse rechtshulp in strafzaken.

480 Zie art. 25 en 26 richtlijn 95/46/EG; art. 45-50 algemene verordening gegevensbescherming; Vgl. Art. 36–40 richtlijn gegevensverwerking politie en justitie. Vgl. Russische wetgeving: http://www.ibls.com/internet_law_news_ portal_view .aspx?s = latestnews&id=2609.

van personen. Bij een gebrek aan een passend beschermingsniveau[481] kan een doorgifte enkel onder strenge voorwaarden. De onvoorwaardelijke toestemming van de betrokkene op wie de persoonsgegevens betrekking hebben, kan de doorgifte dan mogelijk maken.[482] In geval van zo een toestemming kan in onze visie dan ook gesproken worden van een virtuele overschrijding van grenzen door die dienstengebruiker zelf. Een bijkomende mogelijkheid bestaat erin het binnenlandse dataverkeer af te schermen door de tussenkomst van buitenlandse Internet Exchange Points te beperken of uit te sluiten.[483] Willen we zo een verbrokkeling van het wereldwijde Internet tegengaan[484], dan dienen we dringend rond de internationale tafel te gaan zitten en overeenstemming te bereiken over hoe we de staatssoevereiniteit en het territorialiteitsbeginsel in hun oorspronkelijke (dubbele) functie kunnen herstellen.

6.3.5. Symbolische concretisering: cyberspace als virtueel territorium

VIRTUEEL TERRITORIUM – Uit voorgaande blijkt dat de focus op het subject en diens virtuele overschrijding van grenzen de voorkeur verdient, als we de territoriaal begrensde soevereiniteit en daarmee beoogde rechtsbescherming in stand houden. We stellen zo voor dat verschillende overheden kunnen beschikken over een autonome bevoegdheid tot het opsporen van dezelfde virtuele gegevens, ieder op grond van een gefundeerde link tussen het fysieke territorium van de staat en het onderzochte subject en zijn gegevens. Het territorialiteitsbeginsel blijft o.i. bijgevolg werkbaar. Een symbolische concretisering kan het voorstel verduidelijken. Het Internet *an sich,*

---

481. Over de vraag waar dat beschermingsniveau moet liggen, en in het bijzonder over de adequaatheid van het aan EU-eisen aangepaste Amerikaans systeem voor gegevens van EU-burgers en –bedrijven, bestaat er al jarenlang een politiek-juridisch dispuut in de EU. Zie bv. HvJ, C-362/14, *Maximilian Schrems/Data Protection Commissioner,* 2015; F. COUDERT, 'Schrems vs. Data Protection Commissioner: a Slap on the Wrist for the Commission and New Powers for Data Protection Authorities', *European Law Blog,* 15 oktober2015, www.europeanlawblog.eu; P. VALCKE, 'VS niet langer een veilige haven voor uw persoonsgegevens', *RW* 2015-16, afl. 14, 522.

482 Zie art. 26 richtlijn 95/46/EG; art. 49 algemene verordening gegevensbescherming.

483 Zie bv. http://tweakers.net/nieuws/92198/deutsche-telekom-wil-binnenlands-internetverkeer-gaan-afschermen.html.

484 Zie in dit verband 'The NSA and the risk to the internet. The US must give Assurances to stop Balkanisation of the web.', *The Financial Times Limites 2013,* http://www.ft.com/intl/cms/s/0/e1643694-4619-11e3-9487-00144feabdc0.html#axzz2kQ1Shqum.

als netwerk van netwerken[485], kunnen we zien als een *res communis,* zoals de open zee.[486] Iedereen mag het gebruiken gelet het algemeen belang dat ermee wordt gediend. Alles wat daar gebeurt draagt echter één of meerdere vlaggen.[487] Zo een vlag duidt op een voldoende gefundeerde link tussen de data en het fysieke territorium van een bepaalde staat. Alle data met de vlag van een bepaalde staat vormen samen het *virtuele territorium* van die staat. De metafoor van het *virtuele territorium* geeft duidelijk weer hoe we de soevereine bevoegdheid van een staat wensen af te bakenen in cyberspace. Hoewel deze woordkeuze op het eerste gezicht een *contradictio in terminis* lijkt op te leveren, kan het helpen bij de visualisering van de voorgestelde benadering. Het virtueel territorium vormt een uitbreiding op het fysieke territorium en is hier onlosmakelijk mee verbonden. Iedere staat heeft bijgevolg niet alleen soevereine bevoegdheden binnen zijn fysieke territorium, maar ook, weliswaar vaak gedeelde, soevereine bevoegdheden binnen zijn virtuele territorium. Opsporingshandelingen gesteld op het virtuele territorium van een staat vallen zo binnen diens territoriale bevoegdheidssfeer. Net zoals staten elkaars soevereiniteit dienen te erkennen m.b.t. het fysieke territorium, dienen zij dat ook te doen m.b.t. het virtuele territorium (externe erkenning). Het virtueel territorium is opgebouwd uit vijf elementen (vgl. vijf soorten virtuele vlaggen).

GEWOONLIJKE VERBLIJFPLAATS M.B.T. VIRTUEEL VERLEDEN – De veranderlijke grenzen van het virtuele territorium worden op de eerste plaats getekend door de toegangsbevoegdheid tot virtuele plaatsen van de personen met gewoonlijke verblijfplaats op het fysieke grondgebied. Hun volledig virtueel verleden behoort tot het virtuele territorium van de betrokken staat. Een illegale toegang (bv. hacking) kan evenwel de territoriale bevoegdheid van de betrokken staat niet uitbreiden aangezien de daders daardoor illegaal in de virtuele leefwereld van een ander persoon zijn binnengedrongen. Wanneer de overheid van het land van de hacker hiertoe toegang zou willen nemen, vereist dit toestemming van de overheid die de soevereine bevoegdheid heeft over het gehackte systeem. Dit geldt bijvoorbeeld ook voor het bekomen van verkeersgegevens, opgeslagen bij een dienstenaanbieder, waar-

485 G.L. HERRERA, 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space', 2005, kms2.isn.ethz.ch, 23.

486 M. HILDEBRANDT, 'Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace', *University of Toronto Law Journal*, 2013, afl. 63, 211.

487 Vgl. W.H. VON HEINEGG, 'Legal implications of Territorial Sovereignty in Cyberspace', in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 9.

toe het subject zelf geen toegang heeft. Een nationale bevoegdheid tot het hacken van het informaticasysteem van een buitenlandse dienstenaanbieder om zo toegang te verkrijgen tot die verkeersgegevens is o.i. uitgesloten.

LOCATIE SUBJECT M.B.T. VIRTUEEL HEDEN – Anderzijds krijgt het virtueel territorium mee vorm door de virtuele real-time activiteiten van personen die actief zijn op het reële grondgebied van de betrokken staat. Die activiteiten kunnen eveneens, onder voorwaarden vastgelegd in de nationale wetgeving, worden afgetapt of geobserveerd. Ook hier zijn enkel de gegevens die voor het getapte of geobserveerde subject zelf toegankelijk zijn, ook voor de tappende of observerende staat toegankelijk.

LOCATIE DIENSTENAANBIEDER – Een derde onderdeel van het virtueel territorium van een staat zijn de gegevens gelinkt met diensten die worden aangeboden vanuit het territorium van die staat. De staat kent niet alleen een opsporingsbevoegdheid ten aanzien van de dienstenaanbieders zelf op basis van het eerste onderdeel van het virtuele territorium ('*de gewoonlijke verblijfplaats*'). Ook kunnen de opsporingsinstanties van die staat onder het plaatselijke recht toegang nemen tot gegevens, verbonden aan het gebruik van die dienst door een onderzocht subject. Het is belangrijk dat de dienst effectief door het subject werd geconsulteerd en dat het niet gaat om data die om louter technische redenen passeren over de kanalen van de dienstenaanbieder. De dienstenaanbieder moet over een toegangsbevoegdheid tot de gezochte gegevens beschikken. Gegevens over een onderzocht subject, die enkel legitiem toegankelijk zijn voor de dienstenaanbieder, vallen enkel onder de soevereine bevoegdheid van de staat van waaruit de diensten worden aangeboden. De subject-staat of de staat van gewoonlijk verblijf heeft hier geen rechtstreekse toegang toe aangezien ook het subject geen toegang heeft tot die gegevens.

LOCATIE OPSLAG DOOR SUBJECT – Verder maken ook data, opgeslagen op het territorium van een staat, deel uit van diens virtuele territorium. Het gaat daarbij evenwel enkel over de gegevens die het onderzochte subject bewust op het territorium van de staat opslaat. Enkel in dat geval begeeft het subject zich op het virtuele territorium van de betrokken staat. Indien de gegevens daarentegen werden opgeslagen door een door het subject geconsulteerde dienstenaanbieder (bv. aanbieder van een clouddienst) en het subject niet heeft ingestemd met die specifieke plaats van opslag, dan begeeft enkel de dienstenaanbieder zich op het virtuele territorium van de betrokken staat en niet het subject. De staat heeft dan enkel toegang tot de

op zijn territorium opgeslagen gegevens die betrekking hebben op de dienstenaanbieder zelf en niet op het subject dat de dienst consulteert.

INTERNET ALS OPEN BRON – Tot slot maken ook data die toegankelijk zijn voor iedereen, al dan niet onder beperkte voorwaarden zoals registratie of betaling, deel uit van het virtuele territorium van de staat. Vandaag bestaat hier op internationaal vlak reeds overeenstemming over. Op dit vlak zou dus weinig veranderen. In de nieuwe visie maakt het open gedeelte van Internet deel uit van de virtuele leefwereld van ieder individu. Dit gedeelte behoort in principe dan ook tot het virtuele territorium van de verschillende staten. Het open gedeelte van de virtuele wereld vormt dan ook bij uitstek een voorbeeld van een gedeeld territorium waar verschillende staten over autonome bevoegdheden beschikken.

NOOD AAN INTERNATIONALE VERANKERING – Het is van groot belang dat het internationale debat omtrent digitale opsporing zich niet enkel focust op een verbetering en versnelling van internationale rechtshulp. De onderliggende en tot voor kort onderbelichte vraag wanneer een staat internationale rechtshulp nodig heeft dan wel unilateraal kan handelen, verdient dringend de nodige aandacht. We gaven reeds aan dat die vraag momenteel niet uitdrukkelijk genoeg aan bod komt in de relevante internationale regelgeving en er bovendien impliciet op uiteenlopende wijzen wordt beantwoord. De digitalisering van het bewijsmateriaal brengt het lokalisatievraagstuk aan de oppervlakte en dwingt ons een duidelijk standpunt in te nemen. Dat standpunt wordt bij voorkeur zo internationaal mogelijk verankerd, al laat het Cybercrime-verdrag vandaag o.i. ruimte voor een goed onderbouwde nationale beantwoording van het lokalisatievraagstuk.[488] Ook de Europese Unie kan hier een belangrijke rol in spelen en hierin voortbouwen op het reeds ingenomen standpunt in de EU-overeenkomst inzake wederzijdse rechtshulp. De expliciete beantwoording van het lokalisatievraagstuk in een Cybercrime-verdrag II van de Raad van Europa met mogelijke aansluiting van externe staten zou uiteraard nog wenselijker zijn, maar wellicht moeizamer verlopen.[489] De EU zou het pad evenwel reeds kunnen effenen door interne wetgeving, eventueel aangevuld met een

488 Art. 32 Cybercrime-verdrag laat verregaandere bevoegdheden niet toe, maar sluit ze ook niet uit. Toelichtend rapport bij het Cybercrime-verdrag, §294.

489 Het probleem oplossen via een protocol lijkt ons niet realistisch aangezien er dan ogenschijnlijke tegenspraak kan bestaan tussen de impliciete beantwoording van het lokalisatievraagstuk in het bestaande Cybercrime-verdrag en de beantwoording daarvan in het protocol.

overeenkomst met de Verenigde Staten, die immers alleen al omwille van het aantal Amerikaanse dienstenaanbieders een belangrijke speler vormt en die vandaag al expliciet met het lokalisatievraagstuk wordt geconfronteerd.[490] Indien de beantwoording van het lokalisatievraagstuk een zekere internationale gelding krijgt en bovendien succesvol blijkt, kan de benadering verder doorsijpelen in nieuwe overeenkomsten en op termijn uitgroeien tot internationaal gewoonterecht.[491]

6.4. Werkbaarheid nieuwe benadering

6.4.1. Praktische stappen voorwaarts

VERSNELLING STRAFRECHTELIJK ONDERZOEK – Via een theoretische analyse kwamen we tot het besluit dat voor de lokalisatie van opsporingshandelingen in cyberspace een subject-georiënteerde benadering het beste aansluit bij het oorspronkelijke idee van de territoriale staatssoevereiniteit. Hieronder gaan we na of een focus op het subject (en zijn virtuele overschrijding van grenzen) ook werkbaar is in de opsporingspraktijk. We zagen al dat de huidige object-georiënteerde benadering voornamelijk voor problemen zorgt, omdat ze een buitensporig beroep op trage internationale samenwerking noodzakelijk maakt. De idee van het virtuele territorium zou aan dit probleem tegemoetkomen en het strafrechtelijk onderzoek aanzienlijk kunnen versnellen. Gelet op het vluchtige karakter van digitale gegevens is die snelheid van primordiaal belang voor het veilig stellen van bewijs, niet enkel à charge, maar ook à decharge.

COHERENTE LOKALISATIE – De subject-georiënteerde benadering zorgt voor een coherente beantwoording van het lokalisatievraagstuk. Om klassieke opsporingsbevoegdheden in het buitenland te stellen, was steeds een fysieke overschrijding van de grenzen nodig. De territoriale begrenzing van de staatssoevereiniteit sluit echter uit dat de opsporingsinstanties autonoom fysiek grenzen zouden mogen oversteken. De telefoontap vormde een eerste uitdaging voor het denken in termen van territorialiteit. Een fysieke overschrijding van grenzen was niet altijd meer noodzakelijk voor het aftappen van een persoon in het buitenland. Waar de gezochte gegevens (de communicatie) zich bevinden, valt moeilijk te bepalen. De nationale en Europese wetgevers gingen de lokalisatieproblematiek in stilte uit de weg door de nadruk te leg-

490 Zie o.a. J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, 326-398. Zie i.v.m. de Microsoft-zaak *supra* noot 374.

491 Zie eveneens DASKAL, *ibid.*, 395.

gen op de locatie van het onderzochte individu. Zo is een staat enkel autonoom bevoegd als de onderzochte persoon zich op zijn grondgebied bevindt. De Raad van Europa bevestigde deze visie later deels in het Cybercrimeverdrag voor virtuele opsporing in real time. De door ons voorgestelde focus op het subject bij virtuele zoekingen zorgt voor een coherente benadering op het vlak van opsporing, waarbij geen nood is aan fysieke overschrijding van territoriale grenzen omdat het bewijs rechtstreeks bereikbaar is vanop het territorium van de onderzoekende staat. De locatie van de onderzochte persoon dan wel de gewoonlijke verblijfplaats van die persoon bepaalt op de eerste plaats waar de opsporingsbevoegdheid plaatsvindt. Belangrijk is dat de gebruiker zelf ook geen grenzen hoeft over te steken om de gegevens te consulteren. Ook de staat wiens territorium het onderzochte subject virtueel betreedt, krijgt rechtsmacht. Opnieuw ligt de focus op het subject. De staat van waaruit Internetdiensten door het subject worden geconsulteerd of de staat waar het subject zijn gegevens opslaat zijn bijvoorbeeld bevoegd. Een technische toevalligheid (vgl. art. 20 EU-Overeenkomst inzake wederzijdse rechtshulp en art. 31 EOB) of een grensoverschrijdende opslag door een dienstenaanbieder is dan weer niet voldoende om de betrokken staat een opsporingsbevoegdheid te geven m.b.t. het onderzochte subject. Daarvoor ontbreekt een gefundeerde link met die laatste.

6.4.2. Probleempunten

AFHANKELIJKHEID MEDEWERKING STAAT – We nemen de volgende situatie als vertrekpunt: Het te onderzoeken subject wordt ervan verdacht een Belgisch minderjarig meisje te hebben aangezet tot ontucht. Hij maakte daarvoor onder een fictieve identiteit gebruik van een online aangeboden communicatiedienst (bv. Facebook) en de opsporingsinstanties willen virtuele onderzoeksdaden t.a.v. de verdachte stellen. Het subject-georiënteerd uitgangspunt geeft op de eerste plaats de bevoegdheid aan de staat waar het onderzochte subject (*in casu* de verdachte) zich bevindt of zijn gewoonlijke verblijfplaats heeft (*in casu* onbekend). Die bevoegdheid wordt aangevuld met een soevereine bevoegdheid van de staat van waaruit de door het subject geconsulteerde dienst (*in casu* Facebook) wordt aangeboden (*in casu* de Verenigde Staten). Zolang opsporingsinstanties niet weten of de onderzochte persoon zich ten tijde van de opsporing op het grondgebied van de onderzoekende staat bevindt of daar zijn gewoonlijke verblijfplaats heeft, kunnen ze in principe geen rechtstreekse *real time* of virtuele onderzoeksdaden stellen ten aanzien van die verdachte. De onderzoekende staat heeft dan twee opties. Ofwel vraagt hij medewerking van de dienstenstaat, die bevoegd is vanwege de locatie van de

geconsulteerde dienstenaanbieder. Ofwel tracht de onderzoekende staat zelf de locatie of gewoonlijke verblijfplaats van de onderzochte persoon te achterhalen. De digitale omgeving maakt het evenwel soms erg moeilijk het individu achter een virtuele handeling of communicatie te lokaliseren in de fysieke wereld.[492] Internet Service Providers (ISP's) en Internet Access Providers (IAP's) vormen op dit vlak een belangrijke hulp voor opsporingsinstanties.[493] Een ISP (*in casu*: Facebook) kan in principe nagaan met welk IP-adres op welk ogenblik iemand toegang heeft genomen tot hun diensten, als zij die gegevens bewaren. In het voorbeeld zou Facebook kunnen nagaan met welk IP-adres het onderzochte fictieve profiel op het ogenblik van de aanzet tot ontucht verbinding heeft gemaakt. Het IP-adres toont aan welke IAP (bv. Proximus, Telenet) toegang heeft verleend tot het Internet en dus vanuit welk land de verdachte opereerde of communiceerde.[494] De IAP kan op zijn beurt meer concrete identificatiegegevens verstrekken over de gebruiker van zijn diensten (bv. het nummer van de geconsulteerde modem of de abonneegegevens).[495] De onderzoekende staat heeft bijgevolg ook voor de tweede optie de medewerking nodig van de buitenlandse ISP. Dat maakt het verdere verloop van het onderzoek dus sterk afhankelijk van de medewerkingsbereidheid van de staat vanwaar de gebruikte diensten worden aangeboden.

RECHTSTREEKS BEVEL AAN BUITENLANDSE ISP? – Er bestaan vandaag uiteenlopende visies over de vraag of de unilaterale afdwinging van een nationaalrechtelijke medewerkingsplicht t.a.v. een buitenlandse dienstenaanbieder in bepaalde omstandigheden in overeenstemming kan zijn met het internationaal recht.[496] Het Belgische Hof van Cassatie vindt van wel bij

---

492 Zie eveneens *ibid*., 374-375.

493 C. CONINGS, P. VAN LINTHOUT, 'Sociale media: een nieuwe uitdaging voor politie en justitie', *Panopticon* 2012, afl. 3, (205) 208-209.

494 Zie bv. voor België: http://www.nirsoft.net/countryip/be.html. Die gegevens kunnen, naargelang de omstandigheden, ernstige aanwijzingen vormen van de locatie van het subject of diens gewoonlijke verblijfplaats.; zie hierover eveneens: B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 43.

495 C. CONINGS, P. VAN LINTHOUT, 'Sociale media: een nieuwe uitdaging voor politie en justitie', *Panopticon* 2012, afl. 3, (205) 208-209.

496 Zie P. DE HERT en G. BOULET, 'De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten', *Computerr.* 2012, afl. 5, 324-330; K. DE SCHEPPER, 'Medewerking in een virtuele context? Ya! Hoo echter afdwingen?', *AM* 2012, afl. 2-3, 239-243; K. DE SCHEPPER en F. VERBRUGGEN, 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverle-

de plicht tot het overhandigen van identificatiegegevens (art. 46bis B.Sv), als de geviseerde operator of verstrekker zijn economische activiteit actief op consumenten in België richt.[497] Zelfs wie de medewerkingsplicht van een buitenlandse ISP op het eigen territorium lokaliseert, kan er niet omheen dat ter voldoening van die plicht er technische bijstand uit het buitenland nodig is, die klassieke internationale samenwerking tussen staten zal vergen. Bovendien kan de dienstenaanbieder zich geconfronteerd zien met conflicterende wetgeving waarbij de wetgeving in de ene staat hem verplicht informatie te geven terwijl de wetgeving in staat hem verplicht tot geheimhouding.[498] Beide staten trachten hun plicht daarenboven mogelijks af te dwingen met strafsancties. Het lijkt daarom hoe dan ook aangewezen samen te werken met de staat waar de dienstenaanbieder zich bevindt, wanneer men de medewerking van die dienstenaanbieder nodig heeft.

GEBREK SAMENWERKING – Alles laten afhangen de medewerking van de staat waar de dienstenaanbieder zich bevindt, is echter ook niet altijd aangewezen. Wanneer de medewerking uitblijft, loopt het strafrechtelijk onderzoek mogelijks vast. Dan kan iemand voor zijn criminele activiteiten bewust beroep te doen op diensten aangeboden vanuit staten die erom bekend staan dat ze weinig of niet internationaal samenwerken in strafzaken. Zo kan de crimineel zelf het vastlopen van een plaatselijk strafrechtelijk onderzoek in de hand werken. Dat haalt de interne erkenning van de soevereiniteit (ordehandhaving en bescherming door de staat), als substantiele bestaansvoorwaarde van die soevereiniteit, onderuit. Dit probleem kan alleen worden opgelost als de staat van de dienstenaanbieder bereid is om afspraken te maken. Wanneer de locatie of gewoonlijke verblijfplaats van de onderzochte persoon onbekend is, zullen opsporingsinstanties zich in

---

ners', *T.Strafr.* 2013, afl. 3, 157 e.v.; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime,* Brussel, Politeia, 2013, 353-360; J. VANDENDRIESSCHE, 'The effect of 'virtual presence' in Belgium on the duty to cooperate with criminal investigations: some prudence may be required when confronted with a request from a Belgian public prosecutor', *Digital Evidence and Electronic Signature Law Review* 2011, afl. 8, 194; F. VERBRUGGEN, 'Om af te sluiten, druk op Start: zesde rechter in Belgische Yahoozaak schaart zich achter eerste', *Computerr.* 2014, afl. 3, (129) 135-138; zie i.v.m. de onduidelijkheid hieromtrent in het Cybercrime-verdrag: *supra* noot nr. 420. Er gelden zelfs verschillende standpunten over de verenigbaarheid van een rechtstreeks grensoverschrijdend verzoek om medewerking met het internationaal recht. Zie B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 58-59.

497 Cass. 1 december 2015, AR P.13.2082.N.

498 J. DASKAL, 'The UN-Territoriality of Data', *Yale L.J.* 2015, vol. 125, (326) 391-392.

gevallen van anonimiteit en gebrek aan internationale rechtshulp genoodzaakt zien te veronderstellen dat ze als subject-staat of verblijf-staat bevoegd zijn.[499] Zodra ernstige aanwijzingen voorhanden zijn dat het subject zich in een derde staat bevindt (real time onderzoek) of er zijn gewoonlijke verblijfplaats daar heeft (onderzoek naar opgeslagen gegevens, 'digitaal huis'), dringen de internationale regels inzake samenwerking zich opnieuw op.

TRAGE SAMENWERKING – Wanneer de staat van de dienstenaanbieder wel bereid is tot samenwerking neemt dat vaak te veel tijd in beslag. Versnelling van de internationale samenwerking bij opsporing in een virtuele omgeving is een blijvende opdracht. Het verzoek tot bevriezing bestaat al. Dat moet wel gericht aan de staat waar de dienstenaanbieder is gevestigd.[500] Wanneer de verzochte staat ontdekt dat een dienstenaanbieder uit een derde staat of uit de verzoekende staat eveneens werd geconsulteerd in verband met de gezochte gegevens (bv. IAP (Telenet)) kan die staat de nodige verkeersgegevens onmiddellijk aan de verzoekende staat meedelen opdat die laatste in de mogelijkheid wordt gesteld om bij alle betrokken dienstenaanbieders de gezochte gegevens veilig te stellen.[501] Medewerking kan worden geweigerd als (1) het om een politiek misdrijf gaat of (2) de verzochte staat de bevriezing of mededeling in strijd acht met zijn soevereiniteit, veiligheid, openbare orde of andere essentiële belangen. Een rechtstreekse aanspreekbaarheid van dienstenaanbieders zou evenwel efficiënter zijn. De bescherming van

---

499 Zolang de opsporingsinstanties niet weten welke de subject-staat of de verblijf-staat is, is onbekend wiens soevereiniteit wordt geschonden. Zo een veronderstelling van bevoegdheid dringt zich o.i. ook op wanneer zowel de plaats van waaruit de diensten worden aangeboden als de plaats waar de onderzochte persoon zich bevindt of zijn gewoonlijke verblijfplaats heeft onbekend is. Bv. een onderzoek naar een criminele service provider via dewelke een verdachte een illegale handel opzet. Wanneer enkel de plaats van waaruit de dienst wordt aangeboden onbekend is, zou een staat o.i. ook als dienstenstaat bevoegdheid kunnen veronderstellen indien de medewerking van een staat die bevoegd is op grond van een ander criterium, onwerkbaar is. In alle gevallen dient het onderzoek op de eerste plaats gericht te zijn op het bepalen van de onbekende factoren.

500 Vgl. art. 29 Cybercrime-verdrag dat voorziet in de mogelijkheid om een weinig formalistisch rechtshulpverzoek tot bevriezing van gegevens te richten aan de staat van opslag, in afwachting van een meer gefundeerd verzoek tot verstrekking van de gezochte gegevens. (Toelichtend rapport bij het Cybercrime-verdrag, §283). Een verzoek aan de staat van opslag lijkt ons echter moeilijk werkbaar. Meestal zullen opsporingsinstanties immers technische bijstand van de dienstenaanbieder nodig hebben om gegevens te bevriezen. Bovendien is de staat van opslag vaak onbekend of heeft men de medewerking van de dienstenaanbieder nodig om die staat van opslag te identificeren. Een verzoek aan de staat waar de dienstenaanbieder is gevestigd, lijkt ons bijgevolg noodzakelijk.

501 Vgl. Art. 30 Cybercrime-verdrag.

mensenrechten mag echter niet ondergeschikt worden aan de efficiëntie van het strafrechtelijk onderzoek. Toch zou het o.i. mogelijk moeten zijn en aangewezen zijn om via een Cybercrime-verdrag II staten de verplichting op te leggen om hun ISP's op te dragen op bepaalde vragen van bepaalde buitenlandse overheden rechtstreeks te antwoorden.[502]

RECHTSTREEKSE MEDEWERKING TUSSEN RECHTSSTATEN – Het zou op de eerste plaats gaan om vragen betreffende de lokalisatie. De ISP zou zo kunnen aangeven naar welk land het gebruikte IP-adres verwijst zonder het IP-adres zelf mee te delen. Wanneer blijkt dat het onderzochte subject handelt op het territorium van de onderzoekende staat of wanneer de ISP over informatie beschikt die erop wijst dat het onderzochte subject zijn gewoonlijke verblijfplaats op het territorium van de onderzoekende staat[503] heeft, zou de rechtstreekse aanspreekbaarheid van de ISP in stand kunnen blijven. Zij zouden dan rechtstreeks een IP-adres kunnen meedelen of de betrokken overheid kunnen bijstaan in hun zoeking naar gegevens. Een rechtstreeks bevriezingsbevel zou eveneens een mogelijkheid kunnen zijn in afwachting van een meer gefundeerd verzoek tot verstrekking van gegevens. De verdragsluitende staten zouden een nationale instantie moeten aanduiden die in de mogelijkheid wordt gesteld om ISP's rechtstreeks aan te spreken. Die keuze wordt meegedeeld aan de andere verdragsluitende staten. Op die manier kan misbruik door onbevoegden worden vermeden. De rechtstreekse beantwoording van vragen dient o.i. evenwel afhankelijk te worden gesteld van het respect voor fundamentele mensenrechten door de verzoekende staat. Ten aanzien van de partijen bij het EVRM of een gelijkwaardig rechtsinstrument (zowel wat betreft de inhoud als het controlemechanisme)[504] zou een weerlegbaar vermoeden van respect voor grondrechten kunnen gelden. Verder zal er een soort standaardformulier moeten komen voor de opsporingsinstanties in de verzoekende staten, met o.a. het vermoede misdrijf, de redenen van verdenking en de noodzaak van de zoeking. De vereiste informatie zou beperkter zijn voor het bevriezingsbe-

502 Zie bv. m.b.t. de V.S. en het Verenigd Koninkrijk: https://www .wash ington-post.com/ world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

503 De Europese Unie zou misschien zelfs kunnen denken aan EU-wijde bevoegdheid, d.w.z. dat politie en justitie van EU-landen de gegevens ook zouden krijgen als het om een IP uit een andere EU-lidstaat gaat.

504 Vgl. EHRM 30 juni 2005, nr. 45036/98, Bosphorus/Ierland, §155.

vel dan voor het bevel tot verstrekking van gegevens.[505]

SUBSIDIARITEITSPRINCIPE – Een goede bereikbaarheid van ISP's is belangrijker dan men op het eerste gezicht zou denken. Het subsidiariteitsprincipe (de minst ingrijpende maatregel die geschikt is voor het beoogde doel, verdient de voorkeur) is o.i. inherent aan een systeem van effectieve grondrechtenbescherming.[506] In het licht van dit beginsel verdient de rechtstreekse bevraging of internationale samenwerking de voorkeur op bijvoorbeeld een nationale bevoegdheid tot het heimelijk inbreken in informaticasystemen[507] (bv. de mailbox van het subject met gewoonlijke verblijfplaats in opsporende staat) als hetzelfde resultaat kan worden bereikt. Er is echter geen gelijk resultaat als de rechtstreekse bevraging of internationale samenwerking niet effectief werkt. Wanneer enkel een rechtstreekse toegang (zoals de hacking) tot een bevredigend resultaat kan leiden, zal de opsporende staat zich genoodzaakt (en waarschijnlijk ook gelegitimeerd) voelen om die bevoegdheid in te zetten als de nationaalrechtelijke voorwaarden daartoe zijn vervuld.

ANONIMISERENDE TOOLS – Anonimiserende tools stellen evenwel nog een bijkomend probleem. Zelfs indien opsporingsinstanties erin slagen om het nodige IP-adres via een ISP te bemachtigen is niet zeker of zij het onderzochte subject effectief kunnen lokaliseren en identificeren. Allerhande voor het publiek beschikbare tools, zoals proxyservers[508] of The Onion

---

505 Zie m.b.t. het bevriezingsbevel: art. 29, 2 Cybercrime-verdrag.

506 Zie i.v.m. art. 8 EVRM: P. DE HERT, *Art. 8 EVRM en het Belgische recht,* Gent, Mys & Breesch, 1998, 42: '*Het beginsel komt tegemoet aan het belang dat in een correcte grondrechtentheorie aan de rechten en vrijheden van de burger dient toe te komen*.'

507 Zie i.v.m. de heimelijke zoeking op afstand: voorgesteld art. 126nba, *supra*, 2.2. Die nationale hackingsbevoegdheid is problematisch als de staat waar het gehackte systeem zich bevindt, dit als een strafbare toegang tot het informaticasysteem beschouwt. (C. CONINGS, J.J. OERLEMANS, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend', *Computerr.* 2013, afl. 1, 30.) Op basis van wederkerigheid kunnen staten een dergelijk optreden door 'bevriende staten' met een legitieme claim op de gegevens wel dulden, doch duidelijke internationale afspraken zijn dan echt wel wenselijk (*supra*, 2.3). Voor de stand van zaken in 2009-10, zie CYBERCRIME CONVENTION COMMITTEE (T-CY) AD-HOC SUB-GROUP ON JURISDICTION AND TRANSBORDER ACCESS TO DATA, *Transborder access and jurisdiction: What are the options? Report of the Transborder Group adopted by the T-CY on 6 December 2012*, 30: alleen Bosnië-Herzegovina, Japan en misschien Chili leken dit toe te laten voor een '*hack*' die verder gaat dan het '*gebruik van het rechtmatig bekomen paswoord*'.

508 Zie bv. www.proxy4free.com. Door gebruik te maken van een daar aangeboden proxy kan een gebruiker de indruk wekken dat hij toegang neemt tot het Internet

Router (TOR)[509], stellen Internetgebruikers immers in de mogelijkheid om hun identiteit te verbergen.[510] Niet alleen de identiteit, maar ook de locatie van de betrokken persoon valt dan moeilijk of niet te achterhalen. Opsporingsinstanties zullen dan enkel verder kunnen opereren in samenwerking met het land waar de door het onderzochte subject geconsulteerde dienstenaanbieder zit of het land waar het subject zich schijnbaar (maar niet effectief) bevindt.

ERNSTIGE AANWIJZINGEN ANONIMISERENDE TOOL – Wij pleiten er bij ernstige aanwijzingen dat het subject gebruik maakt van anonimiserende tools, staten unilateraal moeten kunnen optreden. Dat zou wel alleen kunnen als de medewerking van de staat van de door het onderzochte subject geconsulteerde dienst geen uitweg kan bieden. Zolang de opsporingsinstanties niet weten wie de verblijf-staat of de subject-staat is, weten ze niet van wie ze soevereiniteit zouden schenden door de verdere uitvoering van het onderzoek. Opsporingsinstanties zouden daarom hun eigen bevoegdheid moeten kunnen veronderstellen. Zij moeten echter alles in het werk te stellen om op de eerste plaats de locatie van het subject of diens verblijfplaats te achterhalen. Zodra er ernstige aanwijzingen zijn dat het subject zich op het territorium van een derde staat bevindt of daar zijn gewoonlijke verblijfplaats heeft, moet de soevereiniteit van die staat worden gerespecteerd en medewerking verkregen voor de verderzetting van het onderzoek. Anders raakt het evenwicht tussen individu en staat opnieuw grondig ver-

---

vanuit een ander land dan het land waar hij zich werkelijk bevindt. Via dergelijke sites worden IP-adressen tussen verschillende gebruikers uitgewisseld.

509 Het TOR-netwerk maakt gebruik van de techniek van Onion Routing. Die techniek houdt in dat een boodschap herhaaldelijk wordt versleuteld en van verzender naar ontvanger wordt verzonden via zogenaamde *onion routers*. Iedere *onion router* verwijdert een laag encryptie en komt zo te weten naar welke volgende router de boodschap dient te worden verzonden. Zo voorkomt men dat die tussenstations de herkomst, de bestemming en de inhoud van het bericht zouden kennen. Dit maakt het praktisch onmogelijk voor opsporingsinstanties om de weg tussen verzender en ontvanger te reconstrueren. Via een *exit node* verlaat de boodschap het TOR-netwerk en bereikt ze de gewenste eindbestemming. Voor opsporingsinstanties is enkel het IP-adres van de *exit node* zichtbaar. Het houden van een exit node houdt dus heel wat risico's in. Zie D. GOLDSCHLAG, M. REED, P. SYVERSON, *Onion Routing for Anonymous and Private Internet Connections,* Communications of the ACM, februari 1999, vol. 42 No. 2, 39-41 en 'HTG explains: Is Tor really Anonymous and Secure', http.//www.howto geek.com.

510 Zie hierover ook: B.J. KOOPS en M.E.A. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, The Hague/Tilburg, WODC/TILT, 2014, 43.

stoord. Het individu zou zo immers teveel macht in handen krijgen om een strafrechtelijk onderzoek te belemmeren.

Discussiepunten:

1. Is, om uit te maken of een staat zelf territoriaal bevoegd is dan wel rechtshulp van een andere staat nodig heeft, het lokaliseren van real-time zoekingen (bewakingsmaatregelen) op de plaats waar het geviseerde subject zich bevindt en van zoekingen naar opgeslagen gegevens in de thuisstaat van het doelwit een betere manier dan de koppeling aan de plaats van opslag van de gegevens?
2. Kan de notie van 'virtueel territorium', als aanvulling op het fysieke territorium, de behoefte aan internationale rechtshulp verkleinen en beletten dat er in cyberspace een aantal 'rechtsvrije' plaatsen zouden ontstaan? Met dat 'virtueel grondgebied' bedoelen we soevereine rechtsmachtsaanspraken van een staat over gegevens die in het buitenland zitten, maar die vanaf het fysiek territorium van die staat worden gecontroleerd door een subject of dienstenverlener.
3. In welke gevallen is het eenzijdig doorzoeken van gegevens door politie of justitie van een staat, zonder het medeweten of zonder de toestemming van een andere staat, verantwoord of zelfs wenselijk?

Hoe kunnen België en Nederland 'bewuste onwetendheid' van speurders omtrent hun territoriale bevoegdheid om te doorzoeken, vermijden of sanctioneren? Schendt een miskenning van een internationaal publiekrechtelijke bevoegdheidsregel enkel de belangen van de staat van wie de soevereiniteit is miskend? Of schendt ze meteen ook de rechten van het individu wiens gegevens zijn verkregen, het loyaliteitsbeginsel of het recht op een eerlijk proces?[511]

---

511 Art. 28 §3 B.Sv verplicht het OM te waken over de wettigheid van de bewijsmiddelen en de loyaliteit waarmee ze worden verzameld. We nemen aan dat wettigheid ook conformiteit met het (internationaal) recht omvat, wat bij bewuste onwetendheid een probleem oplevert. Het Hof van Cassatie ziet het loyaliteitsbeginsel vooral als een verbod op het achterhouden bij de bewijsvoering van gegevens *à décharge* (Cass. 19 december 2012, P.12.1310.F/1, *JT* 2013, noot F. KONING.) Hier gaat het echter niet om de bewijsmiddelen, maar om de manier waarop ze zijn verzameld. Het Hof van Cassatie beschouwt '*het feit dat de overheid de onrechtmatigheid al dan niet opzettelijk heeft begaan*' als een factor bij de beoordeling of bewijs al dan niet moet worden uitgesloten wegens strijdigheid met het recht op een eerlijk proces (Cass. 28 mei 2013, AR P.13.0066.N., *RW* 2013-14, 1616, noot B. DE SMET). Zie voor de specifieke kwestie echter *supra*, voetnoot 196.

Conclusie

MOEILIJK – Het zal de leden van de Vereniging niet verbazen dat Nederland en België voor heel gelijkaardige situaties en problemen verschillende oplossingen kiezen. Soms is het verschil vooral semantisch, soms gaat het over het raffinement in de begrippen, soms gaat het over fundamentele keuzes (of het uitblijven ervan).

Net doordat de structuur van de wetgeving in Nederland anders is dan in België, viel het ook niet altijd mee om beide regelingen op een evenwichtige manier te analyseren. Soms helt de analyse wat over naar een heel Nederlandse discussie, soms was de analyse van de Belgische wetgeving of praktijk misschien wat uitgebreider. Met Deel 2 hebben we ook geprobeerd het recht zoals het is los te laten en krijtlijnen te trekken voor het recht van de (nabije of verre) toekomst.

Bij wijze van conclusie overlopen we nog vlug enkele punten die ons bij vergelijking het meest in het oog zijn gesprongen.

VERWERKER EN DRAGER – Het begon al met de afbakening van het onderwerp, de computer. De Nederlandse wetgever koos voor het begrip '*geautomatiseerd werk*', terwijl België met het bredere concept '*informaticasysteem*' ook de loutere dragers omvat. Moeten alle dragers gelijke behandeling krijgen en verdient de USB-staaf of chip dus dezelfde behandeling als de kartonnen doos met papieren? Dat lijkt de Nederlandse keuze. De vluchtigheid, het bijzonder precair karakter van gegevens verdwijnt immers eens ze zijn opgeslagen. Of zijn het net de typerende kenmerken van '*digitale dragers*' die gelijkschakeling met computers verantwoorden? Dan denken we aan een massale hoeveelheid gegevens op een kleine plaats, snel kopieer-, verplaats- en verwijderbaar. Kopiëren, verwijderen of vernietigen kan soms zelfs via ingebouwde mechanismes of vanop afstand. Ook lijkt het moeilijker om binnen een grote hoeveelheid gegevens voorafgaande beperkingen in te voeren om bij zoeking de selectie te beperken tot de voor het onderzoek relevante gegevens. Dat lijkt de reden waarom België, zonder al te veel debat of verantwoording, voor de gelijkschakeling van dataverwerkers en -dragers heeft gekozen. Verder valt op dat de definities van computers zeer ruim uitvallen, nu navigatiesystemen, 'slimme' voorwerpen en andere interactieve systemen aan belang winnen, waarbij het voor de gebruikers zelden duidelijk is welke gegevens waar (niet) worden opgeslagen. Het is tijd voor opheldering van de mogelijkheden om ook dergelijke apparaten, die niet met traditionele computers worden geassocieerd, te doorzoeken op basis van de informaticabevoegdheden. Het valt trouwens op dat

beide landen het moeilijk hebben om computers nauwkeurig en duurzaam te omschrijven en op enigszins tautologische definities terugvallen.

DOORZOEKING EN BESLAG – Voor de doorzoeking maakt Nederland, veel meer dan België, een onderscheid naar gelang het doel van de zoeking. Nederland heeft verschillende, nogal gedetailleerde regimes naargelang die zoeking gericht is op inbeslagname dan wel op de vastlegging van gegevens. Wel zijn de voorwaarden en beslissende instanties uiteindelijk vaak gelijklopend. Over het algemeen is de vaststelling dat binnen de huidige regeling nog niet genoeg nagedacht is over de beste plaats van een zoekingsbevoegdheid in computers. In beide landen ligt de openlijke zoeking in computers nog te veel gebonden aan plaatsen: de huiszoeking of de zoeking in voertuigen of op openbare plaatsen. Nochtans is gedeeltelijke loskoppeling van de plaats net kenmerkend voor de informaticazoeking. Ook zat de bevoegdheid in België tot nu toe te veel vastgehaakt aan de klassieke, eerder summier geregelde beslagbevoegdheid. De aparte regeling voor databeslag slaat vooral op de vraag hoe in dergelijke gevallen beslag kan gebeuren, niet wanneer. Daarvoor valt men grotendeels op de klassieke doorzoekingsbevoegdheden terug. Vooral op het vlak van toegang tot gegevens zonder rechterlijke machtiging roept de rechtspraak vragen op. Momenteel is de logica van de wettelijke systematiek dat de plaats waar de gegevensdrager is aangetroffen het niveau van bescherming bepaalt, terwijl de inhoud en de privacygevoeligheid ervan een beter criterium zouden zijn. In de Nederlandse rechtspraak is het debat hierover begonnen, in België zit de rechtspraak voorlopig nog op de traditionele lijn. De Belgische regering lijkt het thema wel op tafel te leggen voor het najaar van 2016.

HEIMELIJKE DOORZOEKING OP AFSTAND – Wat zeker een debat verdient, is de heimelijke doorzoeking op afstand. In beide landen is het voorlopig niet als zodanig geregeld (waardoor het niet toegestaan is behoudens enkele specifieke uitzonderingen), maar zijn er plannen voor een nieuwe wetgeving met ruime zoekmogelijkheden. De focus ligt meestal op de manier van binnendringen ('hacken'). Dat is van belang, want het heimelijk karakter en zeker het bewust verschalken of beliegen van mensen door de overheid roepen fundamentele vragen op. Dat geldt des te meer als die overheid daarbij heimelijk de identiteit van anderen gaat misbruiken. Toch waarschuwen we de wetgevers ervoor om zich niet blind te staren op de vraag *hoe* de overheid binnendringt, maar vooral ook te kijken naar het *waarom*: voor welke onderzoekshandelingen? Het plaatsen van technische middelen onder de huidige tapwet is van een andere orde dan het eenmalig heimelijk

doorzoeken van op een computer opgeslagen gegevens. Nog behoorlijk wat indringender, en dus hopelijk heel uitzonderlijk, is een heimelijke bewakingsmaatregel waarbij de overheid iemands volledige computergebruik heimelijk bespiedt. We hebben er ook op gewezen dat in een interactieve wereld het gevaar groot is dat naast het eigenlijke doelwit ook andere mensen in het sleepnet van de heimelijke informatieverzameling verstrikt geraken.

NETWERKZOEKING – Beide landen hebben een wettelijke regeling voor de netwerkzoeking, die Nederland iets meer aan banden lijkt te leggen dan België. Niet alleen is er de beperking tot situaties van een doorzoeking, terwijl er ook in andere gevallen behoefte bestaat aan deze mogelijkheid; ook is een zgn. 'dubbele band' vereist tussen de persoon en de locatie van de oorspronkelijke zoeking en tussen de toegangsbevoegdheid van de persoon en de gegevens. België voorziet alleen deze laatste (koppeling aan de toegangsbevoegdheid) en rekent voor de beperking vooral op het bevel van de onderzoeksrechter. Daarbij baarde vooral een 'verglijding' van een netwerkzoeking naar een 'feitelijke tap' zorgen, omdat voor die tap striktere regels golden. Vanwege de eerder vermelde brede conceptie van informaticasysteem is de uitbreiding via netwerkzoeking tot gegevensdragers in België wel mogelijk, in Nederland niet. In Nederland kan de netwerkzoeking niet vanaf een politiekantoor, in België is de situatie op dat vlak wat dubbelzinnig. Beide landen doen er goed aan te expliciteren onder welke voorwaarden dit mogelijk is.

OPSPORINGSRECHTSMACHT – Een debat dat momenteel volop woedt in de opsporingswereld en op het politieke forum is de vraag naar de grensoverschrijdende inzet van nationale opsporingsbevoegdheden. De voorafgaande vraag is wanneer er in de digitale wereld sprake is van een dergelijke grensoverschrijding. De erop volgende vraag is wanneer die overschrijding een inbreuk vormt op de soevereiniteit van een andere staat. De laatste vraag is welke rechtsgevolgen een eventuele schending dan heeft. Het bleek dat Nederland en vooral België een vrij optimistische interpretatie hanteren van wat het internationaal publiekrecht hier en nu toelaat. Ook is het onduidelijk of de bestaande regels inzake het waarschuwen van buitenlandse overheden en het verkrijgen van hun instemming worden toegepast in de praktijk. In de hedendaagse digitale wereld lijkt de plaats waar de gegevens zich bevinden, niet stabiel genoeg om een werkbaar aanknopingspunt voor rechtsmacht te vormen, maar over de alternatieven bestaat nog lang geen consensus.

ONTSLEUTELBEVEL – Beide landen kennen een regeling tot het vorderen van medewerking aan ontsleutelen of ongedaanmaken van computerbeveiligingen. De Belgische regeling is ruimer, niet alleen omdat deze ziet op meer handelingen (bijvoorbeeld ook het helpen zoeken naar gegevens) en meer situaties (de Nederlandse regeling beperkt zich tot doorzoekingssituaties), maar ook omdat de informatieplicht (hoewel niet de medewerkingsplicht) ook op de verdachte rust. Althans volgens de wet – het Hof van Beroep te Gent oordeelde dat dit in strijd is met het *nemo tenetur*-beginsel. De discussie over een ontsleutelplicht aan verdachten speelt in beide landen, zeker ook omdat onverdachte derden vaak geen kennis hebben van de versleuteling en omdat moderne encryptie (mits goed gebruikt) vrijwel onkraakbaar is. Nu kan een met voldoende waarborgen omklede ontsleutelplicht voor verdachten in beginsel een toets aan art. 6 EVRM doorstaan, maar alleen bij een lage strafbedreiging; dat laatste maakt zo'n ontsleutelplicht niet effectief. Daarom kan de discussie hierover beter ophouden; wetgevers richten zich best op alternatieve mogelijkheden, zoals de doorzoeking van computers vanop afstand of eventueel het gebruiken van decryptieweigering bij bewijs- of straftoemetingsbeslissingen.

BIJZONDERE GEGEVENS EN BEWARING – Een van de grootste problemen bij computers is het doortrekken van de bijzondere bescherming voor bepaalde typen gegevens. Die vallen immers moeilijk van andere gegevens te onderscheiden. De beschermingsmechanismen voor papieren documenten van beroepsgeheimhouders (filtering door de disciplinaire overheid) vallen ook niet altijd gemakkelijk door te trekken naar de '*digitale zoeking*'. Ook de grens tussen de inhoud van communicatie, die traditioneel extra bescherming krijgt, en andere gegevens valt niet altijd gemakkelijk te trekken. De klassieke koppeling bij de bescherming van communicatie-inhoud aan het al dan niet '*onderweg*' zijn van de boodschap, lijkt onvoldoende bescherming te bieden in het cloud-tijdperk, maar een duidelijk alternatief is er nog niet. Zowel in Nederland als in België zit er enige inconsistentie in de bestaande regeling. Zo kunnen Belgische onderzoeksrechters bijvoorbeeld wel brieven openmaken in een onderzoek naar misdrijven waarvoor zij geen telecommunicatie (zoals e-mails) mogen onderscheppen. De moeilijke kwestie van selectie van relevante gegevens en de vernietiging van irrelevante gegevens, hebben we slechts summier behandeld. Inconsistenties in de Nederlandse vernietigingsregeling tussen doorzoeking en bijzondere opsporingsbevoegdheden vragen in elk geval om uitleg, terwijl ook de Belgische overheid meer duidelijkheid zou moeten verschaffen over het lot van de verzamelde gegevens.

KRIJTLIJNEN VOOR DE TOEKOMST. DIGITAAL HUISRECHT? – Om de plaats van 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden te begrijpen en te bepalen, moet volgens ons het begrip 'plaats' net tot op zekere hoogte worden losgelaten. De huidige benadering in het Nederlandse en Belgische recht is sterk plaatsgebonden, zowel voor de doorzoekingsbevoegdheden als in de object-georiënteerde benadering van rechtsmachtvraagstukken. Computers kenmerken zich door een lossere band tussen gegevens en gegevensdrager dan bij papier het geval is, en zijn door de miniatuuromvang van chips ook veel mobieler dan papier. Dat maakt het onderzoek van in computers opgeslagen gegevens veel minder plaatsgebonden dan klassiek gegevensonderzoek. Vanwege de verplaatsing van gegevens die voorheen vooral binnen het huis lagen opgeslagen naar de cloud, en de opkomst van persoonlijke draagbare computers waarin een belangrijk deel van het (huidige en verleden) digitale leven opgeslagen ligt, is een nieuwe, plaatsonafhankelijker vorm van rechtsbescherming nodig. Het concept van een 'digitaal huisrecht', dat de digitale ruimte beschermt waarover een burger het *ius excludendi* kan uitoefenen, zou een geschikte basis kunnen zijn om de rechtsbescherming, en daarmee de reikwijdte van digitale opsporingsbevoegdheden, in de 21e eeuw vorm te geven.

AANKNOPINGSPUNTEN RECHTSMACHT – Het debat over rechtsmacht voor speurders in cyberspace woedt volop en de plaats waar gegevens zich bevinden, biedt te weinig houvast. Daarom hebben de Belgische preadviseurs het voorstel van Conings voor alternatieve aanknopingspunten hernomen. De lokalisering van real time onderzoeksmaatregelen op de plaats waar de betrokken persoon zich bevindt, maakt de plaatselijke overheid conform haar wetgeving bevoegd. Buitenlandse speurders hebben dus haar instemming (en eventueel rechtshulp) nodig. Mensen laten als ze zich verplaatsen echter hun 'digitaal verleden' op de plaats waar ze hun gebruikelijke verblijfplaats hebben. Die verblijfstaat is dan bevoegd om, op basis van zijn eigen wetgeving, doorzoekingen uit te voeren, ook zoekingen op vraag van buitenlandse speurders. We gebruikten de notie 'virtueel territorium' om de band te onderstrepen tussen de staat die rechtsmacht heeft en de gegevens. Het voordeel van de nieuwe criteria is dat ze ook de rechtsbeschermende functie van soevereniteit erkennen: de plicht van een staat om personen op zijn grondgebied te beschermen, ook tegen de overheid van vreemde staten. Tijdens het speurwerk zullen deze aanknopingspunten niet altijd volstaan, bv. als de verblijfplaats van het doelwit onbekend is. Daarom zijn er ook andere aanknopingspunten voor rechtsmacht: de staat waar de verstrekker van elektronische diensten gevestigd is, heeft rechtsmacht over

die dienstverlener en corresponderende hulpverplichtingen ten opzichte van partnerstaten. De staat van feitelijke opslag of transit van de gegevens heeft slechts zwakke rechtsmachtaanspraken. Soms kunnen speurders ook met vermoedens van rechtsmacht werken, bv. het vermoeden dat het doelwit zich op hun grondgebied bevindt.

Discussiepunten

1. Moeten apparaten als navigatiesystemen, slimme koelkasten, tv's en pacemakers (die wel geautomatiseerd gegevens verwerken, maar een ander karakter hebben dan de traditionele computer) onder de (strafvorderlijke) definitie van 'geautomatiseerd werk' vallen?

2. De Belgische definitie van informaticasysteem is heel ruim. Te ruim of is dat juist een voordeel? Is het wenselijk om, anders dan in Nederland, digitale gegevensdragers (zoals usb-staafjes of geheugenkaarten) onder de (strafvorderlijke) definitie te laten vallen?

3. De bevoegdheid tot binnendringen in computers moet anders worden vormgegeven dan in het Nederlandse wetsvoorstel. In plaats van een Zwitsers zakmes met te veel 'handige' functionaliteiten, moet het beter worden ingebed in de wetssystematiek. Het voorstel in dit preadvies geeft aan hoe dat zou kunnen.

Binnendringen voor zoeking is minder problematisch dan binnendringen voor vernietiging of ontoegankelijkmaking. Dat laatste zou best openlijk (en achteraf?) moeten gebeuren.

4. Het onderzoek aan inbeslaggenomen smartphones, tablets en andere persoonlijke ('echte') computers behoeft een machtiging van de rechtercommissaris of onderzoeksrechter, omdat de privacyinbreuk vergelijkbaar is met die van een woningdoorzoeking.

5. De netwerkzoeking moet mogelijk worden in alle gevallen waarin computers in het kader van de opsporing onderzocht worden, onder nader te bepalen voorwaarden.

6. Kunnen we de regels van de tapwetgeving ten aanzien van geheimhoudergegevens wel veralgemenen tot alle zoekingen? Talloze personen van wie politie en justitie de computer onderzoekt, gaan communicatie met talloze mensen opslaan, waaronder die met advocaten en artsen. Het is maar de vraag of de disciplinaire overheden van advocaten en artsen bereid zijn om quasi-permanent ter beschikking te staan om telkens als de computer van een patiënt of cliënt wordt doorzocht, bij te springen om het beroepsgeheim te beschermen. Als advocatuur en medische wereld nog in het beroepsgeheim geloven, zouden ze er goed aan doen om met de ICT-wereld na te denken over technische manieren (elektronische watermerken, bijzondere

codes, ...) om binnen grote hoeveelheden gegevens gemakkelijker detecteerbaar te maken welke daarvan door het beroepsgeheim zijn gedekt.

7. De aanvullende bescherming van 'gevoelige' persoonsgegevens moet niet worden afgeschaft bij de Nederlandse regeling van gegevensvordering, maar anders worden vormgegeven. Bovendien moet deze bescherming systematisch worden doorgevoerd bij andere opsporingsbevoegdheden. Gezocht moet worden naar een geschikt aanknopingspunt om situaties te definiëren waarin op voorhand te verwachten valt dat 'gevoelige' persoonsgegevens zullen worden vergaard en onderzocht.

8. Om burgers adequaat te beschermen tegen overheidsonderzoek in computers, waarbij het persoonlijke leven indringender in beeld komt dan bij vrijwel elke andere opsporingsbevoegdheid, is een zware, grondrechtelijke vorm van rechtsbescherming nodig. Die rechtsbescherming kan worden gestoeld op het concept van 'digitaal huisrecht', dat de digitale ruimte beschermt waarover een burger het *ius excludendi* kan uitoefenen.

Moet de wetgever bij de regeling van de opsporingsmethoden de eigenheid van het 'digitale huis' als aparte omgeving erkennen en beschermen, zodat naast de fysieke woning ook het digitale huis bescherming zou bieden aan zijn 'bewoner'? Of is het veeleer wenselijk om geen apart regime te voorzien voor de digitale omgeving, maar te werken met de bescherming van de persoonlijke omgeving als zodanig? Die omvat dan zowel fysieke plaatsen met een grote privacyverwachting (zoals de woning) als de 'digitale privéwereld' en alle dienstverlening waarbij de gebruiker redelijke privacyverwachting heeft.

9. Is, om uit te maken of een staat zelf territoriaal bevoegd is dan wel rechtshulp van een andere staat nodig heeft, het lokaliseren van real-time zoekingen (bewakingsmaatregelen) op de plaats waar het geviseerde subject zich bevindt en van zoekingen naar opgeslagen gegevens in de thuisstaat van het doelwit een betere manier dan de koppeling aan de plaats van opslag van de gegevens?

Kan de notie van 'virtueel territorium', als aanvulling op het fysieke territorium, de behoefte aan internationale rechtshulp verkleinen en beletten dat er in cyberspace een aantal 'rechtsvrije' plaatsen zouden ontstaan? Met dat 'virtueel grondgebied' bedoelen we soevereine rechtsmachtsaanspraken van een staat over gegevens die in het buitenland zitten, maar die vanaf het fysiek territorium van die staat worden gecontroleerd door een subject of dienstenverlener.

In welke gevallen is eenzijdig doorzoeken van gegevens door politie of justitie van een staat, zonder het medeweten of zonder de toestemming van een andere staat, verantwoord of zelfs wenselijk?

Hoe kunnen België en Nederland 'bewuste onwetendheid' van speurders omtrent hun territoriale bevoegdheid om te doorzoeken, vermijden of sanctioneren? Schendt een miskenning van een internationaalpubliekrechtelijke bevoegdheidsregel enkel de belangen van de staat van wie de soevereiniteit is miskend? Of schendt ze meteen ook de rechten van het individu wiens gegevens zijn verkregen, het loyaliteitsbeginsel of het recht op een eerlijk proces?

Over de auteurs

Prof.dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT—Tilburg Institute for Law, Technology, and Society van de Universiteit van Tilburg. Hij doet onderzoek naar computercriminaliteit, cyberopsporing, privacy en dataprotectie. Hij is ook geïnteresseerd in onderwerpen als DNA-opsporing, identiteit, digitale grondrechten, regulering door techniek, de maakbare mens, en reguleringsvraagstukken rond genetica, robotica en neurotechnologie. In het academisch jaar 2016/2017 is hij Distinguished Lorentz Fellow bij het NIAS en Lorentz Center. Met een persoonlijke postdoc-subsidie (1999), VIDI (2003) en VICI (2014) is Koops een van de weinige Nederlandse onderzoekers die alle drie stadia van NWO's (Nederlandse Organisatie voor Wetenschappelijk onderzoek) persoonsgerichte subsidies heeft ontvangen. Van 2005-2010 was hij lid van De Jonge Akademie, een onderdeel van de Koninklijke Nederlandse Akademie van Wetenschappen.

Dra. Charlotte Conings is doctoraatsbursaal aan het Instituut voor Strafrecht van de KU Leuven. Ze finaliseert momenteel haar doctoraat met als titel "*een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld*" onder leiding van haar promotor prof. F. Verbruggen en haar co-promotor prof. R. Verstraeten. Zij heeft in dat kader al verschillende publicaties over digitalisering en opsporing achter haar naam staan en heeft over datzelfde onderwerp ook al verscheidene nationale en internationale presentaties verzorgd.

Prof.dr. Frank Verbruggen is hoogleraar aan de KU Leuven, Instituut voor Strafrecht en gastdocent aan de UHasselt. Zijn publicaties gaan vooral over algemene beginselen in het strafrecht, mensenrechten, bijzondere opsporingsmethoden en internationale samenwerking in strafzaken. Momenteel bestudeert hij o.m. hoe strafrecht en strafprocesrecht moeten omgaan met de digitalisering van het dagelijks leven en van het strafrechtelijk bewijs.