Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming

Thomas Incalza

Onder wetenschappelijke begeleiding van prof. dr. F. Hutsebaut en Femke Van Damme

1. INLEIDING

De razendsnelle ontwikkeling van de moderne mens tot een ware *homo informaticus* heeft enige tijd zowel het Strafwetboek als het Wetboek van Strafvordering doen daveren op hun negentiende-eeuwse grondvesten, die immers niet opgewassen waren tegen de informaticatechnologie als een volstrekt nieuw "*middel om criminele feiten te plegen*" en haar als "*doelwit van criminele activiteiten*" al evenmin een afdoende bescherming konden bieden[1]. Op materieelrechtelijk vlak werd de juridische vindingrijkheid inzake strafrechtelijke kwalificatie van menig parketmagistraat danig op de proef gesteld – getuige daarvan onder meer de zaak BISTEL[2] – en ook de strafprocedure bleek niet aangepast aan de noden en mogelijkheden van het digitale tijdperk.

Reeds in 1982 trokken de materieelrechtelijke hiaten in menig nationale strafwetgeving de aandacht van internationale organisaties zoals de OESO en later ook die van de Raad van Europa[3], die in 1989 via een – weliswaar bijzonder vaag omschreven – aanbeveling[4] de eerste stappen zette richting 'synchronisatie' van wetgeving en technologie. De procedurele tekortkomingen werden evenwel pas aangekaart in een aanbeveling van 1995,

---

1 Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 4; T. VERBIEST en J. DERVAUX, "La criminalité informatique dans tous ses états", *TBH* 2002, afl. 8, (607) 607.

2 Corr. Brussel 8 november 1990, *Computerr.* 1991, 31, noot A. MEIJBOOM, *DIT* 1991, afl. 1, 51, noot C. ERKELENS en *JT* 1991, 11, noot, gewijzigd door Brussel 24 juni 1991, *Computerr.* 1992, 253.

3 F. DE VILLENFAGNE en S. DUSOLLIER, "La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *AM* 2001, afl. 1, (60) 61; C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 617.

4 Aanbeveling R(89) 13 september 1989 van het Comité van Ministers aan de lidstaten betreffende computergerelateerde misdaad, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.

overwegende dat "*criminal procedural laws of member states often do not yet provide for appropriate powers to search and collect evidence in [electronic information systems] in the course of criminal investigations*"[5]. Op 23 november 2001 mondden beide aanbevelingen uit in het zogenaamde 'Cybercrimeverdrag', gesloten in de schoot van de Raad van Europa, dat er in de eerste plaats toe strekte "*a common criminal policy*" te bereiken, "*aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation*"[6].

Geïnspireerd door de toenmalige ontwerptekst van dat verdrag[7] en nadat reeds verschillende andere Staten hun strafwetgeving – althans op materieelrechtelijk vlak (zie randnr. 4) – hadden aangepast, gaf ook het Belgische Parlement uiteindelijk op 28 november 2000 zijn zegen aan de langverwachte wet inzake informaticacriminaliteit (hierna: 'WIC')[8]. Naast een aanvulling van de Telecommunicatiewet[9] en een aantal wijzigingen aan de 'tapmaatregel' in art. 90ter e.v. Sv., voerde de WIC op materieelrechtelijk vlak vier nieuwe, zogenaamd 'specifieke'[10], informaticamisdrijven in in het Strafwetboek, en op procedureel vlak twee bijkomende onderzoekshandelingen in het Wetboek van Strafvordering, namelijk de 'netwerkzoeking' en het 'databeslag', die kunnen worden beschouwd als bijzondere modaliteiten van de gemeenrechtelijke zoeking en inbeslagneming.
Tijdens de parlementaire werkzaamheden van de WIC, werd door commissielid Poncelet uitdrukkelijk gewezen op de laattijdigheid van het wetsontwerp[11]. Ook Verbiest en Dervaux noemen de Belgische wetgever "*[un] élève quelque peu tardif de la classe européenne*"[12]. Die berisping lijkt ons evenwel enkel terecht voor wat betreft de materieelrechtelijke aspecten van de strafwetgeving. Zo schreef de Franse '*loi Godfrain*'[13] weliswaar reeds in 1988 een aantal 'informaticagerelateerde' misdrijven in in de *Code pénal*, maar bleef een aanpassing van de strafprocedure uit tot 18 maart 2003[14]. De

---

5 Aanbeveling R(95) 11 september 1995 van het Comité van Ministers aan de lidstaten betreffende problemen van strafprocesrecht inzake informatietechnologie, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2.

6 Verdrag van Boedapest inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van 23 november 2001, *European Treaty Series No. 185* en http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc.

7 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 619.

8 Wet 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 2909.

9 Wet 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 23 april 1991, 8388.

10 J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, afl. 2, (44) 44.

11 Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 26.

12 T. VERBIEST en J. DERVAUX, "La criminalité informatique dans tous ses états", *TBH* 2002, afl. 8, (607) 607.

13 Loi du 5 janvier 1988 relative à la fraude informatique, *JORF* 6 janvier 1988, 231.

14 Loi du 18 mars 2003 pour la sécurité intérieure, *JORF* 19 mars 2003, 4761.

Nederlandse 'Wet Computercriminaliteit I' van 23 december 1992[15] voorzag daarentegen wel reeds in enkele procedurele aanpassingen die evenwel later – vooral inzake de inbeslagneming van elektronische gegevens – ontoereikend bleken, zodat men pas in 2006[16] slaagde in een volwaardige modernisering van de strafprocedure, terwijl de Belgische wetgever reeds zes jaar voordien zowel de zoeking als de inbeslagneming in belangrijke mate had vernieuwd.

Dit werkstuk vormt een bescheiden poging een overzicht te bieden van de toepassingsmogelijkheden van die twee onderzoeksdaden in een geïnformatiseerde omgeving. Het voornaamste doel daarbij ligt in het verduidelijken van een aantal bekende en minder bekende juridische problemen met behulp van de uitgebreide parlementaire werkzaamheden en in het benadrukken van enkele blijvende knelpunten in de nieuwe wetgeving. Het weze evenwel nu reeds opgemerkt dat de WIC over het algemeen wordt beschouwd als een voorbeeld van geslaagd wetgevend optreden[17]. Gelet op de bijzonder beperkte toepassing ervan in de rechtspraak en bijgevolg het geringe aantal concrete voorbeelden van praktische toepassingsproblemen, is het geen sinecure de juistheid van die bewering na te gaan. Toch lijkt de huidige situatie voor enige verbetering vatbaar, zoals verder zal worden betoogd in een noodzakelijk abstracte analyse. Immers, om nog maar eens met Bacon te spreken: *"new laws are like the apothecarics' drugs; though they remedy the disease, yet they trouble the body"*.

2. ONDERZOEK

Hieronder worden de zoeking en de inbeslagneming achtereenvolgens besproken, waarbij telkens in een eerste onderdeel de nog steeds van kracht zijnde gemeenrechtelijke regelgeving wordt toegepast in een geïnformatiseerde omgeving en vervolgens in een tweede onderdeel de bijzondere, door de WIC ingevoerde modaliteiten worden toegelicht. De zogenaamde 'medewerkingsplicht' krijgt een afzonderlijk hoofdstuk toebedeeld, aangezien zij zowel geldt voor de zoeking als voor de inbeslagneming. Ook de grensoverschrijdende aspecten van beide onderzoeksdaden worden afzonderlijk behandeld, vermits een zoeking over de staatsgrenzen heen

[15] Wet 23 december 1992 tot aanvulling van het Wetboek van Strafrecht, het Wetboek van Strafvordering, de Wet voorlopige regeling schadefonds geweldsmisdrijven en andere wetten met voorzieningen ten behoeve van slachtoffers van strafbare feiten (computercriminaliteit I), *Stb*. 1993, 33.

[16] Wet 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), *Stb*. 2006, 300.

[17] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 8; I. DELBROUCK, "Informaticacriminaliteit" in H. BERKMOES, W. BRUGGEMAN, I. DELBROUCK, D. DEWANDELEER, F. DESTERBECK, H. FRANSEN, P. HERBOTS, A. MARUT, C. NUYTS, E. VAN DEN HEUVEL *et al.*, *Postal Memorialis*, Antwerpen, Kluwer, 2007, (122) 144.

rechtstreekse gevolgen heeft voor de inbeslagneming van de aldus aangetroffen gegevens.

2.1. ZOEKING

Naargelang de zoeking plaatsvindt in één welbepaald informaticasysteem, dan wel in meerdere informaticasystemen die zich bevinden op geografisch verspreide punten maar door middel van een netwerk met elkaar verbonden zijn, kan een onderscheid worden gemaakt tussen respectievelijk de unilokale zoeking enerzijds, die wordt beheerst door de gemeenrechtelijke regelgeving, en de bijzondere modaliteit van de 'netwerkzoeking' anderzijds, die per definitie een multilokaal karakter heeft.

2.1.1. Unilokale zoeking

Elk initieel bevel tot zoeking in een informaticasysteem geschiedt overeenkomstig de gemeenrechtelijke regelgeving die reeds bestond vóór de inwerkingtreding van de WIC. Anders dan de Nederlandse wetgever bijvoorbeeld, die in art. 125i Sv. voor de 'doorzoeking van een plaats ter vastlegging van gegevens', uitdrukkelijk verwijst naar de gemeenrechtelijke regelgeving, heeft het Belgische Parlement er evenmin als de Franse wetgever[18] voor geopteerd zulks expliciet te bepalen, hetgeen te wijten kan zijn aan het feit dat België en Frankrijk pas enkele jaren na Nederland zijn overgegaan tot procedurele aanpassingen (zie randnr. 4), zodat de praktijk intussen via interpretatietechnieken reeds bepaalde leemten had weten op te vullen.

Toch lijkt de huidige Belgische wetgeving ter zake te kort te schieten. Zo is het zeer de vraag in welke mate de gemeenrechtelijke voorwaarden kunnen worden toegepast op de zoeking in een informaticasysteem. De weinige auteurs die die vraag uitdrukkelijk behandelen, zijn geneigd een unilokale zoeking gelijk te schakelen met een huiszoeking. Zo moeten volgens Verstraeten de informaticagegevens van een persoon beschouwd worden als "*vallende onder de persoonlijke levenssfeer*" en is de doorzoeking ervan bijgevolg "*aan dezelfde voorwaarden onderworpen […] als de huiszoeking*"[19], zodat, behoudens in de gevallen van toestemming of ontdekking op heterdaad, een bevel van de onderzoeksrechter vereist is. Ook Meunier is die mening toegedaan, overwegende dat "*[c]e parallélisme justifie que l'ordinateur se voie également reconnaître un statut calqué sur l'inviolabilité dont la*

[18] B. BOULOC, *Procédure pénale*, Parijs, Dalloz, 2007, 390.

[19] R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 459; F. VERBRUGGEN en R. VERSTRAETEN, *Strafrecht en strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2007, 210.

Constitution et certains traités internationaux dotent le domicile"[20].

Als uitgangspunt is die stelling uiteraard verdedigbaar op grond van de in het strafrecht algemeen aanvaarde en zelfs wenselijk te achten redenering naar analogie in het voordeel van de verdachte. Bovendien lijkt ook de wetgever ervan uit te gaan dat een unilokale zoeking in een informaticasysteem enkel kan worden bevolen door een onderzoeksrechter, gelet op de inleidende bewoordingen in het door art. 8 WIC ingevoegde art. 88ter Sv. "*[w]anneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan*". Het gebruik van het voornaamwoord 'wanneer' in plaats van 'indien', wijst immers eerder dan op een voorwaarde voor het bevelen van een netwerkzoeking (zie ook randnr. 54), op de erkenning van een bestaande rechtspraktijk.

De rechtswaarde van een dergelijke preambule mag evenwel niet worden overschat. Zo staat immers als een paal boven wetgevend water dat een zoeking in een informaticasysteem ook zonder het bevel van een onderzoeksrechter kan plaatsvinden, bijvoorbeeld in de gevallen van toestemming of ontdekking op heterdaad (zie randnr. 9). Bovendien lijken bepaalde auteurs, zoals Van den Wyngaert[21] maar ook De Hert en Lichtenstein[22], minstens impliciet te suggereren dat ook de procureur des Konings kan overgaan tot een dergelijke zoeking. Uit de parlementaire werkzaamheden blijkt daarenboven duidelijk dat, hoewel commissielid Charles Michel opmerkt dat de tekst van art. 88ter Sv. "*uitgaat van een huiszoekingsbevel*"[23], de wetgever wel degelijk ook andere situaties voor ogen had. Zo bevatte het oorspronkelijke wetsontwerp onmiddellijk na de hierboven beschreven inleidende bewoordingen, nog de vermelding "*hetzij in het kader van een huiszoeking, hetzij anderszins*"[24]. Nadat die tweede optie was 'weggeamendeerd' tijdens de eerste behandeling in de Senaat[25], besloot de minister de zinsnede in haar geheel te schrappen, rekening houdende met "*de realiteit van draagbare computers*" en "*mobiele telecommunicatie*"[26]. Daarnaast heeft de wetgever, door de procureur des Konings in het nieuwe art. 39bis Sv. uitdrukkelijk de mogelijkheid te geven om over te gaan tot databeslag (zie randnr. 99), impliciet te kennen gegeven dat ook hij een

[20] 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.

[21] C. VAN DEN WYNGAERT, *Strafrecht, strafprocesrecht & internationaal strafrecht in hoofdlijnen*, Antwerpen, Maklu, 2006, 973.

[22] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 63.

[23] Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 62.

[24] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 37.

[25] Amendement (N. DE T' SERCLAES), *Parl.St.* Senaat 1999-2000, nr. 2-392/002.

[26] Amendement (Regering), *Parl.St.* Kamer 1999-2000, nr. 50-0213/010.

zoeking in een informaticasysteem kan laten verrichten.

Toch lijkt ook bijvoorbeeld de correctionele rechtbank te Brussel, net als Verstraeten en Meunier (zie randnr. 9), van oordeel te zijn dat "*une […] recherche informatique n'est […] admissible qu'aux mêmes conditions qu'une perquisition*"[27], waarbij zij verwijst naar het advies van de Raad van State bij de WIC dat vermeldt dat een netwerkzoeking de mogelijkheid biedt "*d'étendre une perquisition depuis le système désigné par le mandat qui l'autorise*"[28]. Daarbij lijkt de rechtbank evenwel de Nederlandstalige versie van de tekst over het hoofd te zien, waarin '*perquisition*' niet met 'huiszoeking' wordt vertaald, maar wel met 'opsporing', hetgeen dat advies onzes inziens in een heel ander daglicht stelt.

Aldus rijst de vraag of, indien de zoeking in een informaticasysteem geen deel uitmaakt van een meer algemene huiszoeking, nog steeds in alle gevallen buiten die van toestemming of ontdekking op heterdaad, een bevel van de onderzoeksrechter vereist moet worden. Verstraeten lijkt alvast te betogen van wel (zie randnr. 9), maar, zoals hierboven reeds aangestipt (zie randnr. 10), kan die stelling slechts als uitgangspunt gelden. Andere rechtsleer vermijdt dit vraagstuk liever en gaat blijkbaar gemakshalve uit van het reeds voorhanden zijn van een huiszoekingsbevel. Het lijkt ons dan ook wenselijk in dit werkstuk een bescheiden antwoord te bieden op de vraag welke aspecten van de gemeenrechtelijke regeling inzake de huiszoeking effectief kunnen worden toegepast op de zoeking in een informaticasysteem, aan de hand van een eigen indeling naargelang de aard van het systeem en de plaats waarop het zich bevindt.

a. Private informaticasystemen op private plaatsen

Indien het informaticasysteem zich bevindt op een plaats die niet toegankelijk is voor het publiek, zoals een privéwoning of een privéclub[29], behoeft het geen betoog dat de doorzoeking ervan enkel kan worden bevolen onder de voorwaarden die gelden voor een huiszoeking. Een dergelijke zoeking kan immers worden beschouwd als "*une modalité de la perquisition*"[30], op voorwaarde uiteraard dat de zoeking 'binnenskamers' blijft (zie randnr. 63). Wel wordt in de Belgische rechtsleer – net zoals in de Nederlandse overigens[31] – aangenomen dat "*wanneer een huiszoekingsbevel werd afgeleverd en een informaticasysteem aanwezig is in de woning waarop het*

[27] Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, afl. 2, 149, noot, gewijzigd door Brussel 26 juni 2008, *T.Strafr.* 2008, afl. 6, 467, noot.
[28] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 46.
[29] F. VERBRUGGEN en R. VERSTRAETEN, *Strafrecht en strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2007, 207-208.
[30] Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, afl. 2, 149, noot, gewijzigd door Brussel 26 juni 2008, *T.Strafr.* 2008, afl. 6, 467, noot.
[31] C. VAN DIJK en J. KELTJENS, *Computercriminaliteit*, Zwolle, Tjeenk Willink, 1995, 224-226.

huiszoekingsbevel betrekking heeft, geen afzonderlijk bevel vereist is voor de zoeking in dit informaticasysteem"[32]. Ook de voorafgaande schriftelijke toestemming tot huiszoeking overeenkomstig art. 1bis Huiszoekingswet[33], treft de volledige woning met inbegrip van de aldaar aanwezige informaticasystemen, tenzij de toestemming werd beperkt tot bepaalde delen ervan[34].

b. Private informaticasystemen op openbare plaatsen

Minder voor de hand liggend is het geval waarin een informaticasysteem dat toebehoort aan een privépersoon, zich bevindt op een openbare plaats. Te denken valt aan de druk bezette zakenman die in een treinstation een aantal documenten doorneemt op zijn draagbare computer. Voortbouwend op de hierboven als uitgangspunt verdedigde stelling van Verstraeten (zie randnrs. 9-10), moet ook in dit geval een bevel worden geëist van de onderzoeksrechter. Het loutere feit dat het private informaticasysteem zich bevindt op een openbare plaats, doet immers niets af aan het vertrouwelijke karakter van de daarin opgeslagen gegevens.

Toch kunnen in dit geval, anders dan in het vorige (zie randnr. 14), niet alle voorwaarden die gelden voor de huiszoeking, onverkort worden toegepast op de zoeking in een informaticasysteem wanneer dat zich bevindt op een openbare plaats. Van zodra het informaticasysteem de woning verlaten heeft, moet immers worden aangenomen dat het ook buiten de beschermende sfeer treedt van die rechten die wezenlijk verbonden zijn met de woning. Als mogelijk criterium van onderscheid kan bijgevolg de vraag gelden of de voorwaarde wel een bescherming beoogt te bieden aan het recht op eerbiediging van het privéleven, gewaarborgd door art. 8 EVRM en art. 17 IVBPR, hetgeen duidelijk het geval is bij de vereiste van een huiszoekingsbevel, wat dan ook een analogische toepassing op de zoeking in een informaticasysteem verantwoordt. Hetzelfde geldt bijvoorbeeld voor de vereiste van een voorafgaande schriftelijke toestemming in de zin van art. 1bis Huiszoekingswet, die overigens een "*algemeen geldende regel inhoudt, […] ongeacht of de opsporingen of huiszoekingen 's nachts of overdag plaatshebben*"[35], en een gelijkaardige redenering gaat op voor de bijzondere voorwaarden die gelden voor een huiszoeking bij personen onderworpen aan een beroepsgeheim. De tijdsvoorwaarden van art. 1 Huiszoekingswet lijken daarentegen niet zozeer het recht op eerbiediging van het privéleven te

[32] R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 459; F. VERBRUGGEN en R. VERSTRAETEN, *Strafrecht en strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2007, 210.

[33] Wet 7 juni 1969 tot vaststelling van de tijd gedurende welke geen opsporing ten huize of huiszoeking mag worden verricht, *BS* 28 juni 1969, 6470.

[34] F. VERBRUGGEN en R. VERSTRAETEN, *Strafrecht en strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2007, 208; Pol. Roeselare 25 januari 1990, *T.Vred.* 1991, 128.

[35] Cass. (2de k.) 3 december 1996, AR P960257N, *AJT* 1998-99, 20, noot L. ARNOU, *Arr.Cass.* 1996, 1154, *Bull.* 1996, 1226, *Pas.* 1996, I, 1226 en *RW* 1996-97, 1361.

beschermen, doch eerder het door art. 15 GW gewaarborgde recht op onschendbaarheid van de woning en het rustig woongenot, die geen van beide ter zake doen wanneer het informaticasysteem zich niet bevindt in die woning. Om die reden moet dan ook worden aangenomen dat zij niet van toepassing kunnen zijn op de zoeking in een informaticasysteem op een openbare plaats.
Een tweede probleem dat enige opheldering verdient, betreft de vraag of een zoeking in een informaticasysteem kan worden bevolen via een zogenaamde 'mini-instructie'. Ook hier kan de regelgeving die geldt voor de huiszoeking, niet zonder meer van toepassing worden geacht. Er anders over oordelen, zou immers aanleiding geven tot de paradoxale situatie waarin een unilokale zoeking niet zou kunnen worden bevolen via mini-instructie – art. 28septies Sv. sluit de huiszoeking immers uitdrukkelijk uit van zijn toepassingsgebied – terwijl algemeen wordt aanvaard dat zulks wel mogelijk is voor een netwerkzoeking[36] (zie ook randnr. 61). Die laatste mogelijkheid zou nagenoeg inhoudloos worden indien reeds een gerechtelijk onderzoek zou moeten worden opgestart om de oorspronkelijke situatie van een unilokale zoeking tot stand te brengen.

c. Openbare informaticasystemen

Ten slotte kan de vraag worden gesteld aan welke voorwaarden de doorzoeking van een informaticasysteem is onderworpen, dat op zichzelf een openbaar karakter heeft, bijvoorbeeld een voor het publiek toegankelijke computer in een openbare bibliotheek. In een onopvallende voetnoot stelt Meunier dat "*il nous paraît évident que, si l'ordinateur est un ordinateur public […] ces restrictions ne s'imposeront pas*"[37]. Het lijkt ons evenwel belangrijk ook die stelling enigszins te nuanceren. Theoretisch zijn twee uiterste standpunten denkbaar. Een eerste, collectivistische benadering – waar Meunier lijkt op aan te sturen – zou kunnen inhouden dat de sporen van de door de gebruiker verrichte operaties, delen in het openbaar karakter van het informaticasysteem waarin zij zijn opgeslagen, zodat geen bevel van de onderzoeksrechter is vereist. Een tweede, meer individualistische visie zou kunnen leren dat die gegevens hun private karakter behouden, ongeacht de aard van het informaticasysteem. Aan de hand van een aantal noodzakelijk fictieve voorbeelden, wordt hieronder een poging ondernomen om die twee uitersten met elkaar te verzoenen in een tussenstelling.

Zolang voor de op het informaticasysteem uitgevoerde operaties geen wachtwoord of een andere bijzondere machtiging vereist is, lijkt het collectivistische standpunt van Meunier verdedigbaar. Zo zal het doorzoeken van de sporen die door een naar kinderpornografie surfende bibliotheekbezoeker werden achtergelaten in de *temporary internet files* (zie

[36] C. VAN DEN WYNGAERT, *Strafrecht, strafprocesrecht & internationaal strafrecht in hoofdlijnen*, Antwerpen, Maklu, 2006, 973.
[37] 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.

ook randnr. 118) van een openbare computer, ook kunnen geschieden zonder het bevel van een onderzoeksrechter. Voor het bezoeken van dergelijke voor het publiek toegankelijke webpagina's, is immers geen bijzondere machtiging vereist. Bovendien valt moeilijk in te zien waarom voor de doorzoeking van op een openbare plaats achtergelaten beeldmateriaal in de regel geen bevel van een onderzoeksrechter is vereist, terwijl wanneer dat materiaal in elektronische vorm werd achtergelaten, opeens wel een dergelijk bevel zou moeten worden afgeleverd.

Geheel anders is evenwel het geval waarin een zakenman op een openbare computer een aantal e-mailberichten bekijkt die bijvoorbeeld belangrijke aanwijzingen zouden bevatten over prijsafspraken met een concurrent. Om toegang te krijgen tot een e-mailaccount, moet immers een wachtwoord worden ingevoerd, zodat de gebruiker erop mocht rekenen dat de gegevens die hij via die beveiligde verbinding verzendt en ontvangt, hun vertrouwelijke karakter niet verliezen, zelfs indien geen wachtwoord meer moet worden ingevoerd voor het in het kader van een unilokale zoeking opnieuw raadplegen van de intussen op de harde schijf opgeslagen sporen. De doorzoeking van dergelijke gegevens kan onzes inziens dan ook enkel plaatsvinden op rechterlijk bevel.

Die laatste hypothese zal zich in de praktijk evenwel niet dikwijls voordoen. Wanneer de te raadplegen gegevens zich bevinden op een andere plaats dan die waar de unilokale zoeking materieel plaatsvindt, zoals bijvoorbeeld het geval is voor het doorzoeken van de nog ongelezen berichten in een hotmailaccount (zie randnr. 66), moet immers een netwerkzoeking plaatsvinden die hoe dan ook enkel kan geschieden op rechterlijk bevel (zie randnr. 61). Bevinden de gegevens zich wel in het onderzochte informaticasysteem, dan is het bovendien niet uitgesloten dat de overheid, teneinde toegang te krijgen tot de gegevens, alsnog moet beschikken over het juiste wachtwoord, dat zij doorgaans slechts te weten kan komen ofwel doordat de betrokkene zijn toestemming heeft gegeven tot de zoeking, in welk geval de procureur des Konings volledig bevoegd is om de zoeking verder te zetten (zie immers randnr. 9), ofwel doordat een informaticus via een bevel tot medewerking werd opgedragen het wachtwoord te achterhalen, hetgeen reeds de tussenkomst van een onderzoeksrechter veronderstelt (zie randnr. 102). Het lijkt erop dat deze hypothese zich in de praktijk bijna uitsluitend zal voordoen wanneer geen wachtwoord meer moet worden ingevoerd voor het bekijken van via een beveiligde verbinding ontvangen gegevens, zoals bijvoorbeeld de *cache*-versies van reeds geopende webmailberichten. Toch is zij ook in andere situaties niet helemaal uitgesloten. Zo is het mogelijk dat een andere persoon dan de gebruiker, bijvoorbeeld diens echtgenoot, de overheid uit vrije wil in kennis stelt van het juiste wachtwoord. Bij gebrek aan toestemming van de gebruiker zelf, is de procureur des Konings in dat geval niet bevoegd om op eigen initiatief tot een zoeking over te gaan, en aangezien het wachtwoord uit vrije wil werd meegedeeld, moest de medewerking niet worden bevolen door

een onderzoeksrechter. Ook in dat geval moet evenwel worden aangenomen dat alsnog een bevel van de onderzoeksrechter vereist is, hetgeen verantwoord wordt door het beveiligde karakter van de gegevens.

Bij een aandachtig lezer kan ten slotte reeds de vraag zijn gerezen wat de in dit werkstuk verdedigde verschillende behandeling verantwoordt van de gebruiker die op een openbaar informaticasysteem naar kinderpornografie surft, en hij die precies diezelfde verrichtingen doet op een eigen informaticasysteem dat zich bevindt op een openbare plaats. Hierboven werd immers betoogd dat voor het doorzoeken van de *temporary internet files* bijvoorbeeld, in het eerste geval geen bevel van de onderzoeksrechter moet worden vereist (zie randnr. 19) en in het tweede geval wel (zie randnr. 15). Die nadelige behandeling van de gebruiker van een openbare computer kan worden gestaafd op grond van twee argumenten, namelijk het openbaar karakter van het informaticasysteem en de afwezigheid van dwang of geweld bij het doorzoeken ervan.

Een eerste argument wordt gevormd door het openbaar karakter van het informaticasysteem. Met een juridische metafoor zou men immers kunnen stellen dat er 'vermenging' plaatsvindt tussen de door de private gebruiker ingevoerde gegevens en het geheel van de reeds in het informaticasysteem opgeslagen openbare informatie (zie randnr. 19), tenzij die vermenging wordt verhinderd door een bepaalde vorm van beveiliging (zie randnr. 20). Het informaticasysteem dient dan ook te worden beschouwd als een 'voor het publiek toegankelijke plaats', waarvoor geen bevel moet worden afgeleverd door de onderzoeksrechter. Een dergelijke vermenging kan evenwel in geen geval plaatsvinden in een privaat informaticasysteem. Het feit dat het zich zou bevinden op een openbare plaats, doet daaraan niets af. Als criterium moet namelijk in aanmerking worden genomen het karakter van het informaticasysteem zelf en niet de plaats waar dat systeem zich bevindt. Er anders over oordelen, zou immers tot gevolg hebben dat ook bijvoorbeeld een handtas en andere persoonlijke zaken een openbaar karakter zouden krijgen van zodra zij verplaatst worden naar een openbare plaats.

De verschillende behandeling is bovendien verdedigbaar op grond van de afwezigheid van dwang of geweld bij het doorzoeken van een openbaar informaticasysteem, dat immers per definitie toegankelijk is voor iedereen en dus ook voor de overheid. Van zodra de gebruiker een openbaar informaticasysteem verlaten heeft, verliest hij het recht om zich te verzetten tegen het gebruik ervan door een ander (zie evenwel randnr. 20). Zulks is fundamenteel verschillend voor een privaat informaticasysteem, waarop de gebruiker immers een eigendomsrecht kan laten gelden, zodat elke niet toegestane doorzoeking ervan, in beginsel een vorm van dwang uitmaakt.

d. Besluit

Uit het voorgaande kan worden besloten dat de zoeking in een informaticasysteem slechts in beginsel onderworpen moet worden aan de voorwaarden die gelden voor de huiszoeking, zodat de hierboven als uitgangspunt verdedigde stelling (zie randnrs. 9-10) enige nuancering behoeft. Zo kunnen voor de zoeking in een privaat informaticasysteem dat zich bevindt op een openbare plaats, enkel die voorwaarden van toepassing worden geacht die werkelijk een bescherming beogen te bieden aan het recht op eerbiediging van het privéleven (zie randnr. 16). Bovendien moet worden aanvaard dat ook een unilokale zoeking in een dergelijk informaticasysteem, kan worden bevolen via de techniek van de mini-instructie (zie randnr. 17). Ten slotte werd hierboven verdedigd dat de doorzoeking van gegevens opgeslagen in een openbaar informaticasysteem, moet kunnen plaatsvinden zonder het bevel van een onderzoeksrechter (zie randnr. 19), tenzij die gegevens hun private karakter blijven behouden dankzij een bepaalde beveiliging (zie randnr. 20).

2.1.2. Multilokale zoeking ('netwerkzoeking')

Een belangrijk nadeel van de zoeking in een informaticasysteem overeenkomstig de gemeenrechtelijke regeling is dat zij, zoals de memorie van toelichting van de WIC aangeeft, "*enkel mag worden uitgevoerd ten aanzien van de plaats waarvoor ze werd bevolen*"[38]. Steeds vaker echter worden verschillende informaticasystemen met elkaar verbonden door middel van netwerken, waardoor de kans bestaat dat bepaalde, voor het onderzoek relevante elektronische gegevens "*zich niet op dezelfde plaats [bevinden] als waar het onderzoek materieel plaats heeft*", terwijl die gegevens daar niettemin "*beschikbaar [zijn] door middel van een netwerk*"[39]. Vóór de inwerkingtreding van de WIC bestond de enige mogelijkheid om die gegevens te doorzoeken, in het uitvoeren van verschillende huiszoekingen op de diverse plaatsen waar de gegevens zich materieel bevinden, behoudens, zoals hierboven verdedigd (zie randnr. 19), in het uitzonderlijke geval waarin die gegevens opgeslagen zouden zijn in een openbaar informaticasysteem.

Het behoeft geen betoog dat die situatie aanleiding gaf tot een aantal juridische patstellingen. Zo is het niet ondenkbaar dat speurders tijdens een unilokale zoeking bepaalde gegevens aantreffen waarvan zij de precieze locatie niet kunnen vaststellen of waarbij het achterhalen van die locatie enige tijd in beslag neemt, zodat het risico bestaat dat "*bewijsmateriaal […] vernietigd*,

[38] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 22; P. DE HERT, en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 64.

[39] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 64.

gewijzigd of verplaatst wordt"[40]. Ten slotte is het duidelijk dat, zelfs indien de precieze locatie van de verschillende gegevens vrijwel meteen kan worden vastgesteld, het uitvoeren van diverse huiszoekingen op al die plaatsen veelal een onevenredige maatregel uitmaakt, die voor de overheid erg tijdrovend kan zijn en voor de burger bijzonder ingrijpend.

Door de onderzoeksrechter in art. 88ter Sv. uitdrukkelijk de mogelijkheid te verschaffen om een unilokale zoeking in een informaticasysteem uit te breiden tot een multilokale netwerkzoeking, verhielp de wetgever in grote mate aan de hierboven geschetste belemmeringen. Toch laat de huidige wetgeving een aantal belangrijke vragen onbeantwoord. In dit onderdeel wordt het jonge art. 88ter Sv. dan ook op zijn juridische deugdelijkheid beoordeeld en wordt de vinger gelegd op een aantal oude zere plekken en op enkele gloednieuwe, door de WIC zelf geslagen wonden.

a. Het begrip 'informaticasysteem'

Onder de gemeenrechtelijke regelgeving, zoals hierboven geschetst in het kader van de unilokale zoeking, was een duidelijke omschrijving van het begrip 'informaticasysteem' geen absolute noodzaak. Nu de wetgever echter zelf die term in de mond neemt, stelt zich een belangrijk afbakeningsprobleem. In art. 88ter Sv. is immers noch een eenduidige definitie te vinden, noch een exemplatieve lijst die aangeeft wat precies bedoeld wordt met een 'informaticasysteem'. Toch valt die 'open' werkwijze, zeker in een algemeen wetgevend kader als het Wetboek van Strafvordering, eerder toe te juichen dan af te keuren. Op die manier wordt de rechtspraktijk immers in de mogelijkheid gesteld om de technologische evolutie op de voet te volgen. Bovendien kan bij het invullen van het begrip maximaal rekening worden gehouden met meer uitgebreide interpretatiebronnen, zoals de parlementaire werkzaamheden, waarin de wetgever overigens zelf verklaart 'technologie-neutraal' te willen zijn[41].

De memorie van toelichting geeft aan dat het begrip 'informaticasysteem' doelt op "*alle systemen voor de opslag, verwerking of overdracht van data*", waarbij "*vooral gedacht [wordt] aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT*"[42]. Het weze dus duidelijk dat het begrip 'informaticasysteem' in de ruimste zin moet worden uitgelegd, rekening houdend met het doel van de wet. Van zodra een systeem zich leent tot het uitwisselen van elektronische gegevens,

[40] J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, afl. 2, (44) 60.

[41] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 12.

[42] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 12.

moet, in het kader van een netwerkzoeking, aanvaard worden dat het gaat om een informaticasysteem. Aldus moet worden aangenomen dat ook voor een 'permanente en stabiele' (zie randnr. 48) verbinding tussen twee gsm-toestellen bijvoorbeeld, in beginsel een netwerkzoeking kan worden bevolen.

b. Inhoud en draagwijdte van de maatregel

Overeenkomstig art. 88ter §1 lid 1 Sv. kan een onderzoeksrechter die "*een zoeking beveelt in een informaticasysteem of een deel daarvan*", die zoeking uitbreiden naar "*een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt*". Die uitbreiding mag zich evenwel, aldus art. 88ter §2 Sv., "*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*". De draagwijdte van de maatregel wordt derhalve beperkt door twee belangrijke factoren, die echter niet altijd even duidelijk van elkaar worden onderscheiden, noch in de rechtsleer, noch in de parlementaire werkzaamheden. Desondanks is het belangrijk hier een dubbele beperking in te lezen, die in dit werkstuk wordt ontleed in een subrogatievoorwaarde enerzijds en een specialiteitsvoorwaarde anderzijds.

Alvorens dieper in te gaan op elk van die beperkingen, moet worden benadrukt dat, wat betreft de inhoud van de maatregel, de netwerkzoeking, evenals het databeslag (zie randnr. 72), door de wetgever strikt wordt onderscheiden van een overeenkomstig art. 90ter e.v. Sv. bevolen 'informaticatap', die immers "*betrekking heeft op het capteren van data in transmissie*"[43], en bijgevolg, in tegenstelling tot de 'statische' netwerkzoeking, eerder een 'dynamisch' karakter vertoont. Anders dan waar haar naamgeving op het eerste gezicht lijkt op aan te sturen, wordt tijdens een netwerkzoeking dus niet zozeer het netwerk zelf onderzocht, maar wel de informaticasystemen die via dat netwerk in verbinding staan met het informaticasysteem waarin de oorspronkelijke zoeking plaatsvindt. Aldus dient de onderzoeksrechter die bepaalde elektronische gegevens wil doorzoeken, vooraf na te gaan of die gegevens nog 'in overbrenging' zijn, in welk geval een informaticatap moet worden bevolen met inachtneming van bijvoorbeeld de beperkingen voortvloeiend uit art. 90ter Sv., dan wel hun bestemming reeds hebben bereikt, in welk geval kan worden overgegaan tot een netwerkzoeking.

Het spreekt voor zich dat een dergelijk onderscheid in de praktijk niet altijd even eenvoudig te maken is. Zo merkt Dewandeleer op dat de wetgever zelf ooit – bij het invoeren van art. 314bis Sw. – het begrip 'overbrenging' heeft

[43] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 21.

omschreven als "*het traject tussen de zender en de ontvanger*"[44], maar voegt hij daar meteen aan toe dat "*[w]aar dat traject in het geval een telefoongesprek in reële tijd eenvoudig kan worden afgebakend, […] de kwestie complexer [wordt] wanneer er geen sprake is van een 'live' gesprek*"[45], bijvoorbeeld bij voicemail- of e-mailberichten, die immers een bijkomende tussenkomst vereisen vanwege de bestemmeling, teneinde kennis te kunnen nemen van hun inhoud.

In de rechtsleer leven dan ook uiteenlopende opvattingen omtrent het begrip 'overbrenging' en de vraag wanneer de communicatie tussen zender en ontvanger van bijvoorbeeld een e-mailbericht tot een einde komt. Een eerste, eerder restrictieve strekking beschouwt de invulling van het begrip 'overbrenging' als een louter technische aangelegenheid. In die zin stelt Vandermeersch bijvoorbeeld dat "*la communication n'est plus […] en cours de transmission lorsqu'elle est stockée par le fournisseur d'accès sur son disque dur*", in welk geval "*ce dernier agit, en quelque sorte, comme mandataire du destinataire pour recevoir le message et le mettre en mémoire à disposition de ce dernier*"[46]. Ook Meunier lijkt een dergelijke restrictieve interpretatie toegenegen, gelet op zijn opmerking dat "*la consultation, par le magistrat, d'e-mails après délivrance à leur destinataire, ou des messages stockés sur le serveur d'un fournisseur de messagerie dans l'attente de la délivrance à l'abonné, ne relève pas de l'interception de télécommunications, mais plutôt de la recherche informatique*"[47].

Geheel terecht verwijt Dewandeleer een dergelijke strikt technische uitlegging van het 'traject tussen zender en ontvanger' (zie randnr. 33) het toepassingsgebied van de informaticatap al te drastisch in te perken, "*nu het vaak slechts zal handelen om een tijdsfractie van enkele seconden*"[48]. Meer verdedigbaar is dan ook zijn ruimere interpretatie dat "*de transmissie van het bericht pas voltooid zal zijn wanneer het ('fysiek') de mailbox van de bestemmeling zal hebben bereikt*"[49], zonder dat evenwel vereist moet worden

---

[44] Wetsontwerp ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, *Parl.St.* Senaat 1992-93, nr. 843-1, 6.

[45] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 153.

[46] D. VANDERMEERSCH, "Le droit pénal et la procédure pénale confrontés à internet (les apprentis surfeurs)" in P. MANDOUX en C. DOUTRELEPONT (eds.), *Internet sous le regard du droit*, Brussel, Editions du jeune barreau de Bruxelles, 1997, (243) 253.

[47] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 661.

[48] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 154.

[49] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 154.

dat de bestemmeling het bericht ook daadwerkelijk heeft gelezen, hetgeen hij enerzijds onderbouwt met de 'analogische vaststelling' dat ook een klassieke brief zijn bestemmeling bereikt "*zodra de post […] in zijn brievenbus is gedeponeerd, […] ook indien de bestemmeling zijn post nog niet heeft geopend en gelezen*", en anderzijds met een vonnis van de correctionele rechtbank te Leuven waarin gesteld werd dat "*[e]en toegezonden e-mail [pas is] 'ontvangen' door de bestemmeling wanneer deze laatste zijn mailbox activeert en 'zijn' post kan openen en lezen*"[50].

Die ruimere interpretatie verdient navolging, niet alleen om de door Dewandeleer zelf aangehaalde redenen (zie randnr. 35), maar ook omdat zij de persoon ten aanzien van wie de tapmaatregel wordt bevolen, de beste strafprocesrechtelijke bescherming biedt en bijgevolg het meest nauw aansluit bij de bedoeling van art. 90ter Sv. "*de risico's voor de bescherming van de persoonlijke levenssfeer ten gevolge van de aanwending van deze uitzonderlijke maatregel zoveel mogelijk te beperken*"[51]. Het behoeft immers geen betoog dat het onderscheppen van gegevens tijdens de uitwisseling ervan, een grotere inbreuk uitmaakt op de persoonlijke levenssfeer van de verdachte dan het achteraf doorzoeken van die gegevens. Aangenomen moet dan ook worden dat de bijzondere bescherming geboden door art. 90ter Sv., blijft gelden tot aan het einde van de gehele communicatie tussen zender en ontvanger, zodat Dewandeleer terecht als enige relevante criterium teneinde te bepalen of het bericht nog 'in overdracht' is of niet, in aanmerking neemt het *opvragen* van het bericht door de bestemmeling – of eventueel op automatische wijze door diens *Mail User Agent* (zie ook randnr. 66) – hetgeen "*samenvalt met het ophalen van het bericht naar [zijn] persoonlijke mailbox*"[52].

Op welke wijze dat 'opvragen' geschiedt en vooral op welk tijdstip, is dan weer afhankelijk van het type mailbox dat wordt aangewend om de berichten te ontvangen en van de manier waarop die mailbox wordt gebruikt. In hun uitvoerige analyse onderscheiden Van Linthout en Kerkhofs drie 'situaties' waarvoor zij telkens een 'geïndiceerd noodzakelijk eindstation' bepalen, een begrip dat zij omschrijven als "*de plaats waar een mail gelet op zijn aard en de aard van de mailconfiguratie indicatief kan worden geacht noodzakelijk tot een eindpunt te zijn gekomen*"[53]. Een uitgebreid onderzoek van elk van die drie

---

[50] Corr. Leuven 4 december 2007, *T.Strafr.* 2008, afl. 3, 223, noot L. CEULEMANS.

[51] Verslag namens de commissie voor de justitie uitgebracht door de heer Pierre BEAUFAYS over het wetsontwerp ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en telecommunicatie, *Parl.St.* Kamer, 1993-94, nr. 1450/3, 4.

[52] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 155.

[53] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87; D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en

situaties zou het algemeen karakter van dit werkstuk evenwel ver overstijgen en verdient een meer gedetailleerde uiteenzetting. Toch kan niet zonder meer worden voorbijgegaan aan het verdienstelijke denkwerk van de auteurs, dat immers mede bepalend is voor het afbakenen van het toepassingsgebied van de netwerkzoeking, zodat hieronder een korte samenvatting wordt gegeven van hun analyse, gevolgd door enkele kritische bemerkingen.

Voor de eerste situatie, namelijk wanneer de bestemmeling van het bericht een popmailconfiguratie gebruikt, duiden de auteurs als 'geïndiceerd noodzakelijk eindstation' aan (zie ook randnr. 37) het informaticasysteem "*waarop de bestemmeling van de mail zijn popmailbox heeft geïnstalleerd*"[54]. Wordt daarentegen een webmailconfiguratie gebruikt, dan is dat eindstation "*de webmailbox die voor de bestemmeling beschikbaar is bij de webmailprovider*"[55]. Wordt ten slotte een popmailconfiguratie gebruikt 'als webmail', bijvoorbeeld een hotmailaccount gekoppeld aan het programma Outlook Express, "*dan is niet de webmailbox het geïndiceerd noodzakelijk eindstation, doch dan blijft daarentegen het [informaticasysteem] waarop de bestemmeling van de mail zijn popmailbox heeft geïnstalleerd […] het geïndiceerde noodzakelijk eindstation*"[56]. Aan dat eindstation komt een weerlegbaar vermoeden toe, zodat een onderzoeksrechter, behoudens tegenbewijs, ervan uit mag gaan dat bijvoorbeeld "*de popmail die zich (nog) bevindt in de webmailbox van de ISP en nog niet werd doorgesluisd naar de popmailbox op het [informaticasysteem] van de bestemmeling, zowel feitelijk als strafprocedureel kan worden vermoed nog steeds in transmissie te zijn*"[57].

Die operationele definitie van het begrip 'overbrenging'[58], werd door de auteurs ontwikkeld vanuit de vrees dat "*de onderzoeksrechter, en nadien de feitenrechters, [anders] in de onmogelijke situatie [zouden worden gebracht] dat een in verdenking gestelde – naar waarheid of gelogen – zonder meer de nietigheid van een beschikking van [art. 90ter Sv.] zou kunnen inroepen onder het gezegde dat hij de getapte popmail reeds gelezen had via webmail, dat aldus de communicatie reeds 'uit transmissie' was, en dat aldus niet overeenkomstig [art. 90ter Sv.] had mogen worden getapt*"[59]. Ofschoon

F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 156.

[54] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87.

[55] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87.

[56] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87.

[57] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87.

[58] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 157.

[59] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87.

uiteraard een terechte vrees, kan hierbij evenwel de vraag worden gesteld of het scheppen van een dergelijk vermoeden in het nadeel van de verdachte, buiten elke uitdrukkelijke wettelijke bepaling om, wel toelaatbaar is, vooral wanneer zulks louter gesteund wordt op de pragmatische overweging dat het bewijs of iemand al dan niet reeds kennis heeft genomen van het bericht, door het Openbaar Ministerie bijzonder moeilijk te leveren is. Toch moet het standpunt van Van Linthout en Kerkhofs in dezen worden bijgetreden, aangezien van de verdachte die beweert reeds kennis te hebben genomen van het bericht, toch een minimaal bewijs mag worden verwacht, dat door hem immers op relatief eenvoudige wijze te voeren is, bijvoorbeeld aan de hand van het voorleggen van bepaalde *temporary internet files*. Bovendien zal het belang dat de verdachte heeft bij het weerleggen van het vermoeden, in vele gevallen slechts marginaal zijn, vermits een vooruitziend onderzoeksrechter de gevolgen van een eventueel nietige informaticatap veelal zal opvangen door "*een gecumuleerde toepassing met [art. 88ter Sv.]*"[60], zodat het vaak slechts een theoretische discussie betreft omtrent de correcte rechtsgrond.

Die laatste overweging maakt evenwel tegelijkertijd duidelijk dat het voorstel van Van Linthout en Kerkhofs vooralsnog geen oplossing biedt voor het probleem dat de netwerkzoeking – althans in de 'heimelijke' fase van het onderzoek[61] – bijna automatisch zal worden gecumuleerd met een informaticatap en op die manier wordt gedegradeerd tot 'opvangnet' voor eventuele procedurele nietigheden. Zulks is onzes inziens niet alleen een weinig "*handige manier van werken*"[62], maar vormt bovendien een belangrijk probleem voor de rechtszekerheid van de verdachte en diens rechten van verdediging. Een al te ruime rechtsgrond is immers geen rechtsgrond meer. Het is overigens niet ondenkbaar dat, door de vaagheid van de grenzen tussen art. 90ter Sv. en art. 88ter Sv., de laagdrempelige voorwaarden voor het bevelen van een netwerkzoeking het uitzonderlijk karakter van een informaticatap besmetten in die zin dat een onderzoeksrechter die eigenlijk een informaticatap had moeten bevelen met inachtneming van de voorwaarden bepaald in art. 90ter Sv., die voorwaarden miskent door gegevens 'in overbrenging' te laten doorzoeken op grond van een bevel tot netwerkzoeking. In dat geval zullen de resultaten van dat onderzoek weliswaar niet kunnen worden gebruikt als bewijsmiddel, maar is de schade niettemin aangericht en de eerbiediging van het privéleven van de betrokkene geschonden.

---

[60] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 87.

[61] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 158; P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 94.

[62] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 94.

Ter illustratie van het voorgaande kan worden verwezen naar een arrest van de kamer van inbeschuldigingstelling te Gent van 27 september 2007[63], waarin de kamer werd geconfronteerd met een op foutieve wijze als netwerkzoeking opgevatte informaticatap. De onderzoeksrechter had immers, op grond van art. 88bis Sv. – doch allicht de toepassing van art. 88ter Sv. indachtig – een netwerkzoeking bevolen teneinde een hotmailaccount te doorzoeken waarvan achteraf evenwel bleek dat zij oneigenlijk werd gebruikt als 'elektronische valve'[64], zodat eigenlijk een informaticatap had moeten worden bevolen, aangezien de communicatie tussen zender en ontvanger nog niet tot een einde was gekomen. De kamer besloot uiteindelijk tot de nietigheid van het bevel van de onderzoeksrechter, alsook van de '*fruits of the poisonous tree*', overwegende dat "*het zich inhoudelijk toegang verschaffen tot gegevens, zowel tekst als afbeeldingen, op mailcorrespondentie via msn-berichten, dient aangezien te worden als kennisnemen en opnemen van privécommunicatie of -telecommunicatie in de zin van art. 90ter [Sv.], dat in een strenge motiveringsplicht voorziet*". De onderzoeksrechter kon evenwel op het moment dat hij zijn bevel uitvaardigde, niet met zekerheid weten of de webmailaccount al dan niet oneigenlijk werd gebruikt, zodat Van Linthout en Kerkhofs bij dit arrest ironisch genoeg, doch geheel terecht opmerken dat "*de onderzoeksrechter op voorhand gelijk had (kunnen hebben) om te beschikken overeenkomstig [art. 88ter Sv.], doch dat de kamer van inbeschuldigingstelling achteraf gelijk had om [art. 90ter e.v. Sv.] toe te passen*"[65]. De enige manier waarop een dergelijke nietigheid had kunnen vermeden worden, was een cumulatieve toepassing geweest van die twee artikelen door de onderzoeksrechter, maar, zoals hierboven reeds betoogd (zie randnr. 40), is zulks een bedenkelijke werkwijze te noemen in het licht van de rechtszekerheid.

Het lijkt erop dat alleen een wetgevend ingrijpen een einde zou kunnen maken aan de hierboven geschetste moeilijkheden. De operationele definitie ontwikkeld door Van Linthout en Kerkhofs lijkt voorlopig enige houvast te bieden (zie randnrs. 37-39), maar blijft niettemin een doekje voor het bloeden (zie immers randnr. 40). Zelf stellen de auteurs voor een soort 'informaticazoeking' in te voeren "*die zowel in de heimelijke fase van het onderzoek kan worden aangewend om gegevens op te halen op netwerken of op het internet, zonder dat daarbij dient stilgestaan te worden bij welke positie de verdachte reeds heeft ingenomen ten aanzien van dit bewijsmateriaal*"[66]. Een wetswijziging in die zin lijkt ons inderdaad wenselijk, op voorwaarde dat een aantal garanties wordt ingebouwd wanneer de telecommunicatie wordt

[63] KI Gent 27 september 2007, *T.Strafr.* 2008, afl. 2, 129.

[64] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 81.

[65] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 82.

[66] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 94.

afgetapt buiten het medeweten van de betrokkenen om. Op dat vlak dient het huidige onderscheid tussen art. 90ter Sv. en art. 88ter Sv. onzes inziens dan ook te worden behouden, met dien verstande dat als criterium voor die bijkomende bescherming niet moet gelden de vraag of de gegevens al dan niet 'in overbrenging' zijn, hetgeen immers bijzonder moeilijk te achterhalen is, maar wel het al dan niet heimelijke karakter van de maatregel.

b.1. Subrogatie

Zoals hierboven reeds vermeld (zie randnr. 31), mag de netwerkzoeking zich, overeenkomstig art. 88ter §2 Sv., "*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*". Met het begrip 'toegang' wordt bedoeld dat de overheid als het ware 'in de rechten treedt' van de persoon die gerechtigd is het onderzochte informaticasysteem te gebruiken, zodat in geen geval diens bevoegdheden kunnen worden overschreden. Bij een netwerkzoeking vindt derhalve een soort 'subrogatie' plaats waardoor "*[d]e grens voor het uitoefenen van deze nieuwe bevoegdheid wordt gevormd door de toegangsbevoegdheid van de personen die bevoegd zijn voor het gebruik van het informaticasysteem dat het voorwerp uitmaakt van de zoeking*"[67].

Geheel ten onrechte lijkt Laureys deze subrogatievoorwaarde, eerder dan uit het begrip 'toegang', af te leiden uit de bewoordingen "*die gerechtigd zijn het onderzochte informaticasysteem te gebruiken*"[68]. In die bijzin wordt evenwel niet gerefereerd aan de toegangsbevoegdheid tot het netwerk, maar wel aan de bevoegdheid om het informaticasysteem waarin de *oorspronkelijke* unilokale zoeking plaatsvindt, te gebruiken. Toch is die verwarring niet onbegrijpelijk. In het algemeen taalgebruik omschreven als een 'gelegenheid om binnen te komen' of als een 'weg waarlangs men ergens kan komen', lijkt het begrip 'toegang' immers op zichzelf geen legitimiteitsvoorwaarde in te houden. In dat opzicht heeft ook de *hacker* die via een netwerk op ongeoorloofde wijze binnendringt in andermans informaticasysteem, 'toegang' tot dat informaticasysteem. Beter ware aldus geweest uitdrukkelijk te vermelden dat die toegang niet alleen 'bijzonder' moet zijn (zie randnr. 48), maar ook moet zijn verkregen 'op legitieme wijze', waarmee bovendien het tweeledige karakter van de beperking zou worden benadrukt.

Hierbij kan worden verwezen naar het Nederlandse recht, waarin de subrogatievoorwaarde heel wat duidelijker wordt uitgedrukt aan de hand van een toestemmingsvereiste. Zo bepaalt art. 125j Sv., dat een "*[onderzoek] in een elders aanwezig geautomatiseerd werk [niet verder mag reiken] dan voor*

[67] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 23.

[68] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 64.

zover de personen die plegen te werken of te verblijven op de plaats waar de doorzoeking plaatsvindt, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk, daartoe toegang hebben". Een dergelijke formulering lijkt dan weer de specialiteitsvoorwaarde te verwaarlozen (zie ook randnr. 50), zodat een eventuele toekomstige wetswijziging het het best houdt bij de hierboven vermelde oplossing (zie randnr. 44).

Uit de subrogatievoorwaarde vloeit voort dat het de overheidsdiensten verboden is "*via eigen informaticasystemen binnen [te] dringen in andere systemen die niet openstaan voor het publiek en die ervan verdacht worden aangewend te worden voor criminele doeleinden*", waarmee de Belgische wetgever, net als de Nederlandse overigens[69], *hacking* door de overheid uitdrukkelijk uitsluit[70]. Aangenomen moet worden dat zulks *a fortiori* geldt wanneer informaticasystemen worden gebruikt die toebehoren aan particulieren (zie ook randnr. 55). Het verbod van *hacking* houdt evenwel niet in dat de speurders geen *hacking*-technieken zouden mogen gebruiken om zich toegang te verschaffen tot het informaticasysteem waarin de oorspronkelijke unilokale zoeking plaatsvindt. Dankzij de subrogatie zijn ook zij immers 'gerechtigd om het onderzochte informaticasysteem te gebruiken'. Wil men evenwel binnendringen tot een informaticasysteem dat via een netwerk met het onderzochte informaticasysteem verbonden is en waartoe de gebruikers van dat systeem geen toegangsbevoegdheid hebben, dan is een bevel tot unilokale zoeking noodzakelijk en moet desgevallend een huiszoeking plaatsvinden (zie randnr. 14).

Te dezen wijst Laureys terecht op het probleem van de *insider hacking*. Wanneer namelijk een persoon bewust "*zijn toegangsbevoegdheden [overschrijdt] om 'gevoelige' bestanden [op te slaan op plaatsen] waar hij geen toegangsbevoegdheid toe had*", zal men "*bij een onderzoek naar die persoon, die bestanden niet […] mogen terugvinden*", of nog: "*hoe het ene misdrijf het andere kan toedekken*"[71]. Die *caveat* moet evenwel in belangrijke mate worden genuanceerd, aangezien in dat geval nog steeds een unilokale zoeking kan plaatsvinden in het informaticasysteem dat werd binnengedrongen, waartoe de bevoegde gebruiker, als slachtoffer van de *hacking*, overigens allicht zelfs zijn toestemming zal geven. De subrogatievoorwaarde beoogt immers niet zozeer de gebruiker van het onderzochte informaticasysteem te beschermen, doch eerder de andere deelnemers aan het netwerk en geldt dan ook enkel voor het bevelen van een

[69] G. CORSTENS, *Het Nederlandse strafprocesrecht*, Deventer, Kluwer, 2005, 478.

[70] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 64; I. DELBROUCK, "Informaticacriminaliteit" in H. BERKMOES, W. BRUGGEMAN, I. DELBROUCK, D. DEWANDELEER, F. DESTERBECK, H. FRANSEN, P. HERBOTS, A. MARUT, C. NUYTS, E. VAN DEN HEUVEL *et al.*, *Postal Memorialis*, Antwerpen, Kluwer, 2007, (122) 138.

[71] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 65.

netwerkzoeking.

b.2. Specialiteit

Reeds in haar eerste verslag merkte de Kamercommissie op dat het wenselijk was om in art. 88ter §2 Sv. te verduidelijken dat "*men alleen de uitbreiding beoogt tot die systemen waartoe de gemachtigde personen 'in het bijzonder' toegang hebben krachtens een bijzondere machtiging*"[72], hetgeen vrijwel meteen gebeurde in een amendement van de Regering[73], zodat 'open systemen', zoals het internet, niet voor een netwerkzoeking in aanmerking komen (zie evenwel randnrs. 50-52). De memorie van toelichting verduidelijkt dat de netwerkverbinding "*een element van permanentie en stabiliteit [moet] inhouden en niet louter occasioneel [mag] zijn*"[74], waaruit Meunier bijvoorbeeld afleidt dat *"[l]e juge d'instruction ne pourrait […] étendre sa recherche dans un ordinateur portable dont la connexion au réseau de l'entreprise ne serait que ponctuelle"*[75].

In de rechtsleer werd meer dan eens een poging ondernomen om een algemene omschrijving te bieden van de aard van de verbinding die in aanmerking komt voor een netwerkzoeking. Zo stellen De Hert en Lichtenstein bijvoorbeeld dat "*enkel gebruik [kan worden gemaakt] van de 'normale' verbindingen die de persoon die normaal werkt met het systeem, tot zijn beschikking heeft*"[76]. Eerder dan het door de wetgever aangereikte richtsnoer te verduidelijken, lijkt die 'normaliteitstoets' evenwel nog meer onzekerheid te scheppen, gelet op het bijzondere vage en voor ruime interpretatie vatbare criterium van 'normaal gebruik'. Bovendien kan bezwaarlijk worden volgehouden dat het internet niet zou behoren tot de 'normale' verbindingen, terwijl de *ratio legis* achter de specialiteitsvoorwaarde precies gelegen is in het uitsluiten van dergelijke 'open systemen' (zie randnr. 48). Meer verdedigbaar is dan ook de stelling van Poullet die, gesteund door de Villenfagne en Dusollier[77] en door de correctionele rechtbank te Brussel[78], het beeld vooropstelt van de '*domicile virtuel*', die hij nader omschrijft als "*de tout lieu où une personne a le droit de se dire chez elle, quels que soient le titre juridique de son occupation et*

[72] Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 91.

[73] Amendement (Regering), *Parl.St.* Kamer 1999-2000, nr. 50-0214/006.

[74] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 23.

[75] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 668.

[76] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 65.

[77] F. DE VILLENFAGNE en S. DUSOLLIER, "La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *AM* 2001, afl. 1, (60) 75.

[78] Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, afl. 2, 149, noot, gewijzigd door Brussel 26 juni 2008, *T.Strafr.* 2008, afl. 6, 467, noot.

l'affectation donnée aux locaux"[79]. Dat beeld sluit namelijk niet alleen het geheel van webpagina's op het internet uit, waar een gewone internetgebruiker zich immers geen 'bewoner' van kan noemen, maar omvat bovendien tevens de hierboven vermelde subrogatievoorwaarde. Als voorbeelden voor een dergelijke 'virtuele woonplaats', haalt Poullet aan: "*un compte bancaire accessible par un code secret, les messages vocaux ou non déposés dans une boîte électronique au nom de la personne inculpée*" en "*la base de données externe où cette dernière collecte ou range une information partagée avec d'autres*".

Zoals hierboven reeds vermeld, wordt de specialiteitsvoorwaarde in de Nederlandse wettekst enigszins onderbelicht (zie randnr. 45). Het Franse art. 57-1 CPP bevat evenmin uitdrukkelijk een dergelijke voorwaarde, maar stelt eenvoudigweg dat een netwerkzoeking mogelijk is "*dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial*". Toch mag de waarde van de Belgische specialiteitsvereiste niet worden overschat. Het weze immers duidelijk dat men op basis van de Nederlandse en de Franse wetteksten evenmin kan volhouden dat de overheid de bevoegdheid zou krijgen om via het informaticasysteem van een burger (zie ook randnr. 55), ongebreideld het internet af te speuren naar mogelijke misdrijven. Het uitgangspunt dat het internet in beginsel niet in aanmerking komt voor een netwerkzoeking, moet bovendien nog op tweeërlei wijze worden genuanceerd.

In de eerste plaats merkt Laureys terecht op dat wanneer "*door middel van het internet 'bijzondere toegangen' worden gemaakt tot meer private netwerken*"[80], de netwerkzoeking wel degelijk kan worden bevolen. Die redenering is vergelijkbaar met de hierboven in het kader van de unilokale zoeking verdedigde eigen stelling dat de 'vermenging' van private gegevens met het openbaar karakter van het informaticasysteem waarin zij zijn opgeslagen, kan worden verhinderd door een bepaalde beveiliging (zie randnr. 20). Zo ook moet worden aanvaard dat het beveiligde karakter van een weliswaar via het internet tot stand gekomen verbinding, alsnog een netwerkzoeking mogelijk maakt. Als voorbeeld van een dergelijk geval kan gelden de recent sterk in populariteit toegenomen online opslagsystemen, zoals Windows Live SkyDrive, maar ook een bankrekening die via het internet ter beschikking staat van een cliënt (zie randnr. 49), of nog, het alom bekende Hotmail, dat e-mailberichten online toegankelijk maakt door middel van een wachtwoord. In die zin kwalificeerde de correctionele rechtbank te Brussel de doorzoeking van een hotmailaccount als een netwerkzoeking, overwegende dat "*l'exigence de stabilité et de permanence est rencontrée quand il s'agit*

[79] Y. POULLET, "A propos du projet de loi dit n° 214: la lutte contre la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves" in Y. POULLET en H. VUYE (eds.), *Liber Amicorum Jean du Jardin*, Deurne, Kluwer, 2001, 14.

[80] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 64.

d'étendre une recherche informatique vers un espace situé sur le serveur d'un autre système soit lorsque celui-ci est privatif"[81]. Daarop voortbouwend, moet bovendien worden aangenomen dat ook een verbinding tussen twee welbepaalde informaticasystemen haar bijzondere karakter blijft behouden, wanneer het internet slechts als medium wordt gebruikt om die verbinding tot stand te brengen, zoals dat bijvoorbeeld het geval is bij een *peer-to-peer*-verbinding die door de beruchte *BitTorrent clients* wordt gemaakt tussen zogenaamde *'leechers'* en *'seeders'* voor het uitwisselen van informatie die veelal bestaat uit illegaal gekopieerde audio- of videobestanden. Wanneer aldus een unilokale zoeking naar aanleiding van een beweerde schending van auteursrechten, plaatsvindt in het informaticasysteem van een *leecher*, kan die zoeking worden uitgebreid tot een netwerkzoeking die zich uitstrekt tot de door een *seeder* gedeelde map met bestanden.

In de tweede plaats moet worden vermeld dat in de praktijk algemeen aanvaard wordt dat het politiepersoneel, net zoals iedere internetgebruiker, het recht heeft "*om zich toegang te verschaffen tot elke site die publiekelijk toegankelijk is op het internet*"[82], zodat op die manier nog steeds misdrijven kunnen worden opgespoord, weliswaar met gebruik van de eigen informaticasystemen van de overheid (zie ook randnr. 55). Gelet op het voorgaande, moet aldus worden besloten dat, in tegenstelling tot wat op het eerste gezicht uit de parlementaire werkzaamheden blijkt, de specialiteitsvoorwaarde een bijzonder geringe beperking inhoudt van de mogelijkheden om verbindingen via het internet te doorzoeken. Enerzijds kan een netwerkzoeking nog steeds worden bevolen wanneer een dergelijke verbinding haar bijzondere karakter behouden heeft door middel van een meer private verbinding, en anderzijds mag, wanneer zulks niet het geval is en de verbinding bijgevolg voor het publiek toegankelijk is, nog steeds een doorzoeking plaatsvinden van het internet zelf, die in dat geval evenwel niet kan gelden als netwerkzoeking.

c. Voorwaarden

Op het eerste gezicht lijkt de preambule van art. 88ter Sv. zelf reeds een voorwaarde in te houden voor het bevelen van een netwerkzoeking, namelijk dat de oorspronkelijke unilokale zoeking moet zijn bevolen door de onderzoeksrechter. In dat opzicht zou geen netwerkzoeking kunnen plaatsvinden wanneer het de procureur des Konings is die tot de zoeking is overgegaan, bijvoorbeeld in geval van toestemming of ontdekking op heterdaad, of nog, zoals hierboven werd verdedigd (zie randnr. 19), bij een zoeking in een openbaar informaticasysteem.

[81] Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, afl. 2, 149, noot, gewijzigd door Brussel 26 juni 2008, *T.Strafr.* 2008, afl. 6, 467, noot.

[82] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 73.

Een dergelijke opvatting zou evenwel niet houdbaar zijn. Zoals hierboven reeds aangestipt (zie randnr. 10), wijst de keuze voor het voornaamwoord 'wanneer' in plaats van 'indien' eerder op de erkenning van een bestaande rechtspraktijk dan op een werkelijke voorwaarde voor een netwerkzoeking. Bovendien zou een dergelijke interpretatie de algemeen aanvaarde mogelijkheid om een netwerkzoeking te bevelen via mini-instructie (zie randnr. 61), nagenoeg volledig uithollen. Het is echter zeer de vraag wat dan wel de *ratio legis* is achter de weinig doordachte preambule van art. 88ter Sv., waaraan noch in de voorbereidende werken ervan, noch in de rechtsleer enige aandacht wordt besteed. Het lijkt erop dat de wetgever daarmee trachtte te verduidelijken dat eerst een unilokale zoeking moet plaatsvinden alvorens die kan worden uitgebreid tot een netwerkzoeking – of althans die situatie voor ogen had (zie randnr. 55) – maar het blijft onduidelijk waarom de functie van onderzoeksrechter uitdrukkelijk vermeld wordt. Vast staat hoe dan ook dat zulks geen voorwaarde kan inhouden voor het bevelen van een netwerkzoeking, zodat slechts twee cumulatieve voorwaarden van toepassing zijn, namelijk enerzijds een noodzakelijkheidsvereiste en anderzijds een negatief uitgedrukte proportionaliteitsvereiste dan wel het bestaan van een risico voor de bewijsgaring.

Wel blijkt uit de preambule van art. 88ter Sv. dat de wetgever vooral de situatie in gedachten had waarin een unilokale zoeking wordt uitgebreid tot een netwerkzoeking en aldus geen aandacht heeft besteed aan de mogelijkheid of wenselijkheid van een 'secundaire' netwerkzoeking[83], die zou bestaan in de verdere uitbreiding van een oorspronkelijke netwerkzoeking naar informaticasystemen die weliswaar niet rechtstreeks bereikbaar zijn vanuit het informaticasysteem waarin een eerste, unilokale zoeking plaatsvond, maar wel vanuit het informaticasysteem waarnaar die zoeking ingevolge een eerste, 'primaire' netwerkzoeking werd uitgebreid. De vraag naar de mogelijkheid van een secundaire netwerkzoeking houdt verband met de vraag of een netwerkzoeking noodzakelijkerwijs moet worden uitgevoerd vanaf het informaticasysteem waarin de oorspronkelijke, unilokale zoeking plaatsvindt dan wel of zij ook kan geschieden vanaf informaticasystemen van de overheid. In die eerste interpretatie, verdedigd door bijvoorbeeld Poullet[84], is een secundaire netwerkzoeking uitgesloten, aangezien zij als beginpunt telkens een unilokale zoeking veronderstelt. In de tweede lezing, voorgestaan door bijvoorbeeld Van Linthout en Kerkhofs[85], is een dergelijke verregaande stelselmatige uitbreiding echter niet noodzakelijk uitgesloten. Terecht noemt Dewandeleer die ruime interpretatie evenwel te ingrijpend in het licht van art.

[83] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 148.

[84] Y. POULLET, "A propos du projet de loi dit n° 214: la lutte contre la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves" in Y. POULLET en H. VUYE (eds.), *Liber Amicorum Jean du Jardin*, Deurne, Kluwer, 2001, 15.

[85] P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 90-93.

8 EVRM en art. 22 GW en stelt hij dat "*[art. 88ter Sv.] in de huidige bewoordingen voor dergelijke zoeking geen toereikende rechtsgrond kan vormen [voor een secundaire netwerkzoeking]*"[86]. Aangezien zij, gelet op de inleidende bewoordingen van art. 88ter Sv., het meest nauw aansluit bij wat de wetgever allicht voor ogen had, verdient die stelling onzes inziens navolging, met dien verstande dat weliswaar de mogelijkheid van een secundaire netwerkzoeking moet worden uitgesloten, maar dat zulks niet noodzakelijk de onmogelijkheid inhoudt voor de overheidsdiensten om hun primaire netwerkzoeking verder te zetten op eigen informaticasystemen, bijvoorbeeld wanneer zij beschikken over de gebruikersnaam en het wachtwoord van een hotmailaccount, vermits het tegendeel het onderzoek nodeloos zou bemoeilijken zonder dat sprake is van een verregaande inbreuk op het privéleven van de betrokkene.

c.1. Noodzakelijkheid

Overeenkomstig art. 88ter §1 lid 1, eerste streepje Sv. kan de netwerkzoeking enkel worden bevolen "*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*". Bijgevolg kan een netwerkzoeking enkel dienen om dat misdrijf op te helderen waarnaar reeds onderzoek werd gedaan tijdens de unilokale zoeking, zodat zij niet kan gebruikt worden als een soort 'virtuele infiltratiemethode' waarmee men ongemerkt zou kunnen binnendringen in het informaticasysteem van een verdachte door een netwerkzoeking te bevelen vanuit een willekeurige daarmee verbonden computer.

De netwerkzoeking dient beperkt te blijven "*tot de saisine van de onderzoeksrechter*"[87]. Ontdekt de onderzoeksrechter zelf evenwel bij toeval bepaalde aanwijzingen in de richting van een ander misdrijf, dan kan hij nog steeds zijn zoeking verderzetten en zelfs uitbreiden naar andere delen van het netwerk, "*s'agissant d'une infraction flagrante*"[88]. Worden die toevallige vaststellingen daarentegen gedaan door politiediensten en werd die uitbreiding niet voorzien in het bevel tot netwerkzoeking, dan moet voor een dergelijke uitbreiding onzes inziens een bijkomend rechterlijk bevel worden afgeleverd.

c.2. Negatieve proportionaliteit of risico voor de bewijsgaring

Krachtens art. 88ter §1 lid 1, tweede streepje Sv. kan de netwerkzoeking bovendien enkel worden bevolen "*indien andere maatregelen disproportioneel zouden zijn of indien er een risico bestaat dat zonder deze uitbreiding*

[86] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 148.

[87] R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 459

[88] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 666.

bewijselementen verloren gaan", waaruit twee duidelijk *alternatieve* – anders dan Gevaert bijvoorbeeld lijkt voor te houden[89] – subvoorwaarden kunnen worden afgeleid, die in wezen een weerspiegeling inhouden van de achterliggende beweegredenen om de netwerkzoeking in te voeren (zie randnr. 27). De toepassing van de netwerkzoeking wordt zodoende beperkt tot die situaties waarvoor haar invoering noodzakelijk was.
De eerste subvoorwaarde bestaat in een proportionaliteitsvereiste die evenwel op negatieve wijze is uitgedrukt. Vereist wordt immers niet dat de netwerkzoeking zelf een evenredige maatregel zou zijn, in welk geval men zou kunnen spreken van een 'positieve proportionaliteitsvereiste', maar wel dat andere maatregelen disproportioneel zouden zijn, bijvoorbeeld wanneer meerdere huiszoekingen zouden moeten plaatsvinden[90]. Het lijkt erop dat vrijwel altijd aan de negatieve proportionaliteitsvereiste voldaan zal zijn, aangezien een netwerkzoeking per definitie minder indringend is voor de gebruiker van het informaticasysteem dan wel een bijkomende unilokale zoeking. De onderzoeksrechter beschikt ter zake overigens over "*un large pouvoir d'appréciation*"[91].

Ook in het geval van de tweede subvoorwaarde, namelijk wanneer zich een risico voordoet voor de bewijsgaring, kan de netwerkzoeking worden bevolen, wanneer zij daarenboven noodzakelijk is voor de waarheidsvinding. Net zoals bij de eerste subvoorwaarde, komt het "*aan de onderzoeksrechter toe om dit in redelijkheid te beoordelen*"[92] (zie ook randnr. 59).

d. Bevoegde autoriteit

Anders dan een unilokale zoeking in een informaticasysteem (zie randnr. 25), kan een netwerkzoeking slechts plaatsvinden op bevel van een onderzoeksrechter, ook wanneer de oorspronkelijke zoeking wordt uitgebreid vanuit of naar openbare informaticasystemen. De tekst van art. 88ter Sv. laat daaromtrent immers geen twijfel bestaan, in tegenstelling tot wat het geval is bij de unilokale zoeking, waarvoor – op de onduidelijke preambule van art. 88ter Sv. na (zie randnrs. 10-11 en 54) – geen uitdrukkelijke bevoegdheidsregeling werd opgesteld. Bovendien werd hierboven reeds vermeld dat in vele gevallen de precieze locatie van de gegevens niet kan worden vastgesteld (zie randnr. 27), zodat men vaak niet op voorhand weet of zij zich al dan niet op een openbare plaats bevinden, waardoor de vereiste van een rechterlijk bevel in alle situaties de meest veilige oplossing biedt. De bewering van Meunier dat "*le magistrat compétent pour la recherche*

[89] P. GEVAERT, *Het gerechtelijk onderzoek*, Gent, Story Publishers, 2006, 115.
[90] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 23.
[91] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 667.
[92] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 23.

informatique est également compétent pour en requérir l'extension"[93], moet om die redenen dan ook worden afgewezen. Wel wordt in de rechtsleer terecht aangenomen dat de netwerkzoeking kan worden bevolen via mini-instructie, aangezien zij door art. 28septies Sv. niet wordt uitgesloten van haar toepassingsgebied[94].

De uitzonderingsgevallen van toestemming of ontdekking op heterdaad lijken niet vatbaar voor volkomen analogische toepassing op de netwerkzoeking. Het is onzes inziens immers niet alleen de persoon bij wie de unilokale zoeking plaatsvindt, van wie de toestemming moet worden verkregen, maar ook de gebruiker van het informaticasysteem waarnaar de zoeking wordt uitgebreid, aangezien de gegevens zich bij hem bevinden. In die zin betoogt Meunier geheel terecht dat in dat geval een bijkomende toestemming moet worden vereist van die persoon[95]. Zijn stelling dat in geval van ontdekking op heterdaad zonder meer een netwerkzoeking zou kunnen plaatsvinden door de procureur des Konings, is daarentegen minder verdedigbaar. Anderzijds kan ook de stelling van Verstraeten dat een netwerkzoeking bij heterdaad in het geheel uitgesloten zou zijn "*[v]ermits de netwerkzoeking geregeld wordt door art. 88ter Sv. waarin geen sprake is van een bevoegdheid van de procureur*" en "*[ook de huiszoeking] enkel kan geschieden in de woning van de verdachte, zonder dat dit kan worden uitgebreid*"[96], niet zonder meer worden nagevolgd. Het is immers weliswaar zo dat art. 36 Sv. bijvoorbeeld enkel gewag maakt van de 'woning van de verdachte', maar wanneer men die bepaling beschouwt in samenhang met art. 46 Sv. dat, in geval van toestemming door het hoofd des huizes, ook de woning van anderen openstelt voor de procureur des Konings, lijkt een netwerkzoeking bij heterdaad aanvaardbaar op voorwaarde dat de persoon naar wiens informaticasysteem de zoeking wordt uitgebreid, daarin toestemt. De betrapping op heterdaad doet als het ware enkel de toestemmingsvereiste uit hoofde van de verdachte vervallen, maar niet die uit hoofde van andere deelnemers aan het netwerk.

Gelet op de uitdrukkelijke vermelding van art. 89bis Sv. in art. 88ter §4 Sv., kan de onderzoeksrechter zijn opdracht tot netwerkzoeking evenwel delegeren aan een officier van gerechtelijke politie bij "*met redenen omklede beschikking en enkel wanneer het noodzakelijk is*". Volgens Verstraeten moet om die reden worden aanvaard dat "*wanneer de zoeking niet door de onderzoeksrechter zelf*

---

93 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 665.

94 P. GEVAERT, *Het gerechtelijk onderzoek*, Gent, Story Publishers, 2006, 115; C. VAN DEN WYNGAERT, *Strafrecht, strafprocesrecht & internationaal strafrecht in hoofdlijnen*, Antwerpen, Maklu, 2006, 973; I. DELBROUCK, "Informaticacriminaliteit" in H. BERKMOES, W. BRUGGEMAN, I. DELBROUCK, D. DEWANDELEER, F. DESTERBECK, H. FRANSEN, P. HERBOTS, A. MARUT, C. NUYTS, E. VAN DEN HEUVEL *et al.*, *Postal Memorialis*, Antwerpen, Kluwer, 2007, (122) 147.

95 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 665.

96 R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 335-336.

wordt verricht, een uitbreiding van de zoeking naar een ander informaticasysteem slechts mogelijk is wanneer het bevel tot huiszoeking dit expliciet vermeldt"[97]. Is zulks niet het geval of beschikken de onderzoekers in het geheel niet over een huiszoekingsbevel (zie randnr. 25), dan moet een bijkomend bevel worden afgeleverd door de onderzoeksrechter[98].

Commissielid Michel vreesde om die reden dat de wet "*niet zal beletten dat bewijzen verloren gaan*" en stelde voor "*een dergelijke beslissing over te laten aan de onderzoekers of aan het parket*"[99], waarop tijdens de verdere parlementaire werkzaamheden evenwel niet dieper is ingegaan. De vermelding in de uiteindelijke memorie van toelichting dat het "*aan de onderzoeksrechter [toekomt]*" de vervulling van de voorwaarden voor een netwerkzoeking te beoordelen, lijkt erop te wijzen dat de stelling van Verstraeten inderdaad navolging verdient. Wil het Openbaar Ministerie aldus vermijden dat bewijselementen verloren gaan, dan is het aangewezen in elk geval alvast de onderzoeksrechter te verzoeken om een bevel tot netwerkzoeking, alvorens over te gaan tot enige unilokale zoeking in een informaticasysteem.

In dit verband kan worden gerefereerd aan het hierboven reeds terloops aangehaalde vonnis van 10 januari 2008 van de correctionele rechtbank te Brussel, waarvoor de regelmatigheid werd aangevochten van de doorzoeking van een hotmailaccount uitgevoerd op grond van een eenvoudig 'kantschrift geldend als vordering'[100]. De rechtbank oordeelde dat "*dès lors que la perquisition ayant donné lieu à l'examen d'un système informatique avait été autorisée par mandat, rien n'imposait que le juge d'instruction décerne une nouvelle ordonnance pour qu'il puisse être régulièrement procédé par les enquêteurs à une extension de la recherche initiale*"[101], hetgeen in de rechtsleer enige kritiek uitlokte, onder andere van Dewandeleer die, net als Van Linthout en Kerkhofs[102], van oordeel is dat in het licht van art. 8 EVRM en art. 22 GW een dergelijke "*ingreep op het [privéleven] in ieder geval een a priori controle door de onderzoeksrechter vergt en dus slechts toelaatbaar is op grond van een voorafgaand bevelschrift dat vaststelt dat de voorwaarden van [art. 88ter Sv.] vervuld zijn, dus ook wanneer de netwerkzoeking zou*

---

97 R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 460.

98 D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 144.

99 Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 62-63.

100 D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 144-145.

101 Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, afl. 2, 149, noot, gewijzigd door Brussel 26 juni 2008, *T.Strafr.* 2008, afl. 6, 467, noot.

102 P. VAN LINTHOUT en J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T.Strafr.* 2008, afl. 2, (79) 83-84.

gepaard gaan met de uitvoering van een huiszoekingsbevel"[103]. Enige tijd later wijzigde het Hof van Beroep te Brussel de beslissing van de correctionele rechtbank dan ook geheel terecht in die zin dat wel degelijk een bijkomend rechterlijk bevel vereist was dat kan bestaan in hetzij *"un mandat de perquisition autorisant l'accès aux locaux du fournisseur de service",* hetzij *"une ordonnance motivée sur la base de l'article 88ter CIC permettant aux enquêteurs d'accéder au disque dur dudit fournisseur*"[104]. Een eenvoudig 'kantschrift geldend als vordering' beantwoordt bijgevolg niet aan de wettelijke vereisten[105]. Niettegenstaande die onregelmatigheid, besloot het Hof uiteindelijk het aldus op onrechtmatige wijze verkregen bewijsmateriaal, niet uit de debatten te weren, overwegende dat "*aucune règle de forme prescrite à peine de nullité n'a été en l'espèce violée*", dat "*l'irrégularité commise n'a pas entaché la fiabilité des retranscriptions des communications électroniques*" en dat "*l'illicéité partielle commise est sans commune mesure avec la gravité des infractions de terrorisme dont le juge d'instruction était saisi*", waarmee het een feilloze toepassing maakt van de drie voorwaarden ontwikkeld in de roemruchte Antigoonrechtspraak van het Hof van Cassatie[106].

In welke vorm de onderzoeksrechter een dergelijk bevel dient af te leveren, heeft de wetgever niet uitdrukkelijk geregeld. Aldus betoogt Meunier, gesteund door Dewandeleer[107], dat een bevel tot netwerkzoeking ook op mondelinge wijze kan worden gegeven, op voorwaarde dat het later wordt bevestigd in een geschrift dat verwijst naar de vroegere mondelinge instructies en de wettelijk vereiste redenen voor de uitbreiding (zie randnrs. 53-60), "*eu regard au caractère écrit de la procédure au stade de l'instruction*"[108]. Die stelling lijkt ons inderdaad navolgbaar, met dien verstande dat een dergelijk mondeling bevel onzes inziens enkel kan worden aanvaard wanneer de tijd die nodig is voor het afleveren van een schriftelijk bevel, een aantoonbaar risico inhoudt voor de bewijsgaring.

Zonder evenwel een antwoord te bieden, vragen De Hert en Lichtenstein zich ten slotte af of men dient te "*beschikken over een apart [bevel] van de onderzoeksrechter om bijvoorbeeld de voicemail te beluisteren [van een gsm-*

---

[103] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 145.

[104] Brussel 26 juni 2008, *T.Strafr.* 2008, afl. 6, 467, noot.

[105] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 146.

[106] F. VERBRUGGEN en R. VERSTRAETEN, *Strafrecht en strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2007, 340-341.

[107] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 143.

[108] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 667-668.

toestel]"[109]. Het lijkt erop dat zulks vooralsnog inderdaad het geval is, zelfs wanneer dat gsm-toestel werd aangetroffen in het kader van een huiszoeking, indien de onderzoeksrechter in het huiszoekingsbevel zou hebben nagelaten een uitdrukkelijke machtiging tot netwerkzoeking te geven (zie randnr. 63). Het komt niettemin als bevreemdend voor dat voor het beluisteren van dergelijke voicemailberichten wel een bijkomend rechterlijk bevel moet worden vereist, terwijl zulks hoegenaamd niet het geval is voor het beluisteren van de audiocassette van een in de woning aangetroffen antwoordapparaat[110], alleen maar omdat in dat eerste geval de gegevens zich strikt genomen niet in de woning zelf bevinden. Het lijkt ons dan ook wenselijk zich grondig te bevragen over de traditionele 'plaatsgebonden' denkpatronen, zodat wellicht in de toekomst zou kunnen worden aanvaard dat voor het doorzoeken van dergelijke gegevens, die in zulke grote mate met het informaticasysteem zelf verbonden zijn en bovendien in de regel enkel voor de gebruiker van dat toestel toegankelijk zijn, geen bijkomend rechterlijk bevel moet worden vereist wanneer reeds een dergelijk bevel voorhanden is voor de doorzoeking van de plaats waar dat toestel zich bevindt. Men kan immers bezwaarlijk volhouden dat het beluisteren van voicemailberichten een grotere inbreuk zou inhouden op de persoonlijke levenssfeer dan het beluisteren van een traditioneel antwoordapparaat. Zo ook kan moeilijk worden ingezien waarom een hotmailaccount een grotere mate van bescherming verdient (zie randnr. 51) dan een e-mailaccount die gekoppeld is aan een zogenaamde '*Mail User Agent*', zoals Outlook Express, die immers ook ongelezen e-mailberichten (zie ook randnr. 21) downloadt en opslaat op de harde schijf. In de huidige stand van de wetgeving lijkt die ongelijke behandeling evenwel te moeten worden gehandhaafd. Toch rijst de vraag of het door de wetgever gehuldigde geografische criterium wel 'pertinent' genoeg is om een eventuele toekomstige grondwettigheidstoetsing te doorstaan. De gekende pennenstrijd tussen de twee hoogste rechtscolleges omtrent de zwaarte van straffen, heeft immers reeds aangetoond dat het Grondwettelijk Hof eerder geneigd is een subjectief criterium voor te staan, zoals het aanvoelen van de gestrengheid van de maatregel door de burger[111].

2.2 INBESLAGNEMING

Net zoals de zoeking, ondervond ook de traditionele inbeslagneming in een geïnformatiseerde omgeving bijzondere toepassingsmoeilijkheden, hetgeen noopte tot een modernisering van de wetgeving. De vroegere regelgeving bleef evenwel ook na de inwerkingtreding van de WIC van toepassing als gemeen recht, zodat een onderscheid kan worden gemaakt tussen de inbeslagneming van een materiële drager van elektronische gegevens enerzijds, die grotendeels

[109] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 74.

[110] Cass. (2de k.) 27 oktober 1999, *Arr.Cass.* 1999, 1346, *Bull.* 1999, 1404, *JT* 2000 (verkort), 522 en *RDPC* 2000, 733.

[111] Arbitragehof 5 oktober 2005, *AA* 2005, afl. 4, 1955.

geschiedt volgens de gemeenrechtelijke bepalingen, en de inbeslagneming van de elektronische gegevens zelf anderzijds, waarvoor de bijzondere modaliteit van het 'databeslag' moet worden gebruikt.

2.2.1. Inbeslagneming van een drager van elektronische gegevens

Een traditionele inbeslagneming overeenkomstig art. 35-37 en 87 Sv., laat niet toe dat immateriële zaken, zoals elektronische gegevens, op zichzelf in beslag zouden worden genomen, vermits zij "*de onttrekking [veronderstelt] van een voorwerp aan de beschikking van degene die het onder zich houdt*"[112] (zie evenwel randnr. 70). De materiële drager van die gegevens kan daarentegen al van oudsher in beslag worden genomen overeenkomstig die gemeenrechtelijke bepalingen, die dan ook *mutatis mutandis* van toepassing zijn in een geïnformatiseerde omgeving. In die zin geeft de memorie van toelichting van de WIC aan dat de inbeslagneming van elektronische gegevens "*volledig volgens de traditionele procedures [kan] verlopen, zolang dit gepaard gaat met de inbeslagneming van de materiële drager daarvan*"[113].

Anders dan de gemeenrechtelijke zoeking (zie randnr. 8), waaraan de wetgever immers geen wijzigingen heeft aangebracht[114], werd de gemeenrechtelijke inbeslagneming in een geïnformatiseerde omgeving echter toch enigszins gewijzigd voor wat betreft de bijzondere verplichtingen die bestaan in hoofde van de bevoegde autoriteit. In art. 39bis §6 lid 3 Sv. wordt namelijk de verplichting tot het aanwenden van "*de passende technische middelen […] om de integriteit en de vertrouwelijkheid van [de] gegevens te waarborgen*" en "*voor de bewaring hiervan op de griffie*" uitgebreid tot de situatie waarin de gehele drager in beslag wordt genomen.

De stelling dat elektronische gegevens op zichzelf niet in beslag kunnen worden genomen overeenkomstig de gemeenrechtelijke regelgeving, is evenwel geen vanzelfsprekendheid te noemen. Zo oordeelde het Hof van Beroep te Antwerpen reeds in 1984 dat "*computergegevens […] voorwerp van diefstal kunnen zijn*", overwegende dat zij "*niet slechts 'een geheel van instructies, intrinsiek intellectueel en niet tastbaar van aard en derhalve niet vatbaar voor wegneming (zijn)' […] maar ook vatbaar zijn voor [reproductie] en overdracht en een economische waarde hebben*"[115]. Volgens die opvatting zouden elektronische gegevens, ofschoon immaterieel, eveneens in aanmerking komen voor een gemeenrechtelijke inbeslagneming, aangezien zij in dat opzicht ook op zichzelf vatbaar zijn voor wegneming. Toch is de

---

[112] J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, afl. 2, (44) 59.

[113] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 19.

[114] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 64.

[115] Antwerpen 13 december 1984, *RW* 1985-86, 244, noot.

invoering van het databeslag zeker geen overbodigheid te noemen, alleen al omwille van de duidelijkheid die zij ter zake heeft geschapen. Volgens een klassieke opvatting blijft immers, zo merkt Verstraeten op, het misdrijf van diefstal – en, bij uitbreiding, de maatregel van inbeslagneming – "*de materiële handeling [veronderstellen] van verplaatsing van de gestolen [of in beslag genomen] zaak*"[116]. Bovendien heeft de wetgever door een bijzondere regelgeving uit te werken, de kans gegrepen om bepaalde nieuwe mogelijkheden in het leven te roepen die allicht niet mogelijk waren op grond van de gemeenrechtelijke inbeslagneming, zoals het blokkeren van de gekopieerde gegevens met behulp van versleutelingstechnieken (zie randnr. 78).

2.2.2. Inbeslagneming van elektronische gegevens ('databeslag')

Tijdens een strafonderzoek in een geïnformatiseerde omgeving kan zich de situatie voordoen dat de inbeslagneming van de drager van elektronische gegevens niet wenselijk is, bijvoorbeeld "*bij een bank of een rekencentrum van de overheid, waarbij elke seconde dat het systeem niet draait, een miljoenenverlies meebrengt*"[117] of wanneer de omvang van het informaticasysteem de inbeslagneming ervan onaantrekkelijk maakt. Daarom werd in het door art. 7 WIC ingevoerde art. 39bis Sv. de mogelijkheid gegund aan de procureur des Konings om de elektronische gegevens zelf in beslag te nemen via een kopiename. De nieuwe mogelijkheid van het 'databeslag' geldt overigens, ingevolge art. 88ter §3 Sv., ook wanneer de gegevens worden aangetroffen ingevolge een netwerkzoeking.

a. Het begrip 'gegevens opgeslagen in een informaticasysteem'

Met het begrip 'gegevens' wordt door de wetgever gedoeld op "*voorstellingen van informatie die geschikt zijn voor opslag, verwerking en overdracht via een informaticasysteem*", waarbij "*[d]e materiële vormgeving […] – electromagnetisch, optisch of anderszins – [irrelevant is]*"[118]. In samenhang gelezen met de hierboven reeds uiteengezette ruime omschrijving van het begrip 'informaticasysteem' (zie randnr. 30), moet aldus worden aanvaard dat ook bijvoorbeeld de foto's opgeslagen in het geheugen van een digitaal fototoestel, in aanmerking komen voor 'databeslag'. Waar het in wezen om gaat, is dat bij het kopiëren van de gegevens geen kwaliteitsverlies optreedt – een digitale kopie is immers identiek aan het origineel – zodat zij probleemloos in beslag kunnen worden genomen. De bewering van Meunier dat geen databeslag zou kunnen worden gelegd op "*des données figurant sur une disquette ou un cd-*

[116] R. VERSTRAETEN, "Diefstal van computergegevens: revolutie in het strafrecht?", *RW* 1985-86, (215) 219.

[117] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 62.

[118] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 12.

rom", omdat die gegevens niet zouden opgeslagen zijn "*dans un système informatique*"[119], kan dan ook in het geheel niet worden nagevolgd. In dat geval moet immers niet de computer van de betrokkene als 'informaticasysteem' worden beschouwd, maar wel de diskette of de cd-rom zelf. Wel moeten de gegevens werkelijk 'opgeslagen' zijn in een informaticasysteem, zodat gegevens 'in overbrenging' – in het Nederlandse recht 'stromende gegevens' genoemd[120] – niet op grond van art. 39bis Sv. kunnen worden onderschept, maar wel op grond van een overeenkomstig art. 90ter e.v. Sv. bevolen informaticatap (zie immers randnr. 32).

b. Inhoud en draagwijdte van de maatregel

Overeenkomstig art. 39bis §2 Sv. kan, "*wanneer de procureur des Konings in een informaticasysteem opgeslagen gegevens aantreft die nuttig zijn voor dezelfde doeleinden als de [gemeenrechtelijke] inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is*", worden overgegaan tot kopiëring van die gegevens, eventueel gevolgd door een verhindering van de toegang of een ontoegankelijkmaking. Ook hier lijkt de wetgever aldus het toepassingsgebied van de nieuwe maatregel te beperken tot die situaties waarvoor zijn invoering noodzakelijk was (zie ook randnr. 58), zodat het databeslag een 'subsidiair karakter' vertoont ten aanzien van de gemeenrechtelijke inbeslagneming van de materiële drager[121]. Daarnaast schept art. 39bis Sv. een aantal bijzondere verplichtingen in hoofde van de bevoegde autoriteit.

b.1. Kopiëring van de gegevens

Aangezien een digitale kopie "*perfect [overeenstemt] met het origineel*"[122], kan de inbeslagneming van elektronische gegevens probleemloos geschieden via kopiename. De wetgever heeft uitdrukkelijk bepaald dat de kopiëring van de gegevens in beginsel moet geschieden op dragers van de overheid, waardoor hem door De Hert en Lichtenstein 'detaillisme' wordt verweten[123]. Die kritiek lijkt ons evenwel overdreven. Op die manier slaagde men er immers in ook een uitzondering op die regel in de wet op te nemen, namelijk dat enkel "*in geval van dringendheid of om technische redenen*", dragers kunnen worden gebruikt die ter beschikking staan van personen die gerechtigd zijn het informaticasysteem te gebruiken, zulks in tegenstelling tot het Franse

---

119 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 671.

120 C. CLEIREN en J. NIJBOER, *Strafvordering: tekst & commentaar*, Deventer, Kluwer, 2007, 347.

121 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 672.

122 Verslag namens de commissie voor de justitie uitgebracht door de heer ISTASSE en mevrouw KAÇAR, *Parl.St.* Senaat 1999-2000, nr. 2-392/003, 26.

123 P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 74.

recht, waarin art. 57-1 CPP uitdrukkelijk voorziet dat "*[les données] peuvent être copiées sur tout support"*.

Wanneer kopiëring van de gegevens niet mogelijk is, bijvoorbeeld omdat de toepassingsprogrammatuur erg ingewikkeld is en elders niet beschikbaar is of omdat de hoeveelheid elektronische gegevens te omvangrijk is, bepaalt art. 39bis §4 Sv. dat enkel de toegang tot de gegevens wordt verhinderd, hetgeen in feite neerkomt op "*de informatische variant van verzegeling*"[124].

b.1.1. Gegevens nuttig voor dezelfde doeleinden als de gemeenrechtelijke inbeslagneming

Voor de eerste categorie van gegevens die in beslag kunnen worden genomen, wordt verwezen naar de gemeenrechtelijke inbeslagneming. Aldus kunnen ook elektronische gegevens die nuttig zijn voor de waarheidsvinding of die in aanmerking komen voor een eventuele latere verbeurdverklaring, in beslag worden genomen[125]. Als voorbeelden van die laatste subcategorie kunnen gelden een *hacking*-programma als *instrumentum sceleris*, kinderpornografisch beeldmateriaal als *obiectum sceleris* of een computervirus als *productum sceleris*[126].

b.1.2.Gegevens noodzakelijk om de voorgaande gegevens te verstaan

De WIC heeft evenwel nog een bijzondere categorie toegevoegd van gegevens die in beslag kunnen worden genomen, gelet op de bijzondere aard van een geïnformatiseerde omgeving, namelijk de gegevens noodzakelijk om de voorgaande gegevens (zie randnr. 76) te kunnen verstaan. Aldus kunnen ook bijvoorbeeld de computerprogramma's worden gekopieerd die noodzakelijk zijn om de gegevens te kunnen lezen die nuttig zijn voor de waarheidsvinding of die in aanmerking komen voor een latere verbeurdverklaring. Men kan zich hierbij evenwel de vraag stellen of het wel noodzakelijk was zulks uitdrukkelijk te vermelden. De gegevens noodzakelijk om de voorgaande gegevens te verstaan, zijn immers op zichzelf reeds 'nuttig voor de waarheidsvinding'. De toevoeging lijkt overigens niet alleen overbodig, maar houdt bovendien een zeker risico in voor wat betreft de bevoegdheid van de procureur des Konings, zoals hieronder wordt uiteengezet (zie randnr. 100).

---

[124] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 21.

[125] I. DELBROUCK, "Informaticacriminaliteit" in H. BERKMOES, W. BRUGGEMAN, I. DELBROUCK, D. DEWANDELEER, F. DESTERBECK, H. FRANSEN, P. HERBOTS, A. MARUT, C. NUYTS, E. VAN DEN HEUVEL *et al.*, *Postal Memorialis*, Antwerpen, Kluwer, 2007, (122) 137.

[126] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 671.

b. 2. Verhindering van de toegang tot en ontoegankelijkmaking van de gegevens

Uit de memorie van toelichting blijkt duidelijk dat een belangrijk onderscheid moet worden gemaakt tussen het 'verhinderen van de toegang' tot de gegevens, hetgeen bestaat in een blokkering van de gegevens, en de 'ontoegankelijkmaking' ervan, waarbij "*het blokkeren van de gegevens kan worden vervangen door het wissen ervan*"[127]. De uiteindelijk aangenomen wettekst hult zich ter zake evenwel in een niet te evenaren taalkundige vaagheid, waardoor het zeker niet onbegrijpelijk is dat dat onderscheid in de rechtsleer zelden consequent wordt gemaakt. Toch zien bijvoorbeeld Roggen, Klees en Vandermeersch geheel terecht een belangrijk verschil tussen "*l'empêchement d'accès […] visée à l'alinéa 1er du § 3 de l'article 39bis*", waarbij "*les données restent dans le système informatique*" en "*l'interdiction d'accès […] visée à l'alinéa 2 du § 3 de l'article 39bis*", in welk geval "*le retrait des données est permis*"[128].

b.2.2.Verhindering van de toegang tot de gegevens

In beginsel wordt de toegang tot de gegevens na kopiëring, steeds verhinderd, hetgeen bijvoorbeeld kan geschieden door middel van versleutelingstechnieken of cryptografie[129]. De procureur des Konings kan evenwel, overeenkomstig art. 39bis §3 lid 3 Sv., "*het verdere gebruik van [de gegevens] toestaan, wanneer dit geen gevaar voor de strafvordering oplevert*", hetgeen aansluiting vindt bij de *ratio legis* van de mogelijkheid van het databeslag (zie randnr. 71).

Hierbij merkt Evrard op dat "*le procureur du Roi ne devrait pas faire usage de cette possibilité lorsque les données […] constituent des infractions [puisque] seul le blocage de l'accès à ces données […] sera de nature à permettre l'exercice efficace des poursuites*"[130]. Een gelijkaardige redenering gaat onzes inziens op voor de inbeslagneming van gegevens die in aanmerking komen voor een latere verbeurdverklaring, die anders immers van haar bestaansreden zelf beroofd zou worden.

Roggen, Klees en Vandermeersch noemen de mogelijkheid voor de procureur des Konings om het verdere gebruik van de gegevens toe te staan, overbodig, gelet op het feit dat in art. 39bis §1 lid 1 Sv. reeds uitdrukkelijk wordt verwezen naar de in art. 28sexies Sv. opgenomen mogelijkheid om de

[127] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 20.

[128] O. KLEES, F. ROGGEN en D. VANDERMEERSCH, "Les saisies en matière pénale" in P. CHOMÉ, A. LORENT, F. ROGGEN, J. COLLIN *et al., Droit pénal et procédure pénale*, Mechelen, Kluwer, 2007, (4) 69.

[129] J. DUMORTIER, B. VAN OUDENHOVE en P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles* 2001, afl. 2, (44) 60.

[130] S. EVRARD, "La loi du 28 novembre 2000 relative à la criminalité informatique", *JT* 2001, (241) 243.

opheffing van een opsporingshandeling te vragen[131]. Aangezien algemeen wordt aanvaard dat de ter zake bevoegde autoriteit 'spontaan' kan overgaan tot opheffing van het beslag[132], lijkt die kritiek op het eerste gezicht inderdaad terecht, ware het niet dat beide bepalingen een verschillende strekking hebben. Een onderscheid moet immers worden gemaakt tussen de modaliteiten waaronder het databeslag *ab initio* werd gelegd, waar art. 39bis Sv. toepassing vindt, en de mogelijkheid om nadien de opheffing ervan te vragen of te bevelen, waarop art. 28sexies Sv. – of, in voorkomend geval, art. 61quater Sv. (zie ook randnr. 94) – betrekking heeft. Aldus kan de procureur des Konings of de onderzoeksrechter, wanneer hij beslist om over te gaan tot databeslag, dat beslag, overeenkomstig art. 39bis §3 lid 3 Sv., *ab initio* beperken tot een loutere kopie zonder een verhindering van de toegang of een ontoegankelijkmaking. Blijkt het beslag nadien evenwel onnodig of voelt een rechtsonderhorige zich erdoor geschaad, dan kan het, met toepassing van art. 28sexies Sv. of art. 61quater Sv., worden opgeheven. Het verwijt dat art. 39bis §3 lid 3 Sv. "*[fait] double emploi avec les articles 28sexies, §3, alinéa 2, et 61quater, §3, alinéa 2*"[133], moet dan ook worden afgewezen als ongegrond, vermits die bepalingen later pas in de strafprocedure toepassing vinden.

b.2.2.1. Ontoegankelijkmaking van de gegevens

Indien de gegevens evenwel het voorwerp uitmaken van het misdrijf 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, worden zij, overeenkomstig art. 39bis §3 lid 2 Sv. 'ontoegankelijk' gemaakt. Omdat de Senaat vreesde dat het begrip 'verwijderen' in het oorspronkelijke wetsontwerp[134], de procureur des Konings de mogelijkheid zou geven de gegevens definitief te vernietigen, werd het begrip 'ontoegankelijkmaking' geïntroduceerd door een subamendement van de heer Van Quickenborne waarin het wordt omschreven als "*het verwijderen (wissen) van de betrokken bestanden, met behoud van een kopie voor justitie*"[135].

Taalkundig valt evenwel niet in te zien wat het verschil tussen een 'verhindering van de toegang' en een 'ontoegankelijkmaking'. Opvallend is overigens dat de wetgever zelf struikelt over zijn eigen terminologie, aangezien bijvoorbeeld in art. 39bis §5 Sv. de 'ontoegankelijkmaking' als

[131] O. KLEES, F. ROGGEN en D. VANDERMEERSCH, "Les saisies en matière pénale" in P. CHOMÉ, A. LORENT, F. ROGGEN, J. COLLIN *et al.*, *Droit pénal et procédure pénale*, Mechelen, Kluwer, 2007, (4) 70.

[132] R. VERSTRAETEN, "Beslag in strafzaken" in *Comm.Straf.*, afl. 43, (57) 87.

[133] O. KLEES, F. ROGGEN en D. VANDERMEERSCH, "Les saisies en matière pénale" in P. CHOMÉ, A. LORENT, F. ROGGEN, J. COLLIN *et al.*, *Droit pénal et procédure pénale*, Mechelen, Kluwer, 2007, (4) 70.

[134] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 37.

[135] Amendement (V. VAN QUICKENBORNE), *Parl.St.* Senaat 1999-2000, nr. 2-392/002.

synoniem lijkt te gelden voor 'verhindering van de toegang' en geenszins wordt gelijkgesteld met de verwijdering van de gegevens, hetgeen in de context van die paragraaf immers zou neerkomen op een tautologie. Het ware dan ook wenselijk geweest dat de wetgever het oorspronkelijke wetsontwerp op dat vlak had behouden, eventueel aangevuld met de vermelding 'na kopiename'.

Hierbij kan overigens worden gerefereerd aan het Nederlandse art. 125o Sv. dat enkel gewag maakt van de mogelijkheid van 'ontoegankelijkmaking' en waarbij in de wettekst zelf wordt verduidelijkt dat daaronder zowel wordt verstaan "*het treffen van maatregelen om te voorkomen dat de beheerder van het […] geautomatiseerde werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens*" als "*het verwijderen van de gegevens uit het geautomatiseerde werk, met behoud van de gegevens ten behoeve van de strafvordering*". Opvallend is dat hier geen bijzondere voorwaarden, zoals de strijdigheid met de openbare orde, worden gesteld voor het verwijderen van de gegevens, zodat die laatste maatregel in het Nederlandse recht, anders dan in het Belgische, geen subsidiaire rol vervult. Wellicht verdient deze methode nog de meeste navolging, vermits bezwaarlijk kan worden ingezien waarom het blokkeren van de gegevens een minder grote inbreuk zou uitmaken op de rechten van de betrokkene dan het verwijderen ervan met behoud van een kopie voor de overheid. In beide gevallen kunnen de gegevens hem immers probleemloos opnieuw ter beschikking worden gesteld bij opheffing van het beslag – een digitale kopie is namelijk identiek aan het origineel (zie randnr. 72) – en zijn de gegevens gedurende de maatregel voor hem ontoegankelijk, tenzij de wetgever zou anticiperen op een eventuele 'kraking' door de betrokkene van de door de overheidsdiensten opgestelde blokkeringsmaatregel, hetgeen uiteraard niet de bedoeling kan zijn van een op haar eigen kunnen vertrouwende overheid.

b.3.Bijzondere verplichtingen in hoofde van de bevoegde autoriteit

Gelet op de bijzondere aard van informaticasystemen en netwerken en op het vluchtige karakter van elektronische gegevens, werd een aantal bijzondere verplichtingen opgelegd in hoofde van de bevoegde autoriteit die kunnen worden ingedeeld in een informatieplicht enerzijds, en een bewaringsplicht anderzijds.

b.3.1. Informatieplicht

Overeenkomstig art. 39bis §5 Sv. brengt de procureur des Konings de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking en deelt hij hem een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd (zie evenwel randnr. 83). Die informatieverplichting geldt eveneens ten aanzien van de verantwoordelijke

van het informaticasysteem waarnaar, ingevolge een netwerkzoeking, de zoeking werd uitgebreid, tenzij, aldus art. 88ter §3 Sv., "*diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden*".

De Raad van State was van oordeel dat het begrip 'verantwoordelijke van het informaticasysteem' nader moest worden omschreven[136], hetgeen uiteindelijk evenwel niet gebeurde met het oog op het toelaten van "*enige flexibiliteit aangaande de te contacteren persoon*", zodat de onderzoeksrechter zelf *in concreto* dient na te gaan "*wie de reële of juridische controle over het systeem heeft*"[137]. Toch ware het wenselijk geweest dat de wetgever het advies van de Raad had gevolgd, eventueel in de vorm van een niet-limitatieve lijst van voorbeelden (zie ook randnr. 89). Uit de huidige wettekst valt immers niet met zekerheid op te maken of ook bijvoorbeeld de verdachte zelf aanspraak zou kunnen maken op een dergelijke samenvatting, aangezien de wetgever in de eerste plaats het inlichten van derden op het oog lijkt te hebben. De memorie van toelichting stelt evenwel dat "*de bedoeling van het op de hoogte brengen van de maatregel, is duidelijk te stellen dat het niet gaat om een geheime maatregel*"[138], waarmee aansluiting wordt gezocht bij de regelgeving inzake de huiszoeking. Daarnaast merkt Meunier op dat de informatieplicht haar nut bewijst "*dans la mesure où les données saisies peuvent se révéler essentielles pour l'exercice, par l'inculpé, de ses activités privées ou professionnelles*" en dat het de verdediging in de mogelijkheid stelt "*d'analyser en connaissance de cause l'opportunité d'un référé pénal*"[139], zodat men ervan uit mag gaan dat ook de verdachte zelf, in zijn hoedanigheid van verantwoordelijke van het informaticasysteem, aanspraak kan maken op de in art. 39bis §5 Sv. bedoelde samenvatting.

Daarop voortbouwend komt het overigens als bevreemdend voor dat blijkbaar geen samenvatting moet worden meegedeeld aan de verdachte die niet verantwoordelijk is voor het informaticasysteem. Het lijkt er evenwel op dat hij in dat geval alsnog aanspraak kan maken op het proces-verbaal in art. 35 §1 lid 1 Sv., waarvan door art. 39bis §5 immers niet uitdrukkelijk wordt afgeweken, zodat beide bepalingen cumulatief kunnen worden toegepast. In dat opzicht heeft een verdachte steeds recht heeft op het in art. 35 §1 lid 1 Sv. bedoelde proces-verbaal, maar moet hem daarnaast, in zijn eventuele hoedanigheid als 'verantwoordelijke van het informaticasysteem', een samenvatting worden meegedeeld van de in beslag genomen gegevens. In het

---

136 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 54.

137 I. DELBROUCK, "Informaticacriminaliteit" in H. BERKMOES, W. BRUGGEMAN, I. DELBROUCK, D. DEWANDELEER, F. DESTERBECK, H. FRANSEN, P. HERBOTS, A. MARUT, C. NUYTS, E. VAN DEN HEUVEL *et al.*, *Postal Memorialis*, Antwerpen, Kluwer, 2007, (122) 138.

138 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 21.

139 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 678-679.

licht van de rechten van verdediging ware het evenwel beter geweest ook de verdachte *qualitate qua* uitdrukkelijk een recht op een dergelijke samenvatting te gunnen. Het College van Procureurs-generaal heeft het in zijn omzendbrief weliswaar vanzelfsprekend genoemd "*dat de processen-verbaal die naar aanleiding van het databeslag dienen te worden opgesteld, nauwgezet de uitgevoerde operaties zullen dienen te beschrijven teneinde elke latere betwisting tegen te gaan*"[140], maar zulks blijft niettemin een minder rechtszekere bescherming dan een door de wetgever zelf uitdrukkelijk erkend recht op een samenvatting van de in beslag genomen gegevens. De vraag rijst overigens of de huidige situatie geen ongeoorloofde discriminatie inhoudt van de verdachte *qualitate qua*, aan wie immers, wegens het loutere feit dat hij niet verantwoordelijk is voor het onderzochte informaticasysteem, een belangrijk hulpmiddel wordt ontnomen om een adequate verdediging op te bouwen.

De Belgische discriminatie lijkt bovendien een unicum in het West-Europese juridische landschap. Zo voorziet het Nederlandse art. 125m lid 1 Sv. in een algemene 'notificatieplicht' in hoofde van de officier van justitie dan wel de rechter-commissaris die "*zo spoedig mogelijk aan de betrokkenen schriftelijk mededeling [doet] van [de] vastlegging of ontoegankelijkmaking [van de gegevens] en van de aard van de vastgelegde of ontoegankelijk gemaakte gegevens*". Daarbij verduidelijkt art. 125m lid 2 Sv. dat "*[a]ls betrokkene [...] worden aangemerkt: de verdachte, de verantwoordelijke voor de gegevens en de rechthebbende van een plaats waar een doorzoeking heeft plaatsgevonden*", zodat een Nederlandse verdachte, in zijn loutere hoedanigheid van 'verdachte', aanspraak kan maken op een dergelijke schriftelijke mededeling, onafhankelijk van de vraag of hij al dan niet verantwoordelijk is voor het informaticasysteem. Afgezien van art. 56 en 97 CPP die uitdrukkelijk bepalen dat de kopiëring van elektronische gegevens moet geschieden "*en présence des personnes qui assistent à la perquisition*", bevat het Franse recht dan weer geen enkele informatieverplichting ten aanzien van de verantwoordelijke van het informaticasysteem[141], hetgeen minder navolging verdient, aangezien het op die manier bijzonder ingewikkeld wordt voor die verantwoordelijke om na te gaan welke gegevens precies in beslag werden genomen en of het verdwijnen of blokkeren van die gegevens te wijten is aan een technische storing of aan een maatregel opgelegd door de overheid. Toch is de Franse lacunaire wetgeving onzes inziens te verkiezen boven de Belgische discriminatoire regelgeving, aangezien zij tenminste geen ongelijke behandeling in het leven roept tussen verschillende categorieën van verdachten (zie randnr. 88).

[140] College van Procureurs-generaal bij de Hoven van Beroep, *Wet inzake de informaticacriminaliteit*, 14 februari 2002, Omzendbrief nr. COL 1/2002, http://www.poldoc.be/data/Data/Active/NL/A02336-01/Col0201n.doc, 16.

[141] C. FÉRAL-SCHUHL, *Cyberdroit: le droit à l'épreuve de l'internet*, Parijs, Dalloz, 2006, 657-662.

Die ongelijke behandeling wordt des te opmerkelijker wanneer men bedenkt dat art. 39 Sv. nog steeds de bewoordingen "*in de vorige artikelen*" bevat, zodat het databeslag, dat pas in art. 39bis Sv. ter sprake komt, blijkbaar niet moet gebeuren in aanwezigheid van de verdachte of zijn gemachtigde. Aldus heeft de wetgever – allicht door nalatigheid – een duidelijk ongeoorloofde discriminatie in het leven geroepen tussen de verdachte ten aanzien van wie een gemeenrechtelijke inbeslagneming werd bevolen en de verdachte wiens elektronische gegevens in beslag worden genomen. Is die verdachte bovendien niet de verantwoordelijke van het informaticasysteem, dan wordt hij zelfs op dubbele wijze benadeeld, aangezien hij dan niet alleen niet aanwezig mag zijn bij het leggen van het databeslag, maar daarenboven geen aanspraak kan maken op een samenvatting van de in beslag genomen gegevens, doch zich slechts tevreden moet stellen met het – allicht meer beknopte (zie evenwel randnr. 88) – proces-verbaal.

Ten slotte laat art. 39bis §5 Sv. een aantal vragen onbeantwoord. Zo heeft de Belgische wetgever – opnieuw in tegenstelling tot de Nederlandse (zie randnr. 89) – in de eerste plaats nagelaten te verduidelijken in welke vorm de mededeling moet geschieden. Gelet op het schriftelijke karakter van het onderzoek en ten bate van de rechtszekerheid, mag worden aangenomen dat zulks op schriftelijke wijze dient te gebeuren. Een tweede, belangrijkere leemte vormt het feit dat geen enkele sanctie wordt gekoppeld aan het ontbreken van een dergelijke mededeling. Volgens Meunier moet art. 39bis §5 Sv. in het algemeen worden beschouwd "*sous l'angle des droits de la défense*"[142], doch een dergelijke redenering lijkt ons voorlopig alleen op te gaan wanneer het de verantwoordelijke van het informaticasysteem zelf is die verdacht wordt (zie immers randnr. 88).

b.3.2 Bewaringsplicht

Op de procureur des Konings rust bovendien een bewaringsplicht die, zoals vermeld (zie randnr. 69), eveneens van toepassing is wanneer een materiële drager van elektronische gegevens in zijn geheel in beslag wordt genomen. Overeenkomstig art. 39bis §6 Sv. moeten "*de passende technische middelen [worden aangewend] om de integriteit en de vertrouwelijkheid van de gegevens te waarborgen*" alsook "*voor de bewaring hiervan op de griffie*". Gesteund door Evrard[143] en door Keustermans en Mols[144], vraagt Meunier zich af of het niet beter was geweest "*de prévoir expressément, outre la copie 'de travail' à disposition permanente des autorités judiciaires, une seconde copie conservée au greffe, pour éviter tout risque de déperdition irrémédiable des*

[142] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 679.

[143] S. EVRARD, "La loi du 28 novembre 2000 relative à la criminalité informatique", *JT* 2001, (241) 243.

[144] J. KEUSTERMANS en F. MOLS, "Informaticacriminaliteit" in *Comm.Straf.*, afl. 50, (45) 65.

données"[145]. Met de uitdrukkelijke vermelding dat de procureur des Konings ook de passende technische middelen moet aanwenden "*voor de bewaring [van de gegevens] op de griffie*", lijkt de huidige wetgeving onzes inziens evenwel ter zake reeds een voldoende garantie te bieden. Bovendien dringt het College van Procureurs-generaal er nu reeds op aan dat "*formeel, [de in beslag genomen voorwerpen] zouden worden neergelegd ter griffie, en dat derhalve een staat van overtuigingsstukken zou worden opgemaakt*"[146].

b.4. Opheffing van het databeslag

In art. 39 §1 lid 1 Sv. wordt art. 28sexies Sv. uitdrukkelijk van toepassing verklaard, zodat "*eenieder die geschaad wordt door een opsporingshandeling met betrekking tot zijn goederen, aan de procureur des Konings de opheffing ervan [kan] vragen*" overeenkomstig de gemeenrechtelijke bepalingen. Aangenomen mag worden dat hetzelfde geldt voor art. 61quater Sv. in het kader van een gerechtelijk onderzoek of in de vonnisfase, "*bien que le texte ne le précise pas*"[147]. Bij het oorspronkelijke wetsontwerp werd immers toegelicht dat zowel art. 28sexies Sv. als art. 61quater Sv. van toepassing blijven als gemeen recht[148].

Een uitdrukkelijke verwijzing werd noodzakelijk geacht omdat art. 28sexies Sv. "*spreekt over 'éénieder die geschaad wordt door een opsporingshandeling met betrekking tot zijn goederen', waar met betrekking tot het informaticasysteem het niet noodzakelijkerwijze duidelijk is of een belanghebbende zich eigenaar kan noemen van de kwestieuze gegevens*"[149]. Het is evenwel zeer de vraag of de uiteindelijk aangenomen wettekst het doorbreken van die eigendomsband wel voldoende benadrukt. Toch moet onzes inziens, op grond van de parlementaire voorbereidende werken, worden aanvaard dat ook de benadeelde die zich geen eigenaar kan noemen van de gegevens, de opheffing van het databeslag kan vragen.

De opheffing van het databeslag kan evenwel ook spontaan gebeuren door de ter zake bevoegde autoriteit. Zoals hierboven reeds aangestipt (zie randnr. 81), wordt immers algemeen aanvaard dat de procureur des Konings tijdens een opsporingsonderzoek of de onderzoeksrechter tijdens een gerechtelijk onderzoek, ambtshalve kunnen overgaan tot opheffing van het beslag[150].

---

145 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 673.

146 College van Procureurs-generaal bij de Hoven van Beroep, *Wet inzake de informaticacriminaliteit*, 14 februari 2002, Omzendbrief nr. COL 1/2002, http://www.poldoc.be/data/Data/Active/NL/A02336-01/Col0201n.doc, 17.

147 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 679.

148 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 21.

149 Amendement (F. ERDMAN), *Parl.St.* Kamer 1999-2000, nr. 50-0214/003.

150 R. VERSTRAETEN, "Beslag in strafzaken" in *Comm.Straf.*, afl. 43, (57) 87.

Hetzelfde geldt overigens voor de strafrechter tijdens de vonnisfase, nu het Hof van Cassatie heeft geoordeeld dat "*le juge qui vide l'action publique peut ordonner d'office la restitution des objets saisis à leur propriétaire*"[151]. Op de schijnbare tautologie die gevormd wordt door de onverkort van toepassing gebleven art. 28sexies Sv. en art. 61quater Sv. enerzijds en het jonge art. 39bis §3 lid 3 Sv. anderzijds, werd hierboven reeds ingegaan (zie randnr. 81).

Het valt te betreuren dat de wetgever niet heeft verduidelijkt op welke manier de opheffing van het databeslag moet gebeuren, zodat een antwoord op die vraag moet worden geboden met behulp van redeneringen naar analogie met gemeenrechtelijke bepalingen. Traditioneel beschikt de bevoegde autoriteit ter zake over een belangrijke beoordelingsmarge en kan hij, overeenkomstig art. 28sexies §3 Sv. of art. 61quater §3 Sv., het verzoek tot opheffing van het beslag afwijzen of geheel of gedeeltelijk toestaan, al dan niet onder bepaalde, door hem vrij op te leggen voorwaarden. Aldus kan worden overgegaan tot "*vrijgave van in beslag genomen documenten mits voeging van kopieën*"[152], in welk geval, bij analogische toepassing op het databeslag, de gevolgen van de opheffing in grote mate overeenkomen met die van de in art. 39bis §3 lid 3 Sv. omschreven modaliteit (zie ook randnr. 79). Wordt de opheffing evenwel onvoorwaardelijk toegestaan, dan lijkt het ons vanzelfsprekend dat de gegevens opnieuw worden overgebracht op het informaticasysteem van de betrokkene of dat zij, in voorkomend geval, opnieuw toegankelijk worden gemaakt, en dat nadien alle kopieën die ter beschikking staan van de overheid, onmiddellijk vernietigd worden. Omwille van de eerbiediging van de persoonlijke levenssfeer, ware het onzes inziens evenwel wenselijk een dergelijke onmiddellijke vernietiging ook uitdrukkelijk in de wet op te nemen, naar het voorbeeld van het Nederlandse art. 125n lid 1 Sv. dat voorschrijft dat "*de gegevens die zijn vastgelegd tijdens een doorzoeking*", worden vernietigd, van zodra "*blijkt dat [zij] van geen betekenis zijn voor het onderzoek*". In die zin betreurt ook Dewandeleer dat "*de wet niet voorziet in een uitdrukkelijk voorschrift betreffende het gebruiksverbod en de uitwisseling van de gegevens, zodra blijkt dat de beslagen data toch niet het vereiste verband met de [onderzochte] strafbare feiten vertonen*"[153].

c. Voorwaarden

In art. 39bis §1 lid 1 Sv. werd bepaald dat het databeslag in beginsel geschiedt overeenkomstig de gemeenrechtelijke regelgeving, aangezien de nieuwe bepaling een "*adequate rechtsbasis [creëert] voor een nieuw dwangmiddel met*

---

151 Cass. 24 oktober 1966, *Pas.* 1967, I, 260.

152 R. VERSTRAETEN, "Beslag in strafzaken" in *Comm.Straf.*, afl. 43, (57) 78.

153 D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 141.

dezelfde finaliteiten als de inbeslagneming"[154], zodat op het databeslag dezelfde voorwaarden van toepassing zijn als op de gemeenrechtelijke inbeslagneming. Hierbij kan evenwel worden opgemerkt dat overeenkomstig art. 39bis §2 Sv. slechts wordt overgegaan tot de inbeslagneming van de elektronische gegevens indien "*de inbeslagneming van de drager daarvan […] niet wenselijk is*", hetgeen een soort subsidiariteitsvoorwaarde lijkt in te houden (zie ook randnr. 73).

d. Bevoegde autoriteit

In art. 39bis Sv. wordt enkel de procureur des Konings aangeduid als bevoegde autoriteit. De WIC voegde in art. 89 Sv. evenwel een referentie aan dat artikel in, waardoor ook de onderzoeksrechter volledig bevoegd wordt om over te gaan tot databeslag. Aangenomen moet worden dat hij, overeenkomstig art. 89bis Sv., die opdracht ook kan delegeren aan een officier van gerechtelijke politie. Het weze bovendien duidelijk dat het databeslag kan worden bevolen via mini-instructie, aangezien die maatregel door art. 28septies Sv. niet wordt uitgesloten. De bewering van Roggen, Klees en Vandermeersch dat zulks niet mogelijk zou zijn, omdat een geïnformatiseerde omgeving zou moeten worden gelijkgesteld met een huiszoeking[155], moet dan ook ten stelligste worden afgewezen.

Een vreemd genoeg door de rechtsleer voorlopig onopgemerkt juridisch-technisch probleem is onzes inziens dat de wetgever heeft nagelaten art. 28bis §3 lid 1 Sv. uit te breiden, waarin wordt gesteld dat de opsporingshandelingen "*de inbeslagneming van de zaken vermeld in de artikelen 35 en 35ter*" kunnen inhouden, zodat ook de procureur des Konings de bevoegdheid geniet om, betreffende die zaken, over te gaan tot dwangmaatregelen. Wat betreft de elektronische gegevens vermeld in art. 39bis Sv., wordt een dergelijke bevoegdheid hem evenwel niet uitdrukkelijk toegekend. Men zou kunnen stellen dat die minstens impliciet besloten ligt in de '*lex specialis*' van art. 39bis Sv., dat anders immers grotendeels buiten werking zou worden gesteld, maar zulks geldt eveneens voor art. 35 en 35ter Sv. die dan weer wel uitdrukkelijk vermeld worden. Voor de 'gegevens nuttig voor dezelfde doeleinden als de gemeenrechtelijke inbeslagneming' (zie randnr. 76) lijkt dat euvel vooralsnog oplosbaar door te stellen dat die zaken ook worden vermeld in art. 35 en 35ter Sv., maar inzake de 'gegevens noodzakelijk om die gegevens te verstaan' (zie randnr. 77), gaat een dergelijke redenering niet op. De tegenstrijdigheid tussen art. 28bis §3 lid 1 Sv. en art. 39bis Sv. kan bovendien evenmin worden opgelost door toepassing van het adagium '*lex posterior anteriori derogat*', aangezien art. 28bis §3 lid 1 Sv. in 2002 nog

[154] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 20.

[155] O. KLEES, F. ROGGEN en D. VANDERMEERSCH, "Les saisies en matière pénale" in P. CHOMÉ, A. LORENT, F. ROGGEN, J. COLLIN *et al.*, *Droit pénal et procédure pénale*, Mechelen, Kluwer, 2007, (4) 68.

werd aangepast[156], overwegende dat "*het maar logisch [is] dat ook deze vorm van inbeslagneming in het raam van een opsporingshandeling mogelijk wordt gemaakt*"[157], hetgeen treffend de op het eerste gezicht logische juridische gevolgen van het ongewijzigd blijven van art. 28bis §3 lid 1 Sv., omschrijft.

2.3. BEVEL TOT MEDEWERKING

Gelet op het hoogtechnologische karakter van een geïnformatiseerde omgeving waarin een bepaalde zoeking of inbeslagneming moet plaatsvinden, is het begrijpelijk dat "*de overheid niet steeds [beschikt] over voldoende gespecialiseerde onderzoekers*"[158]. Teneinde de efficiëntie van het strafonderzoek te bevorderen, voegde art. 8 WIC een nieuw art. 88quater Sv. in, dat voorziet in een bevel tot medewerking, uit te vaardigen door de onderzoeksrechter. In de rechtsleer wordt art. 88quater Sv. doorgaans op onnauwkeurige wijze bestempeld als een 'medewerkingsplicht', hetgeen een soort verplichting tot actief handelen lijkt te impliceren in hoofde van de betrokkenen. De medewerking moet evenwel uitdrukkelijk worden bevolen, waardoor het nauwkeuriger is te gewagen van een 'bevel tot medewerking', zoals Verstraeten nagenoeg als enige doet[159].

2.3.1. Soorten bevelen tot medewerking

Sedert de inwerkingtreding van de WIC, kan de onderzoeksrechter twee soorten bevelen tot medewerking *sensu lato* afleveren, waarvoor een enigszins verschillende regelgeving werd opgesteld, namelijk enerzijds een bevel tot het verstrekken van bepaalde inlichtingen en anderzijds een bevel tot het zelf uitvoeren van bepaalde operaties op het informaticasysteem, dat kan worden beschouwd als een bevel tot medewerking *sensu stricto*. Voor personen die gehouden zijn door het beroepsgeheim wordt in de parlementaire werkzaamheden "*verwezen naar de regels van het gemeen recht*"[160].

a. Bevel tot het verstrekken van bepaalde inlichtingen

Overeenkomstig art. 88quater §1 Sv. kan de onderzoeksrechter "*personen van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking*" of van informaticatechnologie in het algemeen "*bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen*". Dat

[156] Art. 6 wet 19 december 2002 tot uitbreiding van de mogelijkheden tot inbeslagneming en verbeurdverklaring in strafzaken, *BS* 14 februari 2003 (ed. 2), 7547.

[157] Wetsontwerp tot uitbreiding van de mogelijkheden tot inbeslagneming en verbeurdverklaring in strafzaken, *Parl.St.* Kamer 2001-02, nr. 50-0214/001, 45.

[158] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 27.

[159] R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 461.

[160] Wetsontwerp tot uitbreiding van de mogelijkheden tot inbeslagneming en verbeurdverklaring in strafzaken, *Parl.St.* Kamer 2001-02, nr. 50-0214/001, 28.

bevel moet 'de omstandigheden eigen aan de zaak' vermelden en wordt 'met reden omkleed' meegedeeld aan de procureur des Konings. De onderzoeksrechter kan zijn opdracht evenwel delegeren aan een officier van gerechtelijke politie, hulpofficier van de procureur des Konings.

Uit de parlementaire werkzaamheden blijkt dat vooral gedacht wordt aan deskundigen die informatie kunnen verschaffen omtrent "*de toegangsmogelijkheden, de configuratie, de beveiliging en de cryptografische sleutels*"[161]. Deze medewerkingsvorm kan echter – althans volgens de wetgever – ook aan anderen worden opgelegd en zelfs aan de verdachte zelf of aan diens naaste familieleden (zie evenwel randnrs. 106-107). Neemt het bevel tot het verstrekken van bepaalde inlichtingen evenwel de vorm aan van een verhoor, dan moet volgens Meunier worden aangenomen dat de verdachte de bescherming geniet van de in art. 47bis en 70bis Sv. opgenomen bepalingen[162].

b. Bevel tot het uitvoeren van bepaalde operaties

Krachtens art. 88quater §2 lid 1 Sv. kan de onderzoeksrechter daarnaast "*iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen*", waardoor in hoofde van de betrokkene een 'inspanningsverbintenis' ontstaat om die opdracht naar eigen vermogen uit te voeren. In tegenstelling tot een 'bevel tot het verstrekken van bepaalde inlichtingen' (zie randnr. 103), kan dit 'bevel tot het uitvoeren van bepaalde operaties' evenwel niet worden gedelegeerd, aangezien het "*de onderzoeksrechter [toelaat] nog een stap verder te gaan en te eisen van al deze personen dat ze desgevraagd zelf de onderzoekshandelingen stellen*"[163].

Bovendien wordt, eveneens in tegenstelling tot wat het geval is bij het 'bevel tot het verstrekken van bepaalde inlichtingen' (zie randnr. 104), in art. 88quater §2 lid 2 Sv. uitdrukkelijk vermeld dat deze verplichting niet kan worden opgelegd aan de personen bedoeld in art. 156 Sv. of aan de verdachte zelf. Geheel terecht stelt Verstraeten zich de vraag "*waarom de wetgever op grond van het non-incriminatiebeginsel enkel een uitzondering heeft voorzien op het bevel tot [het uitvoeren van bepaalde operaties] en niet op het bevel tot inlichtingen*"[164]. Ook De Hert en Lichtenstein uiten kritiek op die werkwijze en verduidelijken dat zulks zeker geen onzorgvuldigheid betreft, maar een bewust door de wetgever gewilde situatie[165], aangezien hij de "*andere verplichtingen*

[161] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 27; J. KEUSTERMANS en F. MOLS, "De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht", *RW* 2001-02, afl. 21, (721) 731.

[162] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 682.

[163] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 70.

[164] R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 461.

[165] P. DE HERT en G. LICHTENSTEIN, "Huiszoeking en beslag in geautomatiseerde omgevingen", *Custodes* 2003, afl. 4, (59) 72.

in dit opzicht" niet als onverenigbaar beschouwt "*met de vereisten die worden gesteld door het EVRM*", waarbij hij verwijst naar het bekende arrest Saunders van het Europees Hof voor de Rechten van de Mens[166].

Het standpunt van de wetgever kan evenwel in het geheel niet worden gevolgd. Op geen enkele wijze kan immers worden ingezien waarom de verplichting tot het verstrekken van bepaalde inlichtingen opgelegd aan een verdachte, bijvoorbeeld het mededelen van een bepaald wachtwoord, geen schending zou inhouden van het in art. 6 EVRM vervatte non-incriminatiebeginsel, zeker wanneer men bedenkt dat een schending van die verplichting strafrechtelijk wordt gesanctioneerd (zie randnr. 111). De verwijzing naar het arrest Saunders is overigens misplaatst, aangezien het Hof in dat arrest precies besloot tot een schending van art. 6 EVRM, overwegende dat "*the right not to incriminate oneself lies at the heart of a fair procedure and applies to all types of criminal proceedings*" en dat "*[i]t is primarily concerned with respecting the will of an accused person to remain silent*"[167]. Om die redenen moet dan ook worden aangenomen dat, in het licht van art. 6 EVRM, de in art. 88quater §2 lid 2 Sv. vervatte regel moet worden uitgebreid naar de in art. 88quater §1 Sv. beschreven situatie.

Ook hier is overigens een belangrijk verschil op te merken met het Nederlandse art. 125k Sv. dat weliswaar toelaat een 'bevel tot decryptie' uit te vaardigen ten aanzien van "*degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk*", maar dat sedert 1 juni 2006 uitdrukkelijk bepaalt dat een dergelijk bevel "*[niet wordt] gegeven aan de verdachte*", noch aan een aantal 'functioneel verschoningsgerechtigden' opgesomd in art. 96a lid 3 Sv., onder wie de naaste familieleden van de verdachte. Opmerkelijk is overigens dat de Nederlandse wetgever destijds, in tegenstelling tot de Belgische (zie randnr. 106), geenszins bewust heeft nagelaten een dergelijke bescherming in te voeren, maar dat het, aldus Cleiren en Nijboer, slechts een 'omissie' betrof die later werd rechtgezet[168]. De Franse wetgever lijkt daarentegen evenmin als de Belgische voldoende rekening te hebben gehouden met het non-incriminatiebeginsel, gelet op art. 230-1 CPP dat voorschrijft dat de procureur, de onderzoeksrechter of de strafrechter tijdens de vonnisfase "*peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement*".

---

166 Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 27.

167 EHRM 17 december 1996, Saunders/Verenigd Koninkrijk, *JDF* 1997, 98, noot, *JTDE* 1997, 67 en *Rep.Eur.Court H.R.* 1996, afl. 6, 2044.

168 C. CLEIREN en J. NIJBOER, *Strafvordering: tekst & commentaar*, Deventer, Kluwer, 2007, 355.

Bovendien worden in het Franse art. 434-15-2 CP bijzonder zware straffen opgelegd aan "*quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités*". Toch is onzes inziens ook hier de Franse regelgeving te verkiezen boven de Belgische (zie ook randnr. 89). Aangezien het Franse art. 230-1 CPP geen uitdrukkelijk onderscheid maakt tussen het verstrekken van bepaalde inlichtingen en het uitvoeren van bepaalde operaties, zou de rechtspraktijk daar immers eventueel via interpretatietechnieken tot het besluit kunnen komen dat het bevel tot medewerking in het algemeen niet kan worden opgelegd aan de verdachte zelf. De Belgische wetgever daarentegen, heeft wel een dergelijk onderscheid aangebracht, zodat interpretatietechnieken ter zake geen soelaas kunnen bieden en de wettekst op zichzelf hoe dan ook een schending inhoudt van art. 6 EVRM.

Aansluitend bij het non-incriminatiebeginsel waarschuwt ten slotte Verstraeten, gesteund door Keustermans en Mols[169], dat zich de situatie kan voordoen waarin "*een bevel tot medewerking wordt gegeven aan een persoon die op dat ogenblik nog geen verdachte is, doch ingevolge de latere vaststellingen […] wél een verdachte kan/zal worden*", zodat het aangewezen is dat de onderzoeksrechter enkel de medewerking beveelt – ook *sensu lato* (zie randnrs. 102 en 107) – van "*personen waarvan vermoed kan worden dat zij zeker niet betrokken zijn bij eventuele misdrijven die via hun medewerking aan het licht kunnen komen*"[170].

2.3.2. Geheimhouding

Overeenkomstig art. 88quater §4 Sv., is "*iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent*", tot geheimhouding verplicht, hetgeen door art. 458 Sw. strafrechtelijk wordt gesanctioneerd. Om begrijpelijke redenen achtte de wetgever die geheimhoudingsverplichting noodzakelijk teneinde "*het geheim van het onderzoek in deze materie te beschermen*"[171].

---

[169] J. KEUSTERMANS en F. MOLS, "De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht", *RW* 2001-02, afl. 21, (721) 731.

[170] R. VERSTRAETEN, *Handboek strafvordering*, Antwerpen, Maklu, 2007, 461; College van procureurs-generaal bij de hoven van beroep, *Wet inzake de informaticacriminaliteit*, 14 februari 2002, Omzendbrief nr. COL 1/2002, http://www.poldoc.be/data/Data/Active/NL/A02336-01/Col0201n.doc, 22.

[171] Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 10.

2.3.3. Strafrechtelijke handhaving van de medewerking

In art. 88quater §3 Sv. wordt de medewerking strafrechtelijk beteugeld, aan de hand van een nieuw ingevoerd misdrijf dat bestaat in de weigering "*de in §§1 en 2 gevorderde medewerking te verlenen*" of in de loutere 'hindering' van de zoeking in het informaticasysteem. Hierboven werd reeds vermeld dat de strafrechtelijke handhaving van een bevel tot het verstrekken van bepaalde inlichtingen een bijzonder probleem vormt in het kader van het non-incriminatiebeginsel wanneer het wordt opgelegd aan de verdachte zelf (zie randnr. 107). Bovendien laat de redactie van het wetsartikel op materieelrechtelijk vlak te wensen over. Nergens wordt immers een bijzonder opzet vereist[172], zodat voor dit 'nevenwanbedrijf' onachtzaamheid in hoofde van de dader lijkt te volstaan[173]. In tegenstelling tot art. 46bis §2 lid 4 Sv., dat enkel de 'weigering' de gevorderde gegevens mee te delen, strafbaar stelt en aldus minstens een algemeen opzet vereist[174] (zie ook randnrs. 112 en 119), straft art. 88quater §3 Sv. namelijk eenieder die de zoeking in het informaticasysteem 'hindert', zodat ook hij die zulks onopzettelijk doet, bijvoorbeeld wegens een gebrek aan technische kennis, in beginsel bestraft kan worden.

Uit de strafrechtelijke handhaving van de medewerking, kan onder meer worden afgeleid dat, in geval van weigering, de medewerking alsnog kan worden afgedwongen in de vorm van een bevel tot 'teruggave' overeenkomstig art. 161 Sv., eventueel onder verbeurte van een dwangsom. Zulks kan worden afgeleid uit een vonnis van 2 maart 2009 van de correctionele rechtbank te Dendermonde[175] waarin ten aanzien van de Amerikaanse onderneming Yahoo de teruggave werd bevolen van de gegevens die zij krachtens art. 46bis Sv. had moeten meedelen aan de procureur des Konings, overwegende dat "*door de weigering van de beklaagde om de gegevens te verstrekken een met de wet strijdige toestand is ontstaan, namelijk het Openbaar Ministerie komt niet in het bezit van de gegevens waarvan het de mededeling had gevorderd*". Aan die teruggave werd bovendien een dwangsom gekoppeld van 10 000 euro "*per dag vertraging in mededeling van de gevorderde gegevens*", gelet op het feit dat "*[d]e dwangsom [weliswaar] niet opgelegd [kan] worden om recidive te vermijden*", maar wel om het herstel te verzekeren van een wederrechtelijke toestand. Ofschoon zeer betwistbaar in het kader van de internationaalrechtelijke bevoegdheidsregels (zie randnr. 119), verdient het vonnis op dit vlak allicht navolging en kan de redenering die erin besloten ligt, worden uitgebreid naar de in art. 88quater Sv.

---

[172] O. KLEES, F. ROGGEN en D. VANDERMEERSCH, "Les saisies en matière pénale" in P. CHOMÉ, A. LORENT, F. ROGGEN, J. COLLIN *et al.*, *Droit pénal et procédure pénale*, Mechelen, Kluwer, 2007, (4) 76.

[173] F. VERBRUGGEN en R. VERSTRAETEN, *Strafrecht en strafprocesrecht voor bachelors*, I, Antwerpen, Maklu, 2007, 56.

[174] Corr. Dendermonde 2 maart 2009, *T.Strafr.* 2009, afl. 2, 116, noot.

[175] Corr. Dendermonde 2 maart 2009, *T.Strafr.* 2009, afl. 2, 116, noot.

opgenomen medewerkingsverplichting. Alle rechthebbenden, alsook het Openbaar Ministerie, kunnen immers een vordering tot teruggave instellen[176], zodat ook de medewerking die het parket rechtmatig had gevorderd, vatbaar is voor een dergelijke teruggave.

2.3.4. Staatsaansprakelijkheid wegens onopzettelijk veroorzaakte schade

Ten slotte neemt de Staat, volgens art. 88quater §5 Sv., de burgerrechtelijke aansprakelijkheid op zich "*voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de [daarin opgeslagen] gegevens*" wordt veroorzaakt. Het zou immers "*onredelijk zijn dat deze personen hiervoor burgerlijk aansprakelijk zouden worden gesteld, tenzij zij opzettelijk schade zouden berokkenen*"[177]. Voor opzettelijk veroorzaakte schade kan *a contrario* uiteraard een gemeenrechtelijke vordering worden ingesteld op basis van art. 1382 BW jegens de aansprakelijke.

Hierbij merkt Laureys op dat art. 88quater §5 Sv. weliswaar voorziet in een vergoeding voor de gebruiker van een beschadigd informaticasysteem, maar dat geen enkele bepaling een vergoeding toekent aan bijvoorbeeld "*[de] onafhankelijke expert die wordt opgevorderd om drie maanden mee te werken aan een onderzoek*"[178]. Die kritiek, die overigens ook door Meunier wordt geuit[179], lijkt ons inderdaad terecht. Zelfs indien men de geleverde diensten zou beschouwen als een 'burgerplicht', dan nog kan de ongelijke behandeling niet verklaard worden ten opzichte van bijvoorbeeld juryleden, die immers eveneens een burgerplicht uitoefenen en wel een – weliswaar beperkte – vergoeding ontvangen. Bovendien kan een jurylid, in tegenstelling tot een informaticus wiens medewerking werd bevolen, zijn loon gedurende vijf dagen doorbetaald zien wegens 'klein verlet'[180]. Het lijkt erop dat een privédeskundige om die reden slechts sporadisch zal worden opgevorderd en dat het tijdrovende werk veelal door de *Computer Crime Units* van de politiediensten zal gebeuren. Uit de jaarverslagen van het Comité P blijkt evenwel dat ook die gespecialiseerde politiediensten "*over onvoldoende personeelsleden [beschikken] om aan de huidige vraag te voldoen*"[181] en dat de "*problemen bij de aanwerving van bekwame personen*" vooral te wijten zijn

---

176 A. VANDEPLAS, "Teruggave" in *Comm.Straf.*, afl. 43, (241) 270.

177 Verslag namens de commissie voor de justitie uitgebracht door de heer Servais VERHERSTRAETEN, *Parl.St.* Kamer 1999-2000, nr. 50-0213/004, 10.

178 T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 83.

179 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 683.

180 Art. 2, XII KB 28 augustus 1963 betreffende het behoud van het normaal loon van de werklieden, de dienstboden, de bedienden en de werknemers aangeworven voor de dienst op binnenschepen, voor afwezigheidsdagen ter gelegenheid van familiegebeurtenissen of voor de vervulling van staatsburgerlijke verplichtingen of van burgerlijke opdrachten, *BS* 11 september 1963, 8864.

181 Vast Comité van Toezicht op de politiediensten, *Jaarverslag 2000*, http://www.comitep.be/download/2000-nl.pdf, 102.

aan een gebrek aan een competitieve verloning[182]. Aan het huidige gebrek aan specialisatie en expertise zal dan ook enkel volledig kunnen worden verholpen wanneer de Belgische Staat ook voldoende middelen ter beschikking stelt om te kunnen voorzien hetzij in een bijzondere vorming voor de politiediensten, hetzij in een redelijke vergoeding voor externe deskundigen of, in het beste geval, in elk van beide.

2.4. ZOEKING EN INBESLAGNEMING OVER DE STAATSGRENZEN HEEN

Gelet op de internationale verwevenheid van netwerken, is het niet ondenkbaar dat, ingevolge een netwerkzoeking, onbewust staatsgrenzen worden overschreden. In zijn advies over de WIC waarschuwde de Raad van State dan ook voor een mogelijke schending van de territoriale staatssoevereiniteit[183]. Wil men een zoeking uitbreiden over de staatsgrenzen heen, dan moet immers een internationale rogatoire commissie worden opgericht. Omdat op die manier heel wat kostbare tijd verloren dreigt te gaan, besloot de wetgever uiteindelijk de extraterritoriale netwerkzoeking alsnog toe te laten, maar beperkte hij de mogelijkheid van inbeslagneming van de aldus aangetroffen gegevens. Zo bepaalt art. 88ter §3 lid 2 Sv. dat dergelijke 'buitenlandse' gegevens enkel mogen worden gekopieerd en dus niet ontoegankelijk mogen worden gemaakt. De onderzoeksrechter dient bovendien onverwijld, via het parket, het ministerie van Justitie op de hoogte te brengen van de extraterritoriale netwerkzoeking dat op zijn beurt de betrokken Staat inlicht. Die vereenvoudigde procedure kan, volgens een omzendbrief van het College van Procureurs-generaal, evenwel enkel worden gevolgd wanneer de buitenlandse gegevens "*op een toevallige of onopzettelijke manier*" zijn aangetroffen of in het bekende geval van de '*hot pursuit*', namelijk "*in spoedeisende gevallen om de teloorgang van het bewijsmateriaal te vrijwaren*"[184]. Dewandeleer voegt daaraan een derde hypothese toe, namelijk wanneer "*[de onderzoekers] er redelijkerwijze niet in slagen [de betrokken Staat] te identificeren*"[185]. Buiten die drie hypothesen moet bijgevolg alsnog de klassieke internationaalrechtelijke regelgeving worden gevolgd.

Opnieuw verschilt de Belgische oplossing evenwel in belangrijke mate van die van de ons omringende landen die een extraterritoriale zoeking of inbeslagneming aan meer verregaande beperkingen onderwerpen. Zo werd in de memorie van toelichting bij het Nederlandse art. 125j Sv. (zie ook randnr.

---

[182] Vast Comité van Toezicht op de politiediensten, *Jaarverslag 2001*, http://www.comitep.be/2001/PDF/Deel_3.pdf, 152.

[183] Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 50-0214/001, 46.

[184] College van Procureurs-generaal bij de Hoven van Beroep, *Wet inzake de informaticacriminaliteit*, 14 februari 2002, Omzendbrief nr. COL 1/2002, http://www.poldoc.be/data/Data/Active/NL/A02336-01/Col0201n.doc, 18.

[185] D. DEWANDELEER, "Misdrijven en strafonderzoek in de IT-context" in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis: Straf- en strafprocesrecht*, Brugge, die Keure, 2010, (125) 150.

45) de vraag of het is toegestaan dat artikel over de landsgrenzen heen toe te passen, in het geheel ontkennend beantwoord, aangezien "*de Nederlandse wet […] geen grondslag [biedt] voor een onderzoek in een geautomatiseerd werk dat onder de jurisdictie van een ander land valt*"[186], zodat een dergelijk extraterritoriaal onderzoek de toestemming veronderstelt van de bevoegde Staat[187]. Zo ook bepaalt het Franse art. 57-1 CPP uitdrukkelijk dat buitenlandse gegevens onderzocht kunnen worden "*sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur*", zodat ook daar, anders dan in België, de gemeenrechtelijke regelgeving inzake internationaalrechtelijke bevoegdheid onverkort van toepassing blijft.

Het Belgische art. 88ter §3 lid 2 Sv. is dan ook niet gespaard gebleven van ernstige kritiek in de rechtsleer. Zo stelt Meunier radicaal dat "*seule une Convention internationale, qui n'existe pas encore, pourrait autoriser le juge d'instruction à 'déborder' sur le territoire d'un autre Etat pour y poser un acte de contrainte, comme la copie*"[188]. Ook Evrard leest in art. 88ter §3 lid 2 Sv. "*un sérieux problème de droit international public*", maar maakt een voorbehoud voor "*les données qui sont consultables publiquement à partir d'un ordinateur situé en Belgique*" die volgens hem wel gekopieerd moeten kunnen worden, zonder dat zulks een schending van de staatssoevereiniteit inhoudt[189]. Voor andere gegevens moet daarentegen, bij gebrek aan een internationaal verdrag ter zake, een internationale rogatoire commissie worden opgestart. Hierbij kan evenwel worden opgemerkt dat het Europese Cybercrimeverdrag (zie ook randnr. 2) intussen wel voorziet dat "*[a] Party may, without the authorisation of another Party […] access publicly available (open source) stored computer data, regardless of where the data is located geographically*"[190], zodat de territoriale staatssoevereiniteit tussen de Europese Staten die partij zijn bij dat verdrag, geen beletsel meer vormt voor een grensoverschrijdende netwerkzoeking in zogenaamde '*open source data*'[191]. Strekt de netwerkzoeking zich evenwel uit tot in andere Staten of heeft zij betrekking op meer private gegevens, dan lijkt art. 88ter §3 lid 2 Sv. ons niet toepasbaar, gelet op de afwezigheid van een internationale overeenkomst ter zake.

---

186 F. WIEMANS, *Onderzoek van gegevens in geautomatiseerde werken*, Nijmegen, Wolf Legal Publishers, 2004, 152-153.

187 G. CORSTENS, *Het Nederlandse strafprocesrecht*, Deventer, Kluwer, 2005, 479.

188 C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal à l'ère numérique", *RDPC* 2001, (611) 677-678.

189 S. EVRARD, "La loi du 28 novembre 2000 relative à la criminalité informatique", *JT* 2001, (241) 244.

190 Art. 32 verdrag van Boedapest inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van 23 november 2001, *European Treaty Series No. 185*, http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc.

191 P. DE HERT en G. LICHTENSTEIN, "De betekenis van het Europees verdrag cybercriminaliteit voor het vooronderzoek en de internationale samenwerking", *Vigiles* 2004, afl. 5, (153) 168.

Volgens Laureys kon de 'ganse' discussie inzake staatssoevereiniteit worden vermeden "*door het databeslag enkel te leggen op [de] tempory files*"[192] (*sic*), waarmee hij allicht doelt op de *temporary internet files* die op de harde schijf van een informaticasysteem worden opgeslagen. Ofschoon zulks in bepaalde gevallen inderdaad tot gelijkaardige onderzoeksresultaten zal leiden, kan een dergelijke methode onzes inziens evenwel geen volwaardig alternatief bieden voor de netwerkzoeking. Zoals de benaming zelf aangeeft, worden de *temporary internet files* immers slechts 'tijdelijk' opgeslagen in het informaticasysteem en kunnen zij bovendien door de gebruiker zelf probleemloos worden verwijderd, hetgeen allicht geregeld zal gebeuren, zeker wanneer die bestanden belangrijk bewijsmateriaal bevatten, zodat de mogelijkheid van een extraterritoriale netwerkzoeking en databeslag onontbeerlijk blijft.

Niet alleen de zoeking en inbeslagneming, ondervinden ten slotte belangrijke toepassingsproblemen wanneer zij extraterritoriaal worden uitgevoerd, maar ook het bevel tot medewerking dat de onderzoeksrechter immers in bepaalde gevallen zal willen uitvaardigen ten aanzien van buitenlandse ondernemingen. Te dezen kan worden verwezen naar het hierboven reeds aangehaalde vonnis van de correctionele rechtbank te Dendermonde[193] waarin het Amerikaanse bedrijf Yahoo werd veroordeeld tot een geldboete van 55 000 euro en tot 'teruggave' van de gevorderde gegevens (zie randnr. 112) wegens schending van een andere, doch gelijkaarde medewerkingsplicht, namelijk die van art. 46bis §2 Sv. die "*[i]edere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst*" ertoe verplicht bepaalde gegevens ter identificatie van een abonnee of gebruiker van de dienst mee te delen aan de procureur des Konings, wanneer hij zulks vordert. Yahoo had *in casu* geweigerd die persoonsgegevens te verstrekken, verklarende dat een "*dergelijke vraag [ingevolge de US Electronic Communications Privacy Act] moet verlopen via het US Departement of Justice*" (*sic*). De rechtbank besloot echter dat "*de medewerkingsplicht ex [art. 46bis en/of art. 88bis Sv.] zich uitstrekt tot elke ISP die in België diensten ontplooit en aanwezig is*", hetgeen evenwel in het geheel niet kan worden nagevolgd. Tussen de Verenigde Staten en België bestaat immers een bilaterale overeenkomst inzake rechtshulp in strafzaken[194], zodat De Busser terecht opmerkt dat "*[h]et Dendermondse parket […] een rechtshulpverzoek [had] kunnen versturen aan de Amerikaanse autoriteit bevoegd voor Sunnyvale, Californië, waar Yahoo's hoofdzetel is gevestigd*" en de kans dan ook groot acht "*dat Yahoo gelijk krijgt in [hoger] beroep*"[195]. Die

[192] T. LAUREYS, *Informatica criminaliteit: actuele wetgeving*, Gent, Mys & Breesch, 2001, 65.

[193] Corr. Dendermonde 2 maart 2009, *T.Strafr.* 2009, afl. 2, 116, noot.

[194] Overeenkomst tussen het Koninkrijk België en de Verenigde Staten van Amerika aangaande de rechtshulp in strafzaken, ondertekend op 28 januari 1988, *BS* 8 december 1999, 45434.

[195] E. DE BUSSER, "Yahoo weigert IP-adressen door te spelen aan Belgisch gerecht", *De Juristenkrant*, afl. 186, 3.

overwegingen betroffen weliswaar de medewerkingsverplichting van art. 46bis Sv. en, bij uitbreiding, van art. 88bis Sv., doch tonen treffend aan dat ook art. 88quater Sv. niet zonder meer over de staatsgrenzen heen kan worden toegepast. Een wereldwijd initiatief ter zake, gelijkaardig aan dat van de Raad van Europa (zie randnr. 2), lijkt ons dan ook voorlopig de enige uitweg uit de moeilijke verhouding tussen het grenzeloze internet en het staatsgebonden strafrecht.

3. BESLUIT

Besluitend kan worden gesteld dat, ondanks de lovenswaardige inspanningen van de Belgische wetgever ter zake en de uitgebreide parlementaire werkzaamheden die aan de WIC zijn voorafgegaan, de zoeking en inbeslagneming ook in hun huidige, gemoderniseerde vorm nog steeds bijzondere toepassingsproblemen ondervinden in een geïnformatiseerde omgeving. Naargelang de ernst van het probleem en de moeilijkheidsgraad van zijn oplossing, kunnen die knelpunten worden ingedeeld in een drietal categorieën.

Een eerste categorie wordt gevormd door een aantal hindernissen van louter redactionele aard die op relatief eenvoudige wijze kunnen worden overwonnen door rechtsleer en rechtspraak. Zo heeft de wetgever in eerste plaats nagelaten bijzondere bepalingen op te nemen inzake de unilokale zoeking in een informaticasysteem, of zelfs maar, zoals men in Nederland wel heeft gedaan, te verwijzen naar de gemeenrechtelijke regelgeving (zie randnr. 8), hetgeen belangrijke vragen doet rijzen omtrent welke gemeenrechtelijke voorwaarden kunnen worden geëxtrapoleerd naar een geïnformatiseerde omgeving. Een gelijkaardig probleem stelt zich overigens bij de netwerkzoeking, waarbij het evenmin duidelijk is in hoeverre bijvoorbeeld de gemeenrechtelijke uitzonderingsgevallen van toestemming en ontdekking op heterdaad van toepassing kunnen worden geacht. Voor elk van die problemen kon hierboven echter, met behulp van een aantal eenvoudige redeneringen naar analogie, een ondubbelzinnige oplossing worden aangereikt (zie randnrs. 25 en 62), zodat een wetgevend optreden ter zake niet onontbeerlijk is voor een goede rechtsgang. Hetzelfde geldt voor de vraag in welke vorm een rechterlijk bevel tot netwerkzoeking moet worden afgeleverd (zie randnr. 65) of de samenvatting van de in beslag genomen gegevens aan de verantwoordelijke voor het informaticasysteem moet worden meegedeeld (zie randnr. 91). Ten slotte kan ook de bedenkelijke terminologie in bepaalde voorschriften, zoals het begrip ‘toegang’ in art. 88ter §2 Sv. (zie randnr. 44) of de term ‘ontoegankelijkmaking’ in art. 39bis §3 lid 2 Sv. (zie randnr. 83), onder deze categorie van problemen worden gebracht, vermits zij, gelet op de uitgebreide toelichting ervan tijdens de parlementaire werkzaamheden, niet per se noopt

tot een effectieve wetswijziging, ofschoon zulks niettemin aanbevelenswaardig blijft ten bate van de rechtszekerheid van de Belgische burger.

Aan een tweede categorie van problemen kan daarentegen enkel worden verholpen door de wetgever zelf, hetzij omdat de door hem opgestelde tekst zo helder is dat hij geen ruimte laat voor interpretatie, hetzij omdat hij zo vaag werd geformuleerd dat ook rechtsleer en rechtspraak ter zake in het duister tasten. Als voorbeeld van dat laatste geval kan gelden het door de wetgever bijzonder summier omschreven criterium van 'overbrenging' dat de grenzen aangeeft tussen het toepassingsgebied van de netwerkzoeking en dat van de informaticatap (zie randnr. 32). Zoals hierboven werd betreurd, kan de operationele definitie van Van Linthout en Kerkhofs immers slechts als lapmiddel dienen in afwachting van een wetgevend ingrijpen, dat onzes inziens overigens best het criterium zou huldigen van het al dan niet heimelijke karakter van de maatregel (zie randnr. 42). Een ander voorbeeld van problematische legislatieve vaagheid vormt de onduidelijke preambule van art. 88ter Sv., waardoor de mogelijkheid van een secundaire netwerkzoeking voorlopig uitgesloten lijkt (zie randnr. 55), hoewel alleen een wetswijziging in die zin duidelijkheid kan scheppen. Daarnaast zijn bij het invoeren van de WIC ook belangrijke juridisch-technische problemen in het Wetboek van Strafvordering geslopen waarvoor, rekening houdend met het principe van de *acte clair*, geen oplossing kan worden geboden door de rechtspraktijk, ofschoon het vaak slechts een onzorgvuldigheid betreft. Zo moet de dubbele discriminatie van de verdachte ten aanzien van wie de maatregel van het databeslag werd bevolen en die niet verantwoordelijk is voor het informaticasysteem (zie randnr. 90), voorlopig gehandhaafd worden in afwachting van een rechtzetting door de wetgever zelf of een terechtwijzing door het Grondwettelijk Hof. Zo ook blijft het ongewijzigd voortbestaan van art. 28bis §3 lid 1 Sv., zoals hierboven uiteengezet, onzes inziens een probleem vormen voor de bevoegdheid van de procureur des Konings om gegevens in beslag te nemen die noodzakelijk zijn om andere gegevens te kunnen verstaan (zie randnr. 100), hoewel het aannemelijk lijkt dat een niet al te exegetisch ingesteld rechter dat technisch detail alsnog door de vingers zal zien. Toch is het veiliger ook hier spontaan over te gaan tot een bijschaving van de wetgeving, al was het maar omwille van de legislatieve elegantie. In bepaalde gevallen heeft de wetgever echter geheel bewust gehandeld en zal hij allicht niet uit eigen beweging tot een wetswijziging overgaan. Zulks is duidelijk het geval voor het bevel tot het verstrekken van bepaalde inlichtingen, dat volgens de wetgever immers ook moet kunnen worden opgelegd aan de verdachte zelf, hetgeen evenwel hoegenaamd niet in overeenstemming valt te brengen met het non-incriminatiebeginsel, gewaarborgd door art. 6 EVRM (zie randnrs. 106-107). Hiervoor lijkt een rechterlijke uitspraak, hetzij door de interne rechtscolleges, hetzij in Straatsburg, die een schending van dat beginsel vaststelt, de noodzakelijke zweepslag om de wetgever tot handelen aan te sporen.

Voor een laatste categorie van problemen is evenwel meer nodig dan een eenvoudige wetswijziging en moet men zich bevragen over de grondslagen zelf van ons strafprocedureel systeem. Zulks is bijvoorbeeld het geval voor de op het eerste gezicht als ongeoorloofd voorkomende ongelijke behandelingen tussen bijvoorbeeld de persoon wiens voicemailberichten worden beluisterd door de speurders, in welk geval een bijkomend rechterlijk bevel wordt vereist, en de persoon wiens antwoordapparaat wordt beluisterd, hetgeen kan gebeuren zonder een dergelijk bijkomend bevel (zie randnr. 66). Die discriminaties zijn immers niet zozeer te wijten aan een juridisch-technische onvolkomenheid, maar wel aan het feit dat de door de wetgever uitgewerkte regeling berust op de aloude idee dat elk goed, dus ook een verzameling van elektronische gegevens, een welbepaalde plaats heeft en op basis van waar het zich bevindt, een bepaalde bescherming moet worden toegekend. Die opvatting lijkt echter niet meer overeen te komen met de huidige werkelijkheid van het digitale tijdperk waarin elektronische gegevens probleemloos en razendsnel privéwoningen 'verlaten' en bovendien eindeloos kunnen worden vermenigvuldigd, zodat de vraag kan worden gesteld of het handhaven van het traditionele 'geografische' criterium in een geïnformatiseerde omgeving, wel verantwoord valt te noemen. Anderzijds kan bezwaarlijk worden ontkend dat degene naar wiens informaticasysteem de zoeking wordt uitgebreid, toch een zekere bescherming toekomt, ook al zijn de in dat informaticasysteem opgeslagen gegevens rechtstreeks toegankelijk via het netwerk. Daarom weze in dit werkstuk het voorstel gelanceerd om een versoepeling van de netwerkzoeking aan te brengen in die zin dat geen bijkomend rechterlijk bevel moet worden vereist wanneer de gegevens in de regel enkel toegankelijk zijn voor de gebruiker van het informaticasysteem waarin de oorspronkelijke zoeking plaatsvindt. Zulks is bijvoorbeeld het geval voor voicemail- of e-mailberichten waarop de operator of webmailprovider immers bezwaarlijk een volwaardig recht op eerbiediging van zijn privéleven kan laten gelden. Op die manier zou nog steeds een afdoende bescherming worden geboden aan bijvoorbeeld het netwerk dat tussen twee vrienden werd opgezet om op eenvoudige wijze elkaars bestanden te kunnen delen, maar wordt tegelijkertijd verholpen aan de hierboven geschetste ongelijke behandeling tussen twee nochtans vergelijkbare rechtsonderhorigen. Met de huidige louter geografische denkpatronen kan evenwel pas volledig worden gebroken wanneer ook op internationaal vlak belangrijke stappen worden ondernomen teneinde de extraterritoriale zoeking en inbeslagneming verder te versoepelen. Hoe dan ook moet elke toekomstgerichte regelgevende instantie het als van primordiaal belang beschouwen gelijke tred te houden met de technologische evolutie, liefst de in deze tijden meer dan ooit vermeldenswaardige opmerking van Bacon indachtig dat "*time is the greatest innovator*".