Cybercriminaliteit doorgelicht

Jan KERKHOFS * **
Substituut-procureur des Konings bij het parket van de rechtbank van eerste aanleg te Dendermonde

Philippe VAN LINTHOUT * **
Onderzoeksrechter bij de rechtbank van eerste aanleg te Mechelen

I. INLEIDING

Waar vroeger de criminaliteit en het opsporings- en gerechtelijk onderzoek daarnaar zich zelden of nooit in een digitale omgeving afspeelden, lijkt deze uitzondering thans de regel te zijn geworden. Niet enkel dient er te worden vastgesteld dat oude misdrijfvormen steeds vaker gepaard gaan met het gebruik van ICT (computer, internet, handhelds, smart phones...), maar er zijn ook gans nieuwe misdrijven ontstaan door de evolutie van onze digitale maatschappij. Om het anders te stellen: *«Old crimes, new tools and new tools, new crimes»*.

Voor wat de eerste categorie (*old crimes, new tools*) betreft, kan worden verwezen naar de ons klassiek gekende strafbare handelingen als bezit en uitwisseling van kinderporno, belaging, het aanzetten tot ontucht of aanranding van de eerbaarheid, het houden van een valse boekhouding (bijvoorbeeld de fiscale misdrijven), enz. Het is hier duidelijk geworden dat bij de zoektocht naar bewijsmateriaal politie en justitie geconfronteerd worden met nieuw aangewende technieken om enerzijds het misdrijf te plegen, maar anderzijds ook om zich eventueel weg te steken voor correctionele vervolging.

Voor wat de tweede categorie van misdrijven (*new tools, new crimes*) betreft, is het zo dat de Belgische wetgever als goede leerling in de klas inhoudelijk de Cybercrime-Conventie van Budapest van 23 november 2001 reeds – anticiperend – omzette in Belgisch recht op 28 november 2000 (1). Hiermee ontstond onder meer een aantal nieuwe misdrijven die eigen zijn aan de informaticaomgeving en een oplossing boden voor wat voordien in de rechtspraak diende te worden opgelost. Zo ontstonden als totaal nieuwe misdrijven: de valsheid in informatica (art. 210*bis* Sv.), het informaticabedrog (art. 504*quater* Sv.), de interne en externe hacking (art. 550*bis* Sv.) en de datasabotage (art. 550*ter* Sv.).

Eigen aan beide categorieën is het feit dat een nieuwe stijl diende ontwikkeld te worden in het opsporen van deze misdrijven, aan de hand van een nieuw of up-to-date gebracht arsenaal van strafprocesrechtelijke instrumenten. De auteurs van de wet van 28 november 2000 inzake informaticacriminaliteit (2) hadden de niet mis te verstane ambitie om de actoren van justitie de adequate juridische instrumenten aan te reiken om de criminaliteit op de informatiesnelweg te kunnen bestrijden. Men had immers vastgesteld dat men in verschillende rechtstakken verplicht was geworden na te gaan of de klassieke juridische begrippen in staat waren de nieuwe problemen die samenhangen met de IT op te vangen (3). Voor wat het strafprocesrecht betreft, werden de opsporing en bewijsvoering daarbij als voornaamste probleem ervaren bij de bestrijding van de criminaliteit op de informatiesnelweg (4). Ook reeds veel eerder, bij het herwerken van de tapwetgeving, had men ingezien dat het aanwezige strafprocesrechtelijke instrumentarium diende te worden aangepast, nu men onder meer voor de toekomst rekening diende te houden met het feit dat in de informatica- en telecommunicatiesector niet enkel meer met (telefoon)nummers gewerkt werd, maar ook met e-mailadressen, internetsites, enz. (5)

---

* De auteurs van onderhavige wetenschappelijke bijdrage schrijven geenszins uit hoofde van hun ambt, noch vertolken zij op enigerlei wijze (noodzakelijk) het standpunt van het korps of de hiërarchie waarbinnen zij hun ambt uitoefenen, noch verbinden zij op enigerlei wijze hun ambt met de vertolkte standpunten.

** Beide auteurs zijn houder van een D.E.A. strafrecht en strafrechtswetenschappen, Université Panthéon-Assas-Paris II.

(1) *BS* 3 februari 2001; zie voor zeer extensief overzicht van het Belgische wetgevend kader: P. DE HERT en F. VAN LEEUW, *Cybercrime Legislation in Belgium*, Country report of the Cybercrime Section of the IACL Congress in Washington 2010, 68p., http://www.wcl.american.edu/events/2010congress/reports/National_Reports/VI_Internet_Crimes/Belgium_Report.pdf?rd=1; zie ook in die context P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?», *T.Strafr.* 2001, afl. 6, 286-335.

(2) *BS* 3 februari 2001.

(3) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 3.

(4) *Ibid.*, 7.

(5) Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *Parl.St.* Senaat 1997-1998, nr. 1-828/3, 3.

In die context dient te worden vastgesteld dat de ICT-toepassingen van vandaag (legaal en illegaal) zich ver buiten het beeld situeren van wat de wetgever *anno* 1999 voor ogen had en kon hebben (1), al had de regering wel ook haar bezorgdheid uitgedrukt dat met nieuwe technologieën diende rekening te worden gehouden opdat het wetsontwerp niet reeds achterhaald zou zijn (2).

De wijze waarop de cybercriminaliteit thans wordt gepleegd, is dermate inventief, technisch en complex, dat de aanpak daarvan – vaak tevergeefs tot op heden – dezelfde gedrevenheid en kennis vergt van zowel magistraten als politiediensten. Het minste wat gezegd kan worden is dat de vervolging en de vervolgingsmogelijkheden geen gelijke tred houden met de innovatie van deze nieuwe criminaliteit. Een crimineel doet er in de realiteit 120 minuten over om van Brussel naar Parijs te sporen. In de virtuele realiteit van het internet doet hij dat op een fractie van een seconde. Justitie en politie doen daar in beide gevallen sowieso dagen, zo niet maanden over.

Het is dan ook niet verwonderlijk dat heden ten dage op het terrein blijkt dat er voor de concreet voor handen zijnde problemen niet steeds pasklare antwoorden vervat lijken te liggen in de wet of in de schaarse doctrine en rechtspraak.

Wat in deze bijdrage wordt beoogd, is om in een eerste deel de nieuwe cybermisdrijven te evalueren en in kaart te brengen, waar mogelijk gespijsd met de karig bestaande rechtspraak. In een tweede deel wordt beoogd om stil te staan bij de *new tools* en het gebruik daarvan. Niettegenstaande de enorme complexiteit van de rechercheomgeving, kan er best heel wat worden onderzocht indien men 1) weet wat men zoekt, 2) weet waar men moet zoeken, en 3) weet hoe men moet zoeken (met welke juridische tools). Het is de bescheiden betrachting van deze bijdrage om ter zake een minimale klaarheid te brengen.

II. HET MATERIEEL ICT-STRAFRECHT

Ruim tien jaar na het indienen van het wetsontwerp inzake informaticacriminaliteit dient te worden vastgesteld dat het gebruik van de Informatie- en Communicatie-Technologie (verder ICT) door criminelen exponentieel is toegenomen. Niet enkel voor wat betreft de sinds 28 november 2000 nieuwe «ICT-specifieke misdrijven» (informaticavalsheid of informaticabedrog (informatica als tool) en hacking of informaticasabotage (informatica als doel)), maar ook meer algemeen als middel om misdrijven voor te bereiden of te helpen plegen (communicatie door middel van ICT, dataopslag en -verspreiding, ...). Karikaturaal kan worden gezegd dat vandaag niet elke crimineel een wapen draagt, maar hij daarentegen wellicht wel gebruik maakt of zal maken van ICT om zijn misdrijf te (helpen) plegen.

In de memorie van toelichting bij de wet wordt een conceptueel onderscheid gemaakt tussen twee vormen van ICT-criminaliteit: 1) informatica als middel om klassieke misdrijven te plegen (ICT-criminaliteit als middel, *modus operandi*), en 2) informatica als doel van de criminaliteit (3). Elders in de rechtsleer wordt een onderscheid gemaakt tussen instrumentele ICT-misdrijven en intrinsieke ICT-misdrijven (4). Nog elders wordt een onderscheid gemaakt tussen niet-specifieke informaticacriminaliteit en specifieke informaticacriminaliteit (5).

Terminologisch is er evenwel geen bezwaar om, nauw aansluitend bij de memorie van toelichting, eenvoudigweg het onderscheid te hanteren tussen ICT-misdrijven als middel en ICT-misdrijven als doel.

Misdrijven als informaticavalsheid, het gebruik van valse informaticagegevens en ook het informaticabedrog, zijn misdrijven waarbij het gebruik of de manipulatie van ICT hoofdzakelijk een middel is om een welbepaald feit te plegen (een feit dat mogelijks op zijn beurt ook nog *sui generis* strafbaar is als een ander gemeenrechtelijk misdrijf). Zo kan bijvoorbeeld een informaticavalsheid de listige kunstgreep constitueren van een oplichting.

De misdrijven van hacking en informaticasabotage zullen doorgaans een doel op zich zijn van de dader ervan. Het gaat dan zeer specifiek om delicten die een inbreuk plegen op de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen of de gegevens die daarin worden opgeslagen, verwerkt of overgedragen (6).

§ 1. ICT als crimineel middel

A. Valsheid in informatica (art. 210bis, § 1 Sw.)

Artikel 210*bis*, § 1 van het Strafwetboek voert een afzonderlijke strafbaarstelling in voor het opzettelijk vermommen van de waarheid via datamanipulatie met betrekking tot juridisch relevante data (7).

1. Het materieel element

Er moet vooreerst sprake zijn van de **manipulatie van data**. De wijze waarop die manipulatie geschiedt, is van weinig belang. De wetgever stelde uitdrukkelijk dat de manipulatie van data moet worden opgevat in de meest ruime zin (8). Zowel het invoeren van data in

(1) Kenschetsend hiervoor is de verduidelijking door de heer Luc BEIRENS, toenmalig hoofd van het BOGO-team, thans van de FCCU voor de Senaatscommissie voor de Justitie, juni 2000 waar hij stelt dat wat betreft het onderscheppen van mail «eens» met een huiszoekingsbevel de mail opgehaald werd bij de provider, dit het enige geval was waarbij men een mail had onderschept (wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Senaat 1999-2000, nr. 2-392/3, 46).

(2) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/010, 2.

(3) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 5-6.

(4) D. DEWANDELEER, «Misdrijven en strafonderzoek in de IT-context» in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis – Strafrecht- en Strafprocesrecht*, Brugge, die Keure, 2009-2010, 125.

(5) J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 5.

(6) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 1 en 6.

(7) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.

(8) *Ibid.*

een informaticasysteem, als het wijzigen of het wissen ervan is strafbaar. Zo wordt ook het veranderen van de mogelijke aanwending van data in een informaticasysteem met enig ander technologisch middel door de wet beoogd.

Onder *informaticasysteem* in de zin van de wet wordt bedoeld elk systeem voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT (1). De wetgever heeft duidelijk de bedoeling gehad om een technologie-neutrale terminologie te hanteren om te vermijden dat concepten al te snel zouden worden achterhaald door de technische evolutie van ICT.

Zo is bv. «Facebook» een informaticasysteem in de zin van de wet, zo ook Hotmail, MSN, Netlog, Telenet, Skynet, Scarlet, een draadloos netwerk (2), het WiFi-netwerk van een hotel, de hotspot van een McDonalds, een iPhone...

Met betrekking tot de aard van de gegevens of data, voorwerp van de manipulatie, stelt de wet dat het moet gaan om «***gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem***». Ook hier beoogt de wetgever een zeer ruime technologie-neutrale betekenis van het concept *gegevens*. De materiële vormgeving van deze gegevens – elektro-magnetisch, optisch of anderszins – is irrelevant (3).

Wel vereist de wet dat het moet gaan om een **verandering van de juridische draagwijdte** van deze gegevens. Hoe zulks exact dient te worden geïnterpreteerd, blijkt niet exact uit de voorbereidende werken. Er kan worden aangenomen dat ook hier de wetgever een zeer ruim technologie-neutraal toepassingsgebied voor ogen heeft gehad, aangepast aan de specificiteit van de digitale en virtuele mogelijkheden.

De wetgever komt daarbij kennelijk los van de geijkte beginselen met betrekking tot de klassieke valsheid in geschriften, en kadert de informaticavalsheid eerder binnen de andere informaticamisdrijven. Althans dat was toch de initiële *ratio* (4), zulks wellicht juist om reden dat de informaticavalsheid beschouwd wordt als een misdrijf waarbij ICT dient te worden beschouwd als een *crimineel middel* bij het plegen van misdrijven.

Het lijkt aldus ook gevaarlijk om zonder meer – zoals in sommige rechtsleer wordt gedaan (5) – de parallel te trekken met de klassieke valsheid in geschriften en de rechtspraak daaromtrent (6). Immers, de geldende rechtspraak met betrekking tot o.a. het concept van *«het zich opdringen aan de openbare trouw»* kan bezwaarlijk onverkort en ongenuanceerd worden getransponeerd op de informaticavalsheid omdat sowieso het medium van een informaticasysteem altijd reserves met zich meebrengt of moet brengen voor wat de waarachtigheid van het ene of het andere betreft. Zo kunnen de creatie en het gebruik van een hotmailaccount op iemand anders zijn naam (bv. jan.kerkhofs@hotmail.com) zeker een informaticavalsheid constitueren (7), zonder dat eenieder in de samenleving eigenlijk er zonder meer van zou mogen uitgaan dat de account authentiek aan Jan Kerkhofs toebehoort; het is immers inmiddels algemeen geweten dat Hotmail-Microsoft geen identitificatiecontroles uitvoert en dat iedereen een account kan aanmaken onder gelijk welke naam. Om het iets absurder te stellen: het feit dat je een mail krijgt van micky.mouse@yahoo.com geeft je bezwaarlijk het vertrouwen dat je echt te doen hebt met Micky Mouse.

In een virtuele context zou er wat voor te zeggen zijn om *«het zich opdringen aan de openbare trouw»* mede te interpreteren als een subjectieve dadernotie in de zin van *«het succesvol misbruik maken van een redelijke en geloofwaardige schijn»*. Deze interpretatie sluit aan bij de betrachting van de wetgever om los te komen van de klassieke rechtsconcepten, en de betrachting om de rechtshandhaving in de virtuele en digitale realiteit terminologie-neutraal te verzekeren (8).

De juridische draagwijdte van de verandering van gegevens in een informaticasysteem is een feitenkwestie die door de feitenrechter dient te worden beslecht. De wetgever zelf haalt het voorbeeld aan van het vervalsen of namaken van kredietkaarten of valsheid in digitale contracten (9).

Andere voorbeelden kunnen zijn:

– na iemands hotmailaccount te hebben gehackt, zijn loggings veranderen, zodat de account onbeschikbaar wordt voor de titularis ervan (10);
– een e-mailaccount aanmaken op iemand anders zijn naam en een e-mail verzenden naar een derde persoon (11);
– het gebruik maken van tools zoals bv. www.anoniemsmsen.be om een «fake» sms-je of een fake e-mail te verzenden gebruik makend van het gsm-nummer respectievelijk het e-mailadres van iemand anders;
– als bedrijf doen uitschijnen, door gebruik te maken van de URL www.nis-be.com en corresponderende e-mailadressen, dat men handelt als het Nationaal

---

(1) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 12.
(2) Corr. Dendermonde 14 november 2008, *T.Strafr.* 2009, afl. 2, 115.
(3) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 12.
(4) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.
(5) J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 19.
(6) P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?», *T.Strafr.* 2001, afl.6, 315: «*Een geheel nieuwe, op elektronische gegevens afgestemde valsheidbepaling – artikel 210bis van het strafwetboek – moet daarom de kernwaarden achter de valsheiddelicten in de elektronische wereld vertalen zonder over te gaan tot een loutere assimilatie van (alle) elektronische gegevens met geschriften.*»
(7) Zie Corr. Dendermonde 28 november 2005, *NJW* 2006, afl. 138, 229.
(8) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 12.
(9) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.
(10) Corr. Dendermonde 29 september 2008, *T.Strafr.* 2009, afl. 2, 111, noot ed. Ph. VAN LINTHOUT, «Territoriale bevoegdheid in cyberspace».
(11) Corr. Dendermonde 28 november 2005, *NJW* 2006, afl. 138, 229.

Instituut voor Statistiek, om zo vlotter bedrijfscijfers en informatie te bekomen van kmo's (1);
- het aanmaken en gebruiken van een Netlogprofiel op naam van iemand anders (2);
- het aanmaken van een vals datingprofiel waarbij de contactgegevens en het telefoonnummer van een ander persoon worden opgegeven (3);
- het plaatsen van een vals zoekertje met vermelding van iemand anders zijn contactgegevens;
- het aanmaken van een vals profiel (bv. op Netlog, Facebook, MSN, ...) om in contact te treden met minderjarigen met oog op pedo-seksuele praktijken (bv. verleiding met oog op seksueel contact, overhaling tot het doorsturen van zelfgemaakte naaktfoto's, ...);
- door een cv van iemand te hebben aangepast op de jobwebsites www.jobat.be, www.stepstone.be en www.eci.be, nl. door het contact-e-mailadres te hebben gewijzigd en door bewust taalfouten te hebben aangebracht (4);
- het zgn. «skimmen» van bankkaarten, d.i. het frauduleus kopiëren van bankkaarten (5);
- door als ambtenaar bij de FOD Financiën in je eigen dossier de bedrijfsvoorheffing onder code 286 (bedrijfsvoorheffing loon) en code 225 (bedrijfsvoorheffing pensioen) systematisch op te trekken gebruik makend van je toegang tot het informaticasysteem van de FOD, zodat je jaarlijks duizenden euro's te veel terugkrijgt van de belastingen (6).

Voorts *lijkt* het zo dat uit de voorbereidende werken kan worden afgeleid dat, aangezien de toepassing van artikel 210*bis* van het Strafwetboek vereist dat de juridische draagwijdte van data werd gewijzigd, de effectieve realisatie van een specifiek nadeel een vereiste is (7). In de mate dat wordt aangenomen dat een frauduleuze datamanipulatie op zich reeds een nadeel impliceert voor de titularis, is de discussie ter zake zinloos. Evenwel is de situatie denkbaar dat er zich een datamanipulatie voltrekt, zonder dat deze manipulatie haar schadeverwekkende doelstellingen kan bereiken (bv. door vroegtijdige ontdekking). Dit doet o.i. geen afbreuk aan het feit dat de informaticavalsheid voltooid is. Ter zake lijkt een **potentieel nadeel** te volstaan (8).

In de mate dat de informaticavalsheid niet voltooid kan worden geacht, dient te worden vastgesteld dat ook de poging strafbaar is (art. 210*bis*, § 3 Sw.).

2. Het moreel element

Informaticavalsheid vereist een **bijzonder opzet** vermits het gewijzigde artikel 193 van het Strafwetboek bepaalt dat valsheid in geschriften, *in informatica* of in telegrammen, met bedrieglijk opzet of met het oogmerk om te schaden, gestraft wordt overeenkomstig de daarop volgende artikelen (van hoofdstuk IV van het Strafwetboek). Het bijzonder opzet bestaat uit een bedrieglijk opzet of het oogmerk om te schaden.

In de memorie van toelichting stond aanvankelijk te lezen dat de wetgever uitdrukkelijk opteerde voor een algemeen opzet, gelet op het feit dat men uitdrukkelijk de parallel wenste te doorbreken met de klassieke valsheid in geschriften (9). Kennelijk zwichtte men uiteindelijk onder de kritiek van de Raad van State en de daaruit voortvloeiende interpellaties in de wetgevende kamers: *«Met betrekking tot de problematiek van de vereiste van algemeen opzet of bedrieglijk opzet in verband met de verschillende misdrijven, antwoordt de minister dat hier»* (uiteindelijk) *«een parallel werd getrokken met de gewone misdrijven (valsheid in geschrifte, bedrog); in verband met de eerbiediging van het gelijkheidsbeginsel in verband met de valsheid in geschrifte, werd het advies van de Raad van State gevolgd»* (10)*«.»*

Het bedrieglijk opzet of het oogmerk om te schaden is een feitenkwestie die door de bodemrechter soeverein wordt beoordeeld. Men zou kunnen aannemen dat het plegen van valsheid in een geïnformatiseerde omgeving vele natuurlijke hindernissen omvat; het nemen van al die hindernissen of stappen door de dader demonstreert al snel diens inzichten.

Er werd reeds geoordeeld dat het bedrieglijk opzet niet zonder meer wordt weggenomen door het beweerd motief dat men aldus *«de zwakheden van het systeem wou aantonen»* (11). Uit een andere uitspraak vloeit voorts ook voort dat een onvolkomen en weinig doordachte werkwijze evenmin wil zeggen dat er geen sprake zou kunnen zijn van een bedrieglijk opzet (12).

B. Gebruik van valse informaticagegevens (art. 210bis, § 2 Sw.)

Overeenkomstig artikel 210*bis*, § 2 van het Strafwetboek wordt hij die, terwijl hij weet dat de verkregen gegevens vals zijn, hiervan gebruik maakt, gestraft alsof hij de dader van de valsheid was.

Ter zake kan worden verwezen naar de materiële constitutieve bestandelen van de informaticavalsheid zoals hierboven uiteengezet.

---

(1) Corr. Dendermonde 13 februari 2009, onuitg.; *in casu* werd ook de vennootschap in kwestie veroordeeld.
(2) Corr. Dendermonde 21 december 2009, onuitg.
(3) Zie Corr. Luik 18 november 2002, *Computerr.* (Ned.) 2003, afl. 2, 181.
(4) Corr. Dendermonde 29 september 2008, *T.Strafr.* 2009, afl. 2, 111, noot ed. Ph. VAN LINTHOUT, «Territoriale bevoegdheid in cyberspace».
(5) Corr. Dendermonde 14 mei 2007, *T.Strafr.* 2007, afl. 6, 403, noot E. BAYENS, «Informatica en strafrecht: oude griffels – nieuwe leien».
(6) Corr. Dendermonde 15 januari 2010, onuitg.
(7) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.
(8) *Pro*: Corr. Dendermonde 28 november 2005, *NjW* 2006, afl. 138, 229; J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 21.*Contra*: D. DEWANDELEER, «Misdrijven en strafonderzoek in de IT-context» in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis – Strafrecht- en Strafprocesrecht*, Brugge, die Keure, 2009-2010, 126.
(9) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.
(10) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 3-392/3, 21.
(11) Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, afl. 5, 351.
(12) Corr. Dendermonde 2 februari 2009, onuitg.; *in casu* betrof het de beoordeling van een poging tot hacking die nogal klungelig was verlopen.

Het grote verschil met de informaticavalsheid vervat in § 1 van artikel 210*bis* van het Strafwetboek, is het moreel element. Zonder twijfel werd in het wetsontwerp voorzien dat voor het plegen van informaticavalsheid een algemeen opzet vereist is (1). Zoals hierboven beschreven, werd dit algemeen opzet voor wat informaticavalsheid betreft zelf geamendeerd. Artikel 193 van het Strafwetboek consacreert thans zeer uitdrukkelijk dat voor wat valsheid in informatica betreft een bijzonder opzet is vereist. Evenwel dient te worden vastgesteld dat, niettegenstaande de discussies in de wetgevende kamers, aan de tekst van § 2 van artikel 210*bis* van het Strafwetboek geen verandering werd aangebracht.

De goede lezer kan aldus niet anders dan vaststellen dat voornoemde § 2 het moreel element *expressis verbis* dicteert, nl.: *«terwijl hij weet dat aldus verkregen gegevens vals zijn»*. Het betreft ter zake het **algemeen opzet**. Voornoemde tekst gaf in de parlementaire besprekingen geen aanleiding tot opmerkingen (2).

Niettemin blijft de rechtsleer verdeeld. Sommige auteurs signaleren onduidelijkheid met betrekking tot het moreel element zonder standpunt in te nemen (3). Dirk DEWANDELEER argumenteert ter zake dat artikel 213 van het Strafwetboek het bijzonder opzet voor wat betreft het «gebruik» vastlegt, en dat kwestieus artikel 213 van het Strafwetboek een bepaling is *«aan de vier vorige hoofdstukken gemeen»*, dus inclusief hoofstuk IV en artikel 210*bis* van het Strafwetboek. De libellering van het algemeen opzet in § 2 van artikel 210*bis* van het Strafwetboek doet daaraan volgens hem geen afbreuk (4).

De verwijzing naar artikel 213 van het Strafwetboek overtuigt ons evenwel niet. Artikel 213 van het Strafwetboek verwijst enkel naar het gebruik van munten, effecten, rente- en dividendenbewijzen, biljetten, zegels, stempels, merken, telegrammen en geschriften. Nergens verwijst de limitatieve lijst van artikel 213 van het Strafwetboek naar *gegevens* in de zin van artikel 210*bis*, § 1 van het Strafwetboek. Nochtans is het een zeer duidelijk in de wet ingeschreven onderscheiden begrip (5), wars van gelijk welke verwijzing naar de klassieke concepten of begrippen.

Alleszins werd reeds geoordeeld dat voor wat het gebruik van informaticavalse gegevens betreft een algemeen opzet voldoende is (6).

In het licht van de door de wetgever gedane bijsturingen wat betreft het moreel element van de informaticavalsheid zelf, zou men zich de vraag kunnen stellen in hoeverre de vereiste van een algemeen opzet voor wat betreft het gebruik van valse informaticagegevens geen wetgevende vergetelheid is. *Dura lex, sed lex?*

C. Informaticabedrog (art. 504quater Sw.)

De incriminatie «informaticabedrog» stelde in oorsprong gegevensmanipulatie met het oogmerk voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel te verwerven, evenals de realisatie van dit oogmerk, strafbaar. De bepaling werd door de wetgever losgekoppeld van artikel 496 van het Strafwetboek (oplichting), dat in essentie bedrieglijke manoeuvres viseert die het vertrouwen van personen schenden. Computerfraude betreft ongeoorloofde manipulaties van data ten aanzien van een machine, en is in dat opzicht wezenlijk verschillend. De specifieke strafbaarstelling laat bovendien toe om een andere structuur te geven aan het delict dan aan sommige bestaande vermogensdelicten. Zo is het voor het nieuwe delict irrelevant of er voor of na de manipulatie afgifte is geweest van een vermogensonderdeel, terwijl dit essentieel is voor het onderscheid tussen misbruik van vertrouwen en oplichting (7).

Evenwel heeft de wetgever van 28 november 2000 onderkend dat artikel 504*quater* van het Strafwetboek niet geheel op één lijn lag met artikel 8 van de overeenkomst van de Raad van Europa inzake informaticacriminaliteit, opgemaakt te Boedapest op 23 november 2001, daar waar artikel 504*quater* in de dan geldende versie vereiste *«dat een onrechtmatig economisch voordeel werd verworven»* (8). In die zin werd aldus bij artikel 4 van de wet van 15 mei 2006 (*BS* 12 september 2006) § 1 gewijzigd van artikel 504*quater* van het Strafwetboek. Thans vereist informaticabedrog **dat het verwerven van een onrechtmatig economisch voordeel voor zichzelf of voor een ander wordt beoogd**, zonder dat wordt vereist dat er een voordeel van die aard effectief werd verworven. Dit houdt in dat bijvoorbeeld de vervolging van «skimming» (9) niet meer vereist dat de daders ervan ook wel degelijk er in zijn geslaagd om te «cashen».

Samen met andere auteurs zijn wij van oordeel dat het beoogde economisch voordeel zowel van materiële als van immateriële aard kan zijn (10).

---

(1) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.

(2) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 3-392/3, 71.

(3) J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 22.

(4) D. DEWANDELEER, «Misdrijven en strafonderzoek in de IT-context» in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis – Strafrecht- en Strafprocesrecht*, Brugge, die Keure, 2009-2010, 128.

(5) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 12; *cf. supra*.

(6) Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, afl. 5, 351.

(7) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 15.

(8) *Parl.St.* Kamer 2003-2004, nr. 1284/001, 6 en 8.

(9) Skimming is de benaming voor de fraude die er in bestaat dat door criminelen heimelijk apparatuur wordt geïnstalleerd op een bankbiljettenverdeler waardoor de magneetstrip van de bankkaarten van de gebruikers van de automaat wordt gekopieerd terwijl gelijktijdig hun ingetikte pincode wordt geregistreerd (middels een geïnstalleerde camera of middels een klavier-prothese). Dienvolgens worden de bankkaartgegevens gelinkt aan de respectieve codes en overgebracht op zogenaamde «white plastics» (blanco kaarten met een magneetstrip; dit kunnen klantenkaarten zijn van bv. IKEA, of een kaart van het ziekenfonds, ...). Vervolgens worden met de nagemaakte kaarten geldafhalingen verricht in het buitenland.

(10) J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 23.

Informaticabedrog wordt gepleegd op de door de wet gekwalificeerde wijze, nl.:

– **door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem** (1),
– **in een informaticasysteem in te voeren, te wijzigen, te wissen** (2).
– **of** (3) **met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem te veranderen** (4).

De wet vereist uitdrukkelijk een **bijzonder opzet**, nl. het oogmerk om voor zichzelf of voor een ander een onrechtmatig *economisch voordeel* te verwerven. Het gegeven of er sprake is van een economisch voordeel, is een door de feitenrechter te beoordelen feitenkwestie. S. EVRARD is van oordeel dat een student die inbreekt in het informaticasysteem van zijn school teneinde zijn punten op te trekken, niet onder deze omschrijving valt (5). J. KEUSTERMANS en F. MOLS zijn van oordeel dat het behalen van een diploma wel als een economisch voordeel kan worden aangemerkt (6).

Het lijkt ons dat met een *economisch voordeel* in de zin van artikel 504*quater* van het Strafwetboek, door de wetgever in eerste instantie *een vermogensnotie* werd beoogd (7). Dit wil evenwel niet zeggen dat er aan het criterium ter zake enig kwantitatief barema is verbonden. Diegene die de feiten begaat met het oogmerk om er op een of andere manier *«rechtstreeks materieel beter van te worden»* lijkt binnen het kwestieuze toepassingsgebied te vallen. Wel lijken uitgesloten, diegenen die de feiten plegen met het oogmerk om iemand anders zonder meer leed te berokkenen, of diegenen die feiten plegen «voor de sport». Deze laatsten vallen ongetwijfeld wel onder een andere strafbaarstelling (8).

De wetgever gaf als voorbeelden van gevallen die geviseerd worden door artikel 504*quater* van het Strafwetboek (9):

– het gebruik van een gestolen kredietkaart om geld uit een automatische biljettenverdeler te halen;
– het onrechtmatig overschrijden van het krediet van zijn eigen kredietkaart (!);
– het invoeren van programma-instructies waardoor bepaalde verrichtingen een ander resultaat opleveren met het oog op het bekomen van een onrechtmatig financieel voordeel (10);
– het met winstbejag verduisteren van bestanden of programma's die men enkel voor een welbepaald doel toevertrouwd heeft gekregen (11).

Voorts kan nog worden gedacht aan de volgende situaties:

– skimming (12);
– het aanbrengen van een MOD-chip in een spelconsole waardoor het mechanisme voor de bescherming van intellectuele-eigendomsrechten wordt omzeild en de gebruiker het voordeel bekomt van de mogelijkheid om gekopieerde spelsoftware te gebruiken (13);
– het aanwenden van een ontvreemde tankkaart om zich brandstof toe te eigenen (14);
– het afhalen van geld met een gevonden kredietkaart.

---

(1) Daaronder vallen als het ware alle gegevens die je tegenkomt nadat je een welbepaald informaticasysteem bent binnengegaan.

(2) Daaronder valt elke handeling die gelijk welke manipulatie inhoudt van de data van of binnen het informaticasysteem in kwestie. Die handeling op zich zal veelal ook *sui generis* kunnen worden gekwalificeerd als een informaticavalsheid overeenkomstig artikel 210bis van het Strafwetboek. Nochtans zal niet steeds de manipulatie of de handeling op zich strafbaar zijn. Bv. bij het gebruiken van een tankkaart van de werkgever om de auto van een vriend vol te tanken: je bent gerechtigd om de kaart te gebruiken in gelijk welke betaalterminal, doch het beoogde doel (onrechtmatig economisch voordeel voor een ander) maakt dat er sprake kan zijn van informaticabedrog. De wet vereist in artikel 504quater van het Strafwetboek dus niet dat onjuiste gegevens zouden worden ingevoerd (zie D. Dewandeleer, «Misdrijven en strafonderzoek in de IT-context» in R. Verstraeten en F. Verbruggen (eds.), Themis – Strafrecht- en Strafprocesrecht, Brugge, die Keure, 2009-2010, 129). Zie in die zin: Antwerpen 28 mei 2008, *T.Strafr.* 2008, afl. 5, 40, noot.

(3) Ter zake lijkt het duidelijk dat het geen cumulatieve situaties zijn. Zo kunnen feiten van skimming worden ontleed in verschillende fases die telkens kunnen worden beschouwd als een daad van informaticabedrog:
  – het plaatsen van (technologische) middelen waardoor de normale aanwending van gegevens (bankgegevens) in een informaticasysteem wordt of zal worden veranderd;
  – vervolgens worden de bankkaarten van de klanten gekopieerd, hetgeen betekent dat men de op een informaticasysteem (bankkaart) opgeslagen gegevens invoert in een (ander) informaticasysteem (nl. dat van de daders);
  – vervolgens worden de gekopieerde gegevens overgebracht op white plastics, hetgeen andermaal een invoer impliceert van data in een informaticasysteem;
  – tot slot worden de white plastics en bijbehorende codes gebruikt om in te breken in het informaticasysteem van de bank en de elektronische portefeuille van de klant, om aldaar de rekening te debiteren, hetgeen andermaal een invoer en wijziging inhoudt van data in een informaticasysteem. Een en ander toont aan hoe ruim de uitwerking is van de strafbaarstelling van artikel 504quater van het Strafwetboek.

(4) Gedacht kan bijvoorbeeld worden aan het gebruik van bepaalde software of apparatuur om de beveiliging te breken van auteursrechtelijk beschermde werken of software. Voorts kan ook worden gedacht aan het gebruik van skimmingmateriaal.

(5) S. EVRARD, «La loi du 28 novembre 200 relative à la criminalité informatique», *JT* 2001, 242.

(6) J. KEUSTERMANS en F. MOLS, «Informaticacriminaliteit», in X, *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 50.

(7) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 15.

(8) O.a. art. 550*ter* Sw.: informaticasabotage.

(9) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 15.

(10) Zie Corr. Dendermonde 15 januari 2010, onuitg.: door als ambtenaar bij de FOD Financiën in je eigen dossier de bedrijfsvoorheffing onder code 286 (bedrijfsvoorheffing loon) en code 225 (bedrijfsvoorheffing pensioen) systematisch op te trekken, gebruik makend van je toegang tot het informaticasysteem van de FOD, zodat je jaarlijks duizenden euro's te veel terugkrijgt van de belastingen.

(11) Concreet kan er bijvoorbeeld worden gedacht aan de situatie van de werknemer die kiest voor een jobaanbieding bij de concurrentie, doch die de klantenbestanden van de vorige werkgever kopieert en meeneemt.

(12) *Cf. supra*; Corr. Dendermonde 14 mei 2007, *T.Strafr.* 2007, afl. 6, 403, noot E. BAYENS, «Informatica en strafrecht: oude griffels – nieuwe leien».

(13) J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 24.

(14) Cass. 6 mei 2003, P.03.0366.N, *RABG*, 2004/6, 367.

Tot slot, er werd reeds geoordeeld dat de strafuitsluitende verschoningsgrond van bloedverwantschap of aanverwantschap zoals vervat in artikel 462 van het Strafwetboek, ook van toepassing is op artikel 504*quater* van het Strafwetboek (1). Ter zake betreft het een jurisprudentiële uitbreiding van de strafuitsluitende verschoningsgrond, zoals dat ook reeds geschiedde voor wat afpersing (art. 470 Sw.) (2), heling (art. 505 Sw.) (3) en vernieling van documenten (art. 527 Sw.) (4) betreft.

§ 2. ICT als crimineel doel

A. Hacking

Er werd in het Strafwetboek een nieuwe titel IX*bis* ingevoegd inzake de misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen.

De eerste strafbepaling van titel IX*bis* is artikel 550*bis*, dat betrekking heeft op de ongeoorloofde toegang tot een informaticasysteem, ook wel «hacking» genaamd. Centraal hierbij is voor de wetgever de bestraffing van het wederrechtelijk toegang bekomen tot een informaticasysteem of een deel daarvan waartoe men niet is gerechtigd. Hierbij wordt door de wetgever een onderscheid gemaakt tussen aantastingen van buiten het systeem (§ 1 van art. 550*bis* Sw.) en aantastingen door gebruikers die bepaalde toegangsbevoegdheden hebben (§ 2 van art. 550*bis* Sw.) (5).

Het betreft het onderscheid tussen externe hacking en interne hacking.

1. Externe hacking (art. 550bis, § 1 Sw.)

Artikel 550*bis*, § 1 van het Strafwetboek viseert eenieder die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft.

Het materieel element van het misdrijf bestaat uit **het ongerechtigd toegang nemen tot een informaticasysteem van een ander en/of zich daarin handhaven**. De eis dat een beveiligingssysteem werd doorbroken, wordt niet als constitutief element voor de strafbaarstelling gehanteerd, omdat dit een aantal complicaties met zich meebrengt (welk niveau van beveiliging wordt vereist, openbaar worden van de beveiligingsvoorzieningen naar aanleiding van de bewijsvoering, ...) (6). Het spreekt voor zich dat het doorbreken van beveiligingsmechanismen demonstratief kan zijn voor een bedrieglijk opzet, in welk geval alinea 2 van § 1 van artikel 550*bis* van het Strafwetboek voorziet in strafverzwaring. Voorts kan het doorbreken van beveiligingsmechanismen ook aanleiding geven tot toepassing van de verzwarende omstandigheden vervat in § 3 van artikel 550*bis* van het Strafwetboek (*cf. infra*).

Bovendien moet erop worden gewezen dat deze bepaling de ongeoorloofde toegang tot het systeem als zodanig beteugelt. Wanneer een persoon zich op ongeoorloofde wijze toegang verschaft tot persoonsgegevens, zijn de strafbepalingen van de wet van 8 december 1992 op de bescherming van persoonsgevens reeds van toepassing. Overigens blijven, onverminderd de strafbepaling van artikel 550*bis* van het Strafwetboek, ook strafbepalingen uit andere beschermingsregimes voor bepaalde categorieën van gegevens toepasselijk. De filosofie die ten grondslag ligt aan de wet houdt immers in dat, wanneer bepaalde inlichtingen omwille van hun aard zelf een bijzondere bescherming rechtvaardigen, dit het voorwerp moet uitmaken van een apart beschermingsregime: het feit of deze inlichtingen vastgelegd zijn op papier of op een geïnformatiseerde drager, is ter zake irrelevant (offline = online) (7). Het door artikel 550*bis* van het Strafwetboek beschermde rechtsbelang is op de eerste plaats **de integriteit van het systeem op zich** (8).

Betreffende het moreel element opteerde de wetgever uitdrukkelijk voor een **algemeen opzet**, meer bepaald volstaat het dat de «hacker» **weet dat hij niet gerechtigd is** het aan hem vreemde informaticasysteem te betreden. De wetgever was van mening dat externe hacking moet worden beschouwd als een *gevaarzettingsdelict* dat als zodanig strafwaardig is, ongeacht de kwaadwillige bedoelingen of de gerealiseerde effecten (9). Wel voorzag de wetgever in strafverzwaring indien het misdrijf zou worden gepleegd met **bedrieglijk opzet**. Bedrieglijk opzet wordt aldus beschouwd als een *subjectief* verzwarende omstandigheid (10).

Het gegeven dat slechts een algemeen opzet is vereist voor het basismisdrijf van externe hacking leidt tot een laagdrempelige strafbaarstelling (11).

Dit houdt o.a. in dat degene die wetens en willens gebruik maakt van andermans draadloos netwerk, zonder dat hij daartoe de toestemming heeft gekregen van de titularis, strafbaar is op grond van artikel 550*bis*, § 1, alinea 1 van het Strafwetboek. Het feit dat men voorhoudt onwetend te zijn met betrekking tot het al dan niet publiek karakter van een netwerk (bij gebreke van

---

(1) Brussel 12 februari 2004, *Rev.dr.pén.* 2004, afl. 6, 748.
(2) Cass. 3 maart 1941, *Pas.* 1941, I, 63.
(3) Cass. 23 februari 1903, *Pas.* 1903, I, 118.
(4) Cass. 1 december 1930, *Pas.* 1931, I, 1.
(5) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 16.
(6) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001 17.
(7) Zie P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?», *T.Strafr.* 2001, afl. 6, 332-334.
(8) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 17.
(9) *Ibid.*
(10) D. DEWANDELEER, «Misdrijven en strafonderzoek in de IT-context» in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis – Strafrecht- en Strafprocesrecht*, Brugge, die Keure, 2009-2010, 130.
(11) Zie P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?», *T.Strafr.* 2001, afl. 6, 323.

beveiliging), doet daaraan geen afbreuk (1). Het feit dat een netwerk niet beveiligd is, en dat men zonder hindernissen het systeem kon binnendringen, kan wel impliceren dat er geen sprake is van kwaad opzet (2). Doch ook in dat geval blijft alles een feitenkwestie, en sluit het gebrek aan beveiliging geenszins een bedrieglijk opzet uit (3).

Kennelijk dient ervan uitgegaan te worden dat elk netwerk dat niet op ondubbelzinnige wijze publiek wordt aangeboden (bv. hotspots in publieke of private gebouwen), beschermd wordt door artikel 550*bis* van het Strafwetboek.

2. Interne hacking (art. 550bis, § 2 Sw.)

Interne hacking in de zin van artikel 550*bis*, § 2 van het Strafwetboek viseert degene die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn **toegangsbevoegdheid tot een informaticasysteem overschrijdt**. Concreet betreft het de personen die toegang hebben tot een bepaald informaticasysteem, doch slechts binnen bepaalde materiële grenzen of binnen een bepaalde finaliteit.

Voor «insiders» wordt de strafbaarheidsdrempel hoger gelegd: het overschrijden van het verleende autorisatieniveau moet plaatsvinden met een **bijzonder opzet**, namelijk met bedrieglijk opzet of met het oogmerk om te schaden.

De wetgever was van oordeel dat het louter onrechtmatig betreden van delen van het systeem via minder ingrijpende mechanismen moet worden aangepakt (interne sancties, arbeidsrecht, burgerlijk recht, ...). De Raad van State betwistte dit onderscheid inzake de strafwaardigheid van «hacking» door buitenstaanders, dan wel door «insiders». De logica van de wet houdt volgens de wetgever evenwel rekening met de realiteit dat het binnen een organisatie frequenter zal voorkomen dat er een ongeoorloofde toegang is tot bepaalde delen van het netwerk omwille van allerhande factoren (persoonlijke contacten, structuur van het netwerk, werkomgeving). Deze inbreuken kunnen weliswaar intentioneel zijn, maar worden slechts strafwaardig geacht als er een bijzondere negatieve bedoeling achter zit (strafrecht als *ultima ratio*): interne controlemechanismen moeten volgens de wetgever voor de minder ingrijpende gevallen volstaan. Deze situatie is verschillend ten aanzien van derden die buiten het netwerk zitten (externe hackers): hun transgressie brengt op zichzelf de veiligheid van het interne netwerk in gevaar (4).

Het kwestieus aangekaarte (discriminatoir) onderscheid tussen het vereiste bijzonder opzet voor wat interne hacking betreft en het vereiste algemeen opzet voor wat externe hacking betreft, werd inmiddels beslecht door het Grondwettelijk Hof bij arrest van 24 maart 2004, waarin het Grondwettelijk Hof onder meer het volgende overwoog, daarbij de logica van de wetgever volgende: *«Het gehanteerde onderscheidingscriterium is in dit licht pertinent om de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen en data te beschermen. Artikel 550bis van het Strafwetboek is in dit licht evenmin onevenredig. De wetgever vermocht immers van oordeel te zijn dat de externe hacker moet worden gestraft, ook al heeft hij niet gehandeld met bedrieglijk opzet of met het oogmerk om te schaden. Wanneer de hacking gebeurt met bedrieglijk opzet of met het oogmerk om te schaden heeft de wetgever bovendien voor de interne en de externe hacker dezelfde minimum- en maximumstraffen bepaald»* (5)*«.»*

Er zijn in de rechtspraak nauwelijks voorbeelden terug te vinden van interne hacking, wellicht om reden – zoals de wetgever vermoedde – dat dergelijke aangelegenheden veelal resulteren in andere vormen van oplossing. Gedacht kan worden aan:

– werknemers die hun toegangsbevoegdheid in het intern bedrijfsnetwerk misbruiken om bepaalde data voor eigen rekening te benutten;
– een politieambtenaar die zijn toegang tot het rijksregister en de ANG (Algemene Nationale Gegevensbank) misbruikt om informatie te verwerven over een derde (al dan niet ten bate van een derde) buiten de grenzen van de noodwendigheden van zijn ambt;
– de (externe) IT-verantwoordelijke van een bedrijf die zijn toegangsmogelijkheden tot het netwerk misbruikt om «te snuffelen» in vertrouwelijke data;
– de (externe) IT-verantwoordelijke die in het weekend heimelijk inlogt op de servers van zijn klant, om een «error» uit te lokken, teneinde dienvolgens als «reddende engel» tegen weekendtarief te kunnen depanneren.

3. Objectief verzwarende omstandigheden (art. 550bis, § 3 Sw.)

Naast de centrale basisgedragingen zoals hierboven beschreven, wordt door de wetgever eveneens een aantal gevolghandelingen strafbaar gesteld, in de vorm van *objectief* verzwarende omstandigheden bij het basismisdrijf in zijn beide varianten (dus zowel voor externe hacking als voor interne hacking). Het gaat om de

(1) Corr. Dendermonde 14 november 2008, *T.Strafr.* 2009, afl. 2, 114, noot Ph. VAN LINTHOUT (ed.), «Smartphone-, iPhone- en latopliefhebbers: u bent gewaarschuwd!».
Zie ook Corr. Dendermonde 5 oktober 2009, onuitg.: ter zake betrof het een Nederlandse onderdaan die stelde dat hij zich van geen kwaad bewust was gelet op zijn gebrek aan kennis van de gestrengheid van de Belgische wet. De rechtbank was kennelijk van oordeel dat zulks ter zake het algemeen opzet in de zin van artikel 550*bis*, § 1, alinea 1 van het Strafwetboek niet wegneemt.
(2) Corr. Hasselt 21 januari 2004, *Limb.Rechtsl.* 2005, 133.
(3) Denk bijvoorbeeld aan de persoon die doelbewust een onbeschermd draadloos netwerk van een ander opzoekt met als doel kinderporno te downloaden via het internetabonnement en de internettoegang van een ander (mogelijks met het kwalijke gevolg dat de gerechtelijke overheid bij «de verkeerde» gaat aankloppen). Het weze in die context herhaald dat de wetgever duidelijk een *gevaarzettingsdelict* voor ogen had.
(4) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 16.
(5) Arbitragehof 24 maart 2004, arrest nr. 51/2004, www.grondwettelijkhof.be.

volgende gedragingen die kunnen worden gesteld naar aanleiding van het hacken (1):

1°hetzij overnemen van gegevens (bv. het stelen van industriële geheimen in het kader van bedrijfsspionage);

2°hetzij gebruik maken van het systeem dat hij hackt of een ander systeem van een derde (2) (bv. het benutten van de capaciteit van het systeem waardoor de mogelijkheden van andere gebruikers tijdelijk beperkt worden (3));

3°hetzij veroorzaken van schade uit onvoorzichtigheid (opzettelijke sabotage wordt in het kader van art. 550*ter* Sw. zwaarder bestraft) (4).

De wetgever heeft een mooie terechte bekommernis gehad om ter zake een heel gedifferentieerd misdrijf te creëren. In de praktijk dient evenwel te worden vastgesteld dat er zelden situaties voorkomen van hacking die géén verzwarende omstandigheid genereren. Zo is het bijzonder moeilijk om iemands informaticasysteem te hacken zonder overname van bepaalde gegevens die zich in het gehackte informaticasysteem bevinden, zeker indien men ervan zou uitgaan dat het openen van een computerbestand om dit te kunnen lezen doorgaans noodzakelijk een interne reproductie van het betrokken bestand vereist, en de betrokkene hierdoor noodzakelijk het bestand «overneemt» (5). Zo is het evenzo bijzonder moeilijk om een informaticasysteem te hacken zonder daarbij «gebruik» te maken van dat informaticasysteem eens dat men daar in zit. Zo zal ook in de meeste gevallen van hacking sowieso wel enige vorm van schade te weerhouden zijn (bv. afname van downloadcapaciteit, wijziging data, tijdsdiefstal, ...) (6); de verzwarende omstandigheid zal immers ook van toepassing zijn indien de loutere handhaving in het systeem op zich reeds het systeem verstoort (7).

4. Heling van gehackte gegevens (art. 550bis, § 7 Sw.)

Een andere gevolghandeling die door de wetgever strafbaar wordt gesteld, is het «helen» van de naar aanleiding van de hacking bekomen gegevens.

Zo is strafbaar, hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van hacking, **deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt**. Ter zake is het **algemeen opzet** voldoende maar noodzakelijk.

Aangezien het misdrijf heling traditioneel enkel materiële voorwerpen kan betreffen, viseerde de wetgever met deze bepaling vooral de context van spionagebestrijding (8). De formulering is gelijklopend met een soortgelijke bepaling inzake het onderscheppen van communicatie (zie met name art. 314*bis*, § 2 Sw.). Niettemin is evident het toepassingsgebied veel breder dan de bedrijfsspionage. Zo kan bijvoorbeeld worden gedacht aan:

– het geval van hacking van een hotmailaccount waarbij de dader de loggings verandert (en zo de toegang onmogelijk maakt voor de houder van de account), waarna de hacker deze nieuwe valse loggings doorgeeft aan een vriend *«om ook eens te kunnen gaan kijken»*;
– het doorvertellen van de inhoud van een mail die men gelezen heeft naar aanleiding van de hacking van een mailaccount.

5. Poging tot hacking (art. 550bis, § 4 Sw.)

Naast de basisgedraging en de gevolghandelingen, wordt eveneens de poging om zich onrechtmatig toegang te verschaffen tot een informaticasysteem of een deel daarvan, strafbaar gesteld. Gelet op de ernst die de wetgever toekende aan deze gedragingen werd dezelfde strafmaat voorzien als voor het voltooide misdrijf. Een poging om in te breken in een informaticasysteem kan een zekere tijd en manipulatie in beslag nemen met alle risico's van dien voor het systeem.

Zoals gezegd, wilde de wetgever een **gevaarzettingsdelict** creëren.

De wetgever gaf ter zake het voorbeeld van het geautomatiseerd uitproberen van lange listings van mogelijke paswoorden (9) (10).

6. Hackertools (art. 550bis, § 5 Sw.)

De wet voorziet in een specifieke bepaling die degene bestraft die, onrechtmatig, enig instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het hacken mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt. Hierbij worden in de eerste plaats de handel in «hackertools» en

---

(1) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 17.

(2) Dit lijkt te impliceren dat eenieder die niet zijn eigen computer gebruikt om te hacken, sowieso een verzwarende omstandigheid genereert.

(3) Dit lijkt meteen ook te impliceren dat er sprake is van de derde verzwarende omstandigheid aangezien alzo schade ontstaat bestaande uit de daling van de performantie van het informaticasysteem in kwestie.

(4) Zie P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?», *T.Strafr.* 2001, afl. 6, 325-326.

(5) J. DEENE en G. NERINCKX, *Praktijkboek Recht en Internet*, Titel II – Hoofdstuk 10 – Computercriminaliteit, Brugge, Vanden Broele, 2007, 34.

(6) Zie voor een toepassingsgeval: Corr. Dendermonde 29 september 2008, *T.Strafr.* 2009, afl. 2, 111, noot Ph. VAN LINTHOUT (ed.), «Territoriale bevoegdheid in cyberspace».

(7) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Senaat 1999-2000, nr. 2-392/3, 66.

(8) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 18.

(9) *Ibid.*

(10) Corr. Dendermonde 2 februari 2009, onuitg.: de man in kwestie trachtte in de e-mailaccounts van zijn voormalige werkgever te geraken door het uitproberen van tal van paswoorden en door 6.112 maal de knop «paswoord vergeten» in te drukken. De feiten in kwestie werden evenzo gekwalificeerd als informaticasabotage, aangezien derwijze 6.112 mails werden gegenereerd/afgevuurd op de mailbox van de voormalige werkgever, met overbelasting van het informaticasysteem tot gevolg. Voorts werden de feiten evenzo gekwalificeerd als een inbreuk op artikel 145, § 3*bis* van de wet van 13 juni 2005 betreffende elektronische communicatie, artikel dat strafbaar stelt *«een elektronisch communicatienetwerk of -dienst of andere elektronische communicatiemiddelen te hebben gebruikt om overlast te veroorzaken aan zijn correspondent of schade te berokkenen»*.

de toegangscodezwendel geviseerd door de wetgever (1).

Het moreel element is het **algemeen opzet** bestaande uit het wetens en willens onrechtmatig handelen (2).

Andere voorbeelden zijn onder andere:

– diegene die beroepshalve de toegangscode van een IT-systeem kent en die doorgeeft aan een onbevoegde (3);
– diegene die op het internet een programma download om vanop afstand de webcam van een derde te kunnen activeren (4);
– diegene die een programma doorgeeft aan een vriend om op eenvoudige wijze hotmailaccounts te kraken.

Het feit dat bepaalde «spyware» en hackertools zonder meer vrij te verkrijgen zijn op het internet, en/of evenzo «ludieke» doeleinden kunnen dienen en/of met een bijzonder gemak en eenvoud gebruikt kunnen worden, heft de strafbaarheid niet op (5).

De vraag die de feitenrechter telkens zal moeten beantwoorden is de vraag of de tool in kwestie **hoofdzakelijk** is ontworpen of aangepast om het hacken mogelijk te maken. Er mag in die context worden gerekend op de realiteitszin van de bodemrechter. Zeldzaam zijn de wapens die in hoofdzaak worden gemaakt om vrede te sluiten.

7. Uitlokking van hacking (art. 550bis, § 6 Sw.)

De wetgever heeft gewild dat de opdrachtgever of aanzetter tot hacking zwaarder zou worden gestraft dan degene die het misdrijf effectief uitvoerde. De reden hiervoor is dat, waar vroeger hacking in veel gevallen een tijdverdrijf was voor jonge computerfreaks, de wetgever vreesde dat thans professionele criminelen dergelijke personen zouden inschakelen om hun plannen uit te voeren (6).

Het materieel bestanddeel van het misdrijf bestaat uit **het geven van een opdracht tot hacking** en/of uit het **aanzetten tot het plegen van hacking**. Er mag worden aangenomen dat de aanzetting of de opdracht tot hacking niet *intuitu personae* gegeven moeten worden aan derden. Een «oproep» of «uitdaging» tot hacking van een specifiek doel kan zonder meer het misdrijf constitueren (7).

Het moreel element betreft het **algemeen opzet**.

B. Informaticasabotage (art. 550ter Sw.)

Met deze bepaling beoogde de wetgever, net zoals bij de voorgaande bepalingen, een manifeste lacune in ons strafrecht in te vullen. Immers, vernielingen en beschadigingen worden traditioneel in het strafrecht enkel in aanmerking genomen wanneer ze betrekking hebben op tastbare voorwerpen. Dit is het geval wanneer het schade betreft aan een informaticasysteem zelf, maar het is duidelijk dat het beschadigen van data *as such* niet rechtstreeks werd geviseerd door de bepalingen van het Strafwetboek. Daarom opteerde de wetgever ervoor om in artikel 550*ter* van het Strafwetboek op klaar en duidelijke wijze elke kwaadwillige manipulatie van gegevens strafbaar te stellen (8).

Materieel wordt het misdrijf gepleegd **door gegevens in een informaticasysteem in te voeren, te wijzigen, te wissen of of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem te veranderen**. In dat opzicht vertoont de informaticasabotage een zekere gelijkenis met het informaticabedrog (art. 504*quater* Sw.), weze het dat het voor wat informaticasabotage betreft volstrekt irrelevant is of er een onrechtmatig economisch voordeel werd beoogd. Zoals gezegd, is bij informaticabedrog ICT het *middel* en bij informaticasabotage is ICT-crime het *doel* op zich.

Het moreel element van het basismisdrijf (§ 1 van art. 550*ter* Sw.) is het **algemeen opzet** (9): hij die data manipuleert, terwijl hij weet dat hij daartoe niet gerechtigd is.

Bij wijze van **subjectieve verzwarende omstandigheid** voorziet alinea 2 van § 1 van artikel 550*ter* van het Strafwetboek in strafverzwaring indien het misdrijf gepleegd wordt met een **bijzonder opzet**, bestaande uit een bedrieglijk opzet of uit het oogmerk om te schaden.

Voorts voorzag de wetgever ook in een tweetal **objectief verzwarende omstandigheden**. Indien door de datamanipulatie/-sabotage schade ontstaat, wordt ook het veroorzaken van schade aan informaticasystemen in rekening gebracht. In de praktijk zal schade aan data en schade aan het computersysteem zelf vaak samen voorkomen en technisch niet altijd strikt te scheiden zijn. Niettemin achtte de wetgever het wenselijk een juridisch onderscheid te maken tussen de gevolgen voor de data enerzijds en voor het informaticasysteem

---

(1) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 18.

(2) Aanvankelijk werd een bijzonder opzet vereist, doch dat is niet meer het geval sedert de wetswijziging bij de wet van 15 mei 2006 (*BS* 12 september 2006).

(3) *Parl.St.* Kamer 1999-2000, nr. 213/004, 55.

(4) Corr. Dendermonde 1 maart 2010, onuitg.

(5) De grens kan vaak zeer dun zijn: zo worden bepaalde tools op het internet gepresenteerd als «practical jokes», doch die bij nader inzien bedenkelijke toepassingsmethoden kennen. Denk maar aan websites zoals www.anoniemsmsen.be waarmee je een «fake» sms-je of een fake e-mail kan verzenden, gebruik makend van het gsm-nummer respectievelijk het e-mailadres van iemand anders. Strikt genomen dring je in eerste instantie niet binnen in het informaticasysteem van de verzender (de persoon wiens gegevens je valselijk gebruikt om als «afzender» te dienen); je gebruikt enkel valselijk diens adresgegevens (gsm-nummer of e-mailadres). In de mate dat de geadresseerde evenwel op de valse e-mail een reply uitvoert, zal de échte houder van de afzendergegevens de reply ontvangen, waardoor je initiële valse boodschap wél doordringt in diens informaticasysteem, weze het dat de arme ziel zich – geheel terecht – niet gaat herinneren dat hij de initiële boodschap geschreven heeft...

(6) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001 18.

(7) Zie Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, afl. 5, 351: een geldsom uitloven ten aanzien van derden om in te breken in een computersysteem constitueert het misdrijf van aanzetting tot externe hacking.

(8) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 19.

(9) Het algemeen opzet werd ingevoerd bij wet van 15 mei 2006 (*BS* 12 september 2006); voorheen was een bijzonder opzet vereist voor het basismisdrijf.

anderzijds. Gelet op het belang dat informaticasystemen in onze samenleving innemen, wordt **het belemmeren van de correcte werking van een informaticasysteem** (§ 3 van art. 550*ter* Sw.) zwaarder bestraft dan het louter **berokkenen van schade aan de data** (§ 2 van art. 550*ter* Sw.). Net zoals hiervoor met betrekking tot hacking en de daarbij behorende verzwarende omstandigheden reeds werd geopperd, kan men ook hier weer de vraag stellen in welke mate dat informaticasabotage überhaupt mogelijk kan zijn zonder de data te beschadigingen en/of op een of andere manier een belemmerende werking uit te oefenen op de correcte werking van het informaticasysteem in kwestie.

Naast de delicten die kwaadwillige manipulaties en de gevolgen die daaruit voortvloeien viseren, wordt ook een strafbaarstelling voorzien inzake bepaalde **voorbereidingshandelingen**. Hierbij wordt gedacht aan de ontwikkeling en de verspreiding van schadelijke gegevens en computerprogramma's zoals virussen of programma's om dergelijke virussen te genereren (§ 4 van art. 550*ter* Sw.) (1). De strafbaarstelling is gelijklopend met deze vervat in artikel 550*bis*, § 5 van het Strafwetboek, zodat ter zake dan ook kan worden verwezen naar de toelichting dienaangaande hierboven.

Er kan worden opgemerkt dat de tenlasteleggingen vervat in artikelen 550*bis* en 550*ter* van het Strafwetboek vaak perfect combineerbaar zijn en aanleiding zullen kunnen geven tot een situatie van eendaadse samenloop. Een eenvoudige intrusie in andermans informaticasysteem, waarbij schade ontstaat, zal al snel aanleiding kunnen geven tot zowel de toepassing van artikel 550*bis*, §§ 1 en 3, als de toepassing van artikel 550*ter*, §§ 1 en 2 of 3 van het Strafwetboek. Zo zal een hackertool (art. 550*bis*, § 5 Sw.) in veel gevalen ook te beschouwen zijn als een sabotage-instrument (art. 550*ter*, § 4 Sw.); denk bijvoorbeeld maar aan een Trojaans paard, waarbij een hacking wordt gefaciliteerd door middel van het inbrengen van een virus.

De wetgever gaf zelf enkele voorbeelden van beoogde inbreuken op artikel 550*ter* van het Strafwetboek (2):

- de daadwerkelijke vernietiging van een bestand of een gedeelte daarvan;
- de onbruikbaarmaking van een harde schijf of een centrale server;
- de ontregeling van het besturingssysteem.

Voorts kan ook nog worden verwezen naar de volgende praktijkvoorbeelden (3):

- het inbrengen van een virus;
- het herschrijven van bepaalde werkingsinstructies van een informaticasysteem;
- het wissen van data (bv. een commercieel belangrijk gegevensbestand) of van een programma(onderdeel);
- het misbruik maken van een gestolen bankkaart (4): door een wederrechtelijk verkregen bankkaart en bankkaartgegevens te hebben ingegeven in een terminal van een geïnformatiseerd banktransactiesysteem met het bedrieglijk oogmerk om in de geïnformatiseerde portefeuille van derden in te breken en gelden te debiteren en/of toe te eigenen, met de verzwarende omstandigheid zoals bedoeld in § 2 van artikel 550*ter* van het Strafwetboek doordat de elektronische portefeuille van het slachtoffer werd gedebiteerd (en er aldus schade is aan de data), én met de verzwarende omstandigheid zoals bedoeld in § 3 van artikel 550*ter* van het Strafwetboek doordat de correcte werking van de geïnformatiseerde portefeuille van het slachtoffer werd belemmerd (5);
- door op de website van zijn voormalige werkgever de e-mailadressen van zijn voormalige werkgevers te hebben ingegeven op het inlogscherm en daarna middels het indrukken van de knop «paswoord-vergeten» minstens 6.112 mails te hebben gegenereerd/afgevuurd in de kwestieuze mailboxen teneinde de digitale overlast te veroorzaken (6);
- een inbreuk op artikel 550*bis*, § 5 van het Strafwetboek (hackertools) én op artikel 550*ter*, § 4 van het Strafwetboek (sabotage-instrumenten) werd weerhouden (eendaadse samenloop) voor wat het bezit van «messenger discovery live» en «webcam spy» betreft, zijnde twee programma's die intrusie mogelijk maken in het informaticasysteem van derden (7);
- een inbreuk op artikel 550*ter*, §§ 1-2 werd weerhouden lastens de beklaagde die was ingebroken in de hotmailaccount van zijn *ex*-vriendin, waarna hij de instellingen en loggings had veranderd (8);
- diezelfde beklaagde werd evenzo veroordeeld voor inbreuk op artikel 550*ter*, §§ 1-3 van het Strafwetboek omdat hij derwijze de account onbeschikbaar had gemaakt voor het slachtoffer, en de correcte werking van haar account aldus werd aangetast (9).

III. HET OPSPORINGSINSTRUMENTARIUM VAN HET WETBOEK VAN STRAFVORDERING

Het werken in een steeds meer digitale omgeving bracht uiteraard met zich mee dat aanpassingen zich opdrongen aan het Wetboek van Strafvordering.

Concreet lijkt de basis voor elke digitale recherche, wat het Belgische Wetboek van Strafvordering betreft, zich te herleiden tot zes artikelen. Hieronder worden zij een voor een behandeld.

Uit rechtspraak en rechtsleer blijkt dat zij vaak onontgonnen terrein zijn, in schril contrast tot hun steeds belangrijker wordende rol.

---

(1) *Parl.St.* Kamer 1999-2000, nr. 0213/004, 7; nr. 0213/001, 19; 2003-2004, 51-1284/0001, 6.
(2) *Parl.St.* Kamer 1999-2000, nr. 0213/004, 7.
(3) Zie ook D. DEWANDELEER, «Misdrijven en strafonderzoek in de IT-context» in R. VERSTRAETEN en F. VERBRUGGEN (eds.), *Themis – Strafrecht- en Strafprocesrecht*, Brugge, die Keure, 2009-2010, 133.
(4) Op zich ook reeds te kwalificeren als een inbreuk op art. 504*quater* Sw.
(5) Corr. Dendermonde 8 juni 2009, onuitg.
(6) Corr. Dendermonde 2 februari 2009, onuitg.
(7) Corr. Dendermonde 1 maart 2010, onuitg.
(8) Corr. Dendermonde 8 juni 2009, onuitg.
(9) *Ibid.*

Elke «*live*»-confrontatie in de praktijk toont aan dat het juridisch matchen van rechtsregel en problemen in de praktijk geen eenvoudige opdracht is. Snel zal ook duidelijk worden dat onze wetgever nog een hele uitdaging heeft in het trachten vinden van gepaste oplossingen voor een evoluerende digitale wereld waar de cybercriminelen steeds een ruime voorsprong lijken te hebben op politie en justitie.

Voor wat de problematiek van het moeilijke evenwicht tussen enerzijds de rechtsfiguur van de netwerkzoeking en anderzijds de informaticatap betreft, wordt *in extenso* verwezen naar het artikel «Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel» verschenen in het *Tijdschrift voor Strafrecht* (1). De paragrafen 5 en 6 zijn wat dit betreft grotendeels een uittreksel uit het voornoemde artikel.

Het is daarbij zeer belangrijk om weten dat gelet op de moeilijkheden van de internetrecherche, in de voornamelijk heimelijke fase van het gerechtelijk onderzoek, de wetgever op dit moment bezig is met het totaal – en broodnodig – herschrijven van het artikel 88*ter* van het Wetboek van Strafvordering waarbij *de lege ferenda* een nieuw onderscheid zou kunnen gaan bestaan tussen het eenvoudig **databeslag** (art. 39*bis* Sv.), het databeslag van op afstand (de **netwerkzoeking** vervat in art. 88*ter* Sv. –in een **niet-heimelijke fase**), het **databeslag in de heimelijke fase** en van op afstand, desgevallend met gebruik van speciale technieken (hackertools, spyware, ...; een nieuw te schrijven art. 88*quinquies* Sv.?) en het **databeslag van gegevens van telecommunicatie tijdens hun overbrenging** (tap zoals voorzien in art. 90*ter* e.v. Sv.).

Op het terrein wordt alleszins door onderzoekers en magistraten reikhalzend uitgekeken naar dit nieuw noodzakelijk wetgevend initiatief, dat op papier al concrete vorm zou hebben, doch in de huidige politieke constellatie zijn weg nog niet vindt doorheen het parlementair landschap.

§ 1. Artikel 39bis van het Wetboek van Strafvordering – digitaal databeslag

De wetgever heeft met het artikel 39*bis* van het Wetboek van Strafvordering een oplossing geboden voor wat in de praktijk dikwijls een probleem was. Immers, in tegenstelling tot de gebruikelijke inbeslagname van bewijsmateriaal in de niet-digitale omgeving, waarbij manueel voorwerpen konden ter hand genomen worden om ze op de griffie neer te leggen, was dit in een digitale omgeving niet steeds mogelijk. Als klassiek voorbeeld uit de praktijk kan worden verwezen naar de politieman die in het kader van een financieel dossier een huiszoeking diende te verrichten in een bank en op de hoofdzetel van de bank geconfronteerd werd met een ganse zaal vol computers waarbij het een hele klus zou geweest zijn om deze als bewijsmateriaal alle in beslag te nemen. Uiteraard stelde zich in die gevallen ook steeds het probleem van de eventuele schade die kon worden toegebracht wanneer hardware werd in beslag genomen en waardoor het bedrijf, *in casu* de bank, niet verder zou kunnen functioneren. Nochtans was men in de bewijsvoering, gelet op de eventuele nood aan tegenspraak, zeer gewend van bewijsmateriaal letterlijk te kunnen vastnemen, te kunnen voorleggen aan een expert, te kunnen laten tegen-expertiseren en te kunnen tonen voor de rechter ten gronde. Voor wat het digitaal bewijs betreft, merkte men snel dat dit in de klassieke benadering van bewijsmateriaal en de inbeslagname niet mogelijk was.

De wetgever heeft in artikel 39*bis* van het Wetboek van Strafvordering gekozen voor een zeer pragmatische oplossing: niet enkel mag digitaal bewijs nog steeds materialiter in beslag worden genomen (bv. een computer of een smartphone), maar het mag evenzo en evenwaardig ook worden gekopieerd of ontoegankelijk gemaakt en verwijderd, om als bewijsmateriaal te dienen. Wanneer de inbeslagname van de dragers van het digitaal bewijs niet wenselijk is, **kan worden geopteerd om enkel de gegevens te kopiëren en zelfs ook de gegevens nodig om deze eerste gegevens te kunnen lezen**.

Een eerste kritische bedenking bij deze laatste mogelijkheid kan men maken vanuit auteursrechtelijk oogpunt, waarbij – terecht – de vraag dient gesteld te worden of de overheid zo maar gerechtigd is om zich niets aan te trekken van eventuele licenties verbonden aan software nodig om data te lezen.

Om te voorkomen dat er later discussie zou ontstaan over de wijze waarop informatie werd in beslag genomen, stelde de wetgever dat bij het eventuele kopiëren van data dit dient te gebeuren op dragers van de overheid. Enkel in dringende zaken of omwille van technische redenen (speciale soort van hardware, ...) mag gebruik worden gemaakt van de dragers van de gebruiker van het informaticasysteem.

De wetgever heeft ook voorzien dat, wanneer om technische redenen of omwille van de omvang, het louter kopiëren niet mogelijk is (denk bv. aan de data van een grote bank), men de gegevens ter plekke mag laten staan, waarbij de toegang tot de gegevens en de eventuele kopieën dient te worden geblokkeerd en de integriteit van de gegevens te worden gewaarborgd. Zeer verregaand, en in tegenstelling tot de gebruikelijke gevolgen van een inbeslagname, heeft de wetgever in de digitale omgeving toegelaten om de in beslag genomen data toch te laten gebruiken zolang dit geen gevaar is voor de strafvordering. Enkel wanneer de in beslag genomen data in strijd zijn met de openbare orde of de goede zeden (bv. in geval van kinderporno), of een gevaar opleveren voor de integriteit van informaticasystemen (bv. hacker tools), dient het gebruik ervan steeds te worden verhinderd.

De uitdaging welke de wetgever had om regelgeving te maken die de snel evoluerende informaticawereld kon bijbenen, blijkt, voor wat dit artikel betreft, tegelijkertijd een grote zwakte en de uitdaging voor hen die de rechtsgeldigheid van de digitale inbeslagnames wensen aan te vechten. De wetgever heeft immers op het snel evoluerende technische landschap willen anticiperen door op verschillende plaatsen in artikel 39*bis* van het Wetboek van Strafvordering te spreken van de ***«passende technische middelen»***, dit wellicht in de hoop dat voor eenieder duidelijk zou zijn wat deze zouden inhouden. In deze wens naar flexibiliteit ligt

(1) P. VAN LINTHOUT en J. KERKHOFS, «Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel», *T.Strafr.* 2008, afl. 2, 79-95.

tegelijkertijd een bijzondere zwakte. Zolang niet technisch zal omschreven zijn, zoals dat in andere landen van de Europese Unie het geval is, hoe volgens de regels van de kunst het databeslag dient te gebeuren, is dit mogelijks voorwerp van discussie.

§ 2. Artikel 46bis van het Wetboek van Strafvordering – identificatie

Anonimiteit op het internet en in de digitale omgeving bestaat niet voor zover de wetgever heeft toegelaten om over te gaan tot identificatie van de gebruikers van ICT-toepassingen. Waar er in de rechtspraak discussie was met welke soort vordering (Openbaar Ministerie of onderzoeksrechter) kon worden overgegaan tot de identificatie van de gebruiker van een ICT-toepassing, heeft de wetgever dit bij de wet van 23 januari 2007 (1) definitief geregeld.

Artikel 46*bis* van het Wetboek van Strafvordering laat immers toe om bij gemotiveerde en schriftelijke beslissing van een parketmagistraat of een onderzoeksrechter te identificeren wie achter een IP-adres (2) schuilgaat. De gemotiveerde beslissing dient de proportionaliteit te toetsen van de maatregel met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad. In de praktijk vertaalt zich dit meestal tot een typevordering of kantschrift. Deze extra vereiste, welke door de wetgever in 2007 werd opgelegd, staat in schril contrast met het feit dat totaal niet dient gemotiveerd te worden voor sommige andere maatregelen welke naar de bescherming van de privacy een veel verdere impact hebben (hierover meer in § 3). Gelet op het feit dat deze regel niet op straffe van nietigheid is voorgeschreven, en gelet op de huidige Antigoon-rechtspraak, kan men zich ernstige vragen stellen bij de toegevoegde waarde van deze inhoudelijke vormvereiste.

Dit artikel wordt in de praktijk bijzonder vaak gebruikt, o.a. voor de identificatie van een telefoonnummer, de identificatie via een IMEI-nummer, de identificatie via een e-mail of een IP-adres. Hetzelfde artikel wordt ook gebruikt voor het opvragen van de telefoonnummers welke gekoppeld zijn of waren aan een SIM-kaart («SIM-track»), of het opvragen van de IMEI-nummers welke gekoppeld waren aan een telefoonnummer (de zgn. «IMEI-track»).

In meer algemene termen kan worden gezegd dat artikel 46*bis* van het Wetboek van Strafvordering een juridisch instrument is dat toelaat om de identificatie en/of vereenzelviging te bekomen van deelnemers aan communicatie, en dit op basis van **statische gegevens** (3).

Waar naar het doel en de reikwijdte van het inhoudelijke toepassingsveld van artikel 46*bis* van het Wetboek van Strafvordering – gelukkig – op dit moment zich geen juridische problemen meer lijken te stellen, dient helaas te worden vastgesteld dat over het bepalen van wie onder de noemer valt van de bepaling *«operator van een elektronisch communicatienetwerk»* of van *«verstrekker van een elektronische communicatiedienst»* nog wel veel inkt lijkt te zullen vloeien. Zo meende de verstrekker van de elektronische webmail dienst Yahoo! Inc. niet te moeten antwoorden op de vorderingen van de procureur des Konings te Dendermonde betreffende de vraag tot identificatie van webmailadressen van personen welke misdrijven leken gepleegd te hebben op het Belgische grondgebied. Yahoo! Inc. werd echter op grond van artikel 46*bis*, § 2 van het Wetboek van Strafvordering op 2 maart 2009 veroordeeld door de correctionele rechtbank van Dendermonde. De rechtbank was o.i. terecht van oordeel dat de medewerkingsplicht *ex* artikel 46*bis* van het Wetboek van Strafvordering (en/of 88*bis* Sv.) zich uitstrekt tot elke *internet service provider* die in België diensten ontplooit en aanwezig is (4). Een andere interpretatie van het begrip *«verstrekker van een elektronische communicatiedienst»* zou de nuttige toepassing van artikel 46*bis* van het Wetboek van Strafvordering totaal onmogelijk maken. Bovendien dreigt er alsdan een discriminatoir onderscheid te ontstaan tussen de aanbieders van internetdiensten op Belgisch grondgebied in functie van de plaats waar ze hun bedrijfszetel hebben gevestigd (in België, dan wel buiten de landsgrenzen). Inmiddels werd het door Yahoo! Inc. ingestelde hoger beroep tegen de veroordeling door de correctionele rechtbank te Dendermonde op 2 maart 2009, bij arrest van het hof van beroep te Gent van 30 juni 2010 hervormd tot een vrijspraak. Het hof van beroep is van oordeel dat Yahoo! Inc. in de zin van de Belgische wet geen operator van een elektronisch communicatienetwerk is, noch een verstrekker van een elektronische communicatiedienst. De beslissing en de overwegingen van het hof zullen ongetwijfeld nog in *extenso* hun bespreking kennen in navolgende literatuur. Het openbaar ministerie tekende cassatie aan tegen het arrest in kwestie.

---

(1) *BS* 14 maart 2007.

(2) Een IP-adres is gemakkelijkheidhalve te vergelijken met een «jetton» die men nodig heeft om op het internet te kunnen gaan. Deze «jetton» wordt gegeven door een *internet access provider* (bv. Skynet, Telenet, ...) welke verplicht is te registreren aan wie op welk moment (datum en tijd) deze «jetton» werd gegeven.

(3) Statische gegevens in de zin van art. 46*bis* Sv. zijn punctuele (kruispunt)gegevens die zich afgelijnd en geïsoleerd kunnen aandienen: zo kan men bijvoorbeeld op basis van een exact IP-adres (bv. 82.192.168.1), in combinatie met een exact tijdstip (bv. 15 juni 2010 om 10u15) op grond van art. 46*bis* Sv. de accesprovider (bv. Telenet, Scarlet, Skynet...) vorderen om de identiteit van de abonnee mede te delen.
Indien men te maken heeft met een dynamisch gegeven, dient men zijn toevlucht te nemen tot art. 88*bis* Sv.: bv. indien men over een IP-adres beschikt, zonder dat men exact het tijdstip van misbruik kent, dan kan men een historische bevraging doen, bv. van 13 juni 2010 te 11u00 tot en met 15 juni 2010 te 23u00. Alsdan wordt gerechercheerd op basis van dynamische gegevens (een tijdsperiode). Gelet op het feit dat de impact op de privacy op dat ogenblik substantieel zwaarwichtiger zou kunnen dreigen te worden, lijkt de wetgever te vereisen dat alsdan art. 88*bis* Sv. wordt toegepast en dat aldus een onderzoeksrechter tussenkomt. Ook al ligt het niet in de lijn van de *ratio* van de wet, niets lijkt zich wettelijk te verzetten tegen *«meerdere statische bevragingen»* in de plaats van één dynamische bevraging: met andere woorden lijkt het wettelijk niet uitgesloten om in een welbepaald (dynamisch) tijdvak meerdere (statische) bevragingen te doen: bv. voor de periode van 13 juni 2010 te 11u00 tot en met 15 juni 2010 te 23u00 tien statische (steekproef)bevragingen doen op willekeurige tijdstippen; wellicht is de grootste gemene deler de identiteit die je zoekt...

(4) Corr. Dendermonde 2 maart 2009, *Juristenkrant* 2009 (weergave E. De Busser), afl. 186, 3; *T.Strafr.* 2009, afl. 2, 116.

§ 3. Artikel 88bis van het Wetboek van Strafvordering – Opsporen en lokaliseren

In het kader van een strafrechtelijk onderzoek is het ook ten zeerste van belang te kunnen nagaan wie met wie gecommuniceerd heeft, wanneer dit gebeurde en in vele gevallen ook zeer van belang te weten waar. Artikel 88*bis* van het Wetboek van Strafvordering laat toe om deze **dynamische gegevens** van communicatie op te vragen bij de operatoren en verstrekkers van een dienst op het internet.

Merkwaardig genoeg en in contrast met de inhoud van de wetswijziging van 2007 voor wat het artikel 46*bis* van het Wetboek van Strafvordering betreft, waar de inbreuk op de privacy veel minder ver lijkt te gaan, dient uit herhaalde en vaststaande rechtspraak (1) afgeleid te worden dat de vordering om deze gegevens te bekomen en welke dient te worden uitgeschreven door een onderzoeksrechter, niet dient te worden gemotiveerd voor wat het opvragen van gegevens uit het verleden betreft.

Anders is het, wanneer in «real time», door gebruik van een «zoller-malicieux» de communicatie geobserveerd wordt. In dat geval dient de onderzoeksrechter te motiveren welke de feitelijke omstandigheden zijn van de zaak, die de maatregel wettigen. Zo een observatie in reële tijd kan worden bevolen voor maximum 2 maand maar is onbeperkt verlengbaar. In de realiteit wordt niet vaak van deze maatregel op zich gebruik gemaakt omdat de beperking aan artikel 88*bis* van het Wetboek van Strafvordering bestaat in het feit dat dit enkel gegevens van communicatie zijn, en geen inhoud kan worden opgevraagd (hiervoor zal een tapmaatregel zich opdringen, vaak gepaard gaand met de maatregel zoals voorzien door art. 88*bis* Sv.).

Net zoals kritisch overwogen werd bij het bespreken van artikel 46*bis* van het Wetboek van Strafvordering, werd door de wetgever ook hier geen nietigheidssanctie voorzien zodat voor wat eventuele vormfouten betreft, dient verwezen te worden naar de Antigoon-rechtspraak.

Verder dient nog gezegd te worden dat in tegenstelling tot artikel 46*bis* van het Wetboek van Strafvordering, een vordering op grond van artikel 88*bis* van het Wetboek van Strafvordering in de regel enkel kan worden genomen door een onderzoeksrechter. Wel is het mogelijk voor het Openbaar Ministerie om deze maatregel te vorderen bij mini-instructie (mini-onderzoek) (2). Op deze regel bestaan twee uitzonderingen, zijnde: enerzijds bij een ontdekking op heterdaad voor feiten die worden opgesomd in artikel 90*ter*, §§ 2, 3 en 4 Sv. (de taplijst), waar het Openbaar Ministerie dit zelf kan, en waar de onderzoeksrechter dient te bevestigen binnen de 24 uur (bij gebreke van sancties in het Wetboek van Strafvordering is het onduidelijk wat het lot is van de informatie welke bekomen werd door het Openbaar Ministerie op het moment dat een onderzoeksrechter *post factum* niet zou bevestigen; ook hier lijkt de Antigoon-rechtspraak van toepassing). Anderzijds is er eveneens een uitzondering van toepassing in het kader van de wet van 13 juni 2005 betreffende de elektronische communicatie, bij bedrog en overlast wanneer de klager daarom verzoekt, en de maatregel onontbeerlijk lijkt (vaak toegepast in het kader van stalkingdossiers).

Artikel 88*bis* van het Wetboek van Strafvordering wordt in de praktijk toegepast voor het opvragen van gsm- en internetverkeer, voor de lokalisatie van een gsm ten aanzien van een mast, voor het nagaan van het mastverkeer op een mast en voor de geografische lokalisatie van een telefoontoestel met hulp van speciale telecomdiensten (BIPT). Het betreffende artikel is niet toepasselijk voor het opvragen van een dekkingsplan van een telefoonmast (dit kan bij eenvoudig kantschrift), voor het terugvinden van een gestolen auto (technisch niet mogelijk tenzij bijzondere apparatuur in de wagen werd aangebracht) en ook niet voor het volgen op afstand van een voertuig (hier is de BOM-wetgeving van toepassing in het kader van observatiemaatregelen).

Ook in het licht van artikel 88*bis* van het Wetboek van Strafvordering is de discussie volop gaande voor wat de invulling van de begrippen *«operator van een telecommunicatienetwerk»* of *«verstrekker van een telecommunicatiedienst»* betreft. Opnieuw mag hier verwezen worden naar het belangwekkende standpunt van de strafrechter te Dendermonde (3).

§ 4. Artikel 88quater van het Wetboek van Strafvordering – Medewerkingsverplichting

Het artikel 88*quater* van het Wetboek van Strafvordering is een weinig gebruikt maar wellicht volledig miskend artikel waar het voor de onderzoeksrechter mogelijk is om iemand met een bijzondere kennis van een informaticasysteem aan te duiden en te gelasten om hem te helpen bij het zoeken naar bewijsmateriaal. Het spreekt voor zich dat dit artikel niet van toepassing is op verdachten, die sowieso niet kunnen worden verplicht om tegen zichzelf te getuigen of lastens zichzelf bewijsmateriaal te verzamelen. Ook de personen opgesomd in het artikel 156 van het Wetboek van Strafvordering (bloedverwanten, aanverwanten...) vallen buiten het toepassingsbereik van dit artikel.

Aangezien dit artikel het mogelijk maakt om personen te dwingen de beveiliging van gegevens en/of de versleuteling van gegevens te doorbreken, en de gegevens in verstaanbare vorm voor te leggen aan de onderzoeksrechter, dient goed te worden verstaan dat het belang van dit artikel enkel nog zal toenemen. Steeds vaker wordt men immers geconfronteerd met geëncrypteerde gegevens waarbij het decrypteren een schier onmogelijke taak is. De Belgische wetgever heeft – bewust of onbewust – gekozen voor de vrijheid van encryptie. Deze keuze heeft gunstige effecten voor het vertrouwen dat mensen hebben voor wat commerciële activiteiten op het internet (bv. internetbankieren) betreft, maar heeft desastreuze effecten wanneer criminelen worden toegelaten om al hun gegevens op versleutelde wijze te bewaren.

In België bestaat op dit moment, buiten deze verplichting welke van toepassing is op derden, geen dwangmaatregel naar de verdachte toe om aangetroffen maar

(1) Cass. 19 januari 2005, www.cass.be.

(2) Art. 28*septies* Sv.

(3) Corr. Dendermonde 2 maart 2009, *Juristenkrant* 2009 (weergave E. De Busser), afl. 186, 3; *T.Strafr.* 2009, afl. 2, 116.

geëncrypteerd bewijsmateriaal om te zetten naar begrijpbare en leesbare inhoud. De Franse wetgever heeft wat dit betreft in artikel 434-15-2 van het Franse Strafwetboek voorzien in een afzonderlijke strafbaarstelling voor iedereen (ook de verdachte) die niet de sleutel aflevert van vercijferde data wanneer deze data gelinkt zijn aan het plegen of gepleegd zijn van een misdrijf. De Franse wetgever heeft zelfs in een strafverzwaring voorzien wanneer het onthullen van deze informatie het misdrijf had kunnen voorkomen. Naar Belgisch recht valt dit nog het meest te vergelijken met de strafbaarstelling in het verkeersrecht voor een persoon die weigert een ademtest, ademanalyse of bloedproef af te leggen. Deze stelt zich dus ook strafbaar door niet mee te werken aan het verdere onderzoek. Het valt alleszins af te wachten of de Franse oplossing de toets van het Europese Hof van de Rechten van de Mens zal blijven doorstaan.

Gelet echter op de mogelijkheden die worden aangeboden tot encryptie op het internet (*nota bene* dikwijls gratis) lijkt de enige mogelijkheid, naast deze welke in beperkte mate door artikel 88*quater* van het Wetboek van Strafvordering wordt geboden, erin te bestaan encryptie niet langer vrij te maken, door bijvoorbeeld de sterkte van de versleutelingscode (uitgedrukt in het aantal bits) te beperken of door een soort van centrale autoriteit op te richten waarbij de sleutels van alle vormen van encryptie bewaard worden en welke op rechterlijk bevel in de gevallen door de wet te bepalen, zouden kunnen worden opgevraagd.

Dit lijkt alleszins efficiënter dan de Belgische oplossing op dit moment, waar ook voor derden, de wetgever er veiligheids- of gemakkelijkheidhalve van is uitgegaan dat deze zich slechts dienen te engageren voor zover het in hun mogelijkheden ligt, waarbij onmiddellijk de vraag kan worden gesteld hoe dit überhaupt meetbaar is.

§ 5. Artikel 90ter van het Wetboek van Strafvordering – Informaticatap (1)

Zonder twijfel werd de tapwetgeving (2) nog geschreven in een wereld die ver stond van de huidige digitale wereld, een wereld waar de klassieke spraaktelefonie nog hoogtij vierde en Belgacom hoofdrolspeelster was.

Bij de wetswijziging van 10 juni 1998 (3) werd door de minister verduidelijkt dat door amendementen van de regering rekening gehouden werd met de voortdurende evolutie in deze telecommunicatiesector, dat de medewerkingsplicht van operatoren werd uitgebreid tot de zogenaamde dienstenverstrekkers die op de geliberaliseerde telecommunicatiemarkt een steeds grotere rol waren gaan spelen en dat ook diende rekening gehouden te worden met het feit dat in de informatica- en telecommunicatiesector niet enkel meer met nummers gewerkt werd, maar ook met e-mailadressen, internetsites, enz. (4)

Eenzelfde bezorgdheid om mee te evolueren met de voorhanden zijnde technologie werd door de minister uitgedrukt naar aanleiding van de algemene bespreking van het op tafel liggende wetsontwerp en de wetsvoorstellen betrekking hebbend op het artikel 90*ter* van het Wetboek van Strafvordering voor de commissie voor de Justitie in de Kamer.

De minister heeft daar immers een zeer duidelijk standpunt ingenomen en aan artikel 90*ter* van het Wetboek van Strafvordering een interpretatie gegeven die het artikel mee aanpaste aan de voorhanden zijnde internetrealiteit en de nieuw opgedoken problematieken.

De minister had – terecht – vastgesteld dat wat de elektronische gegevensoverdracht via informaticanetwerken (zoals e-mail op het internet) betreft, het tot dan zeer moeilijk bleek om een circulerende boodschap te onderscheppen tijdens de werkelijke transmissie. Hij heeft daarom expliciet en in niet mis te verstane bewoordingen gesteld dat het volgens hem mogelijk en door artikel 90*ter* van het Wetboek van Strafvordering toegestaan is om deze gegevens op de plaats waar ze – tijdelijk – terechtkomen (*«zulks wordt een «mailbox» genoemd»*) te onderscheppen. Nog volgens de minister, blijft een bericht immers in het stadium van de overbrenging zolang het niet door de geadresseerde werd ontvangen.

De minister verduidelijkte daarbij dat indien de Afluisterwet niet van toepassing zou zijn op zo een mailbox, dan ook de bescherming (5) zou wegvallen van deze e-mailberichten en dus zou ongeoorloofde kennisname niet bestraft kunnen worden. Hij stelde ter zake een redenering *a contrario* te volgen: *«Aangezien afluistering een uitzondering vormt op het in de wet van 30 juni 1994 vervatte beginsel van de bescherming van de privételecommunicatie en het aangewezen is ook de elektronische post te beschermen, moet die onderschept kunnen worden wanneer het onderzoek dat vereist. Zodra het bericht ter bestemming is gekomen, kan hoe dan ook via een huiszoekingsbevel hiervan kennis worden genomen»* (6).

Meer nog dan de *a contrario*-redenering die door de minister werd meegegeven en welke, ofschoon helder van inhoud, het voorwerp was van discussie in de rechtsleer (7), is het inzicht van de minister over het

---

(1) Uit P. VAN LINTHOUT en J. KERKHOFS, «Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel», *T.Strafr.* 2008, afl. 2, 79-95.

(2) Wet 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privécommunicatie en -telecommunicatie, *BS* 24 januari 1995.

(3) Wet tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *BS* 22 september 1998.

(4) Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *Parl.St.* Senaat 1997-1998, nr. 1-828/3, 3.

(5) Art. 259*bis* en art. 314*bis* Sw.

(6) Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, wetsvoorstel tot aanvulling van art. 90*ter* Sv. en wetsvoorstel tot aanvulling van art. 90*ter* Sv., om bewakingsmaatregelen mogelijk te maken ten aanzien van verdachten van hormonenmisdrijven, *Parl.St.* Kamer 1996-1997, 1075/9, 15.

(7) J. DUMORTIER e.a., «Laat de Belgische wetgeving gerechtelijk aftappen van privé-communicatie via GSM of internet toe?», *Computerrecht* 1997, 149 waarnaar verwezen wordt door L. ARNOU, «Afluisteren tijdens het gerechtelijk onderzoek» in *Commentaar Strafrecht en Strafvordering*, Wolters Kluwer België, 2006, deel I, 13.

feit dat ook op het moment van de «tijdelijke» opslag van een bericht in een mailbox kan worden getapt, correct en conform de wet.

In het verslag namens de commissie voor de Justitie bij de oorspronkelijke Tapwet staat immers reeds met zoveel woorden te lezen dat «telecommunicatie» (in tegenstelling tot de communicatie die het voorwerp kan zijn van een maatregel van direct afluisteren) betrekking heeft op de communicatie over een afstand, met dien verstande dat er ook een verschil in tijd kan zijn, aangezien het denkbaar is dat de informatie eerst opgeslagen wordt vooraleer ze wordt doorgezonden (1).

Deze duidelijke stelling gekoppeld aan de op zich ruime interpretatie die door het Hof van Cassatie werd gegeven aan wat precies privécommunicatie en -telecommunicatie is (*«tout énoncé, oral ou non oral, fait directement ou à distance, et notamment les déclarations et conversations directes ou téléphoniques de même que toutes les formes modernes de la télématique»* (2)), maakt het mogelijk om het artikel 90*ter* van het Wetboek van Strafvordering aan te wenden in het nieuw licht van de internetrealiteit.

Het hoeft hierbij geen betoog dat waar het Hof van Cassatie stelt dat alle nieuwe en moderne vormen van de telematica inschuifbaar zijn onder het artikel 90*ter* van het Wetboek van Strafvordering, de tapbepalingen ook netjes toepasbaar blijken te zijn op nieuwe – vaak oneigenlijke – vormen van communicatie op het internet.

De wet zoals ze uitgelegd werd door de minister, aangevuld door de rechtspraak van het Hof van Cassatie, is dus duidelijk. Telecommunicatie, onder welke vorm ook, is tapbaar of afluisterbaar tijdens de overbrenging ervan, dit wil zeggen op het traject tussen de zender en de ontvanger.

Uitgesloten is echter de communicatie alvorens ze in transmissie is (een ontwerp van een mail die men wenst te versturen, het moment van het intypen van een SMS-bericht alvorens te verzenden, hetzelfde voor een chatbericht, ...) en wanneer ze volledig ter bestemming is gekomen bij het geïndiceerd eindstation (popmail die is toegekomen op de computer van de verdachte nadat hij werd overgezonden vanuit de mailbox (...@telenet.be, ...@skynet.be, ...@scarlet.be, ...@just.fgov.be), de webmail die werd ontvangen op een webmailaccount bij een normaal gebruik ervan (...@hotmail.com, ...@yahoo.fr, ...@gmail.com) of het achtergelaten bericht op de voice-mail) (3).

Het is evenmin toegelaten om via een tapbeschikking een informaticasysteem binnen te dringen (4). De tapmaatregel beperkt zich tot het onderscheppen van de transmissie. Het binnendringen in een informaticasysteem zal daarentegen wel mogelijk zijn met een netwerkzoeking, wat een maatregel is van een totaal andere orde.

Transmissie is dus de overbrenging van de boodschap van verzender naar ontvanger, waarbij een bericht volgens de wetgever enkel wordt aanzien als aangekomen wanneer er een *tastbaar* (5) resultaat is.

Gelet op de bijzondere omstandigheden van de internetomgeving, dient te worden benadrukt dat het daarbij bijzonder van belang is om tevens als **criterium** te hanteren bij het bepalen of een bericht is toegekomen, of het **geïndiceerd noodzakelijk eindstation** bereikt werd (voicemail, webmail, popmail, ...).

Te vaak wordt in de klassieke rechtsleer immers vergeten dat onmogelijk op voorhand zal kunnen worden uitgemaakt hoe de ontvanger zich ten aanzien van het in transmissie zijnde bericht zal gedragen (eigenlijk of oneigenlijk gebruik van het internet, tijdstip van onderschepping van het bericht door de bestemmeling).

Nochtans is de wijze van hoe de ontvanger kennis zal nemen van het verstuurde bericht determinerend om te weten of het bericht is aangekomen (het tastbaar resultaat) en desgevallend in welke stadium van de overbrenging naar het noodzakelijk geïndiceerd eindstation. Het zou immers *a posteriori* kunnen blijken door het gevoerde onderzoek dat gebruik werd gemaakt van een gefaciliteerd en niet op voorhand te voorzien eindstation bij het tot stand komen van de communicatie, bijvoorbeeld wanneer de eindgebruiker van een popmailaccount via een webmail kennisneemt van zijn berichten wanneer deze zich nog in de mailbox van zijn provider bevinden.

Het is onmogelijk om *a priori* te weten welke strikt omlijnde vordering zal dienen genomen te worden wanneer mailberichten moeten worden geïntercepteerd, omdat alles zal afhangen van de gedragingen van de ontvanger die niet op voorhand te voorzien zijn, alsook van de eventuele verklaringen die een in verdenking gestelde *a posteriori* naar vrije verdedigingsinzichten zal geven omtrent het feit of hij de ene of andere mail nu al dan niet reeds gelezen heeft. Wel laten de artikelen 88*ter* en 90*ter* van het Wetboek van Strafvordering toe om dit probleem te ondervangen.

De zwakte van sommige modellen (6) welke naar voor worden geschoven en besproken in de rechtsleer, is dat geen enkel van deze modellen afdoende rekening houdt met de gedragingen van de bestemmeling in het ganse proces van overbrenging en de voorhanden zijnde internetrealiteit.

Dit geldt voor **het extensieve model** waar men stelt dat overbrenging het ganse traject behelst tussen verzender en ontvanger met inbegrip van alle tussenstations.

---

(1) Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *Parl.St.* Senaat 1993-1994, 843-2, p. 38.

(2) Cass. 26 maart 2003, AR P.03.0412.F (B.L., A., J.), *Arr.Cass.* 2003, afl. 3, 791, *Juristenkrant* 2003, afl. 71, 1, http://www.cass.be, *JT* 2003, afl. 6107, 626, *Pas.* 2003, afl. 3, 664, *Rev.dr.pén.* 2003, afl. 7-8, 1080, noot T. HENRION, *Vigiles* 2003, afl. 4, 145, noot S. VANDROMME, zoals ook geciteerd in H.-D. BOSLY en D. VANDERMEERSCH, *Droit de la procedure pénale*, La Charte, 2003, 635.

(3) Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *Parl.St.* Senaat 1992-1993, 843-1, p. 6 en *Parl.St.* Senaat 1993-1994, 843-2, p. 9-10.

(4) *Parl.St.* Senaat 1992-1993, 843-1, p. 6 en *Parl.St.* Senaat 1993-1994, 843-2, p. 12.

(5) *Parl.St.* Senaat 1992-1993, 843-1, p. 6 en J. DUMORTIER e.a., *l.c.*, 148.

(6) L. ARNOU, *l.c.*, 13 en J. DUMORTIER e.a., *l.c.*, 149.

Onze kritiek hierop is: men houdt geen rekening met de hypothese dat een eindgebruiker al kennis kan hebben genomen van het bericht op het moment dat het zich nog in de mailbox bevindt.

Dit geldt ook voor **het restrictieve model** waarbij de overbrenging beperkt wordt tot de momenten dat het bericht effectief in beweging is en welke dus stelt dat het bericht niet tapbaar is op de momenten dat het in een tussenstation (mailbox) «rust».

Onze kritiek hierop is: men houdt hier geen rekening met het feit dat wanneer de eindgebruiker niet kennisneemt van het bericht op het moment dat het zich in de mailbox zou bevinden, de communicatie tastbaar en nuttig pas ten einde kan komen wanneer het bericht toekomt op de computer van de eindgebruiker.

Tot slot geldt deze kritiek zeker voor **het fictiemodel** waarbij men uitgaat van de fictie dat de mailbox dient gelijkgesteld te worden met de thuisbasis van de ontvanger (mailbox wordt gezien als «thuis», zelfs al staat die fysiek aan de andere kant van de wereld), zodat het bericht niet meer in overbrenging kan zijn eens het daar is toegekomen.

Onze kritiek hierop is: ook hier houdt men geen rekening met het feit dat wanneer de eindgebruiker niet kennisneemt van het bericht op het moment dat het zich in de mailbox zou bevinden, de communicatie tastbaar en nuttig pas ten einde kan komen wanneer het bericht toekomt op de computer van de eindgebruiker, het geïndiceerd noodzakelijk eindstation.

Het is gevaarlijk om in een poging de internetrealiteit juridisch te trachten beheersen om gebruik te maken van parallellismen van de analoge realiteit naar de digitale realiteit. Een vergelijking tussen mail en klassieke post gaat om verschillende redenen niet op, minstens reeds omwille van het feit dat het ondenkbaar zou zijn om als bestemmeling van een klassieke brief kennis te kunnen nemen van deze brief nog vóór hij in de brievenbus belandt (zie het voorbeeld van het kennisnemen van popmail door middel van webmailtoepassingen), ook omwille van het feit dat een «brievenbus» zich in de digitale realiteit – ofschoon met een muisklik raadpleegbaar – aan de andere kant van de wereld kan bevinden.

Een zuivere definitie formuleren van het begrip **«transmissie» en/of «overbrenging»** in de zin van artikel 90*ter* van het Wetboek van Strafvordering is geen eenvoudige opdracht, zeker niet voor wat de virtuele realiteit van het internet- en mailverkeer betreft. Louter afgaande op de limieten en eigenheid van het mailverkeer en het internetgebeuren, kan o.i. evenwel **«transmissie» en/of «overbrenging»** worden omschreven als:

– de communicatiefase;
– met als beginpunt de afzender die het commando geeft een bericht te verzenden;
– en met als eindpunt het zgn. *«geïndiceerd noodzakelijk eindstation»*.

Onder «geïndiceerd noodzakelijk eindstation» kan worden verstaan: 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, nl.:

– In het geval van popmail is alzo het geïndiceerde noodzakelijk eindstation het werkstation (pc, laptop, ...) waarop de bestemmeling van de mail zijn popmailbox heeft geïnstalleerd (bv. Microsoft Outlook (Express), ...).
– In het geval van webmail (Hotmail, MSN, Gmail, Yahoo!, ...) is alzo het geïndiceerde noodzakelijk eindstation de webmailbox die voor de bestemmeling beschikbaar is bij de webmailprovider.
– Indien de popmailconfiguratie wordt geconsulteerd als webmail (m.a.w. de bestemmeling checkt zijn popmail niet via zijn mailbox op zijn werkstation, maar via de door de ISP (Telenet, Skynet, ...) beschikbaar gestelde webmailtoepassing), dan is niet de webmailbox het geïndiceerd noodzakelijk eindstation, doch dan blijft daarentegen het werkstation (pc, laptop, ...) waarop de bestemmeling van de mail zijn popmailbox heeft geïnstalleerd (bv. Microsoft Outlook (Express), ...) het geïndiceerd *noodzakelijk* eindstation.

Dit impliceert dat de popmail die zich (nog) bevindt in de webmailbox van de ISP en nog niet werd doorgesluisd naar de popmailbox op het werkstation van de bestemmeling, **zowel feitelijk als strafprocedureel kan worden vermoed** nog steeds in transmissie te zijn.

Immers, de wetenschap of een (pop-)mail reeds werd gecheckt – desnoods van de andere kant van de wereld – via webmail is *a priori* louter speculatief. Het is om die reden dat het gewettigd en gerechtvaardigd voorkomt, gelet op de bedoeling van de wetgever en de bijzonderheid van de virtuele realiteit, om het criterium te hanteren van het geïndiceerde noodzakelijk eindstation voor wat het eindpunt van de transmissie betreft.

Anders redeneren brengt de onderzoeksrechter, en nadien de feitenrechters, in de onmogelijke situatie dat een in verdenking gestelde – naar waarheid of gelogen – zonder meer de nietigheid van een beschikking artikel 90*ter* van het Wetboek van Strafvordering 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 artikel 90*ter* van het Wetboek van Strafvordering had mogen worden *«getapt»* (1)· (2). Hoe dan ook, het (tegen)bewijs dat de ene of de andere persoon al dan niet reeds kennis zou hebben genomen van een webmail is bijna onleverbaar.

Dit zou impliceren dat de toepassing van artikel 90*ter* van het Wetboek van Strafvordering onderworpen wordt aan **een potestatieve ontvankelijkheidsvoorwaarde**, d.i. een grond van (on)ontvankelijkheid die louter afhangt van de (willekeurige) verklaring van een persoon/in verdenking gestelde met betrekking tot het feit of hij al dan niet reeds kennis heeft genomen van een mail.

Het is ook om die reden dat het gewettigd en gerechtvaardigd voorkomt, gelet op de bedoeling van de wetgever en de bijzonderheid van de virtuele realiteit, om

(1) Zie J. DUMORTIER e.a., *l.c.*, 148.
(2) Anders zal dit zijn indien de exceptie dienaangaande van de in verdenking gestelde/beklaagde niet ontbloot is van enige geloofwaardigheid en gekoppeld kan worden aan objectieve aanwijzingen dienaangaande.

het criterium te hanteren van het geïndiceerde noodzakelijk eindstation voor wat het eindpunt van de transmissie betreft, waarbij het adjectief *«geïndiceerd»* doelt op *«wat in alle redelijkheid a priori zou kunnen worden verwacht»* het noodzakelijk eindstation te zijn (1).

Deze analyse neemt evenwel niet weg dat dit gerechtvaardigd «**vermoeden van transmissie**» in de fase tussen afzender en geïndiceerd noodzakelijk eindstation, een potentieel **weerlegbaar** vermoeden is dat openstaat voor het tegenbewijs (nl. het aanvoeren van geloofwaardige elementen waaruit zou blijken dat de ene of andere communicatie reeds uit transmissie was).

De eventuele gevolgen van de weerlegging van dat vermoeden kunnen evenwel *preventief* worden opgevangen door een gecumuleerde toepassing met artikel 88*ter* van het Wetboek van Strafvordering.

Het komt aangewezen voor dat de onderzoeksrechter, die *a priori* zoals gezegd niet weet welke de exacte status (in transmissie of niet (meer) in transmissie) zal zijn van de telecommunicatie waarvan hij de onderschepping heeft bevolen, zou overwegen om desgevallend artikel 90*ter* van het Wetboek van Strafvordering en artikel 88*ter* van het Wetboek van Strafvordering te combineren in één en dezelfde beschikking (de zgn. vordering overeenkomstig art. 90*ter juncto* 88*ter* Sv.).

Daarbij kan de onderzoeksrechter motiveren dat het *a priori* door hem niet geweten kan zijn op welke wijze de mailaccount werd geconfigureerd en op welke wijze (popmail of webmail) en wanneer dat betrokkenen kennisnemen van de elektronische communicatie, zodat *a priori* ook niet door hem geweten kan worden of de te onderscheppen elektronische communicatie zich (nog) in het stadium van transmissie bevindt op het ogenblik van de onderschepping. De onderzoeksrechter kan alzo bevelen dat de (tele)communicatie die in transmissie is overeenkomstig artikel 90*ter* van het Wetboek van Strafvordering dient te worden onder bewaking gesteld overeenkomstig artikel 90*ter* e.v. van het Wetboek van Strafvordering, én dat met betrekking tot de eventuele (tele)communicatieberichten die zich niet (meer) in transmissie bevinden overeenkomstig artikel 88*ter*, § 3 van het Wetboek van Strafvordering dient te worden gehandeld.

In de mate dat er vervolgens in het navolgend gerechtelijk onderzoek discussie ontstaat met betrekking tot de status van de ene of de andere onderschepte communicatie, beperkt die discussie zich hooguit met betrekking tot de «vorm» van de verwerking en presentatie van die informatie. De discussie met betrekking tot de keuze van de juiste «rechtsgrond» (en de nietigheidssanctie vervat in art. 90*quater* Sv.) wordt alzo in ieder geval ontzenuwd.

In de mate dat de onderzoeksrechter er gerechtvaardigd van uit zou mogen gaan dat hij – gelet op de aard van het geïndiceerde noodzakelijk eindstation – enkel data zou gaan aantreffen die in transmissie dienen te worden geacht te zijn, en aldus toepassing maakt van artikel 90*ter* e.v. van het Wetboek van Strafvordering, en indien navolgend zou moeten worden vastgesteld dat er niettemin telecommunicatie wordt aangetroffen waarvan men zou moeten aannemen dat het **communicatie** betreft die **niet (meer) in transmissie** is, dan sluit o.i. niets uit dat de onderzoeksrechter deze data, die werden ontmoet *naar aanleiding van een wettige tapmaatregel*, **in beslag** zou **nemen overeenkomstig artikel 39*bis*** van het Wetboek van Strafvordering.

Ondertussen wordt volledigheidshalve herhaald dat de informaticatap beperkt is tot het gerechtelijk onderzoek naar de misdrijven welke zijn opgenomen in de limitatieve lijst van artikel 90*ter*, §§ 2 tot en met 4 van het Wetboek van Strafvordering en dat de vormvoorschriften zijn voorgeschreven op straffe van nietigheid zoals blijkt uit artikel 90*quater* van het Wetboek van Strafvordering. De netwerkzoeking kent die beperkingen en nietigheidssanctie niet. In de mate dat de onderzoeksrechter de artikelen 90*ter* en 88*ter* van het Wetboek van Strafvordering zou combineren, zal de onderzoeksrechter de netwerkzoeking binnen de toepassingslimieten van artikel 90 e.v. van het Wetboek van Strafvordering dienen te houden.

§ 6. Artikel 88ter van het Wetboek van Strafvordering – Netwerkzoeking (2)

Volledigheids- en voorzichtigheidshalve wordt er aan herinnerd dat dit artikel het voorwerp zal uitmaken van een noodzakelijke wetswijziging welke enerzijds de slagkracht van de digitale recherche zal vergroten en terug op bijna hetzelfde peil zal brengen als dat van de mogelijkheden van de cybercrimineel (indien al mogelijk) en welke anderzijds op het terrein elke onduidelijkheid zal doen ophouden te bestaan over welke rechtsfiguur (tap en/of netwerkzoeking) dient te worden aangewend.

De wetgever had met de wet van 28 november 2000 getracht om de actoren van justitie de adequate juridische instrumenten aan te reiken om de criminaliteit op de informatiesnelweg te kunnen bestrijden (3).

Zo was het de wetgever daarbij opgevallen dat geconfronteerd met de mogelijkheden van een klassiek huiszoekingsmandaat, dat per definitie enkel mag worden uitgevoerd ten aanzien van de plaats waarvoor het wordt bevolen, dit problemen stelde wanneer ter plaatse werd vastgesteld dat niet enkel een computer werd aangetroffen, maar dat deze ook verbonden bleek aan een of meerdere netwerken. Wanneer men immers het onderzoek wilde voortzetten naar deze informaticasystemen en deze zich op verschillende plaatsen bevonden welke niet voorzien waren in het huiszoekingsmandaat, waren in de tot dan geldende context meerdere nieuwe bevelen tot huiszoeking vereist (de kans bestond zelfs dat deze systemen op hun beurt met andere informaticasystemen verbonden waren, zodat er eigenlijk een sneeuwbaleffect kon zijn van huiszoekingen en huiszoekingsmandaten).

---

(1) Waarbij alzo enige voorzichtigheid wordt ingebouwd voor wat het bestaan van allerhande internet- en mailtoepassingen betreft die allerhande mengvormen zouden kunnen mogelijk maken, zoals het configureren van webmail (Hotmail, Gmail, MSN, Yahoo!, ...) als popmail.

(2) Uit P. VAN LINTHOUT en J. KERKHOFS, «Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel», *T.Strafr.* 2008, afl. 2, 79-95.

(3) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 3.

De wetgever heeft gesteld dat deze benadering van het gerechtelijk onderzoek problematisch was: niet alleen bestond immers het risico dat bij niet gelijktijdig optreden (trouwens zeer arbeidsintensief) bewijsmateriaal verloren ging, maar bovendien kon in veel gevallen *a priori* niet vastgesteld worden op welke plaatsen de zoeking moest plaatsvinden, welke bestanden relevant konden zijn of zelfs waar de computers geografisch gesitueerd konden zijn (1).

Vanuit deze probleemanalyse die duidelijk gestoeld is op de eventuele uitvoeringsproblemen van de huiszoeking heeft de wetgever het mogelijk gemaakt aan de onderzoeksechter om, na de voorwaarden vervat in artikel 88*ter* van het Wetboek van Strafvordering *a priori* en *«in redelijkheid»* (2) te hebben afgetoetst, toe te laten dat niet enkel wordt gezocht in het voorhanden zijnde informaticasysteem of een deel daarvan maar ook in het informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt.

De wetgever heeft hierbij in de cumulatieve voorwaarde voorzien dat dit enkel kan 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 (lijkt nogal logisch) **én** indien andere maatregelen disproportioneel zouden zijn **of** indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

Het valt op dat het tweede luik van de cumulatieve voorwaarde dat twee gelijkwaardige condities vooropstelt («of»), meer nog dan het eerste luik, bijna automatisch zal vervuld zijn in de mate dat door de eigenheid van de internetomgeving en de beweeglijkheid en vluchtigheid van de bewaarde gegevens, er steeds een risico zal bestaan dat bewijsmateriaal verloren gaat (alle elektronische gegevens kunnen bijna steeds gewist worden met een druk op de knop). Bovendien is het zo dat doordat de netwerkzoeking een alternatief is voor meerdere huiszoekingen op plaatsen die men nooit op voorhand kent, ook steeds de alternatieve maatregel van een cascade van huiszoekingen disproportioneel zal zijn, zowel naar de inzet van mensen als naar de aantasting van het beschermde goed, met name de privacy van alle geviseerde adressen (3).

De wetgever stelt verder dat de onderzoeksrechter ook dient toe te zien dat de uitbreiding van de zoeking in een informaticasysteem zich niet verder uitstrekt 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 wetgever heeft hiermee willen stellen dat de maatregel van de netwerkzoeking niet zo ver gaat dat de overheid gerechtigd zou worden om onbeperkt alle systemen die mogelijk met het onderzochte computersysteem in verbinding staan of kunnen worden gebracht te doorzoeken. De technische verbinding via de netwerken moet een element van permanentie en stabiliteit inhouden en niet louter occasioneel zijn (4). Concreet zal dit probleem in de praktijk meestal opgelost worden doordat gebruik wordt gemaakt van een login en een paswoord die de garantie zullen zijn voor tegelijk de toegangsbevoegdheid als voor de begrenzing ervan (iemand heeft toegang, want een login; door gebruik te maken van deze login en paswoord komt men in het «vreemde» systeem nooit verder dan waar de betreffende persoon zou toegang toe gehad hebben).

Waar het op eerste gezicht zou kunnen lijken dat de wetgever in artikel 88*ter* van het Wetboek van Strafvordering een nieuwe figuur heeft ontwikkeld welke gelijkloopt of een logisch verlengde is van de huiszoeking en sommige auteurs de netwerkzoeking als een aanpassing zien van de huiszoeking (5), is het tegendeel waar.

De netwerkzoeking is zeer duidelijk door de wetgever bedoeld als een *sui generis* - figuur (6)' (7).

Dit blijkt reeds onder meer uit het feit dat in tegenstelling tot de huiszoeking, de netwerkzoeking niet uitgesloten werd van de maatregelen welke aan de onderzoeksrechter kunnen worden gevraagd door het instellen van een vordering tot minionderzoek zoals voorzien door het artikel 28*septies* van het Wetboek van Strafvordering (het is dus perfect mogelijk dat het Openbaar Ministerie aan de onderzoeksrechter verzoekt door middel van een vordering tot minionderzoek om vanaf een gsm of een pda de data op te vragen (voicemail, mailberichten, ...) welke zich op een andere plaats bevinden, maar waaraan door middel van een netwerkverbinding de gsm of pda verbonden is) (8).

---

(1) *Ibid.*, 22.

(2) *Ibid.*, 23 en *Parl.St.* Senaat 1999-2000, 2-392/3, 8.

(3) *Parl.St.* Kamer 1999-2000, nr. 0213/004, 62.

(4) *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 23.

(5) C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *RDP* 2001, 663 e.v.; Y. POULLET, «A propos du projet de loi dit n° 214. La lutte de la criminalité dans le cyberspace à l'épreuve du principe de régularité des preuves», *Liber Amicorum du Jardin*, 12.

(6) 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, 60-81 (die enerzijds stellen dat de netwerkzoeking *«une institution singulière dans notre procédure pénale»* is maar anderzijds onterecht en foutief vervolgen dat de netwerkzoeking *«par voie de conséquence (...) ne pourra prendre place que dans le cadre d'une perquisition physique. (...) Les recherches seront limitées au temps de la perquisition et ne peuvent s'effectuer qu'au départ du système informatique visé par de cette dernière»*.).

(7) P. DE HERT en G. LICHTENSTEIN, «De wet van 28 november 2000 inzake informaticacriminaliteit en het formeel strafrecht», *CBR Jaarboek 2002-2003*, 401; P. DE HERT en G. LICHTENSTEIN, «De betekenis van het Europees Verdrag Cybercriminaliteit voor het vooronderzoek en de internationale samenwerking», *Vigilis – Tijdschrift voor politierecht*, 2004/5, 163.

(8) Zie *contra*: C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique», *RDP* 2001, 664 (voetnoot 208).
De auteur in kwestie schakelt de netwerkingzoeking – zoals gezegd o.i. ten onrechte – volledig gelijk met de huiszoeking. Dit noopt de auteur tot de in zijn visie noodzakelijke – doch in wezen *contra legem*-conclusie dat de netwerkzoeking alzo dan ook uitgesloten moet worden van de miniinstructie, net zoals de huiszoeking, ofschoon artikel 28*septies* van het Wetboek van Strafvordering nergens melding maakt van de uitsluiting van de netwerkzoeking en/of artikel 88*ter* van het Wetboek van Strafvordering.

Verder heeft de minister na wat getouwtrek tussen Kamer en Senaat duidelijk aangegeven dat de netwerkzoeking niet enkel betrekking heeft op computers die bijvoorbeeld in een gebouw staan, maar ook op draagbare computers en telefoons (1)' (2). Waar de oorspronkelijke tekst van artikel 88*ter* van het Wetboek van Strafvordering voorzag in *«Wanneer de onderzoeksrechter een zoeking verricht in een informaticasysteem, hetzij in het kader van een huiszoeking, hetzij anderszins ...»* en de Senaat door het laten wegvallen van de woorden *«hetzij anderszins»* (3) had getracht om de mogelijkheden van de netwerkzoeking in te perken, heeft de minister duidelijk door het op zijn beurt laten wegvallen van de woorden *«in het kader van een huiszoeking»* getracht om de bevoegdheid voor de uitbreiding van de zoeking in een informaticasysteem in lijn te brengen met de technologische realiteit. De minister heeft verduidelijkt dat in netwerk verbonden computers niet enkel gehanteerd worden als in gebouwen opgestelde systemen, maar dat meer en meer vormen van mobiele telecommunicatie en -dataverkeer worden ontwikkeld. Het was zijn betrachting om de realiteit van de draagbare computers reeds in rekening te brengen teneinde te vermijden dat het ontwerp in dat opzicht reeds achterhaald zou geweest zijn (4). Er werd tevens verduidelijkt dat dan met het woord *«zoeking»* elk mogelijke technische en procedurele vorm wordt bedoeld (5).

De netwerkzoeking staat als *sui generis*-figuur los van de huiszoeking, al zal ze in de praktijk wel vaak gelijktijdig met een huiszoeking worden uitgevoerd. Het is daarom ook noodzakelijk dat de onderzoeksrechter een afzonderlijke en gemotiveerde beschikking maakt voor de netwerkzoeking waarin hij de voorwaarden van artikel 88*ter* van het Wetboek van Strafvordering kan aftoetsen (naar de vorm kan worden gediscussieerd of het netwerkzoekingsmandaat desgevallend niet in hetzelfde stuk of dezelfde akte kan worden opgenomen als het huiszoekingsmandaat, zolang de scheiding tussen het ene en het andere mandaat kan blijken uit de tekstopmaak).

De wetgever heeft weliswaar de oorspronkelijke tekst aangepast in die zin dat de woorden *«Wanneer de onderzoeksrechter een zoeking* ***verricht****...»* werden vervangen door de woorden *«Wanneer de onderzoeksrechter een zoeking* ***beveelt****...»* met de verduidelijking dat voor de uitbreiding van de zoeking naar het tweede systeem geen tweede mandaat van de onderzoeksrechter dient te worden bekomen, maar hiermee wordt duidelijk bedoeld dat de onderzoeksrechter niet moet wachten bij het onderzoeken van een informaticasysteem totdat de omvang van het netwerk blijkt, maar daarentegen voor de effectiviteit van de maatregel dit op voorhand kan worden *«bevolen»* (6) wanneer hij over voldoende gegevens beschikt om naar de voorwaarden van artikel 88*ter*, § 1, *in fine* en § 2 van het Wetboek van Strafvordering te motiveren.

Een onderscheid lijkt wat dit betreft trouwens pertinent tussen een netwerkzoeking in de heimelijke fase van het onderzoek en in de open fase van het gerechtelijk onderzoek.

In de open fase van het gerechtelijk onderzoek, dit is bijvoorbeeld wanneer personen werden gearresteerd of wanneer wordt overgegaan tot het uitvoeren van een huiszoeking, zal de onderzoeksrechter om te kunnen motiveren op voorhand dienen te weten welk soort netwerk hij kan verwachten om zijn netwerkzoekingsmandaat te koppelen aan welomschreven logins of parameters (noodzakelijke beperking van de toegangsbevoegdheid). Als een netwerk (bv. een abonnement bij Yahoo) zich slechts openbaart tijdens de huiszoeking zal noodgedwongen een afzonderlijk en nieuw mandaat dienen te worden opgemaakt en kan men niet automatisch verder de (netwerk)zoeking uitbreiden naar de webmailaccount, *in casu* Yahoo.

In de heimelijke fase van het gerechtelijk onderzoek (dit is bijvoorbeeld van op de computers van de politie met de login en het paswoord van de verdachte) is het evident dat bij het bevelen van een netwerkzoeking steeds een afzonderlijke beschikking nodig zal zijn. Het is hier dat het *sui generis*-karakter van de netwerkzoeking het meest tot uiting komt.

Er dient in deze hypothese nog verduidelijkt te worden dat het voorschrift van artikel 88*ter*, § 3, eerste lid, *in fine* van het Wetboek van Strafvordering dat voorschrijft dat de onderzoeksrechter de verantwoordelijke van het informaticasysteem op de hoogte brengt, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden, geen enkel beletsel vormt om ook in de heimelijke fase de netwerkzoeking te hanteren. Eigen aan de internetrealiteit is het probleem dat zelden zal kunnen worden achterhaald wie de echte verantwoordelijke van het informaticasysteem is, nu, zelfs abstractie makend van de juridische moeilijkheden om in de verschillende landen van de wereld de verantwoordelijke te kunnen aanduiden, er vaak technische instrumenten worden gehanteerd om de – soms malafide – verantwoordelijken af te schermen voor de buitenwereld (bv. het maskeren van IP-adressen of URL's of IP- en URL-spoofing). Er dient tot slot ook te worden vastgesteld dat deze bepaling, die reeds haar eigen zwakte in zich draagt (*«tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden»*) ook geen termijn voorschrijft, en niet op straffe van enige sanctie werd voorgeschreven.

---

(1) Wetsontwerp inzake informaticacriminaliteit, *Parl.St.* Senaat 1999-2000, nr. 2-392/3, 76-77.

(2) *Parl.St.* Kamer 1999-2000, nr. 0213/011, 3-4.

(3) Amend. nr. 18; *Parl.St.* Senaat 1999-2000, nr. 2-392/2, 11 (*«De toevoeging van die woorden zou niet nader gespecificeerde onderzoekshandelingen kunnen dekken, wat principieel onaanvaardbaar is»*.).

(4) *Parl.St.* Kamer 1999-2000, nr. 0213/010, 2 (Amend. nr. 12 van de regering).

(5) *Parl.St.* Kamer 1999-2000, nr. 0213/011, 8.

(6) *Parl.St.* Kamer 1999-2000, nr. 0213/004, 64-65 en *Parl.St.* Kamer 1999-2000, nr. 0214/006, 2.

Volledigheidshalve dient tot slot benadrukt te worden dat hoewel uit de toelichting (1) in de voorbereidende werken over de toepassing van de netwerkzoeking zou kunnen blijken dat deze zeer ruim werd bedoeld en waar dit ten andere ook zou kunnen blijken uit de definitie van wat onder een «*informaticasysteem*» (2) wordt verstaan, het niet de bedoeling van de wetgever was om met het instrument van de netwerkzoeking een totale vrijgeleide te maken om het «hacken» van computersystemen door politie en justitie mogelijk te maken.

De wetgever heeft gesteld dat het niet is toegelaten dat de overheidsdiensten bijvoorbeeld via eigen informaticasystemen binnen zouden dringen in andere systemen die niet openstaan voor het publiek en die ervan verdacht worden aangewend te worden voor criminele doeleinden: *««hacking» door de overheid als nieuwe, geheime bewakingsmaatregel is derhalve verboden»* (3).

Het dient wel verduidelijkt te worden dat waar de politie geen site of webaccount mag hacken (dit is «inbreken» zonder toegangscodes of met gebruik van hackertools), de politie uiteraard wel binnen de restricties van het gemotiveerde netwerkzoekingsmandaat en aan de hand van login en paswoord, heimelijk kennis kan gaan nemen van een site of een account van op het eigen informaticasysteem. Deze nuance is evident zeer belangrijk. Gelet op de ruime omschrijving van wat een informaticasysteem is, is het immers – binnen de restricties dat de netwerkzoeking zich niet verder uitstrekt dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken in het bijzonder toegang hebben (dit wordt gegarandeerd door de login en het paswoord) – perfect mogelijk dat de onderzoeksrechter een netwerkzoeking beveelt in de «hotmailaccount» van de persoon welke gebruik maakt van een bepaalde login. Dit is duidelijk niet hetzelfde als het hacken door de politie van het «hotmailsysteem» en dus toegelaten. Nu de verdachte zelf deze webmailaccount van op elke computer ter wereld verbonden aan het internet zal kunnen raadplegen, zal ook de politie dit kunnen doen in dezelfde omstandigheden, inclusief van op de eigen computer (met de restricties zoals hierboven aangegeven).

IV. CONCLUSIE

Iedereen die actief is in de wereld van de digitale recherche dient tot het besluit te komen dat deze recherche steeds complexer is geworden en er een bijzondere nood is aan aangepaste en vooral up-to-date gehouden wetgeving.

Zoals reeds geschreven, wordt wel door onze wetgever op dit moment gewerkt aan adequate oplossingen voor de nieuw voorhanden zijnde problemen, maar er kan niet genoeg worden benadrukt dat het vijf voor twaalf is en een reactie van onze wetgever zich zeer dringend en zonder dralen opdringt. Anders zal de strijd tegen de cybercrimineel verloren worden.

Het uitwerken van deze nieuwe wetgeving is een moeilijke oefening in het balanceren op de lijn tussen de mogelijkheid tot efficiënte strafvervolging enerzijds en privacyrechten en rechten van verdediging anderzijds, tussen soevereiniteit van staten en de nieuwe wereld van de cyberspace waar andere bevoegdheidsregels kunnen of dienen te gelden, tussen de onbeperkte vrijheid en (vermeende of afgedwongen) anonimiteit van het internet en de nood aan regels en identificatie van de cybernauten.

Vanaf het najaar 2010 zou er een nationaal expertisecentrum over cybercriminaliteit operationeel moeten zijn (4). Althans dat waren de voornemens van de regering tot *medio* 2010. Hiertoe werd op initiatief van de K.U.Leuven, reeds een intentieverklaring ondertekend door de ministers Stefaan DE CLERCK, Annemie TURTELBOOM en Vincent VAN QUICKENBORNE, de bedrijven Microsoft, CSC Belgium, Cisco Systems en Atos Origin Belgium, en Febelfin, de koepelorganisatie van de financiële sector.

Alle partners engageerden zich om mee te werken aan de oprichting van het «Belgium Cybercrime Centre of Excellence for Training, Research and Education», een drietalig nationaal kenniscentrum voor de bestrijding van cybercriminaliteit. Het centrum, dat in Kortrijk gevestigd zou worden, zou vooral gericht zijn op training en onderzoek. Het kenniscentrum zou vanaf oktober 2010 in een eerste fase operationeel moeten zijn.

Het was onder meer de bedoeling dat het expertisecentrum een platform zou creëren waar de verschillende spelers op het vlak van cybercriminaliteit met elkaar ervaringen, standpunten en «good practices» zouden kunnen uitwisselen. Het zou ook multidisciplinair academisch onderzoek verrichten, alsook agenten, de magistratuur en private spelers opleiden met als doel de strijd tegen cybercriminaliteit te optimaliseren en op te voeren.

Het komt ons voor dat de wetgever bij voorkeur het paard *voor* de kar zou spannen, en alleszins zou verzekeren dat hoe dan ook gedegen wettelijke aangepaste tools zouden worden ter beschikking gesteld om überhaupt ter velde niet roemloos ten onder te gaan. Het goed equiperen van een doe-tank is minstens zo heilzaam als het goed equiperen van een denk-tank.

Hoe dan ook: elke verbeteractie verdient meer dan ooit applaus.

---

(1) *Parl.St.* Kamer 1999-2000, nr. 0213/011, 8.

(2) *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 12: *«Informaticasysteem: hiermee wordt gedoeld op alle systemen voor de opslag, de verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT.»*

(3) *Parl.St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, p. 23 en *Parl.St.* Kamer 1999-2000, nr. 0213/004, p. 9.

(4) Zie *Het Nieuwsblad*, 20 april 2010.