Strafrecht

Technische en juridische aspecten van ICT criminaliteit[1]

Philippe VAN LINTHOUT
onderzoeksrechter bij de Rechtbank van Eerste Aanleg te Mechelen

1 Philippe VAN LINTHOUT: de door de auteur ingenomen standpunten zijn van juridisch wetenschappelijke aard en verbinden geenszins het door hem uitgeoefende Ambt noch de magistratuur voor wat betreft de aangenomen interpretaties van het recht.

I. Inleiding

1. Waar vroeger het opsporings- en gerechtelijk onderzoek 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 betreft kan verwezen worden 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 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 ontstonden onder meer een aantal nieuwe misdrijven welke 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 (artikel 210bis Sv.), het informaticabedrog (artikel 504quater Sv.), de interne en externe hacking (artikel 550bis Sv.) en de datasabotage (artikel 550ter Sv.).

Eigen aan beide categorieën is het feit dat een nieuwe stijl diende ontwikkeld te worden in het opsporen van deze misdrijven. Dit aan de hand van een nieuw of up to date gebracht arsenaal van strafprocesrechtelijke instrumenten.

II. Instrumentarium van het wetboek van strafvordering

2. Het werken in een steeds digitalere 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.
Het is een betrachting om tijdens de uiteenzetting op de VRG Alumni dag verschillende toepassingsvoorbeelden *"live"* te kunnen demonstreren en om aan te tonen dat het juridisch matchen van rechtsregel en problemen in de praktijk

1 *B.S.*, 3 februari 2001

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 betreft de problematiek van het moeilijke evenwicht tussen enerzijds de rechtsfiguur van de netwerkzoeking en anderzijds de informaticatap wordt in extenso verwezen naar het artikel *"Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel"* verschenen in het Tijdschrift voor Strafrecht[2]. De paragrafen 5 en 6 zijn wat dit betreft 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 88ter Sv. waarbij *de lege ferenda* een nieuw onderscheid zou kunnen gaan bestaan tussen het eenvoudig **databeslag** (artikel 39bis Sv.), het databeslag van op afstand (de **netwerkzoeking** vervat in artikel 88ter Sv. – dit is in een niet heimelijke fase), het **databeslag in de heimelijke fase** en van op afstand, desgevallend met gebruik van speciale technieken (hacking tools, spyware,…; een nieuw te schrijven artikel 88quinquies Sv.?) en het databeslag van gegevens van telecommunicatie tijdens hun overbrenging (**tap** zoals voorzien in artikel 90ter Sv.).
Op het terrein wordt alleszins door onderzoekers en magistraten reikhalzend uitgekeken naar dit nieuw noodzakelijk wetgevend initiatief.

§1. Artikel 39bis Sv. – digitaal databeslag

3. De wetgever heeft met het artikel 39bis Sv. een oplossing geboden voor wat in de praktijk dikwijls een probleem was. Immers, in tegenstelling tot de gebruikelijke in beslagname 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 verwezen worden 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 betreft het digitaal bewijs merkte men snel dat dit in de

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

klassieke benadering van bewijsmateriaal en de in beslagname niet mogelijk was.

De wetgever heeft in artikel 39bis Sv. gekozen voor een zeer pragmatische oplossing: niet enkel mag digitaal bewijs nog steeds materialiter in beslag worden genomen (bijvoorbeeld 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 in beslagname 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 in beslagname, 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 is met de openbare orde of de goede zeden (bv in geval van kinderporno), of een gevaar oplevert 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 zij 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 39bis 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 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 het mogelijks voorwerp van discussie (In de mondelinge uiteenzetting worden hiervan een aantal concrete problemen getoond en besproken.).

§2. Artikel 46bis Sv. – identificatie

4. 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[3] definitief geregeld.

Artikel 46bis Sv. laat immers toe om bij gemotiveerde en schriftelijke beslissing van een parketmagistraat of een onderzoeksrechter te identificeren wie achter een IP-adres[4] 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 type vordering of kantschrift. Deze extra vereiste, welke door de wetgever in 2007 werd opgelegd, lijkt 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 ('emei-track').

Waar naar het doel en de reikwijdte van het inhoudelijke toepassingsveld van artikel 46 Sv. – 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 de 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 webmail adressen van personen welke misdrijven leken gepleegd te hebben op het Belgische grondgebied. Yahoo! Inc. werd echter op grond van artikel 46bis §2 Sv. op 2 maart 2009 veroordeeld[5]. De visie van de strafrechter te Dendermonde dient te worden gedeeld. De rechtbank was terecht van oordeel dat de medewerkingsplicht ex artikel 46bis Sv. (en/of

3 *B.S.*14 maart 2007

4 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.

5 Tegen deze veroordeling werd beroep aangetekend.

88bis Sv.) zich uitstrekt tot elke internet service provider die in België diensten ontplooit en aanwezig is.[6] Een andere interpretatie van het begrip *"verstrekker van een elektronische communicatiedienst"* zou de nuttige toepassing van artikel 46bis Sv. totaal onmogelijk maken.

§3. Artikel 88bis Sv. – Opsporen en lokaliseren

5. 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 is te weten waar. Artikel 88bis Sv. 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 betreft het artikel 46bis Sv., waar de inbreuk op de privacy veel minder ver lijkt te gaan, dient uit herhaalde en vaststaande rechtspraak[7] afgeleid te worden dat de vordering die om deze gegevens te bekomen en welke dient te worden uitgeschreven door een onderzoeksrechter, niet dient te worden gemotiveerd voor wat betreft het opvragen van gegevens uit het verleden.

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 bevolen worden 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 88bis Sv. 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 artikel 88bis Sv.).

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

Verder dient nog gezegd te worden dat in tegenstelling tot artikel 46bis Sv., een vordering op grond van artikel 88bis Sv. in de regel enkel kan genomen worden door een onderzoeksrechter. Wel is het mogelijk voor het openbaar ministerie om deze maatregel te vorderen bij mini-instructie (mini-onderzoek)[8]. Op deze regel bestaan twee uitzonderingen, zijnde: enerzijds bij een ontdekking op heterdaad voor feiten die worden opgesomd in artikel 90ter §§ 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 aan sancties in het wet-

6 Corr. Dendermonde 2 maart 2009, *Juristenkrant*, 2009 (weergave DE BUSSER, E.), afl. 186, 3; *T.Strafr.,* 2009, afl. 2, 116
7 Cass. 19 januari 2005
8 Artikel 28septies Sv.

boek 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 stalking dossiers).

Artikel 88bis Sv. wordt in de praktijk toegepast voor het opvragen van GSM- en internetverkeer, voor de localisatie van een GSM ten aanzien van een mast, voor het nagaan van het mastverkeer op een mast en voor de geografische localisatie 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 88bis Sv. is de discussie volop gaande voor wat betreft de invulling van de begrippen *"operator van een telecommunicatienetwerk of van de verstrekker van een telecommunicatiedienst"*. Opnieuw mag hier verwezen worden naar het belangwekkende standpunt van de strafrechter te Dendermonde[9].

§4. Artikel 88quater Sv. – Medewerkingsverplichting

6. Het artikel 88quarter Sv. is een weinig gebruikt maar wellicht volledig miskend artikel waar het 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 verplicht worden om tegen zichzelf te getuigen of lastens zichzelf bewijsmateriaal te verzamelen. Ook de personen opgesomd in het artikel 156 Sv. vallen 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 geïncrypteerde 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 in het vertrouwen dat mensen hebben voor wat betreft commerciële activiteiten op het internet (bv. internetbankieren) maar

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

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 geïncrypteerd 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 is aan het plegen of gepleegd zijn van een misdrijf. De Franse wetgever heeft zelfs 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 (dikwijls gratis), en waarbij ook voor het Frans systeem (zie de demonstratie tijdens de uiteenzetting) oplossingen worden geboden, lijkt de enige mogelijkheid naast deze welke in beperkte mate door artikel 88quater Sv. wordt geboden, erin te bestaan encryptie niet langer vrij te maken, door bijvoorbeeld de sterkte van de versleutelingcode (uitgedrukt in het aantal bits) te beperken (zie demonstratie) 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 (hoe is dit meetbaar?)

§5. Artikel 90ter Sv. – Informaticatap[10]

7. Zonder twijfel werd de tapwetgeving[11] 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.

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

11 Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en –telecommunicatie, *B.S.*, 24 januari 1995.

Bij de wetswijziging van 10 juni 1998[12] 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-mail-adressen, internetsites, enzovoort…[13].

Eenzelfde bezorgdheid om mee te evolueren met de voor handen 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 90ter 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 90ter van het Wetboek van Strafvordering een interpretatie gegeven die het artikel mee aanpaste aan de voor handen 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 90ter van het Wetboek van Strafvordering toegestaan is om deze gegevens op de plaats waar ze – tijdelijk – terechtkomen (*"zulks wordt een «mail box» 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[14] zou wegvallen van deze e-mail berichten en dus zou ongeoorloofde kennisname niet bestraft kunnen worden. Hij stelde terzake 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 privé-telecommunicatie 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"* [15].

---

12 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, *B.S.*, 22 september 1998.

13 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, *Gedr. St.*, Senaat, 1997-98, nr. 1-828/3, p. 3.

14 Artikel 259bis en artikel 314bis van het Strafwetboek.

15 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 artikel

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[16], is het inzicht van de minister over het feit dat ook op het moment van de "tijdelijke" opslag van een bericht in een mailbox kan getapt worden, 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[17].

Deze duidelijke stelling gekoppeld aan de op zich ruime interpretatie die door het Hof van Cassatie werd gegeven aan wat precies privé-communicatie en telecommunicatie is, met name *"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"*[18], maakt het mogelijk om het artikel 90ter 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 90ter 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.

90ter van het Wetboek van Strafvordering en Wetsvoorstel tot aanvulling van artikel 90ter van het Wetboek van Strafvordering, om bewakingsmaatregelen mogelijk te maken ten aanzien van verdachten van hormonenmisdrijven, *Gedr. St.*, Kamer, 1996-97, 1075/9, p. 15.

16 J. DUMORTIER e.a., "Laat de Belgische wetgeving gerechtelijk aftappen van privécommunicatie via GSM of internet toe?", *Computerrecht*, 1997, p. 149 waarnaar verwezen wordt door ARNOU, Luc, "Afluisteren tijdens het gerechtelijk onderzoek", in *Commentaar Strafrecht en Strafvordering*, Wolters Kluwer België, 2006, deel I, p. 13.

17 Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, *Gedr. St.*, Senaat, 1993-94, 843-2, p. 38.

18 Cass., AR P.03.0412.F, 26 maart 2003, (B.L., A., J.), *Arr. Cass.*, 2003, afl. 3, 791, *Juristenkrant* 2003, afl. 71, 1, *http://www.cass.be*, *J.T.*, 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, p.635.

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 (pop-mail 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 webmail account bij een normaal gebruik ervan (…@hotmail.com, …@yahoo.fr, …@gmail.com) of het achtergelaten bericht op de voice-mail)[19].
Het is evenmin toegelaten om via een tapbeschikking een informaticasysteem binnen te dringen[20]. 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*[21] 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 uitgemaakt worden 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 totstandkomen van de communicatie, bijvoorbeeld wanneer de eindgebruiker van een popmail account via een webmail kennis neemt 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 inverdenkinggestelde *a posteriori* naar vrije verdedigingsinzichten zal geven

19 Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, *Gedr. St.*, Senaat, 1992-93, 843-1, p. 6 en *Gedr. St.*, Senaat, 1993-94, 843-2, p. 9 – 10.
20 *Gedr. St.*, Senaat, 1992-93, 843-1, p. 6 en *Gedr. St.*, Senaat, 1993-94, 843-2, p. 12.
21 *Gedr. St.*, Senaat, 1992-93, 843-1, p. 6 en J. DUMORTIER e.a., *l.c.*, p. 148.

omtrent het feit of hij de éne of andere mail nu al dan niet reeds gelezen heeft. Wel laten de artikelen 88ter en 90ter van het Wetboek van Strafvordering toe om dit probleem te ondervangen.

De zwakte van sommige modellen[22] welke naar voor worden geschoven en besproken worden 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 zowel voor het extensieve model waar men stelt dat overbrenging het ganse traject behelst tussen verzender en ontvanger met inbegrip van alle tussenstations.
Onze kritiek hierop is: men houdt geen rekening met de hypothése 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 géén kennis neemt 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 géén kennis neemt 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 pop-mail 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.

22 L. ARNOU, *l.c.*, p. 13 en J. DUMORTIER e.a., *l.c.*, p. 149.

Een zuivere definitie formuleren van het begrip "transmissie" en/of "overbrenging" in de zin van artikel 90ter van het Wetboek van Strafvordering is geen eenvoudige opdracht, zeker niet voor wat betreft de virtuele realiteit van het internet- en mailverkeer. 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, d.i.:

- In het geval van pop-mail is alzo het geïndiceerde noodzakelijk eindstation het werkstation (PC, laptop, ...) waarop de bestemmeling van de mail zijn pop-mailbox heeft geïnstalleerd (bvb. 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 pop-mailconfiguratie wordt geconsulteerd als webmail (m.a.w., de bestemmeling checkt zijn pop-mail 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 pop-mailbox heeft geïnstalleerd (bvb. Microsoft Outlook (Express), ...) het geïndiceerd *noodzakelijk* eindstation.

Dit impliceert dat de pop-mail die zich (nog) bevindt in de webmailbox van de ISP en nog niet werd doorgesluisd naar de pop-mailbox 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 betreft het eindpunt van de transmissie.

Anders redeneren brengt de onderzoeksrechter, en nadien de feitenrechters, in de onmogelijke situatie dat een inverdenkinggestelde – naar waarheid of gelogen – zondermeer de nietigheid van een beschikking artikel 90ter 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 90ter van het Wetboek van Strafvordering had mogen worden "getapt".[23] [24] Hoe dan ook,

23 Zie J. DUMORTIER e.a., *l.c.*, p. 148.

het (tegen)bewijs dat de éne of de andere persoon al dan niet reeds kennis zou hebben genomen van een webmail is quasi onleverbaar.

Dit zou impliceren dat de toepassing van artikel 90ter 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/inverdenkinggestelde 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 het criterium te hanteren van het geïndiceerde noodzakelijk eindstation voor wat betreft het eindpunt van de transmissie, waarbij het adjectief "*geïndiceerd*" doelt op "wat in alle redelijkheid *a priori* zou kunnen worden verwacht" het noodzakelijk eindstation te zijn[25].

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 éne of andere communicatie reeds uit transmissie was). De eventuele gevolgen van de weerlegging van dat vermoeden kan evenwel worden opgevangen door een gecumuleerde toepassing met artikel 88ter van het Wetboek van Strafvordering, waarover hierna meer.

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 90ter §§ 2 tot en met 4 van het Wetboek van Strafvordering en dat de vormvoorschriften zijn voorgeschreven op straffe van nietigheid zoals blijkt uit artikel 90quater van het Wetboek van Strafvordering.

§6. Artikel 88ter Sv. – Netwerkzoeking[26]

8. 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 quasi 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.

---

24 Anders zal dit zijn indien de exceptie dienaangaande van de inverdenkinggestelde/beklaagde niet ontbloot is van enige geloofwaardigheid en gekoppeld kan worden aan objectieve aanwijzingen dienaangaande.

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

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

De wetgever had met de wet van 28 november 2000 getracht om de actoren van de justitie de adequate juridische instrumenten aan te reiken om de criminaliteit op de informatiesnelweg te kunnen bestrijden[27].
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 sneeuwbal effect kon zijn van huiszoekingen en huiszoekingsmandaten).
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[28].

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 88ter van het Wetboek van Strafvordering *a priori* en *"in redelijkheid"* [29] 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 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, quasi 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 dispropor-

27 Wetsontwerp inzake informaticacriminaliteit, *Gedr. St.*, Kamer, 1999-2000, nr. 0213/001 en nr. 0214/001, p. 3.
28 *Ibidem*, p. 22.
29 *Ibidem*, p. 23 en *Gedr. St.*, Senaat, 1999-2000, 2-392/3, p. 8

tioneel zal zijn, zowel naar de inzet van mensen als naar de aantasting van het beschermde goed, met name de privacy van alle geviseerde adressen[30].
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 gebracht worden te doorzoeken. De technische verbinding via de netwerken moet een element van permanentie en stabiliteit inhouden en niet louter occasioneel zijn[31]. 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 zicht zou kunnen lijken dat de wetgever in artikel 88ter van het Wetboek van Strafvordering een nieuwe figuur heeft ontwikkeld welke gelijk loopt of een logisch verlengde is van de huiszoeking en sommige auteurs de netwerkzoeking als een aanpassing zien van de huiszoeking[32], is het tegendeel waar.

De netwerkzoeking is zeer duidelijk door de wetgever bedoeld als een *sui generis* figuur[33] [34].

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 on-

30 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/004, p. 62.
31 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/001 en nr. 0214/001, p. 23.
32 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", *R.D.P.* 2001, p.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*, p. 12.
33 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 recherche seront limitées au temps de la perquisition et ne peuvent s'effectuer qu'au départ du système informatique visé par de cette dernière.").
34 P. DE HERT en G. LICHTENSTEIN, "De wet van 28 november 2000 inzake informaticacriminaliteit en het formeel strafrecht", *CBR Jaarboek 2002-2003,* p. 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,* p. 163.

derzoeksrechter kunnen gevraagd worden door het instellen van een vordering tot mini-onderzoek zoals voorzien door het artikel 28septies van het Wetboek van Strafvordering (het is dus perfect mogelijk dat het openbaar ministerie aan de onderzoeksrechter verzoekt door middel van een vordering tot mini-onderzoek 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).[35]

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[36] [37]. Waar de oorspronkelijke tekst van artikel 88ter 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"*[38] 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 de 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 ten einde te vermijden dat het ontwerp in dat opzicht reeds achterhaald zou geweest zijn[39]. Er werd tevens verduidelijkt dat dan met het woord *"zoeking"* elk mogelijke technische en procedurele vorm wordt bedoeld[40].

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

---

35 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", *R.D.P.* 2001, p.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 mini-instructie, net zoals de huiszoeking, ofschoon artikel 28septies van het Wetboek van Strafvordering nergens melding maakt van de uitsluiting van de netwerkzoeking en/of artikel 88ter van het Wetboek van Strafvordering.

36 Wetsontwerp inzake informaticacriminaliteit, *Gedr. St.*, Senaat, 1999-2000, nr. 2-392/3, p. 76-77.

37 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/011, p. 3-4.

38 Amendement nr. 18; *Gedr. St.*, Senaat, 1999-2000, nr. 2-392/2, p.11 (*"De toevoeging van die woorden zou niet nader gespecificeerde onderzoekshandelingen kunnen dekken, wat principieel onaanvaardbaar is."*).

39 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/010, p. 2 (amendement nr. 12 van de regering).

40 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/011, p. 8.

gemotiveerde beschikking maakt voor de netwerkzoeking waarin hij de voorwaarden van artikel 88ter van het Wetboek van Strafvordering kan aftoetsen (naar de vorm kan gediscussieerd worden 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"*[41] wanneer hij over voldoende gegevens beschikt om naar de voorwaarden van artikel 88ter §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). Zo een netwerk (bijvoorbeeld 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 webmail account, *in casu* Yahoo.

In de heimelijke fase van het gerechtelijk onderzoek (dit is bijvoorbeeld vanop 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 88ter §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 achterhaald worden wie de echte verantwoor-

41 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/004, p. 64-65 en *Gedr. St.*, Kamer, 1999-2000, nr. 0214/006, p. 2.

delijke 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 (bijvoorbeeld 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.

Volledigheidshalve dient tot slot benadrukt te worden dat hoewel uit de toelichting[42] 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"*[43] 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"*[44].
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 "hotmail" account van de persoon welke gebruik maakt van een bepaalde login. Dit is duidelijk niet hetzelfde als het hacken door de politie van het "hotmail" systeem en dus toegelaten. Nu de verdachte zelf deze webmail account van op elke computer te 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).

---

42 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/011, p. 8.

43 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/001 en nr. 0214/001, p. 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."*.

44 *Gedr. St.*, Kamer, 1999-2000, nr. 0213/001 en nr. 0214/001, p. 23 en *Gedr. St.*, Kamer, 1999-2000, nr. 0213/004, p. 9.

III. Conclusie

9. Zoals ook meer in extenso zal zijn gedemonstreerd en uitgelegd in de uiteenzetting naar aanleiding van de VRG Alumnidag, dient door iedereen die actief is in de wereld van de digitale recherche tot het besluit te worden gekomen 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.

Een oefening die zeker met de hulp en praktische inzichten van de onderzoekers en magistraten actief in de *"fight against cybercrime"* zich in de schoot van onze Alma Mater verder kan voltrekken.