Faculteit Rechtsgeleerdheid

"Cybercrime": analyse en evaluatie van Belgische regelgeving

Scriptie neergelegd tot het behalen van de graad van Licentiaat in de Criminologische Wetenschappen door

Koen VAN POUCKE

Academiejaar 2001 – 2002

Promotor: **Prof.Dr. G. Vermeulen** **Commissarissen:** **Prof.Dr. P. Ponsaers**
Lic. A. Dormaels

Faculteit Rechtsgeleerdheid

"Cybercrime":
analyse en evaluatie van Belgische regelgeving

Scriptie neergelegd tot het behalen van de graad van Licentiaat in de Criminologische Wetenschappen door

Koen VAN POUCKE

Academiejaar 2001 – 2002

Promotor: **Prof.Dr. G. Vermeulen** **Commissarissen:** **Prof.Dr. P. Ponsaers**
Lic. A. Dormaels

Woord vooraf

Dit eindwerk kwam tot stand in het kader van het behalen van het diploma van Licentiaat in de Criminologische Wetenschappen aan de Universiteit Gent.

Graag wens ik promotor Prof. Dr. G. Vermeulen te danken voor zijn steun en advies gedurende de maanden dat deze scriptie tot stand kwam. De nuttige wenken en tips hebben ongetwijfeld voor een meerwaarde gezorgd.

Ook wil ik alle leden van de Federal Computer Crime Unit te Brussel speciaal bedanken voor de vele informatie die ze me ter beschikking stelden tijdens de leerrijke stageperiode die ik daar kon doorlopen. Sommige interessante bronnen zijn voor studenten immers moeilijk toegankelijk. De stage bleek dan ook de ideale voorbereiding voor het schrijven van deze eindverhandeling.

Tenslotte wens ik ook mijn ouders en vriendin Virginie te danken. Hun geduld en zenuwen werden gedurende de laatste maanden herhaaldelijk op de proef gesteld. Mijn vader Romain en Björn verdienen een speciaal woord van dank. Ze waren namelijk beide onmiddellijk bereid om dit eindwerk te onderwerpen aan een kritische lezing.

Inhoudstafel

Lijst met grafieken en tabellen

GRAFIEKEN

TABELLEN

Algemene Inleiding

Onze maatschappij ondergaat op drastische wijze verschillende veranderingen. Eén daarvan heeft te maken met de doorbraak van de informatie- en communicatietechnologie in alle sectoren van het economisch en maatschappelijk leven. De laatste decennia werd de maatschappij in toenemende mate geïnformatiseerd en geautomatiseerd.

Zonder enige twijfel hebben technologische innovaties hun impact op de samenleving. De informatiemaatschappij levert tal van nieuwe technologieën die het dagdagelijkse leven een stuk eenvoudiger maken. Desondanks de voordelen zijn er ook negatieve gevolgen gekoppeld aan de vooruitgang. Zo wordt het voor de wetgever steeds moeilijker om op een snelle en adequate wijze te reageren op nieuwe ontwikkelingen in de ICT-sector. De vrije en vaak ook grensoverschrijdende uitwisseling van informatie heeft ervoor gezorgd dat heel wat regelgeving achterhaald raakt door de feiten. Dit veroorzaakt op zijn beurt lacunes in de wetgeving.

De snelle evolutie in de informatica- en telecommunicatiesector heeft er ongetwijfeld mede toe bijgedragen dat er de laatste jaren een stijging waar te nemen is van allerlei vormen van zogenaamde "ICT-crime". Om aan deze trend tegemoet te komen, werden er begin de jaren '90 in België gespecialiseerde eenheden in het leven geroepen om informaticacriminaliteit te bestrijden en om bijstand te leveren in het kader van gerechtelijke dossiers die ICT-onderzoek vergen.

Ook heeft de Belgische wetgever recentelijk werk gemaakt van wetgeving ter beteugeling van informaticacriminaliteit. Op Europees niveau tenslotte, heeft de bezorgdheid rond het thema "ICT-crime" uiteindelijk geleid tot de redactie van een verdrag dat gewijd is aan "cybercrime".

In deze eindverhandeling zal getracht worden om deze ontwikkelingen overzichtelijk in kaart te brengen. Daarbij is het interessant om na te gaan in welke mate de Belgische wetgever heeft geanticipeerd op verschillende vormen van criminaliteit die gerelateerd zijn aan informatica. In dit verband zal getracht worden om enkele kritische bemerkingen te formuleren.

Ook zal aandacht uitgaan naar de problemen die kunnen rijzen bij de afwikkeling van delicten die gepleegd worden via het Internet. Deze worden gekaderd in de context van de territoriale werking van het recht enerzijds, en de internationale rechtsorde anderzijds.

Tevens is het relevant om na te gaan of de nieuwe strafbaarstellingen en onderzoekstechnieken die in het leven werden geroepen in de praktijk soelaas bieden aan de opsporings- en vervolgingsdiensten. Zijn er genoeg financiële en logistieke middelen ter beschikking zodat de opsporing in de best mogelijke omstandigheden kan verlopen? Dit zijn maar enkele vragen die in deze eindverhandeling aan bod zullen komen.

❖

Deel I van deze eindverhandeling is gewijd aan de digitale informatiesnelweg, ook wel Internet genoemd. Opdat de lezer zich een duidelijk beeld zou kunnen vormen van "cybercrime", dient hij vooreerst te beschikken over de nodige technische bagage. Het eerste deel van deze thesis schetst dan ook de geschiedenis, evolutie en de mogelijke toepassingen van het Internet. Eveneens werd aandacht besteed aan het Internetgebruik in België.

Het tweede deel is opgebouwd rond informaticacriminaliteit en "cybercrime". Naast de historische ontwikkeling wordt dieper ingegaan op het definitiedebat dat gevoerd wordt rond termen zoals "computer crime", "computer abuse", enz. Veel aandacht gaat in hoofdstuk 2 en 3 van dit deel ook uit naar de typologie van computercriminaliteit en "cybercrime". Vooraleer de toepasselijke strafrechtelijke bepalingen te analyseren, dient men immers een onderscheid te kunnen maken tussen de verschillende soorten computercriminaliteit. Ook de prevalentie van computergerelateerde misdrijven komt kort aan bod.

Deel III is integraal gewijd aan de recente Belgische Wet op de Informaticacriminaliteit. In een eerste hoofdstuk wordt de aanloop geschetst naar deze wet. De volgende hoofdstukken behandelen de nieuwe incriminaties en de strafprocesrechtelijke implicaties. Gezien deze wet ook zorgde voor een aanpassing van de Telecomwet, worden deze wijzigingen ook behandeld in een apart hoofdstuk. Een laatste hoofdstuk van deel III is gewijd aan de bestraffing van misdrijven die sterk verwant zijn aan deze die in de Wet Informaticacriminaliteit behandeld worden. Daarom worden ze ook opgenomen in dit deel.

Het voorlaatste deel van deze thesis, deel IV, is gewijd aan de supranationale initiatieven ter beteugeling van computercriminaliteit. Staten kunnen immers hun nationale regelgeving niet

langer loskoppelen van de ruimere internationale context. Het is onmogelijk om in deze eindverhandeling een exhaustief overzicht te geven van alle initiatieven die door internationale organisaties genomen werden in de strijd tegen "cybercrime". Toch worden enkele belangrijke evoluties geschetst. Meer uitgebreid wordt tenslotte stilgestaan bij de initiatieven van de Raad van Europa die o.a. geleid hebben tot de Europese Cybercrime-Conventie.

Deel V is gewijd aan de digitale recherche in België. Het is immers zinloos om "cybercrime" enkel vanuit theoretisch oogpunt te bestuderen. Zonder gespecialiseerde teams die beschikken over de nodige kennis en middelen, blijft de toepassing van de wet dode letter. In enkele hoofdstukken worden de Federal Computer Crime Unit en de regionale Computer Crime Units van dichtbij bekeken. Ook gaat aandacht uit naar het Centraal Gerechtelijk Meldpunt.

Het laatste hoofdstuk van Deel V schetst enkele kritische beschouwingen ten aanzien van de digitale recherche in België. Deze bedenkingen zijn grotendeels gebaseerd op de stage-ervaringen tijdens de maanden augustus-september 2001 bij de Federal Computer Crime Unit te Brussel.

Informaticacriminaliteit bestrijkt een zeer ruim domein van computergerelateerde misdrijven. Het is niet evident om informatica en recht met elkaar te verzoenen. Toch hoop ik dat ik de lezer in deze eindverhandeling een logisch overzicht kan geven van de grote variëteit aan strafbare gedragingen die verband houden met het gebruik van computers en Internet.

Deel I: De digitale informatiesnelweg

Hoofdstuk 1: ontstaan en evolutie van het Internet

1.1. Van Internet tot World Wide Web

1.1.1. "Arpanet"

De oorsprong van het Internet ligt in het tijdperk van de Koude Oorlog. In de jaren '60 werden de militaire computers van de Verenigde Staten met elkaar verbonden door middel van een kwetsbare communicatielijn[1]. De vrees voor een nucleaire oorlog met het Sovjetblok deed de Amerikaanse overheid zoeken naar een meer stabiele manier om computers met elkaar te verbinden.[2]

Enkele universiteiten van Californië kregen de vraag voorgeschoteld om een systeem uit te bouwen dat bestand zou zijn tegen eventuele nucleaire conflicten. De bedoeling was om een gedecentraliseerde netwerkstructuur uit te bouwen zodat bij de onderbreking van een netwerkverbinding de informatie-uitwisseling automatisch zou worden omgeleid langs een alternatieve weg. Dit principe noemt men "dynamic rerouting". Met behulp van deze techniek kan netwerkverkeer opgesplitst worden in kleinere pakketten die zich kunnen verplaatsen langs verschillende routes. De verzonden informatie kan terug leesbaar gemaakt worden door de aaneenschakeling van de reeks pakketjes.

In 1969 werden in de Verenigde Staten vier computers van het militaire *Advanced Research Projects Agency* (ARPA) op die manier met elkaar verbonden. *Arpanet* kende een groot succes en werd in 1972 uitgebreid zodat ook wetenschappelijke en universitaire instellingen konden aansluiten op dit netwerk. Een jaar later werden de eerste internationale verbindingen gelegd zodat academici uit verschillende werelddelen met elkaar informatie konden uitwisselen.

Begin de jaren '80 werd een universele taal ontwikkeld (TCP/IP) die toeliet dat verschillende computers, verspreid over de hele wereld, met elkaar konden communiceren. Voortaan werd het mogelijk om aparte netwerken met elkaar te verbinden door het gebruik van het "TCP/IP-protocol". De officiële benaming van dit overkoepelende netwerk werd *Internet*.

[1] KÖHLER, M. en ARNDT., H.W., *Recht des Internet*, Heidelberg, Müller Verlag, 2000, 2-3.
[2] HAFNER, K. en Lyon, M., *Where Wizards Stay Up Late: The Origins of the Internet*, New York, Simon & Schuster, 1998, 10-14.

1.1.2. "World Wide Web" (WWW)

Eén van de meest bekende toepassingen van het Internet is ongetwijfeld het "World Wide Web"[3] of kortweg WWW. Het werd door Tim Berners-Lee samen met de Belg Robert Cailliau in 1989 ontwikkeld aan het Europees Instituut voor Deeltjesfysica te Genève, Zwitserland (CERN[4]) en is gebaseerd op "Hyper Text Markup Language" of HTML. Dankzij deze taal is het mogelijk om pagina's op het Web te maken die voorzien zijn van tekst, beeld, bewegende beelden en zelfs geluid. Eén van de belangrijkste kenmerken van HTML is de mogelijkheid om documenten met elkaar te verbinden via automatische verwijzingen of "hyperlinks".[5] Door een hyperlink te activeren, belandt de internetgebruiker op een andere webpagina. Dankzij deze techniek kan informatie aan elkaar gekoppeld worden, zonder dat deze zich op dezelfde computer hoeft te bevinden. In 1990 had Berners-Lee al een toepassing klaar om webpagina's te kunnen bekijken: de "browser".[6]

In de daarop volgende jaren groeide het bewustzijn omtrent het nut van het WWW. Marc Andreessen, student aan het Amerikaanse *National Centre for Supercomputing Applications*, zag al gauw de commerciële mogelijkheden in van het Web en ontwikkelde de browser "Mosaic". Via enkele berichten die hij postte in verschillende nieuwsgroepen, maakte Andreessen reclame voor zijn browser en stelde deze zelfs gratis ter beschikking aan het wijde publiek.[7] Halfweg de jaren '90 werd het bedrijf *Mosaic Communications Corporation* omgedoopt tot *Netscape*.[8] Ongeveer op hetzelfde moment kwam ook softwareproducent *Microsoft* met een browser op de markt: "Internet Explorer".[9]

Inmiddels was het Europees Instituut voor Deeltjesfysica tot de conclusie gekomen dat de verdere uitbouw van het WWW geen taak was van het instituut. Daarom werd in 1994 het *World Wide Web Consortium*[10] (W3C) gesticht met Tim Berners-Lee als directeur. Het W3-

---

[3] X. (1997//03/12) 'An overview of the World Wide Web' [WWW]. European Organisation for Nuclear Research: http://public.web.cern.ch/Public/ACHIEVEMENTS/WEB/Welcome.html [19/10/01]

[4] CERN staat voor Conseil Européen pour la Recherche Nucléaire. Het is een Europees laboratorium voor atoomfysica te Genève, Zwitserland.

[5] KASSENAAR, P., *Basiscursus Dreamweaver 4*, Schoonhoven, Academic Service, 2001, 6-14.

[6] Timbl (1991/08/06) 'WorldWideWeb: Summary' in alt.hypertext [news]. timbl@info_.cern.ch [12/12/01]

[7] Marca (1993/03/14) 'NCSA Mosaic for X 0.10 available' in comp.infosystems.gopher [news]. marca@ncsa.uiuc.edu [12/12/01]

[8] X. (1994/14/11) 'Mosaic Communications changes name to Netscape Communications Corporation' [WWW]. Netscape: http://home.netscape.com/newsref/pr/newsrelease5.html [19/10/01]

[9] HAFNER, K. en LYON, M., *Where Wizards Stay Up Late: The Origins of the Internet*, New York, Simon & Schuster, 1998, 263-265.

[10] Het *World Wide Web Consortium* (W3C) werd in oktober 1994 opgericht om de prestaties en de beschikbaarheid van het World Wide Web te verbeteren. Inmiddels maken meer dan vijfhonderd organisaties,

consortium tracht samen met enkele universiteiten en bedrijven uit de industriële sector om de toepassingsmogelijkheden van het Web uit te breiden.

1.1.3. E-mail

Een andere, veel gebruikte toepassing van het Internet is het uitwisselen van elektronische boodschappen of e-mail. Hoewel elektronische post pas sinds enkele jaren gemeengoed is geworden, werd deze toepassing reeds dertig jaar geleden ontwikkeld.[11]

Ray Tomlinson werkte begin de jaren '70 als jonge ingenieur voor het bedrijf *BBN Technologies*, dat in opdracht van de Amerikaanse regering werkte aan de ontwikkeling van Arpanet. In 1971 slaagde hij er in om berichten door te sturen naar andere computers binnen hetzelfde netwerk. Een programma voor de eigenlijke bestandsoverdracht was eerder reeds ontwikkeld als toepassing van Arpanet. Tomlinson zocht vervolgens naar een symbool dat kon gebruikt worden als scheidingsteken in een e-mailadres en koos voor het "@"-teken omdat dit in geen enkele naam voorkwam. De elektronische post was een feit.[12]

Dertig jaar later is het aantal elektronische berichten dat dagelijks via Internet verzonden wordt niet meer bij te houden.[13] Volgens recent onderzoek van *The Gallup Organization*[14] is e-mail zonder enige twijfel de belangrijkste activiteit van Internetgebruikers. De enquête die door deze organisatie werd afgenomen van vierhonderd Amerikaanse respondenten, toonde zelfs aan dat ongeveer drie vierde van de ondervraagden beschikt over meerdere e-mailadressen.

Hoewel de ontwikkelaars van Arpanet niet de bedoeling hadden om een wereldwijd berichtensysteem te ontwikkelen, kan e-mail tot één van de grootste successen van Arpanet gerekend worden.

---

waaronder tal van universiteiten en grote bedrijven, deel uit van het W3C. Meer informatie over de ontstaansgeschiedenis van het WWW en de rol van Tim Berners-Lee is terug te vinden op de website van het consortium: http://www.w3c.org [19/10/01]

[11] BONI W.C., KOVACICH G.L. en KENNEY J.P., *I-Way Robbery: Crime on the Internet*, Butterworth-Heineman, Woburn, 1999, 20-21.

[12] CAMPBELL, T. (1998/03) 'The first e-mail message, who sent it and what it said' [WWW]. Pretext Magazine: http://www.pretext.com/mar98/features/story2.htm [08/12/01]

[13] WUYTS, S. (2001/10/03) 'Dertig jaar elektronische post, bescheiden programma wordt killer-app' [WWW]. De Cursor: http://www.decursor.be/Nieuwsflash/index.html?330l02 [08/12/01]

[14] JONES, J. (2001/07/23) 'Almost all e-mail users say Internet, e-mail have made lives better' [WWW]. The Gallup Organization: http://www.gallup.com/poll/releases/pr010723.asp [08/12/01]

Elektronische post heeft als belangrijke eigenschap dat het niet plaats- of tijdgebonden is. Het is door de koppeling van netwerken in principe mogelijk om op elke plaats elektronische berichten uit te wisselen. Het gelijktijdig aanwezig zijn van verzender en ontvanger van een boodschap is geen voorwaarde om een bericht te kunnen verzenden.[15]

1.1.4. "Usenet" of Nieuwsgroepen

"Usenet" ontstond eind de jaren '70 en richtte zich aanvankelijk tot universiteiten en commerciële organisaties. Het is een wereldwijd verspreid conferentie- en discussiesysteem dat in de Verenigde Staten ontwikkeld werd door Steve Bellovin, Jim Ellis, Tom Truscott en Steve Daniel aan de *Duke University* in North-Carolina.[16] In 1986 ontwikkelden ze het "Network News Transfer Protocol" (NNTP) dat vandaag nog steeds gebruikt wordt.

Het "Usenet" bestaat uit een reeks discussiegroepen of "newsgroups" die hiërarchisch geclassificeerd zijn naar onderwerp. De eerste indeling van nieuwsgroepen wordt bepaald door de eerste term uit de naam van de nieuwsgroep (het zogenaamde "top-level domain"). Voorbeelden van top-level domains zijn: "alt", "comp" en "sci". Ze staan respectievelijk voor "alternative", "computer" en "science". Na een "top-level domain" volgt een verdere uitsplitsing in subcategorieën. Bovendien bieden tal van providers toegang aan tot hun eigen nieuwsgroep waarin ze gratis ondersteuning bieden.

Vandaag functioneert Usenet als een openbaar forum waar mensen met elkaar discussies kunnen aangaan over de meest uiteenlopende thema's en onderwerpen. Inmiddels zijn er tienduizenden nieuwsgroepen beschikbaar waar iedereen een bericht kan plaatsen. Berichten of artikels die gepost worden in een nieuwsgroep worden automatisch doorgezonden naar andere, met elkaar verbonden computersystemen.

1.1.5. "File Transfer Protocol" (FTP)

De overdracht van bestanden via het Internet is bijna net zo oud als het netwerk zelf. De ingewijden spreken vaak over "FTP" wat staat voor "File Transfer Protocol". Veel mensen maken nog steeds gebruik van dit protocol omdat het een transparant onderdeel is geworden

[15] KASPERSEN, R., HOFMAN, A. en VERBEEK, J., *Vertrouwelijkheid van e-mail*, in *Nationaal Programma Informatietechnologie en Recht*, DE KROON, A. en SCHMIDT, A., (eds.), Deventer, Kluwer, 1999, 83-107.
[16] BENSCHOP, A. (2001/04/14) 'Wat is Usenet?' [WWW] Universiteit van Amsterdam, Social Science Information System: http://www.pscw.uva.nl/sociosite/about_usenet.html [22/12/01]

van toepassingen zoals het *World Wide Web*. Wanneer via "WWW" een bestand wordt opgehaald, gebeurt dit op de achtergrond vaak via FTP.[17]

FTP maakt het mogelijk om toegang te krijgen tot gedeeltes van de harde schijf van andere computers op het Internet. De computer van de gebruiker maakt hiervoor verbinding met een "FTP-server". Deze laatste maken het mogelijk om bestanden te kopiëren naar de eigen harde schijf. Men spreekt daarbij van "downloaden". In sommige gevallen bestaat de mogelijkheid om zelf bestanden of programma's beschikbaar te stellen. Dit wordt "uploaden" genoemd.

1.1.6. "Internet Relay Chat" (IRC)

Eind 1998 was de Fin Jarkko Oikarinen informaticus aan de Universiteit van Oulu. Hij ontwikkelde er een toepassing die het mogelijk maakt om "in real-time" (op hetzelfde moment) met verschillende personen te communiceren. De uitvinding werd IRC genoemd wat staat voor "Internet Relay Chat". Dit kan vrij vertaald worden als "praten op afstand via het Internet".

Na een tijd groeide de populariteit van IRC waarna Oikarinen besloot om ook andere Finse universiteiten te laten kennismaken met zijn uitvinding. De volgende stap was de verspreiding van IRC via het Internet.[18]

In tien jaar tijd maakt IRC deel uit van de meest populaire toepassingen die het Internet rijk is. Het is eigenlijk niets meer dan een gigantische babbelbox waarbij men in staat is om met verschillende personen tezelfdertijd in contact te treden. IRC wordt dan ook beschouwd als het meest interactieve gedeelte van het Internet.[19]

1.2. "E-commerce" of elektronische handel

Recente ontwikkelingen in de informatie- en communicatietechnologie hebben gezorgd voor nieuwe impulsen op het vlak van de economie in het algemeen en de handel in het bijzonder. Elektronische handel biedt de consumenten en de ondernemingen de mogelijkheid om voortaan

[17] X., (s.d.) 'Wat is FTP?' [WWW]. Surfnet: http://www.surfkit.nl/knowledge/ftp/home.html [23/12/01]
[18] WUYTS, S. (s.d.) 'IRC: tien jaar wereldwijd babbelen' [WWW]. De Cursor: http://www.decursor.be/Online/IRC/index.html [23/12/01]
[19] CARABALLO, D. en LO, J. (2000/01/06) 'The IRC Prelude, what is IRC and how does it work?' [WWW]. IRC Help: http://www.irchelp.org/irchelp/new2irc.html [23/12/01]

ook on-line handelsbetrekkingen aan te knopen. De consument krijgt nieuwe mogelijkheden om goederen aan te kopen terwijl producenten toegang krijgen tot een nieuwe markt.[20]

Elektronische handel biedt zowel de consument als de producent nieuwe mogelijkheden aan, maar houdt voor beiden ook onmiskenbare gevaren in. De nieuwe mogelijkheden voor bedrijven zijn legio: grote expansiemogelijkheden, relatief bescheiden investeringen, nieuwe communicatiemogelijkheden, enz. Langs de andere zijde heeft de consument een meer flexibele toegang en doorgaans ook een grotere keuze aan producten en diensten.

De bescherming van de consument, het respect voor de persoonlijke levenssfeer, de bescherming van intellectuele rechten, het afsluiten van elektronische contracten: dit zijn slechts enkele thema's waar de wetgever permanent aandacht zal moeten aan schenken.[21]

[20] DEMOTTE, G., *Elektronische handel*, Brussel, juli 2000, 11 p. (oriëntatienota Ministerie van Economische Zaken).

[21] In de verschillende media wordt regelmatig de aandacht gevestigd op de talrijke risico's die consumenten en producenten lopen op het Internet bij het drijven van "e-commerce" of elektronische handel.
Zie BAEYENS, H., (2001/03/06) 'Het onveiligheidsgevoel op Internet' [WWW]. De Standaard Online: http://www.standaard.be/thema/multimedia/index.asp?doctype=detail.asp&ArticleID=DSM06032001_004 [24/12/01]; zie ook: BETTENS, B., (2001/02/20) 'Vlaamse kmo's hebben schrik voor e-commerce' [WWW]. De Standaard Online: http://www.standaard.be/thema/multimedia/index.asp?doctype=detail.asp&ArticleID=DSM20022001_004 [24/12/01]

Hoofdstuk 2: Internetgebruik in België

2.1. Internet: evolutie of revolutie?

De studie "The Impact of the Internet Economy in Europe", die werd uitgevoerd in 1999 door het Britse onderzoeksinstituut *The Henley Centre*, stelt dat de Internetrevolutie een vergelijkbaar effect teweegbrengt als de Industriële Revolutie in de 18e eeuw.[22]

De duidelijkste conclusie van het onderzoek is dat Europa zich in het middelpunt van de Internetrevolutie bevindt. Belangrijke factor in deze ontwikkeling is de actieve rol die de overheden spelen op het gebied van ICT. Het rapport voorspelt een periode van sterke verandering van de wijze waarop we leren en werken. Zo zullen steeds meer mensen regelmatig van werkgever veranderen. Ook winkelen via Internet zal een sterke vlucht nemen, doordat men alle mogelijke producten, uiteenlopend van etenswaren tot verzekeringen, gemakkelijk via het Internet kan gaan bestellen.

In de paragrafen hieronder wordt aandacht besteed aan enkele meer recente onderzoeken die de Internetpenetratie en –populatie in kaart brengen.

2.2. "Belgian Internet Mapping" (BIM)

Het Gentse onderzoeksbureau *InSites Consulting* doet op regelmatige basis onderzoek naar de Internetgebruikers in België. Dit gebeurt in het kader van de *Belgian Internet Mapping* (BIM). Tweemaal per jaar wordt deze studie georganiseerd teneinde demografische informatie over de Internetgebruikers en hun houding en gedrag tegenover Internet in kaart te brengen.

Het BIM-onderzoek verloopt in twee fasen. Vooreerst wordt een telefonische enquête gehouden met Belgische respondenten van 15 jaar en ouder, representatief aan de Belgische bevolking. Vervolgens wordt een enquête gehouden in samenwerking met enkele toonaangevende websites. Bezoekers worden daarbij gevraagd om mee te werken aan de enquête en krijgen een vragenlijst voorgeschoteld.

[22] CISCO SYSTEMS, *Internet Revolutie zorgt voor omwenteling van de manier waarop we werken, leven, spelen en leren,* Amsterdam, juni 1999. (persbericht).

De resultaten van de zesde uitgave van het BIM-onderzoek werden publiek gemaakt in april 2002[23]. Ons land telt volgens deze studie 3.200.000 regelmatige Internetgebruikers.[24] Dit is een stijging met maar liefst 16 procent in vergelijking met de resultaten van het najaar van 2001. Toen telde InSites 2.750.000 surfende Belgen. Deze stijging toont aan dat nog steeds meer en meer Belgen de weg naar het Internet vinden.

Verder blijkt uit de enquête dat niet alleen het totaal aantal internauten toegenomen is, maar ook de groep surfers die voor een snelle kabel- of ADSL-verbinding kiest, blijft verder uitbreiden. Het aantal gebruikers van breedbandverbindingen is volgens InSites Consulting tijdens de voorbije zes maanden met ongeveer 20% gestegen. België blijft dus samen met Zweden nog steeds koploper in Europa op het vlak van breedbandverbindingen.

De BIM-studie toont aan dat het Internet zijn succes nochtans voornamelijk te danken heeft aan de gemakkelijke communicatiemogelijkheden. De populairste toepassing is nog altijd e-mail: 84 procent van de Belgische internetgebruikers verstuurt minstens één keer per week een e-mailbericht.

2.2.1. België versus Europa

In België beschikt ongeveer een derde van de Internetgebruikers thuis over een breedbandverbinding met het Internet. Dit percentage zorgt er voor dat België in Europa tot de koplopers behoort op het vlak van breedbandpenetratie. In buurland Nederland heeft bijvoorbeeld slechts 25 procent van de regelmatige surfers thuis een breedbandverbinding.

Van alle volwassen Belgen heeft 9 procent een snelle verbinding met het Internet. Het Europees gemiddelde blijft steken op 6 procent. Enkel de Scandinavische landen Zweden en Denemarken doen beter met respectievelijk 14 en 13 procent breedbandgebruikers.

Toch gebruikt in ons land nog steeds 45 procent van de Internetpopulatie een gratis telefonisch abonnement. Dit aantal daalt echter sterk. Meer en meer mensen zien immers de voordelen in van een breedbandverbinding.

---

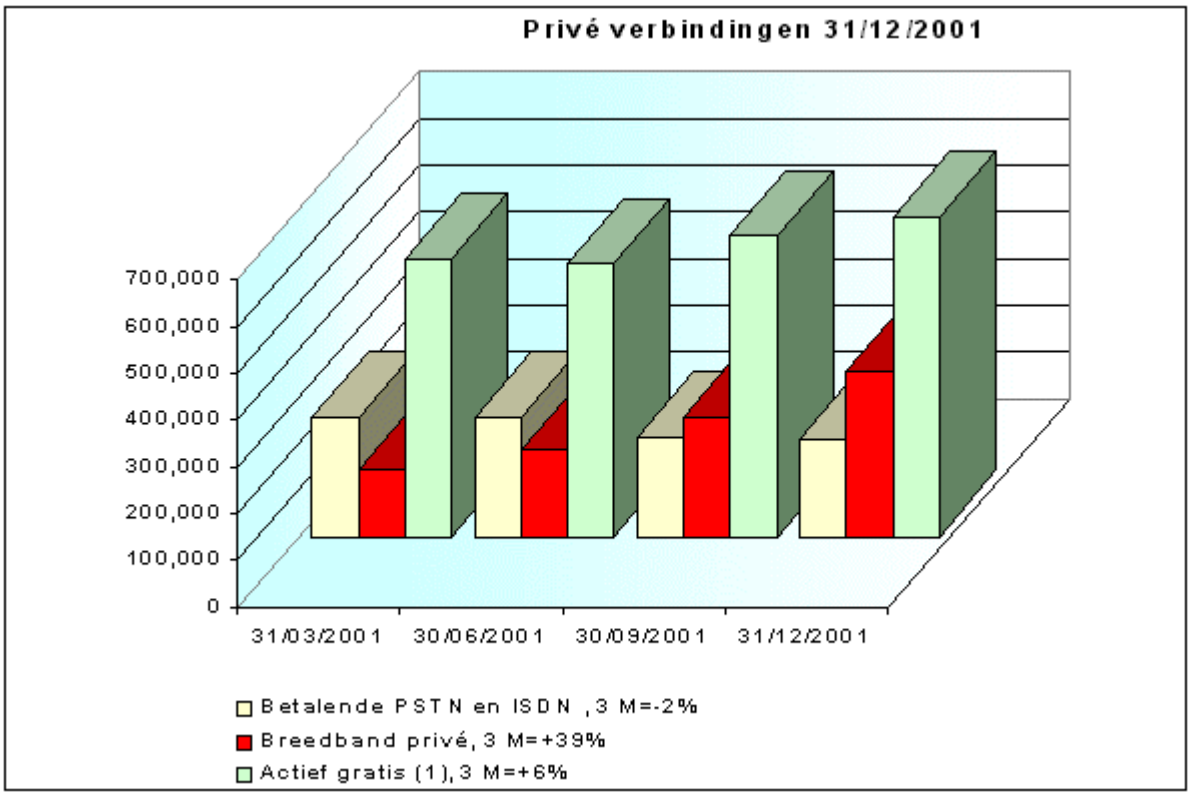
[23] INSITES CONSULTING, *België telt 3,2 miljoen regelmatige internetgebruikers*, Gent, april 2002. (persbericht).

[24] *InSites Consulting* definieert een regelmatige Internetgebruiker als een inwoner van België die gedurende de laatste maand minstens éénmaal actief was op het net.

2.3. Internet Service Provider Association (ISPA)

ISPA België is de Belgische vereniging van de Internet Service Providers. Deze vereniging werd opgericht in 1997 en vertegenwoordigt de meerderheid van de Belgische aanbieders van Internettoegang. Sinds november 1998 publiceert *ISPA* elke vier maanden de statistieken van het Internetgebruik in België. De gegevens van elke deelnemende provider worden vertrouwelijk behandeld en de totalen worden vervolgens openbaar gemaakt.

De elfde marktstudie van *ISPA* is de recentste en dateert van eind december 2001. In onderstaande grafiek krijgt men een overzicht van het aantal private Internetverbindingen in België op 31 december 2001.



Grafiek 1: ISPA Markstudie: individuele Internetaansluitingen op 31 december 2001.
Bron: Internet Service Providers Association[25]

[25] ISPA, (2002/01/23) 'De Internetmarkt' [WWW]. Internet Service Providers Association: http://www.ispa.be/nl/d000200.html [27/02/02]

Uit de resultaten van deze studie[26] blijkt een aanzienlijke stijging van het aantal Internetverbindingen. Het totale aantal particuliere Internetverbindingen schommelt in België rond het kwart miljoen. De grootste toename is te situeren in het vierde kwartaal van 2001. Een blik op het cijfermateriaal leert ons dat de stijging van het aantal Internetverbindingen nagenoeg uitsluitend op de rekening komt van de breedbandverbindingen.[27] Globaal gezien vertegenwoordigt breedband een derde van alle Internetverbindingen, terwijl dat drie maanden daarvoor nog 1 op 4 was.

2.4. Nationaal Instituut voor de Statistiek (NIS)

Het *Nationaal Instituut voor de Statistiek*, kortweg NIS, is een openbare instelling die belast is met de officiële statistiek. Aan de hand van enquêtes en statistische verwerkingen, tracht het NIS tegemoet te komen aan de noden van de Overheid en onze maatschappij.

Het NIS verzamelt zowel kwantitatieve als kwalitatieve gegevens bij particulieren en bedrijven. Na ontvangst worden deze gegevens gecodeerd en gecontroleerd waarna ze verwerkt worden. De informatie wordt verspreid in reeksen en tabellen ten behoeve van de belangstellenden.

Omdat de sector van de informatie- en communicatietechnologie (ICT) een groeiend economisch belang kent, publiceert het NIS ook gegevens over deze branche. Onder het thema "Communicatiemedia en Audiovisuele media" kan men op de website van het NIS cijfermateriaal terugvinden gaande van het aantal Internetaansluitingen in België tot een vergelijking van de Internetpenetratie in de landen van de Europese Unie. Tevens krijgt men een overzicht van het aantal geregistreerde domeinnamen in België.

2.4.1. Internetaansluitingen in België

Voor het overzicht van het aantal Internetaansluitingen in België, baseert het NIS zich op de gegevens die door de *Internet Service Providers Association* worden ter beschikking gesteld. Dit werd reeds hoger behandeld.[28]

---

[26] ISPA, *4de kwartaal van 2001: explosie breedband in België bevestigt trend van het hele jaar 2001*, Brussel, januari 2002. (persbericht).

[27] X., (2002/01/26) 'Explosion des connexions' [WWW]. Le Soir en ligne: http://www.lesoir.com/articles/A_021981.asp [27/02/02];
Zie ook: DJD., (2002/01/22) 'België beleefde breedband-explosie' [WWW]. De Standaard Online: http://www.standaard.be/Nieuws/Economie/index.asp?articleID=DEXA22012002_073&DocType=detail.asp [27/02/02]

[28] Supra 2.4. Internet Service Providers Association (ISPA).

2.4.2. Internetpenetratie in landen van de Europese Unie

Land	Gezinnen met een internetaansluiting (a)			
	1998	1999	2000	2001
Europese Unie	8,3%	12%	28,4%	37,7%
België		12%	29,2%	36,4%
Denemarken	8,2%	35%	51,6%	58,6%
Duitsland	24,6%	11%	27,1%	38,4%
Griekenland	7,1%	3%	11,7%	9,9%
Spanje	5,0%	6%	15,7%	24,7%
Frankrijk	3,9%	8%	19,0%	30,1%
Ierland	8,4%	6%	35,5%	47,6%
Italië	6,1%	7%	23,7%	33,5%
Luxemburg	14,0%	17%	36,3%	43,0%
Nederland	19,6%	21%	54,8%	63,8%
Oostenrijk	6,8%	12%	38,0%	47,2%
Portugal	3,4%	4%	18,1%	26,1%
Finland	17,2%	21%	43,5%	50,2%
Zweden	39,6%	51%	53,8%	60,7%
Verenigd Koninkrijk	10,7%	17%	40,9%	49,3%

Tabel 1: Internetaansluiting bij particulieren – vergelijking Europese Unie 1998 - 2001
Bron: Nationaal Instituut voor de Statistiek[29]

Het cijfermateriaal dat in bovenstaande tabel wordt weergegeven, heeft betrekking op de bevolking van 15 jaar en ouder uit de EU-lidstaten. Bovendien werden enkel gezinnen die beschikken over een telefoonaansluiting onderzocht. De cijfers tonen aan dat in 2001 vier keer zoveel EU-gezinnen beschikken over een Internetaansluiting in vergelijking met het jaar 1998.

Specifiek voor België zien we voor 2001 een verdrievoudiging van het aantal gezinnen dat toegang heeft tot het Internet, in vergelijking met de cijfers van het jaar 1999. De Scandinavische landen staan samen met Nederland aan de top wat betreft de Internettoegang.

2.4.3. Geregistreerde domeinnamen in België

	1995	1997	1998	1999	2000	2001
Aantal domeinen .BE	1.151	7.198	13.410	23.397	89.709	178.834

Tabel 2: Geregistreerde domeinnamen 1995 - 2001
Bron: Nationaal Instituut voor de Statistiek[30]

[29] MINISTERIE VAN ECONOMISCHE ZAKEN, (2002/02/26) 'Communicatiemedia en Audiovisuele media' [WWW]. Nationaal Instituut voor de Statistiek: http://statbel.fgov.be/figures/d75_nl.asp#3 [27/02/02]

De Leuvense professor Pierre Verbaeten (departement Computerwetenschappen) startte in 1989 met de registratie van domeinnamen in België.[31] Tot in 1994 werden er slechts 129 domeinnamen geregistreerd.

Op vraag van professor Verbaeten, werd de verantwoordelijkheid voor de registratie van Belgische domeinnamen op 1 januari 2000 overgedragen aan *Domain Name Registration België*, kortweg *DNS België*. Deze vereniging heeft enerzijds als doel het organiseren en beheren van de registratie van Belgische domeinnamen en staat anderzijds in voor het verzekeren van de continuïteit van de domeinnamen in België.[32]

Begin december 2000 was het aantal geregistreerde Belgische domeinnamen inmiddels gestegen tot 40.000. Dezelfde maand trad een nieuwe registratieprocedure in werking[33]. Deze procedure voorziet in de installatie van een gedecentraliseerd netwerk van agenten die bevoegd zijn om domeinnamen te registreren. Bovendien werd de volledige aanvraagprocedure geautomatiseerd en vereenvoudigd. Voortaan kunnen ook particulieren een domeinnaam aanvragen. Dit nieuwe, meer flexibele systeem zorgde ervoor dat het aantal domeinnamen eind december 2000 opliep tot 89.709.[34]

2.5. De toekomst

Internet raakt steeds meer ingeburgerd bij alle lagen van de bevolking. Toch is de toekomst van dit medium moeilijk te voorspellen door de enorme snelheid waarmee het evolueert. De snelle groei van het aantal Internetgebruikers heeft ervoor gezorgd dat de bestaande infrastructuur om het Internet te verkennen, overbelast raakt en dus steeds minder toereikend wordt. Bovendien neemt het aantal nieuwe websites toe met een enorme snelheid. Ook maken meer en meer websites gebruik van multimediatoepassingen die een hogere bandbreedte vereisen. Dit resulteert onvermijdelijk in ergerlijke wachttijden en zelfs opstoppingen. Een voor de hand liggende oplossing voor dit probleem is het gebruik van breedbandverbindingen zoals kabel en ADSL.[35] De meeste geïndustrialiseerde landen beschikken dan ook reeds over een goed uitgebouwd netwerk van dergelijke aansluitingen.

---

[30] *Ibid.*
[31] Het betreft domeinnamen die beschikken over de extensie ".be". Andere domeinnamen, die bvb. eindigen op ".com", ".net" of ".org" zijn niet opgenomen in deze cijfergegevens.
[32] Verenigingen zonder Winstoogmerk, Statuten DNS België, *B.S.* 17 juni 1999 (bijlage), 5089-5091.
[33] DNS BELGIË, *liberalisering domeinnamen*, Leuven, september 2000. (persbericht).
[34] DNS BELGIË, (2001) 'De historiek van DNS' [WWW]. http://www.dns.be/nl/AboutUs/history.htm [06/03/02]
[35] "ADSL" staat voor "Assymetric Digital Subscriber Line". Dit is een technologie die het mogelijk maakt om sneller datagegevens te versturen door het gebruik van de klassieke telefoonlijn.

Nieuwe fenomenen vormen altijd een uitdaging voor de maatschappij. Het snelle en tevens grensoverschrijdende karakter van het Internet zorgt er vaak voor dat de nationale wetgevers te kort schieten om deze nieuwe fenomenen onder controle te houden. De bescherming van de persoonlijke levenssfeer en de bescherming van de belangen van de consument in het algemeen moeten ook bij nieuwe technologieën zoals Internet voldoende gewaarborgd worden. Zo is het bij elektronische handel van belang dat de overheid de controle bewaart over de verzameling van persoonlijke gegevens via het Internet.

2.6. Conclusie

Uit bovenstaande onderzoeken blijkt dat de Belgische, maar ook de Europese Internetpopulatie nog steeds snel toeneemt. Internet is het snelst groeiende communicatiemedium ooit. Het is nog steeds bezig aan een snelle opmars, dit kan men althans afleiden uit de grote stijging van het aantal gebruikers.

De vaststelling dat meer en meer Belgen beschikken over een breedbandverbinding toont aan dat mensen bewust een maandelijks bedrag uit hun budget voorzien om in optimale omstandigheden van het medium Internet gebruik te maken.

Terwijl 2000 kan beschouwd worden als het jaar van gratis Internet en de grote doorbraak van Internetverbindingen bij het brede publiek, gaat 2001 vooral de geschiedenis in als het jaar waarin de Internetbevolking massaal de overstap maakt naar breedbandinternet.

Deel II: Informaticacriminaliteit en cybercrime

Hoofdstuk 1: Informatisering: crimineel vs. criminoloog?

1.1. Informatisering van criminaliteit?

De voorbije jaren hebben gezorgd voor een turbulente ontwikkeling van de informatie- en communicatietechnologie. Men kan informatie vastleggen en gebruiken op tal van verschillende wijzen: gedigitaliseerde persoonlijke gegevens, mobiele telecommunicatie, elektronische post, Internet, elektronische chips, enz. Meer en meer gaan deze toepassingen de maatschappij blijvend bepalen.

Inmiddels werd reeds duidelijk dat de elektronische informatiesnelweg nood heeft aan formele en informele sociale controletechnieken. De formele controle kwam in België pas recentelijk op gang met de invoering van de Wet Informaticacriminaliteit.[36]

ICT biedt een ruime gelegenheid tot het plegen van nieuwe vormen van criminaliteit of van oude criminaliteit in een nieuw jasje. Vaak zijn deze vormen van criminaliteit traditioneel van aard.[37] Als men via Internet iemand probeert op te lichten en daar ook in slaagt, dan lijkt dit in alle opzichten sterk op oplichting die bijvoorbeeld gebeurt via de telefoon.[38]

Toch biedt ICT wel degelijk nieuwe mogelijkheden tot het plegen van criminele feiten. Denk maar aan het illegaal kopiëren van muziekcd's, computersoftware en videofilms. Ook inbraken in bedrijfsnetwerken door het gebruik van computers en allerhande vormen van kredietkaartfraude maken bijvoorbeeld deel uit van deze nieuwe vormen van criminaliteit.

Nieuwe technologieën kunnen anderzijds een bijdrage leveren tot een betere preventie en opsporing van criminele feiten.[39] Zo komt de systematische opslag van gegevens uit afgeronde rechercheonderzoeken de opsporing in een volgend onderzoek vaak ten goede. Tegen bepaalde vormen van criminaliteit zijn de klassieke opsporingsmethoden niet opgewassen. In de praktijk ontstond daardoor vaak de behoefte om gebruik te maken van bijzondere opsporingsmethoden.

[36] Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.*, 3 februari 2001.
[37] VAN DER VIJVER, C., 'ICT en strafrechtshandhaving', *Tijdschrift voor Criminologie*, 1999, 350-363.
[38] Zie: RINGENOLDUS, D.H., 'De computermisdadiger is de oude oplichter, schade door computerinbraken loopt de spuigaten uit', *Telecommagazine*, 1996, afl. 9, 12-18.
[39] NIEMEIJER, E. en NIJBOER, J., 'Informatisering van samenleving en criminaliteit', *Tijdschrift voor Criminologie*, 1999, 340-349.

Vandaag de dag kan men gesprekken van op afstand afluisteren met behulp van een groot gamma aan technische middelen gaande van richtmicrofoons tot infraroodcamera's[40]. Het spreekt voor zich dat men hierdoor de privacy van de verdachten als van derden schendt. Er dient dus omzichtig te worden omgesprongen met deze nieuwe technologieën.

1.2. De rol van de criminologie

Het is de taak van de wetenschap in het algemeen om de economische, politieke, culturele maar ook de juridische implicaties van de voortschrijdende informatisering van de maatschappij in kaart te brengen. De criminoloog in het bijzonder moet zich richten naar de nieuwe mogelijkheden die ICT schept tot het plegen van nieuwe of bestaande vormen van strafbaar gedrag.

ICT kan anderzijds nieuwe perspectieven bieden aan de criminologie. Met de komst van de computer is empirische kennis beschikbaar gekomen die het mogelijk maakt om de spreiding en concentratiekernen van criminaliteit in kaart te brengen, te analyseren en zelfs bepaalde trends te onderkennen. De geautomatiseerde verwerking van gegevens zorgt er bovendien voor dat grootschalige inzameling en verwerking van onderzoeksdata tot de mogelijkheden behoort.

Voorts zal de criminoloog zich de vraag moeten stellen in hoeverre ICT-criminaliteit de ontwikkeling van nieuwe theoretische verklaringsmodellen nodig maakt. De faciliterende werking van het Internet vestigt de aandacht op de gelegenheidstheorie.

Daarentegen is het ook van belang erop te duiden dat voor bepaalde vormen van criminaliteit die gepleegd worden door het gebruik van informaticamiddelen er bij de pleger ervan, nood is aan specifieke kennis van bepaalde, al dan niet technische, vaardigheden. Deze vaardigheden worden dikwijls aangeleerd door mensen uit de directe omgeving van de crimineel. Zo stelt Sutherland dat crimineel gedrag, via algemene leerprincipes, aangeleerd wordt in persoonlijke interactie en communicatie met anderen.[41]

[40] VAN DEN WYNGAERT, C., *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 1999, 736-741.
[41] NIEMEIJER, E. en NIJBOER, J., 'Informatisering van samenleving en criminaliteit', *Tijdschrift voor Criminologie*, 1999, 340-349.

Hoofdstuk 2: Computercriminaliteit

2.1. Historische ontwikkeling

2.1.1 Oorsprong

Informatie en het uitwisselen ervan is zo oud als de mensheid zelf. Het is pas de laatste decennia dat er grote wijzigingen zijn opgetreden m.b.t. de manier waarop de overdracht en distributie van de informatie gebeurt. De criminelen passen zich aan deze evolutie aan waardoor computercriminaliteit een bittere realiteit is geworden.

Voor de oorsprong van computercriminaliteit dient men terug te gaan naar de periode 1960-1970 wanneer de eerste persartikels werden gepubliceerd rond computercriminaliteit of computergerelateerde criminaliteit. In de meeste gevallen ging het om computersabotage, computerspionage of het illegaal gebruik van computersystemen.

Pas begin de jaren '70 doet men voor het eerst empirisch onderzoek naar computercriminaliteit. Deze studies brachten slechts een beperkt aantal gevallen aan het licht. Onderzoekers waren er zich terdege van bewust dat een groot deel van de criminaliteit die gepleegd werd door het gebruik van computers niet-gerapporteerd of zelfs ongedetecteerd bleef.

2.1.2. "Bistel"-zaak

De wetenschappelijke visie op computercriminaliteit veranderde radicaal in de jaren '80 toen de media gewag maakte van computervirussen[42], softwarepiraterij en spectaculaire inbraken in computers. In België werden we geconfronteerd met de Bistel-zaak.[43] Het *Belgian Information System By Telephone*, kortweg BISTEL is een elektronisch informatiesysteem dat enerzijds

[42] Een computervirus is een programma dat zich aan bestanden op de doelcomputer hecht. Wanneer een bestand wordt besmet, wordt het de drager van het virus en kan het andere bestanden besmetten. Een aantal virussen kunnen gegevens beschadigen, andere kunnen het systeem of zelfs de gehele computer onbruikbaar maken.

[43] OSTC (1999) 'Wetgeving: inbraak' [WWW]. PISA, Providing Information About Internet Security Aspects: http://pisa.belnet.be/pisa/nl/juridisch/crack.htm [17/03/02]

toegang verschaft tot databanken en anderzijds de communicatie tussen de verschillende kabinetten van de Belgische Federale Overheid verzekert door middel van een postdienst.[44]

Een voormalig gedetacheerd milicien van het kabinet van de Eerste Minister verschafte zich, samen met een vriend, tussen augustus en oktober 1988 de toegang tot dit systeem door gebruik te maken van de paswoorden van de premier en een kabinetsmedewerkster.[45] Hierdoor konden ze enerzijds kennis nemen van vertrouwelijke informatie maar anderzijds werd hierdoor het gebruik van het systeem door de personen die rechtmatig over een paswoord beschikten, onmogelijk gemaakt.[46]

De twee beklaagden werden door de Correctionele Rechtbank (in eerste aanleg) veroordeeld op drie gronden[47]:

1. Valsheid in geschriften: de beklaagden hadden immers gebruik gemaakt van een paswoord dat hen niet toebehoorde en bovendien hadden ze zich voorgesteld als rechtmatige gebruikers van het BISTEL-systeem. Zodoende werd een paswoord als een geschrift aanzien.

2. Diefstal van computerenergie: het onrechtmatig gebruik van het paswoord en de toegangscode werd beschouwd als een verzwarende omstandigheid. Volgens de rechtbank ging het over een diefstal met braak, inklimming of het gebruik van valse sleutels.

3. Verduistering van de aan de toenmalige *RTT* toevertrouwde mededelingen om kennis te nemen van de inhoud ervan.

Het grootste deel van deze uitspraak werd door de beroepsrechter ongedaan gemaakt. Een paswoord kon niet beschouwd worden als een geschrift in de zin van artikel 193 Sw. Anderzijds oordeelde het Hof ook dat de hackers niet de bedoeling hadden om computerenergie te stelen. De beklaagden werden enkel nog veroordeeld op basis van een overtreding van de RTT-Wet[48] van 1930.[49] Uit deze uitspraak bleek onmiddellijk dat de Belgische regelgeving niet aan computer-gerelateerde misdrijven was aangepast.

---

[44] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 122-124.
[45] Zie CAUBERGHE, L., 'Een harde noot voor krakers', *Computable*, 1991, afl. 2, 11-12.
[46] DE SCHUTTER, B., 'Het Belgisch Bistel-syndroom', *Tijdschrift voor informatica, telecomunicatie en recht*, 1991, 164-166.
[47] Rb. Brussel, 8 november 1990, *Computerrecht*, 1991, 31.
[48] Wet van 19 juli 1930 tot oprichting van de Regie van Telegraaf en Telefoon, *B.S.*, 2 augustus 1930.
[49] Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991. Deze wet werd meermaals gewijzigd. De recentste aanpassing dateert van eind 2001; Programmawet van 30 december 2001, *B.S.*, 31 december 2001.

2.2. Definitiedebat

Verschillende auteurs houden er zeer uiteenlopende definities op na. Begin de jaren '80 lanceert Herbert Edelherz de term "computer white collar crime". Voor hem is er gewoon sprake van "*manual routines who have been replaced bij Electronic Data Processing*".[50]

☞ Deze term dekt m.i. de lading niet. De term "White Collar Crime" die door Sutherland[51] geïntroduceerd werd, duidt immers op illegaal gedrag dat weinig aantoonbaar is, slechts uitzonderlijk vervolgd wordt en bovendien bedreven wordt door personen uit de hogere socio-economische klasse. Gezien computercriminaliteit niet enkel bedreven worden door personen uit de hogere socio-economische klasse, kan deze definitie m.i. niet weerhouden worden.

Rainer A.H. von zur Mühlen levert kritiek op de Duitse term "Computerkriminalität" door te stellen dat een computer op zich niet crimineel kan zijn. Doordat de term echter veel navolging kent, aanvaardt hij deze en definieert "Computerkriminalität" als "*elke criminele daad gericht tegen computers of gepleegd door middel van computers*".[52]

Donn B. Parker gooit het halfweg de jaren '70 over een andere boeg door de fenomenologische factoren van computercriminaliteit te viseren. Hierbij merkt hij een verschil op met "white collar crime": "*Computer abuse is any intentional act involving a computer where one or more perpetrators made or could have made gain and one or more victims suffered or could have suffered a loss. Computer crime is a common term used to identify illegal computer abuse; however it implies direct involvement of computers in committing a crime. Computer-related crime conveys the broader meaning of any illegal act for which knowledge of computer technology is essential for successful prosecution.*"[53]

In 1983 boog een groep experten die deel uitmaken van de *Organization for Economic Co-operation and Development* (OECD) zich over de definitieproblematiek. Inmiddels was het immers duidelijk geworden dat de notie computercriminaliteit moest gepercipieerd worden als een breed concept zodat ook in de toekomst deze term toepasbaar zou blijven op nieuwe strafbaarstellingen zoals illegale inhoud op het Internet. De OECD definieert "computer crime"

[50] SIEBER, U., *Computerkriminalität und Strafrecht*, München, Heymans, 1980, 25-28.
[51] SUTHERLAND, E., *White Collar Crime*, New York, Holt, Rinehart and Winston, 1949, 15-18.
[52] ERKELENS, C., 'Beteugeling van computercriminaliteit', *Panopticon*, 1985, 334-345.
[53] *Ibid.*, 334-345.

als *"any illegal, unethical, or unauthorised behaviour involving automatic data processing and/or transmission of data."*[54]

Het Amerikaanse Ministerie van Defensie waagde zich recent eveneens aan een definiëring van "computer crime". Ze beschouwen het als *"any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution."*[55]

☞ Deze definiëring raakt kant noch wal want ze omvat een reeks van misdrijven die geen verband houden met computercriminaliteit. Als voorbeeld gebruiken we autodiefstal. Als een politie-inspecteur gebruik maakt van computertechnologie om bijvoorbeeld na te gaan of een bepaald chassisnummer van een wagen gekend is in de database van de politie, dan worden we volgens bovenstaande definiëring geconfronteerd met een computermisdrijf. Het netwerk van de politie wordt immers gebruikt om een misdrijf op te lossen.

Eén van de meest uitgebreide en tevens meest omvattende definitie van computercriminaliteit is terug te vinden bij Bryan Clough. Hij stelt: *"Computer crime embraces everything from stealing hardware to software piracy and crimes committed by computer, through crimes committed on computer. It also embraces espionage, sabotage, blackmail, counterfeiting, the theft of data and the denial of service, and it can range from the opportunistic scams through to the carefully planned heist."*[56]

Bovenstaande definiëringen tonen aan dat een term zoals "computer crime" vaak voor spraakverwarring zorgt. In de literatuur treft men dan ook soms de notie "informatiedelict" aan. Deze term wordt gedefinieerd als *"elke handeling of onthouding daarvan die een aanslag kan uitmaken op lichamelijke en/of onlichamelijke goederen en die direct of indirect voortvloeit uit de tussenkomst van informaticatechnologie."*[57]

Kelleher en Murray stellen dat de term "computer crime" moeilijk definieerbaar is. Terecht stellen ze dat geen enkele definitie allesomvattend kan zijn gezien de complexiteit en de snelheid waarmee nieuwe technologieën zich ontwikkelen. Bovendien vinden ze de term eigenlijk verkeerdelijk gekozen omdat in vele gevallen "abuse" of "misuse" niet onder de

[54] SIEBER, U., *The International Handbook on Computer Crime, Computer-Related Economic Crime and the Infringements of Privacy*, New York, Wiley & Sons, 1986, 1-5.
[55] GOODMAN, M., 'Making computer crime count', *FBI Law Enforcement Bulletin*, 2001, afl. 8, 10-17.
[56] CLOUGH, B., 'Computer Crime', *Intersec*, 1997, 364-366.
[57] COOLS M. en VANKEIRSBILCK K., *Handboek Security, beheersing van criminele risico's*, Diegem, Samsom, 1995, 99-112.

kwalificatie valt van de meest gangbare definities van "computer crime". Daarom spreken ze liever over "computer abuse".[58]

M.i. verdient het de voorkeur om te kiezen voor een weldoordachte classificatie van computercriminaliteit eerder dan te trachten om "computer crime" als dusdanig te vatten in een definitie. In 2.4. wordt dan ook uitgebreid aandacht besteed aan een typologie van computercriminaliteit.

2.3. Fenomenologie

Om een beter zicht te kunnen krijgen op de specificiteit van computercriminaliteit, kan een onderzoek van de fenomenologische factoren soelaas bieden. In het verleden had de computerproblematiek vaak een onzichtbaar karakter. Daarnaast gebeurt het vaak dat fraude door het gebruik van computers op toevallige wijze ontdekt wordt. Bepaalde incidenten leiden tot een onderzoek waardoor andere feiten aan het licht komen.

In vele gevallen worden daders van computercriminaliteit niet echt als "misdadigers" beschouwd door het publiek. Dit is typisch voor ook andere vormen van "white collar crime". De plegers beschouwen zichzelf als een soort Robin Hood die geen schade berokkent aan individuen maar enkel aan computerapparatuur. Een belangrijke factor hierbij is de anonimiteit; fysiek contact met het slachtoffer blijft immers steeds afwezig.

Aan de grond van computercriminaliteit liggen een zestal *fenomenologische factoren* die hieronder besproken worden.[59]

2.3.1. Omgeving waarin het misdrijf gepleegd wordt

In een bepaalde databank kan men enorme hoeveelheden gegevens opslaan. Dit voordeel heeft echter ook zijn nadelen: de kwetsbaarheid en het risico voor fraude is des te groter. Computerchips worden steeds kleiner maar kunnen toch telkens grotere hoeveelheden gegevens bewaren. Microchips zijn zeer snel en gemakkelijk toegankelijk. De opbrengst in geval van fraude, is dan ook navenant.

Een secundair probleem houdt verband met de transfer van data die gebeurt tussen geografisch van elkaar verwijderde computersystemen. Misdrijven kunnen gericht zijn tegen

[58] KELLEHER, D. en MURRAY, K., *IT law in the European Union*, London, Sweet en Maxwell, 1999, 205-207.
[59] ERKELENS, C., 'Beteugeling van computercriminaliteit', *Panopticon*, 1985, 337-339.

computercentra of terminals maar ook tegen gegevensdragers zoals diskettes of cd-rom's. Aanvankelijk werd het grootst aantal misdrijven gepleegd door mensen die rechtstreeks contact hebben met de computer. De laatste jaren is deze trend omgebogen, meer en meer computercriminaliteit gebeurt van op afstand. De grote doorbraak van Internet zit hier ongetwijfeld voor iets tussen.

2.3.2. Modi operandi

Deze zijn specifiek en evolueren sterk met de jaren. In de volgende hoofdstukken wordt een typologie geschetst waarbij aandacht uitgaat naar verschillende vormen van computercriminaliteit.

2.3.3. Nagestreefde voordelen

In essentie wordt bij computercriminaliteit hetzelfde voordeel nagestreefd als bij de klassieke vermogensdelicten. Toch kan men stellen dat bepaalde criminelen ook gedreven zijn door andere beweegredenen. Zo zien sommigen het als een ware uitdaging om bepaalde misdrijven te plegen d.m.v. het gebruik van computers. Anderen doen het om de kick.

2.3.4. Tijdsfactor

De tijd die een crimineel nodig heeft om een computermisdrijf te plegen, verschilt van de tijd die nodig is om klassieke misdrijven te plegen. Sommige vormen van computercriminaliteit kunnen gepleegd worden op slechts een paar seconden tijd. Dit maakt de kans om als dader ontmaskerd te worden bijzonder klein.

2.3.5. Ruimtefactor

Door de recente evoluties in de telecommunicatiesector en de snelle opkomst van bedrijfsnetwerken kan men stellen dat bijna elke fysieke afstand makkelijk kan overbrugd worden door de crimineel. Misdrijven kunnen zonder enig probleem van op duizenden kilometers afstand gepleegd worden. Het spreekt voor zich dat de strafrechtelijke handhaving van deze delicten een kordaat en snel optreden vergt van de politiediensten.

2.3.6. De dader

In het artikel *Explaining Crime in the Year 2010*[60] stelt Wells dat technologische ontwikkelingen een aantal kansen bieden om nieuwe misdrijven te plegen, zoals fraude en afpersing door middel van computergebruik. Hij voegt daaraan toe dat deze misdrijven worden gepleegd door nieuwe soorten daders die niet erg verwant zijn met de traditionele *street crime offender*.

De gemiddelde leeftijd van computercriminelen wordt geschat op 25 jaar. Het gaat vooral om universitair geschoolden. In vele gevallen zijn deze personen nog niet zo lang werkzaam bij het bedrijf of instelling dat hun slachtoffer zal worden. Een van de redenen waarom men vaak overgaat tot het plegen van computercriminaliteit is het afwezig blijven van een positieve identificatie met het bedrijf waarin men werkzaam is. Vaak zijn personen ook overgekwalificeerd voor het werk dat ze moeten verrichten. Het overschot aan creatieve energie kan dan aangewend worden voor criminele doeleinden.

Veelal zijn er ook medeplichtigen of zelfs mededaders in het spel. Vaak gaat het om computerspecialisten die het technische aspect voor hun rekening nemen. Een tweede persoon wordt in bepaalde gevallen ingeschakeld om de technische ingrepen om te zetten in werkelijk gewin.

Competitieve computertechnici zijn er dikwijls op uit om hun superioriteit wereldkundig te maken. De uitdagingen die er zijn binnen de eigen onderneming kunnen leiden tot criminele gedragingen zoals het binnendringen in computersystemen van concurrerende bedrijven, het stelen van boekhoudkundige gegevens, het aftappen van lijnen, enz. Anderen schatten hun positie eerder in als elitair. Daders gaan hierbij uit van de premisse dat ze het recht hebben om de computer te gebruiken om private doeleinden te verwezenlijken.

Auteurs zoals Grabosky stellen dat de mogelijkheden om nieuwe misdaden te plegen op ruime schaal zullen worden benut.[61] Deze nieuwe misdaden kunnen immers snel worden gepleegd en de kans op betrapping is minimaal. Bovendien zijn er maar weinig morele barrières te nemen bij het plegen van dergelijke misdrijven.

---

[60] WELLS, L.E., 'Explaining crime in the year 2010' in *Crime and Justice in the Year 2010,* KLOFAS, J. en STOJKOVIC, S., (eds.), Belmont, CA Wadsworth, 1995, 49-50.
[61] GRABOSKY, P.N. en SMITH, R.G., *Crime in the digital age: controlling telecommunications and cyberspace*, Sydney, Federation Press, 1998, 210-212.

2.4. Typologie[62]

2.4.1. Dichotomie specifieke en a-specifieke computercriminaliteit

Men kan een *tweetal* grote categorieën computercriminaliteit onderscheiden[63]:

- Als informatica en/of telecommunicatie een essentieel onderdeel vormen van het misdrijf, dan spreekt men van *specifieke of typische informaticamisdrijven*. Het hacken van computers en de verspreiding van computervirussen zijn hiervan een goed voorbeeld.

- Anderzijds kan informatica en/of telecommunicatie ook louter een middel zijn om een misdrijf te plegen. In deze gevallen spreekt men van *a-specifieke of a-typische informaticamisdrijven*. Oplichting en diefstal behoren tot deze categorie.

Het spreekt voor zich dat in de praktijk beide categorieën zich met elkaar kunnen vermengen. Zo kan een onderneming opgelicht worden door de manipulatie van het boekhoudkundig programma op de computer van de bedrijfsaccountant.

2.4.2. Specifieke informaticamisdrijven

2.4.2.1. MINIMUMLIJST RAAD VAN EUROPA

De zoektocht naar een sluitende definitie voor dit type van criminele gedragingen heeft in het verleden reeds aanleiding gegeven tot talrijke discussies in verschillende landen.[64] Binnen Europese context werd uiteindelijk voor een classificatie van de verschillende gedragingen gekozen in plaats van een enge definitie van het probleem. Deze classificatie gaat uit van de diverse vormen van informaticamisbruik die totnogtoe werden vastgesteld.[65]

---

[62] Opmerking: In deze typologie wordt een onderscheid gemaakt tussen de verschillende types van computercriminaliteit. Het is geenszins de bedoeling om in dit hoofdstuk een compleet overzicht te geven van de vigerende wetgeving en de toepassingsmodaliteiten ervan. In Deel III daarentegen, dat gewijd is aan de Belgische Wet Informaticacriminaliteit, wordt wel uitvoerig aandacht besteed aan de bestraffing van informaticacriminaliteit.

[63] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 121-122.

[64] Zie SPRUYT, B., 'Computers op de strafbank', in *Informaticacriminaliteit*, DE SCHUTTER, B., (ed.), VII, Antwerpen, Kluwer, 1987, 232-235.

[65] VAN EECKE P., *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 15-16.

De minimumlijst die door de Raad van Europa werd voorgesteld ziet er als volgt uit[66]:

1. *Computer Fraud:* the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person made with the intent of procuring an unlawful economic gain for oneself or for another person or with the intent to unlawfully deprive that person of his property;

2. *Computer forgery:* the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would substitute the offence of forgery if it had been committed with respect to traditional object of such an offence;

3. *Damage to computer data and computer programs:* the erasure, damaging, deterioration or suppression of computer data or computer programs without right;

4. *Computer sabotage:* the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, with the intent to hinder the functioning of a computer or a telecommunication system;

5. *Unauthorised access:* the access without right to a computer system or network by infringing security measures;

6. *Unauthorised interception:* the interception, made without right and by technical means, of communication to, from and within a computer system or network;

7. *Unauthorised reproduction of a protected computer program:* the reproduction, distribution or communication to the public without right of a computer program which is protected by law;

8. *Unauthorised reproduction of topography:* the reproduction without right of a topography, protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right of a topography or a semiconductor product manufactured by using the topography.

[66] COUNCIL OF EUROPE, *Computer-Related Crime*, Recommendation No. R(89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems, *Strasbourg*, 1990.

2.4.2.2. COMPUTERINBRAAK

Hacken is een zuiver ICT-delict. Anders dan bijvoorbeeld de verspreiding van kinderpornografie en het plegen van fraude, is het alleen mogelijk in een geautomatiseerde omgeving.[67]

Computerinbraak kan gedefinieerd worden als "*het op een of andere wijze ongeoorloofd binnendringen in computersystemen*". Dit kan gebeuren door zich opzettelijk met een computer of netwerk in verbinding te stellen zonder dat hiervoor de nodige toestemming werd verkregen. Gevallen waarbij men op onopzettelijke wijze een verbinding maakt met een computersysteem maar vervolgens besluit om deze connectie te handhaven, vallen ook onder de kwalificatie 'hacken' of 'kraken'.[68]

Sinds de introductie van computers heeft men in de informaticawereld af te rekenen met het kraken van netwerksystemen. De introductie van de permanente Internetverbindingen (kabel of ADSL) heeft dit fenomeen nog verder in de hand gewerkt.[69]

De capaciteit of de faciliteiten die een krachtig computersysteem bieden, zijn in sommige gevallen een reden om in te breken.[70] Tevens kan men zonder kosten een telefonische verbinding maken met andere computersystemen. Dit gebeurt vanzelfsprekend niet onopgemerkt, het slachtoffer wordt immers geconfronteerd met abnormaal hoge telefoonkosten.

Enkele jaren terug was het kraken van een computer voorbehouden aan een beperkt aantal getalenteerde computerprogrammeurs.[71] Vandaag zijn zowat alle technieken waarvan hackers zich bedienen in een gebruiksvriendelijk programma gegoten. Een grondige kennis van programmeertalen en besturingssystemen is niet langer vereist waardoor iedereen met een computer en aansluiting op het Web een aanval kan lanceren op een onwetend slachtoffer.

Eind 2001 werden drie tieners door computerspecialisten van de Federale Politie (Computer Crime Unit) geïdentificeerd nadat ze tientallen websites gekraakt hadden. Volgens een Franse

---

[67] STOL, W.P., VAN TREECK, R.J. en VAN DER VEN A.E.B.M., 'Criminaliteit met ICT', *Modus*, 2000, afl. 4, 8-13.
[68] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 122-123.
[69] WUYTS, D., (2001/02/20) 'Hacken: wat is het en wat doe je eraan?' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DSM20022001_001&trefwoord=kredietkaart [02/04/02]
[70] KARTER, D. en KATZ, A., 'An emerging challenge for law enforcement', *FBI Law Enforcement Bulletin*, 1996, afl. 12, 1-8.
[71] FURNELL, S., *Cybercrime, Vandalizing the information society*, London, Addison-Wesley, 2002, 45-93.

bron zou de vijftienjarige hacker "Asmodeus" samen met zijn groep "Belgian Hackers Zone" meer dan honderd kraken gepleegd hebben.[72]

Het kraken van een computer draait in de eerste plaats om het uitbuiten van beveiligingslekken. Dit zijn fouten in software die het mogelijk maken dat onbevoegden via het Internet toegang krijgen tot andermans computer. Speciaal daartoe ontwikkelde softwareprogramma's zoals "Back Orifice"[73] nestelen zich ongemerkt op een computer via een website of een e-mail. Zodra deze programma's geïnstalleerd zijn, zal de computer van het slachtoffer zich gaan gedragen als server. Dit betekent dat de harde schijf potentieel toegankelijk wordt voor alle Internetgebruikers.[74]

2.4.2.3. MANIPULATIE VAN DATA[75]

De manipulatie van elektronische gegevens kan worden omschreven als het toevoegen, wijzigen, verwijderen of overnemen van deze gegevens. Met elektronische gegevens worden zowel data als programma's bedoeld. Typische vormen zijn het vervalsen van computerbestanden of invoergegevens. Ook het inbrengen van computervirussen behoort tot deze categorie.

Het specifieke aan een computervirus is dat het zichzelf kan vermenigvuldigen waarna het, in de meeste gevallen, programma's besmet die geïnstalleerd zijn op de getroffen computer. In het begin van 2001 bevatte gemiddeld één op de 4.500 e-mailberichten een virus. Eind 2001 was reeds ongeveer één op de 500 e-mails besmet met een virus.[76]

"Trojaanse paarden" horen ook thuis in deze familie. Dit is software die er in slaagt om zich voor te doen als een ander programma om op die manier gegevens van een gebruiker te

---

[72] Y.B., (2001/12/12) 'Minderjarige hackers lopen tegen de lamp' [WWW]. De Standaard Online: http://www.standaard.be/Archief/zoeken/DetailNew.asp?articleID=DST12122001_020&trefwoord=hackers [01/04/02]; Zie ook: VAN EECKE, P., (2002/02/18) 'Asmodeus, de webscalpeerder' [WWW]. De Standaard Online: http://www.standaard.be/Archief/zoeken/DetailNew.asp?articleID=DST18022002_124&trefwoord=asmodeus [01/04/02]

[73] "Back Orifice" maakt misbruik van de vele zwakke plekken van het besturingssysteem 'Windows 95' en 'Windows 98'. Het is een "trojaans paard" met kenmerken van een computervirus. Eens geïnstalleerd bij het slachtoffer, kan elke hacker die beschikt over een onderdeel van "Back Orifice" een lijst te zien krijgen van alle geïnfecteerde computers zodat men deze als het ware kan 'aanspreken' om vervolgens allerhande opdrachten te laten uitvoeren.

[74] DE DECKER, K., 'Het weerloze web', *Knack*, 2000, afl. 48, 92-95.

[75] VAN EECKE P., *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 27-28.

[76] F.D.G., (2001/12/24) 'Geen bewondering voor virusschrijvers' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DST24122001_055&trefwoord=virus [04/04/02]

ontfutselen. "Trojaanse paarden" werden bij hackers populair omdat ze o.a. kunnen gebruikt worden om de paswoorden van argeloze gebruikers te verkrijgen.

2.4.2.4. ILLEGAAL KOPIËREN OF DISTRIBUEREN VAN COMPUTERSOFTWARE

Bij programmapiraterij wordt computerprogrammatuur illegaal vermenigvuldigd, verspreid of verkocht zodat het betalen van de verplichte auteursrechten wordt ontdoken.

2.4.2.4.1. Illegaal kopiëren van software[77]

Imitatie is een van de meest drastische vormen van illegaal softwaregebruik. Hierbij wordt getracht het origineel product zo goed mogelijk na te maken. Het namaakproduct wordt vervolgens op de markt verkocht tegen een prijs die vergelijkbaar is met het legale, officiële product. De consument is er in vele gevallen van overtuigd dat hij originele computersoftware heeft aangekocht.

De laatste jaren gebeurt de verspreiding van illegale software meer en meer via Internet. Op het Web zijn massa's "warez-sites" aanwezig. Dit zijn sites met verwijzingen naar andere pagina's waar illegale software, "warez" genoemd, kan worden gedownload. Dikwijls verhuizen deze websites vaak van adres zodat het moeilijk wordt deze op te sporen. Deze sites bieden recente versies aan van zakelijke software en geven tevens een lijst van codes die toelaten de beschermde software te kraken.

2.4.2.4.2 Illegaal gebruik van software binnen bedrijven

Een andere belangrijke vorm van illegaal softwaregebruik is het illegaal kopiëren en ter beschikking stellen van computerprogramma's binnen bedrijven. Veel bedrijfsleiders nemen het niet altijd even nauw met de licentiepolitiek. Ze kopen één softwarepakket aan en installeren dit vervolgens op een groot aantal computers. Nochtans is de basisregel duidelijk en eenvoudig: er moet een licentie zijn voor de gebruikers in relatie met het aantal computers waarop deze software wordt gebruikt.

[77] X., (s.d.) 'De strijd tegen piraterij' [WWW]. Business Software Alliance: http://www.bsa.org/belgium-dutch/antipiracy/imitatie.phtml [09/02/02]

2.4.2.4.3. Illegaal kopiëren van muziek[78]

Muziekpiraterij is een frauduleuze schending van de auteursrechten en betekent tevens een grote bedreiging voor de internationale muziekindustrie. Internetpiraterij is de muziekindustrie al jaren een doorn in het oog. Het populaire muziekformaat "MP3" heeft gezorgd voor een snelle toename van het aantal illegaal verspreide muziekkopieën.

De omstreden firma "Napster", die inmiddels verwikkeld is in talrijke rechtszaken, geeft surfers op grote schaal de gelegenheid tot het illegaal kopiëren en uitwisselen van muziekstukken in MP3-formaat. Napster stelt dat het kopiëren en verspreiden van illegale MP3-files een zaak is van het individu waar een aanbieder van infrastructuur niet verantwoordelijk voor is. In de literatuur wordt de noodklok over het auteursrecht geluid. Dommering spreekt zelfs van een ware "crisis van het auteursrecht".[79]

2.4.2.5. VALSHEID IN INFORMATICA[80]

Valsheid in Informatica is een nieuwe categorie die men sinds kort kan toevoegen aan deze typologie[81]. Onder deze noemer vallen handelingen zoals het vervalsen van kredietkaarten, elektronische geldbeugels of elektronisch opgemaakte contracten. Bij "valsheid in informatica" worden elektronische gegevens door middel van informatica gewijzigd. Hierdoor wordt de juridische draagwijdte van deze gegevens veranderd.

2.4.2.6. INFORMATICABEDROG[82]

De manipulatie van elektronische gegevens gebeurt vaak met het doel een onrechtmatig voordeel te bekomen. Verschillend met diefstal is dat men bij deze handeling geen zaken ontvreemdt maar deze op een vrijwillige wijze laat overhandigen. Dit gebeurt door het stellen van bedrieglijke handelingen zoals het inbrengen van fictieve namen in een bestand of het veranderen van bepaalde gegevens.

---

[78] Zie SABAM, Het auteursrecht in de kijker, 2001, 8 p. (brochure)
[79] DOMMERING, E.J., 'Het auteursrecht spoelt weg door het elektronische vergiet. Enige gedachten over de naderende crisis van het auteursrecht', *Computerrecht*, 1994, 109-110.
[80] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 127-128.
[81] Deze categorie werd ingevoerd door de *Belgische Wet Informaticacriminaliteit van 28 november 2000*. In Deel III gaat bijzondere aandacht uit naar de nieuwe strafbaarstellingen en onderzoekstechnieken die deze Wet heeft ingevoerd.
[82] Cfr. noot 73.

Een mooi voorbeeld hiervan vinden we terug in Duitsland waar de "kindergeldzaak" voor beroering zorgde.[83] Iemand was er in geslaagd om op onrechtmatige wijze kindergeld te ontvangen. Dit gebeurde door de toevoeging van fictieve namen aan de bestanden van een sociale instelling.

Andere gevallen die als informaticabedrog kunnen gekwalificeerd worden zijn het gebruik van een gestolen kredietkaart om geld uit een automatische biljettenverdeler te halen of het invoeren van programma-instructies zodat bepaalde verrichtingen een onrechtmatig financieel voordeel opleveren.[84]

2.4.3. A-specifieke informaticamisdrijven

2.4.3.1. VERSPREIDING VAN ILLEGALE PORNOGRAFIE[85]

Een Amerikaanse studie toont aan dat een belangrijk deel van het pornografisch materiaal dat via computernetwerken wordt rondgestuurd, bestaat uit afbeeldingen en teksten met de nadruk op pedofilie en andere vormen van seksueel afwijkende gedragingen.[86]

De populariteit van het Internet stijgt bij de producenten en consumenten van kinderpornografie. Hiervoor zijn verschillende redenen. Vooreerst maakt de technologie het mogelijk om constant nieuw materiaal beschikbaar te stellen, updates kunnen dus dag en nacht doorgevoerd worden. Ten tweede bereikt men via het Web een enorme massa personen en dit aan een lage kostprijs. Ook wordt de anonimiteit die het Internet biedt, doorgaans ervaren als een groot voordeel.[87]

Men kan een onderscheid maken tussen pornografisch materiaal in het algemeen, kinderpornografie en tenslotte reclame voor seksuele diensten.

[83] SIEBER, U., *Computerkriminalität und Strafrecht*, München, Heymans, 1980, 47-48.
[84] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 128-129.
[85] Voor een case study, zie: MCLEAN, J.J., 'Homocide and child pornography' in *Handbook of Computer Crime Investigation*, CASEY, E., (eds.), London, Academic Press, 2002, 361-373.
[86] RIMM, M., 'Marketing pornography on the information superhigway', *Georgetown Law Journal*, 1995, 1849-1934.
[87] CALCETAS-SANTOS, O., *Child pornography on the Internet*, in *Child abuse on the Internet, ending the silence*, ARNALDO C.A., (ed.), Paris, Unesco publishing, 2001, 57-59.

2.4.3.1.1. De verspreiding van onzedelijk materiaal[88]

De beslissing of bepaalde prenten of afbeeldingen al dan niet strijdig zijn met de goede zeden, wordt genomen door de rechter. Het begrip "goede zeden" moet op evolutieve wijze naar tijd en ruimte worden bepaald a.h.v. het collectief bewustzijn van het ogenblik.[89] Het is dus niet zo dat de inhoud van erotische afbeeldingen automatisch een strijdigheid met de goede zeden inhoudt. De rechter zal soeverein moeten oordelen op grond van de huidige "aanvaardbaarheidsdrempel" in de maatschappij. Het volstaat niet dat het schaamtegevoel van enkele individuen wordt gekwetst opdat er sprake zou zijn van strijdigheid met de goede zeden.

De "aanvaardbaarheidsdrempel" of het "collectief bewustzijn" is een willekeurige en onduidelijke notie, zoveel is duidelijk. De notie "schending van de goede zeden" werd in het verleden reeds door het Hof van Cassatie ingevuld. Afbeeldingen schenden de zeden "*wanneer ze blijkbaar uitsluitend erop gericht zijn om de zinnelijke gevoelens van degene die ze bekijkt buitenmatig te prikkelen of, wegens de vicieuze of onnatuurlijke gedragingen of houdingen op seksueel gebied die ze voorstellen, het schaamtegevoel van de gezonddenkende doorsnee burger kwetsen*".[90]

2.4.3.1.2. Kinderpornografie[91]

De kwalificatie "kinderpornografie" hangt nauw samen met het begrip "goede zeden". Er is sprake van een "pornografisch karakter" zodra producties op expliciete wijze een seksuele inhoud bevatten en bovendien de bedoeling hebben om de seksuele geestdrift van de kijker op te wekken.[92]

In de verschillende Ministeriële Richtlijnen wordt onder kinderpornografie verstaan: "*voorwerpen of beelddragers van welke aard ook, die houdingen of seksuele handelingen met pornografisch karakter vertonen waarbij minderjarigen beneden de zestien jaar worden voorgesteld of betrokken zijn*".[93]

---

[88] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 130-131.
[89] Cass, 15 maart 1994, *Arr. Cass*, 245, noot G.VERMEULEN.
[90] DE ZEGHER, J., *Openbare zedenschennis*, in *APR-reeks*, Gent, Story-Scientia, 1973, 67-70.
[91] Zie VERMEULEN, G., 'Kinderhandel, seksuele uitbuiting van kinderen, kinderporno en kindersekstoerisme', *Panopticon*, 2000, 201-207.
[92] VANDEMEULEBROEKE O. en GAZAN, 'Traite des êtres humains, exploitation et abus sexuels. Les nouvelles lois des 27 mars et 13 avril 1995', *Revue de droit pénal*, 1995, 973-1077.
[93] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 31 mei 1999, omzendbrief nr. COL 12/99.

Verder wordt ook het onderscheid gemaakt tussen kinderporno, pseudo-kinderporno en "child-erotica".[94] Onder "child-erotica" begrijpt men afbeeldingen van naakte of schaars geklede kinderen. Pseudo-kinderporno betreft pornografische afbeeldingen van kinderen die werden bekomen door toepassing van computertechnieken en trucage. Kinderporno betreft de seksuele uitbuiting van minderjarigen.

2.4.3.1.3. Reclame voor seksuele diensten[95]

Via het Internet, maar ook via andere computernetwerken, wordt soms reclame gemaakt voor seksuele diensten die specifiek gericht zijn op minderjarigen of die aangeboden worden door minderjarigen. Sekstoerisme of reclame waar vrouwen- en kinderhandel achter schuilt, vallen ook onder deze noemer.

2.4.3.2. AANRANDING VAN DE EER OF DE GOEDE NAAM VAN PERSONEN[96]

De "aanranding van de eer of de goede naam van personen" is een oud misdrijf. De introductie van nieuwere en meer moderne telecommunicatiemiddelen heeft ervoor gezorgd dat deze delictsvorm een andere dimensie kreeg. Het plaatsen van lasterlijke berichten op websites, het verzenden van laster per e-mail, beledigende informatie die op een persoonlijke website wordt geplaatst. Dit zijn allemaal voorbeelden van de nieuwe varianten van de kwalificatie "aanranding van de eer of de goede naam van personen".

2.4.3.3. RACISTISCHE UITINGEN EN ONTKENNING VAN GENOCIDE

Regelmatig wordt misbruik gemaakt van computernetwerken om racistische of revisionistische teksten te verspreiden.

2.4.3.3.1. Racisme en xenofobie[97]

Publicaties of uitingen die een aanzet geven tot vreemdelingenhaat en discriminatie vallen onder deze categorie. Vaker en vaker gebeurt de verspreiding van racistisch materiaal via diverse audio-visuele media. Zo verspreidde een beklaagde tussen december 1997 en februari

[94] DE CANG, T., PITEUS, K. en VAN WASSENHOVE, I., *Kinderpornografie*, Gent, Academiejaar 2000-2001, 12-13. (scriptie in het kader van het vak Grondige Studie van het Strafrecht).
[95] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 133-134.
[96] VAN EECKE P., *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 64-65.
[97] Zie DUPONT, L., 'De wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden', *Panopticon*, 1981, 504-506.

1999 via het Internet racistische en negationistische teksten. Na herhaaldelijke waarschuwingen diende de provider klacht in met burgerlijke partijstelling.[98]

2.4.3.3.2. Ontkenning van genocide

Met "ontkenning van genocide" wordt bedoeld, de gevallen waarin iemand de genocide, die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistische regime werd gepleegd, ontkent, schromelijk minimaliseert, poogt te rechtvaardigen of goedkeurt.[99] Problematisch hierbij is dat men deze informatie vaak aantreft op servers, die zich in andere landen bevinden, zoals de Verenigde Staten van Amerika. In de V.S.A. zijn deze uitingen immers volstrekt legaal.

2.4.3.4. AANZETTEN TOT CRIMINEEL GEDRAG

Via de digitale snelweg kan men sinds geruime tijd informatie verkrijgen over zaken die in de samenleving niet geaccepteerd worden. Een bekend voorbeeld is "the Anarchist Cookbook".[100] Dit boek, dat op verschillende websites is terug te vinden, verschaft de surfer meer uitleg over de samenstelling van verschillende soorten explosieven, de bereiding van molotovcocktails, het plegen van kredietkaartfraude, enz. Deze informatie is echter ook nog steeds in de niet-virtuele wereld verkrijgbaar. Toch heeft de wijdverspreidheid en de grote toegankelijkheid van het Internet ervoor gezorgd dat dit ongeoorloofd materiaal op een eenvoudige en snelle wijze kan geraadpleegd worden.

2.4.3.5. GOKKEN[101]

Via het Internet is het een koud kunstje om van op Belgisch grondgebied te gokken in een of ander gokpaleis ergens ter wereld. In vele gevallen ontstaat een internationaal goknetwerk dat in grote mate ontsnapt aan enige overheidscontrole. Verschillende bronnen schatten dat meer dan duizend websites in ongeveer vijftig verschillende landen actief zijn in "online gambling".[102]

---

[98] Corr. Brussel, 15 januari 2002, [WWW] Centrum voor gelijkheid van kansen en racismebestrijding: http://www.antiracisme.be/nl/rechtspraak/vonnissen/2002/02-01-15_c_bsl.pdf [03/04/02]
[99] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 138-139.
[100] X., (1994) 'The Anarchist Cookbook' [WWW]. The Little Bookstore: http://come.to/anarchy [27/03/02]
[101] DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 140-141.
[102] SHIPLEY, T.G., 'Internet gambling investigations' in *Handbook of Computer Crime Investigation*, CASEY, E., (ed.), London, Academic Press, 2002, 367-377.

On-linecasino's zijn een gedroomd circuit voor het witwassen van opbrengsten die worden verkregen uit illegale activiteiten. Wanneer hierbij nog eens rekening wordt gehouden met de opkomst van het zogenaamde "E-cash"[103], dan wordt overduidelijk dat deze elektronische casino's een uitgelezen middel zijn om zwarte fondsen in de legale markt te injecteren.

Een bezoekje aan een on-line casino kan bepaalde risico's inhouden. Wie wil meespelen voor de prijzenpot moet bijna altijd een programma downloaden. Hoewel de kans klein is dat daar een virus in verborgen zit, is het wel mogelijk dat zich hierdoor een stukje "spyware" nestelt op de harde schijf. Dat is software die ongemerkt informatie over pc- en Internetgebruik doorstuurt naar agentschappen die op basis daarvan ongewenste reclameboodschappen versturen.

Vaak moet de goklustige surfer ook zijn kredietkaartgegevens invullen, zogezegd om te controleren of hij of zij wel meerderjarig is. De beheerders van de goksite zitten doorgaans ergens in een belastingparadijs van waaruit ze ongestraft transacties kunnen doen.[104]

2.4.3.6. OPLICHTING

Vaak worden moderne telecommunicatiemiddelen toegepast als middel om zichzelf te verrijken op onrechtmatige wijze. Een veel voorkomend geval is oplichting van de telefoonmaatschappij. Zo is het mogelijk een betaallijn aan te vragen bij een provider van telefoondiensten waarbij elke oproeper een bepaald bedrag boven op de verbindingskosten betaalt. Dit extra bedrag wordt verdeeld tussen de telefoonmaatschappij en de huurder van de lijn. Door gebruik te maken van valse telefoonkaarten kan de huurder systematisch telefoneren naar de eigen betaallijn waardoor hij inkomsten verwerft uit deze gesprekken. Deze techniek wordt "phone phreaking" genoemd.

Via het Internet worden vaak tegen betaling een aantal diensten of goederen aangeboden die achteraf onbestaande blijken te zijn. Het aanbod aan producten en diensten is bijna onuitputtelijk, gaande van valse tijdschriftabonnementen tot illegale geldpiramides. Door

[103] "E-cash" is een vorm van digitaal geld, te vergelijken met "Proton" in België. Het gebruik van "E-cash" is volledig anoniem, de virtuele munten bevatten enkel een uniek serienummer dat wordt geëncrypteerd door het gebruik van een "private key" die in het bezit is van de aanwender. Het systeem laat toe giraal geld om te zetten naar "cybergeld", maar het omgekeerde is evenwel ook mogelijk: "cybergeld" kan worden omgezet in giraal geld en uiteindelijk belanden op een bankrekening.

[104] DE GRAEVE, F., (2001/11/23) 'On-line gokken in de lift' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DST23112001_013&trefwoord=virus [04/04/02]

gebruik te maken van de informatiesnelweg is het mogelijk op korte termijn en met weinig financiële middelen een groot aantal slachtoffers te bereiken.[105]

De Britse "Commercial Crime Services" (CCS) heeft een bedrijf ontmanteld dat via het Internet investeerders lokte met valse bankgaranties. De criminele organisatie publiceerde op ten minste negenentwintig verschillende websites valse bankgaranties. Daarmee lokten ze potentiële klanten om niet bestaande projecten te financieren.[106]

2.4.3.7. "ELECTRONIC MONEY LAUNDERING"

Het uiteindelijke doel van "money laundering" of "witwassen" is het injecteren van crimineel geld met een schijnbaar legale herkomst in de "bovenwereld". Schaap en Udink definiëren "money laundering" als: *"Het (doen) verrichten van handelingen, waardoor een voor de wet verzwegen vermogensaanwas ogenschijnlijk een legale oorsprong krijgt".*[107]

De essentie bij witwassen bestaat erin dat verborgen geld, waarvoor de herkomst niet kan worden verantwoord, wordt omgezet in geld waarvan wel de herkomst kan worden verklaard. Dit is het belangrijkste doel van de witwasser. Hij wil de bron van zijn inkomsten verbergen. Immers, wanneer de ware toedracht aan het licht komt, loopt hij het gevaar dat de verdachte gelden zullen worden geconfisceerd. De witwasser zal proberen deze confiscatie te voorkomen zodat het criminele geld vrij kan worden uitgegeven en geïnvesteerd in de legale "bovenwereld".

Bij witwassen kan men een viertal fasen onderscheiden[108]:

- ***Storting of placement:*** de storting of inleg van baar geld in het giraal geldverkeer. Het "vuile" geld stroomt het financiële stelsel van de bovenwereld in.

- ***Opsplitsing en samenvoeging of layering:*** opsplitsing van het gestorte geld in deelbedragen, waarmee vervolgens een aantal girale handelingen wordt uitgevoerd, teneinde het boekhoudspoor te verduisteren of te doorbreken.

---

[105] VAN EECKE P., *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 77-78.
[106] A.N.P., (2001/11/15) 'Fraudenetwerk op web ontmanteld' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Nieuws/2001/04/14/Med/inhoud.html [15/ 11/01]
[107] SCHAAP, C.D., ROZEKRANS, R., VAN DUYNE, P.C., 'Geld witwassen. Een probleemverkenning van de opbrengstkant van op winst gerichte misdaad', *Tijdschrift voor de politie*, 1992, 107-111.
[108] BERKMOES, H., VAN DAELE, R., en DE BIE, B., 'Misdaad loont niet (meer?). De bijzondere verbeurdverklaring van vermogensvoordelen en de bestrijding van het witwassen in België', *Politeia*, 1994, 69-70.

- ***Rechtvaardiging:*** het toekennen van een ogenschijnlijk wettige oorsprong aan het geld. Het geld verkrijgt de status van legaal verdiend geld.

- ***Maatschappelijke invlechting of integration:*** het witgewassen geld komt in het gewone betalingsverkeer terecht. De witwasser heeft zijn doel bereikt: hij kan zijn geld "rechtvaardigbaar" investeren in de legale bovenwereld.

Het risico van witwassen houdt in dat de economie besmet raakt met criminele vermogens. De economische macht kan daardoor in ongewenste handen komen, wat dan weer consequenties kan hebben voor het functioneren van de maatschappij. Dit wordt gelukkig in zeer brede kringen als een groot gevaar beschouwd, hetgeen leidt tot een consensus om het fenomeen witwassen doeltreffend te bestrijden.

Het proces waarbij geld en andere vormen van rijkdom worden witgewassen, wordt enkel beperkt door de spitsvondigheid en middelen van de witwasser. De creatie van complexe netwerken van financiële transacties maakt het er voor de politiediensten zeker niet gemakkelijker om de feiten aan het licht te brengen en de link te leggen tussen het misdrijf en het vermogensvoordeel dat werd gegenereerd.

Computers kunnen van onschatbare waarde zijn in het structureren en opzetten van dergelijke complexe netwerken. In veel gevallen is het zo dat wanneer witwassers worden betrapt dit te wijten is aan het feit dat ze niet langer hun opzet kunnen structureren en controleren. Het gebruik van computers laat zo een grote complexiteit toe bij het opzetten van financiële transacties dat forensische boekhouders het zeer moeilijk krijgen om het web te ontrafelen.

Hoofdstuk 3: Cybercrime

3.1. Inleidend

Criminaliteit is een zeer complex verschijnsel. Enerzijds is er continuïteit in bepaalde types van criminaliteit (woninginbraken, vandalisme, rijden onder invloed) maar anderzijds zijn er permanent nieuwe criminaliteitsproblemen die zich stellen.[109] Het begrip "criminaliteit" bundelt een zeer heterogene verzameling: agressief gedrag, allerlei vormen van geweld, handel in drugs, mensensmokkel, "cybercrime", witwassen, …

De opmars van de moderne informatie- en communicatietechnologie heeft gezorgd voor een sterk wijzigende samenleving. Computers, telecommunicatie en andere nieuwe media raken immers steeds meer en meer verweven met elkaar.[110] Met de komst van het Internet kregen begrippen als tijd, plaats en ruimte een volledig nieuwe dimensie. Vandaag de dag kan eenieder die over de nodige apparatuur beschikt, zich waar ook ter wereld aansluiten op het Internet. Ook criminelen hebben deze wereld inmiddels ontdekt.

Het Internet biedt een aanzienlijke uitbreiding van de traditionele mogelijkheden om delicten te plegen. Bovendien kan men op een anonieme manier de hele wereld verkennen zonder last te ondervinden van controle aan grensovergangen. De drempel om tot misdrijven te komen via het Internet ligt lager dan in de normale samenleving. Dit is grotendeels te wijten aan de afwezigheid van enige sociale controle.

In sommige gevallen doet men beroep op de mogelijkheden van het Internet ter ondersteuning van klassieke misdrijven. Enige tijd voor de start van het voetbaltoernooi "Euro 2000" lanceerden voetbalsupporters met minder goede bedoelingen via het Internet een oproep naar andere supportersgroeperingen toe om een leger van hooligans te vormen.[111] Supporterskernen werden opgeroepen om nummers van mobiele telefoons uit te wisselen. Ook wilden de initiatiefnemers nieuwsbrieven verspreiden. Via discussies op Internet zou gepeild worden naar

[109] BRUINSMA, G.J.N., VAN DE BUNT, H.G. en HAEN MARSHALL, I., *Met het oog op de toekomst, verkenning naar de kennisvragen over misdaad en misdaadbestrijding in 2010,* in *AWT-Achtergrondstudies*, TIMMERHUIS, V. (ed), 24, Den Haag, AWT, 2001, 8-9.
[110] VRIESDE, R., VAN OSS, J. en GELS, M., 'Criminaliteit op Internet, een eerste aanzet voor digitale surveillance en opsporing', *Algemeen Politieblad*, 1999, afl. 12, 8-10.
[111] DE VREESE, S., *Belgische hooligans op het Internet* in *Handboek Politiediensten*, Diegem, Kluwer, 1999, 3-5.

meningen om vervolgens een strategie te bedenken om een gezamenlijk "leger" te vormen. Na korte tijd werd de bewuste website door de politiediensten verwijderd van het net.[112]

3.2. Definiëring

De criminaliteitsvormen die zich op het Internet afspelen, vaak omschreven als *Internetcriminaliteit*, kunnen in vele gevallen niet beschouwd worden als op zichzelf staande criminele feiten waar dit bij klassieke misdrijven zoals bvb. moord wel het geval is.

Een strafrechtelijke definiëring van de term *Internetcriminaliteit* vinden we terug bij Van Vriesde. Hij beschouwt het als *"alle strafbare feiten of strafwaardige gedragingen gepleegd met behulp van het medium Internet"*.[113] Het begrip Internetcriminaliteit werd door de auteur bewust ruim omschreven gezien de zeer uiteenlopende verschijningsvormen in de praktijk.

Douglas waagt zich ook aan een definiëring van Cybercrime. Hij stelt dat "Cybercrime can be regarded as computer-mediated activities which are either illegal of considered illicit by certain parties and which can be conducted through global electronic networks".[114]

3.3. Typologie

Internetcriminaliteit of "cybercrime" kan grofweg verdeeld worden in een zestal categorieën.[115] Voor een goed begrip wordt er voor elke verschijningsvorm een korte toelichting en een voorbeeld gegeven. Het is geenszins de bedoeling om in dit hoofdstuk een overzicht te geven van de vigerende wetgeving en de toepassingsmodaliteiten ervan. In Deel III daarentegen, dat gewijd is aan de Belgische Wet Informaticacriminaliteit, wordt wel uitvoerig aandacht besteed aan de bestraffing van informaticacriminaliteit.

3.3.1. Aantasting van infrastructuur, nationale veiligheid en openbare orde

"Cyberterrorisme" is een typisch voorbeeld van deze categorie. Via het Internet kunnen terroristen publiciteit geven aan hun politieke overtuiging. Sommige terroristische groeperingen trachten het medium Internet zelfs te gebruiken om fondsen te verzamelen voor

[112] X.,(1999/12/01) 'Hooligans met leger op Internet' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Lab/EK2000/veiligheid/veilig991013wwwhool.html [20/03/02]
[113] VRIESDE, R., VAN OSS, J. en GELS, M., 'Criminaliteit op Internet, een overzicht van de verschijningsvorm', *Algemeen Politieblad*, 1999, afl. 13, 8-13.
[114] THOMAS, D. en LOADER B.D., *Cybercrime: law enforcement, security and surveillance in the information age*, London, Routledge, 2000, 3-7.
[115] VRIESDE, R., VAN OSS, J. en GELS, M., 'Criminaliteit op Internet, een overzicht van de verschijningsvorm', *Algemeen Politieblad*, 1999, afl. 13, 8-13.

geplande activiteiten.[116] Minder onschuldig wordt het wanneer criminelen vitale computer- of zelfs energiesystemen als doelwit uitkiezen voor hun terroristische aanslag.[117]

Zo werden Chinese hackers tijdens de NAVO-bombardementen op Joegoslavië in 1999 betrapt bij een inbraak in een NAVO-computer die werd gebruikt voor de logistieke ondersteuning van het luchtoffensief. De computer bevond zich in Nederland. Een rapport van het Amerikaanse Congres waarschuwde in 2.000 voor Chinese hackers en wees op de gevaren van "information-warfare" of "cyberwar". Dit is een generieke term voor een reeks technieken die het mogelijk maken om de vijand op het verkeerde been te zetten of zijn besluitvorming te beïnvloeden. Een specifieke dreiging ontstaat bijvoorbeeld wanneer terroristen infiltreren of spioneren in de computersystemen van de vijand.[118]

In Amerika werd enkele jaren terug door toenmalig president Clinton opdracht gegeven aan het "Presidential Committee on Critical Infrastructure Protection" om na te gaan hoe kwetsbaar de samenleving is voor een eventuele verstoring van de infrastructuren. Opmerkelijk in het onderzoeksrapport van het PCCIP was de vaststelling dat er noch bij de regering, noch bij het bedrijfsleven bewustzijn was voor de veiligheidsproblematiek.[119]

Bij deze eerste categorie behoort tevens het uitlokken van geweld door opruiing. Het Internet biedt een groot aantal mogelijkheden om relschoppers over de hele wereld te bereiken. Hooligans die bijvoorbeeld een bericht plaatsen in een nieuwsgroep of die met elkaar contact houden d.m.v. elektronische post, zijn geen uitzondering maar dagelijkse realiteit.

3.3.2. Delicten die financieel nadeel veroorzaken aan particulieren of bedrijven

3.3.2.1. OPLICHTING

Oplichting is een oud maar populair delict dat met de komst van de virtuele snelweg alleen maar aantrekkelijker is geworden. De anonimiteit is hierbij een belangrijke reden. Doordat men op voorhand de betrouwbaarheid en integriteit van een Internetbedrijf niet kan nagaan, wordt het makkelijk om individuen op te lichten.

---

[116] FURNELL, S., *Cybercrime, Vandalizing the information society*, London, Addison-Wesley, 2002, 253-261.
[117] COLLIN, B.C., 'The future of cyberterrorism: the physical and virtual worlds converge', *Crime and justice international*, 1997, afl. 2, 14-18. Zie ook: POLLITT, M.M., 'Cyberterrorism, fact or fancy?', *Computer Fraud and security*, 1998, afl. 2, 8-10.
[118] STEKETEE, M., (2001/04/04) 'Nieuw Chinees militair zelfvertrouwen' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Nieuws/2001/04/04/Vp/05a.html [28/03/02]
[119] LUIIJF, E., (1999) 'Information warfare: de kwetsbaarheid van de samenleving' [WWW]. TNO Fysisch en Elektronisch Laboratorium: http://www.tno.nl/instit/fel/refs/pub99/io_war.html [28/03/02]

3.3.2.2. "SWEEPSTAKES"

Een populaire techniek zijn de zogenaamde "sweepstakes". Dit zijn loterijen met inleggelden die in hun geheel aan de winnaars worden uitbetaald. In bepaalde gevallen dient een speler vooraf aanbetalingen te doen om deel te kunnen nemen aan een loterij maar van prijzen is er verder nooit sprake…

3.3.2.3. "CRAMMING"

Een andere methode bestaat erin dat bedrijven facturen versturen naar nietsvermoedende consumenten voor diensten die ze nooit besteld hebben. Deze methode wordt ook wel "cramming" genoemd. Ook veelvuldig aan de orde is het frauderen met kredietkaarten. Kredietkaartnummers en identiteitsgegevens zijn immers een makkelijke prooi voor hackers.

3.3.3. Schending van de persoonlijke integriteit en privacy

3.3.3.1. "HACKING"

Het inbreken in computersystemen ("hacking") via het Internet, betekent in vele gevallen een grove aantasting van het recht op privacy. Hackers kunnen kennisnemen van vertrouwelijke bestanden of bepaalde intellectuele werken zonder dat de rechthebbende hier ooit zal van afweten. Inbreuken op de auteursrechten kunnen hier ook gesitueerd worden. Een persoon kan teksten, die hij verkreeg door in te breken in iemands computer, overnemen en zich vervolgens gedragen alsof hij de werkelijke auteur is van de manuscripten. Op deze wijze wordt de integriteit van degene die recht heeft op de auteursrechten aangetast.

3.3.3.2. "CYBERSTALKING"[120]

"Stalking" of "belaging" is een ander flagrant voorbeeld van de schendingen van de privacyrechten. Het woord "stalking" is een oude Engelse jachtterm die duidt op het benaderen van een prooi. Dit kan diverse vormen aannemen. Onder de klassieke gevallen rekent men het achtervolgen of bespieden van een persoon, het voortdurend opbellen, het

[120] VAN EECKE, P., (2001/11/12) 'Cyberstalking' in De Standaard Online [WWW]. De Standaard: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DST12112001_123&trefwoord=stalking [27/03/02]

binnendringen in een huis en het dagelijks versturen van ongewenste liefdesbrieven. Aan dit lijstje kan men ook het lastig vallen via het Internet toevoegen.

In november van vorig jaar werd in de Amerikaanse staat Californië een man schuldig bevonden aan "cyberstalking". Hij had de echtgenoot van een vroegere vriendin belaagd door deze bedreigende e-mails te sturen. De tekst van de laatste e-mail werd ondertekend met "death4u" en luidde "*You are never safe, never. You are always at risk, you fool. Your house could be burned down in the middle of the night.*"

De politiediensten slaagden erin om de stalker op te sporen zodat deze voor de rechter kon worden gebracht. In de Verenigde Staten bestaat er immers specifieke wetgeving die "cyberstalking" strafbaar stelt.

Sinds 1998 heeft België een wet die "stalking" strafbaar stelt. Degene die een persoon belaagt, terwijl hij weet of zou moeten weten dat hij door zijn gedrag de rust van die bewuste persoon ernstig verstoort, doet aan "stalking". De straffen hiervoor kunnen tot twee jaar gevangenis en een fikse geldboete oplopen. De wetgever heeft het begrip "belaging" niet nader omschreven zodat het aan de rechtspractici wordt overgelaten wat er precies mee bedoeld wordt.

De ruime begripsomschrijving laat zeker toe dat het treiteren via het Internet van een persoon als "stalking" beschouwd kan worden. Het is hierbij niet nodig dat er geweld bij te pas komt en belaging blijft ook niet beperkt tot de gevallen van seksuele belaging. Wel moet de rust van het slachtoffer ernstig verstoord worden door het gedrag van de dader. Ook is vereist dat de dader wist of had moeten weten dat de rust van de belaagde persoon ernstig verstoord wordt.

Grosso modo kan men een drietal vormen van "cyberstalking" onderscheiden[121]:

3.3.3.2.1. "E-mail-stalking"

De meest voorkomende vormen van belaging blijven in de fysieke wereld beperkt tot het versturen van ongewenste post, het herhaaldelijk telefoneren of het achtervolgen van het slachtoffer. "Cyberstalking" daarentegen kan verschillende vormen aannemen.[122] Het versturen van ongewenste elektronische post is een vaak voorkomend voorbeeld. Het kan hierbij gaan

[121] OGILVIE, E., 'Cyberstalking' in *Trends and Issues in Crime and Criminal Justice*, Australian Institute of Criminology, 2000, 6 p. (nieuwsbrief).
[122] Zie: CDR, (2000/03/25) 'E-mail stalker terroriseert gezin' [WWW]. De Standaard Online: http://www.destandaard.be/Archief/zoeken/DetailNew.asp?articleID=DST25032000_020&trefwoord=e%2Dmail [01/04/02]

van het versturen van obscene teksten tot echte bedreigingen die per e-mail verzonden worden. Een andere populaire manier bestaat erin dat men het slachtoffer inschrijft op allerlei nieuwsbrieven, vaak van commerciële en/of pornografische aard, zodat deze dagelijks tientallen tot honderden ongewenste berichten te verwerken krijgt. Men spreekt hierbij van "spamming" of "UCE" wat staat voor "Unsolicited Commercial E-mail".[123]

"Mailbombing" behoort ook tot de mogelijkheden. Bij een mailbom worden grote hoeveelheden elektronische postberichten toegestuurd aan het slachtoffer. Meestal hebben deze berichten allemaal dezelfde inhoud en dezelfde afzender.

3.3.3.2.2. "Internet-stalking"

Belaging door het gebruik van e-mail heeft in hoofdzaak een privaat karakter. Het Internet kan echter ook gebruikt worden om aan de belaging een publieke dimensie toe te kennen. Op deze manier krijgt een onbeperkt aantal personen informatie over het privé-leven van het slachtoffer. De gevolgen van de belaging overstijgen het slachtoffer.

3.3.3.2.3. "Computer-stalking"

Bij "computer-stalking" zal de stalker trachten om op allerhande manieren controle te verwerven over de computer van zijn of haar slachtoffer. Het Internet biedt in dit verband ongebreidelde mogelijkheden. Men treft immers her en der op het Web informatie aan over beveiligingslekken in besturingssystemen zodat deze makkelijk kunnen geëxploiteerd worden door personen met malafide bedoelingen.[124] Dit zorgt ervoor dat het een koud kunstje is voor een "cyber-stalker" om een rechtstreekse verbinding te leggen met de computer van het slachtoffer. Telkens het slachtoffer een verbinding maakt met het Internet, krijgt de stalker volledige controle over de computer.

[123] LOUVEAUX, S., *Le Spamming, état de la question*, CRID, Namur, oktober 2000, 1-2. (onderzoekspaper).
[124] X, (1999/07/02) 'Hacker Tool Targets Windows NT' [WWW]. PC World: http://www.pcworld.com/news/article.asp?aid=11662 [31/03/02]

3.3.4. Uitings- en verspreidingsdelicten[125]

Onder verspreidingsdelicten valt een groot aantal strafbare handelingen. Variërend van de verspreiding van schadelijk of illegaal beeldmateriaal zoals kinderporno tot het verspreiden van opruiende teksten. In een groot aantal gevallen gaat het om traditionele delicten die door het Internet alleen nog maar sneller en veel eenvoudiger te plegen zijn.

3.3.5. Economische delicten[126]

Bij economische delicten via Internet kan gedacht worden aan het illegaal gokken of het runnen van illegale casino's. In dit verband kan gewezen worden op het belang van dataprotectie. Aan de spelers van illegale kansspelen op het Web wordt vaak gevraagd naar een resem persoonlijke informatie. Hiervan gaat een reële bedreiging uit wanneer men er mee rekening houdt dat kredietkaartgegevens kunnen gestolen of gekopieerd worden.

Naast de illegale gokparadijzen treft men op Internet ook talrijke manieren aan om criminele gelden wit te wassen. Hierbij wordt vaak gebruik gemaakt van virtuele financiële instellingen die gevestigd zijn op verre, exotische locaties.

3.3.6. Andere delicten

In deze groep kan men een reeks misdrijven onderbrengen die geen verband houden met andere categorieën. Een significant deel van de Internetgemeenschap tracht op allerhande manieren munt te slaan uit het Web door illegale handeltjes op te zetten. Malafide ondernemingen bieden op het "WWW" allerhande goederen aan gaande van vuurwapens en verdovende middelen tot zelfs valse identiteitskaarten en rijbewijzen.

[125] Opmerking: dit type van delicten werd reeds hoger uitvoerig besproken; zie Deel II, Hoofdstuk 2, 2.4. Typologie.
[126] Economische delicten zoals het illegaal gokken op Internet of fenomenen zoals illegale casino's werden eveneens reeds hoger besproken; zie Deel II, Hoofdstuk 2, 2.4. Typologie.

3.4. Prevalentie

3.4.1. PricewaterhouseCoopers[127]

Uit een omvangrijk onderzoek naar fraude in het Europese bedrijfsleven dat door PricewaterhouseCoopers werd uitgevoerd, blijkt dat 42 procent van de 3.400 ondervraagde nationale en multinationale Europese bedrijven en niet-gouvernementele organisaties de voorbije 2 jaar het slachtoffer werd van fraude.

Bedrijven en instellingen maken zich meer zorgen om cybercriminaliteit dan om het even welke andere vorm van fraude. 43 procent van de ondernemingen ziet de digitale informatiesnelweg als de omgeving waar ze in de toekomst het grootste risico op fraude lopen. Ook nu al blijkt 13 procent van de Europese bedrijven de afgelopen 2 jaar slachtoffer te zijn geweest van fraude via het Internet. Klassieke fraudes zijn echter niet verdwenen. De nieuwe technologieën worden benut om gemakkelijker klassieke misdrijven te plegen. De meeste fraudedossiers bereiken de buitenwereld niet, omdat de ondernemingen vrezen dat hen dit negatieve publiciteit bezorgt.

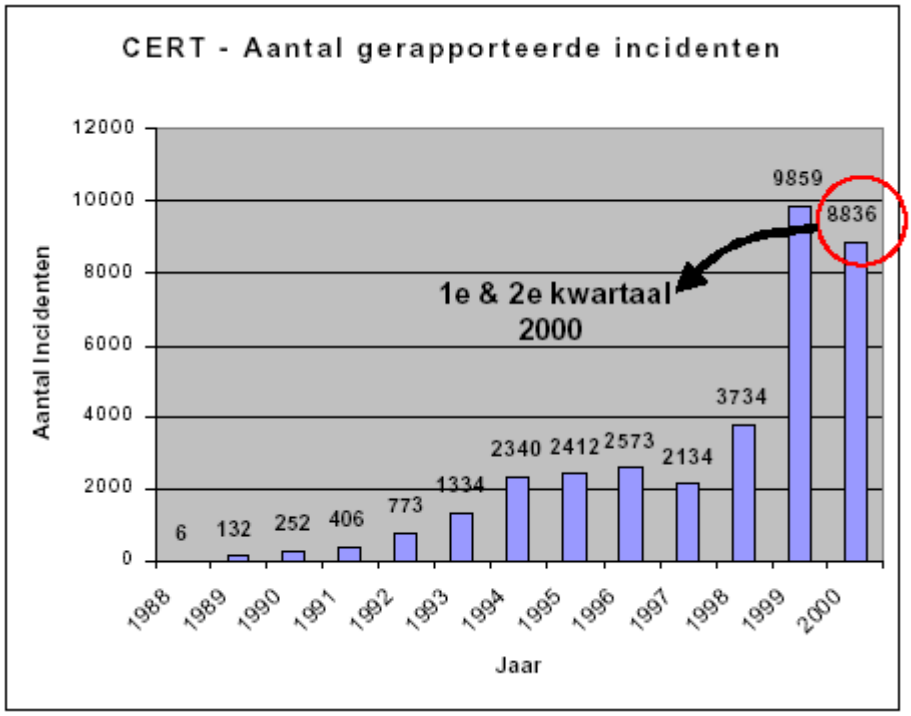
3.4.2. Computer Emergency Response Team Coordination Center (CERT)[128]

Het Amerikaanse "Computer Emergency Response Team Coordination Center" (CERT/CC) waarschuwt gebruikers en beheerders van netwerken al meer dan een decennium voor actuele kwetsbaarheden. CERT is in 1988 naar aanleiding van de "Internet Worm" opgericht. Deze legde in een korte tijd een groot deel van het toen nog beperkte Internet plat. CERT definieert "incident" als "*The act of violating an explicit or implied security policy*".

Voorbeelden van activiteiten die onder deze kwalificatie vallen zijn: de poging om zich zonder toelating de toegang te verschaffen tot een systeem; ongewenste verstoring of "denial-of-service"; ongeautoriseerd gebruik van een systeem; veranderingen aan de systeemhardware of programmatuur zonder tussenkomst van de rechtmatige eigenaar.

[127] PRICEWATERHOUSECOOPERS, *European Economic Crime Survey*, 2001, 18 p. (onderzoeksrapport).
[128] Het CERT beschikt over een eigen website.
Deze is te bereiken op deze URL: http://www.cert.org/nav/index_main.html.

In Grafiek 2 is de toename van het aantal gerapporteerde incidenten sinds de oprichting van CERT afgebeeld.



Grafiek 2: CERT: aantal gerapporteerde incidenten op 1 augustus 2000.
Bron: Eindrapport KWINT Nederland[129]

3.4.3. Internet Fraud Complaint Center (IFCC)

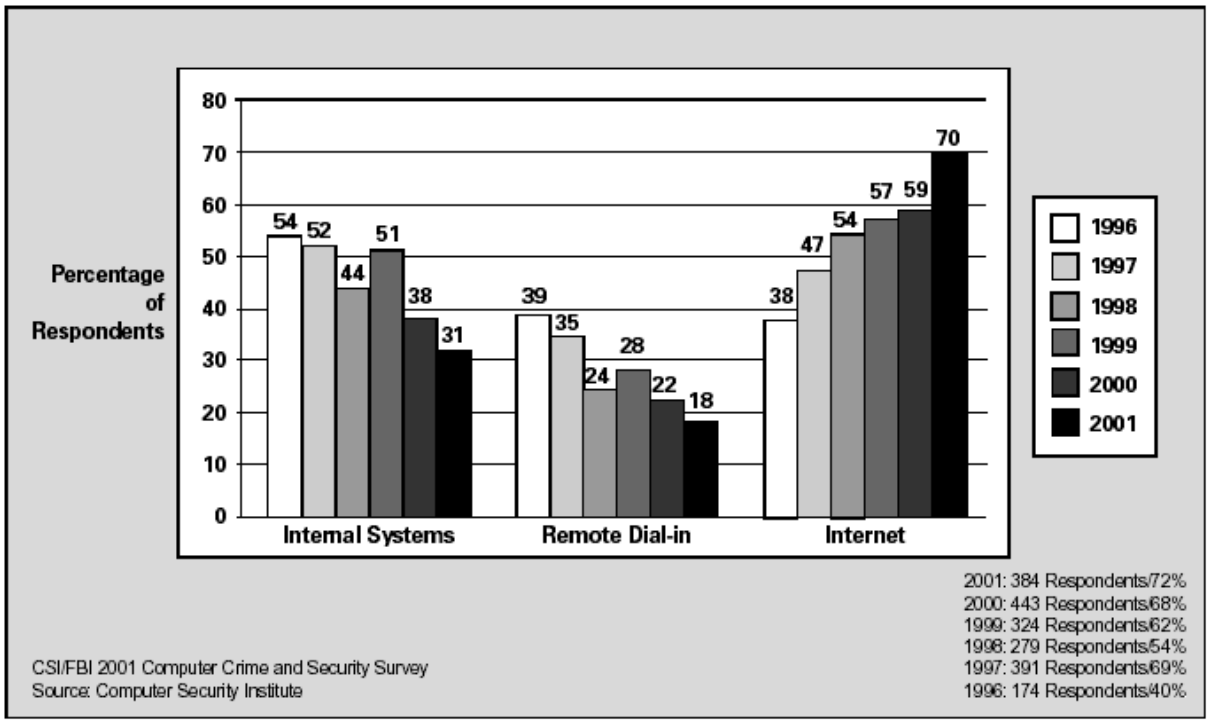
In mei 2000 opende het Amerikaanse "Federal Bureau of Investigation" (FBI) samen met het Ministerie van Justitie het "Internet Fraud Complaint Center". Deze instantie neemt kennis van allerhande vormen van fraude die gepleegd worden via het Internet. Van alle klachten die het IFCC ontving, handelt 48,8 procent over veilingsites. Klachten over fraude op Internet gaan grotendeels over veilingsites, zo blijkt uit onderzoek van de FBI. Het centrum ontvangt wekelijks zo'n 1000 meldingen van ontevreden Internetgebruikers. Na de klachten over veilingsites, is de meest voorkomende klacht het niet geleverd krijgen van bestelde goederen.[130]

[129] MINISTERIE VAN VERKEER EN WATERSTAAT, *Kwetsbaarheid van het Internet*, Stratix Consulting Group, Schiphol, januari 2001, 20-21. (eindrapport).
[130] INTERNET FRAUD COMPLAINT CENTER, *Six-month data trends report*, 2001, 3-4. (onderzoeksrapport).

3.4.4. Computer Security Institute (CSI)

In samenwerking met het "Computer Intrusion Squad" organiseert het "Computer Security Institute" de "Computer Crime and Security Survey".[131] Met dit onderzoek wil men enerzijds zicht krijgen op het fenomeen "computer crime" en anderzijds een bewustzijn inzake "IT security" introduceren.

De Internetconnectie van bedrijven is vaker en vaker het mikpunt van aanvallen van hackers. Bedrijven ervaren elk jaar meer aanvallen op hun systemen via het Internet. In 2000 verklaarde 60 procent van de respondenten dat de Internetverbinding vaak onderhevig is aan allerhande aanvallen van buitenaf. Een jaar later bedroeg dit percentage reeds 70 procent. 91 procent van de respondenten (grote bedrijven) ontdekte de laatste maanden lekken in de beveiliging van het computernetwerk. Meer dan 60 procent ondervond hiervan financieel verlies.



Grafiek 3: CCSI: aanvallen op bedrijfsnetwerken via Internet.
Bron: Computer Crime and Security Survey[132]

[131] COMPUTER SECURITY INSTITUTE, *Computer Crime and Security Survey*, 2001, 4-5. (onderzoeksrapport).
[132] COMPUTER SECURITY INSTITUTE, Computer Crime and Security Survey, 2001, 8-9. (onderzoeksrapport).

DEEL III: Belgische Wet Informaticacriminaliteit

Hoofdstuk 1: Bestraffing van informaticacriminaliteit in België

1.1. Aanloop tot de eerste wetgevende initiatieven

Reeds begin de jaren '90 had de regering de intentie om informaticacriminaliteit te beteugelen. Begrippen zoals valsheid in informatica, informaticabedrog en informaticasabotage kwamen daarbij ter sprake. Het voorontwerp stierf echter een stille dood.[133]

Het duurt tot 1998 vooraleer er sprake was van een tweede ontwerptekst. De Belgische Ministerraad keurde in juli 1998 een voorontwerp van wet goed dat betrekking had op de bestrijding van verschillende vormen van criminaliteit die men aantreft op het Internet. Dit ontwerp had de ambitie om het materieel strafrecht aan te passen. Tevens wou men aan de gerechtelijke instanties een wettelijk kader geven m.b.t. het voeren van onderzoeken in geïnformatiseerde omgevingen. Deze tweede ontwerptekst kwam ook in het gedrang. De regering had immers te kampen met een crisis door de spectaculaire ontsnapping van Dutroux.

Het recentste wetsontwerp inzake informaticacriminaliteit dateert van 3 november 1999. Het werd door de Ministerraad goedgekeurd op 4 oktober 1999. In het ontwerp treft men nieuwe begrippen aan zoals valsheid in informatica, informaticabedrog, ongeoorloofde toegang tot een informaticasysteem en data- en informaticasabotage. Naast dit begrippenkader dat het materiaal strafrecht moet opwaarderen, vinden we tevens nieuwe bepalingen inzake het formeel strafrecht terug. Deze moeten het vooronderzoek in geïnformatiseeerde omgevingen wettelijk regelen. Het betreft o.a. databeslag, netwerkzoeking en de bijzondere medewerkingsverplichting. Ook werden enkele aanpassingen opgenomen van de modaliteiten die van toepassing zijn op de opsporing en onderschepping van telecommunicatie.

België was in de Europese Unie een van de laatste landen die nog geen specifieke wetgeving had uitgevaardigd over informaticacriminaliteit.[134] In het Belgisch Staatsblad van 3 februari 2001 werd de langverwachte *Wet van 20 november 2000 inzake informaticacriminaliteit* gepubliceerd.[135] Deze wet is opgenomen in deze eindverhandeling als Bijlage I.

[133] DE SCHUTTER, B., 'Belgisch voorontwerp van wet inzake informaticacriminaliteit', *computerrecht*, 1990, 208-210.
[134] DROIT ET NOUVELLES TECHNOLOGIES, La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique, 2001, 28 p. (onderzoekspaper).
[135] Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.*, 3 februari 2001.

1.2. Synthese van de materieelrechtelijke en procesrechtelijke implicaties van de Wet Informaticacriminaliteit

1.2.1. Algemeen

We moeten wachten tot 28 november 2000 voor de goedkeuring van de wettekst die informaticacriminaliteit strafbaar stelt. De publicatie volgde op 3 februari 2001. De wetgever wou een aantal concrete stappen nemen om de actoren van de justitie de adequate juridische instrumenten aan te reiken om de crimininaliteit op de informatiesnelweg te kunnen bestrijden.[136] De wet beoogt dus de strafrechtelijke beteugeling van informaticacriminaliteit. Dit begrip is dubbelzinnig en dekt zowel criminele aanvallen tegen computers en netwerken, zoals computerinbraak en de verspreiding van computervirussen, als allerlei soorten van misdrijven waarbij van computers of netwerken gebruik kan worden gemaakt. Men kan hierbij denken aan de verspreiding van kinderpornografie op het Internet, racistische propaganda in nieuwsgroepen of zelfs inbreuken op het auteursrecht of op de privacy (de zogenaamde niet-specifieke informaticamisdrijven).[137]

Vooreerst voert de Wet nieuwe strafbaarstellingen in het Strafwetboek in. Ten tweede wordt voor de gerechtelijke onderzoekers voorzien in een aantal nieuwe bevoegdheden. Deze worden opgenomen in het Wetboek van Strafvordering. Ook werd voorzien in de aanvulling van de Telecomwet.[138]

1.2.2. Overzicht van de nieuwe incriminaties

De nieuwe strafbaarstellingen die ingevoerd werden:

- Valsheid in informatica: dit beoogt de vervalsing van geïnformatiseerde gegevens te bestraffen, inzoverre deze gegevens een juridische draagkracht hebben.

- Informaticabedrog: deze incriminatie beoogt de vervalsing van geïnformatiseerde gegevens met het bijzonder opzet een vermogensvoordeel te verkrijgen te bestraffen.

[136] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 3-4.
[137] GOOSSENS, F., 'De wet inzake Informaticacriminaliteit', *Tijdschrift voor Wetgeving*, 2001, 94-99.
[138] Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991.

- Hacking: hieronder begrijpt de wetgever het inbreken in een systeem of het overschrijden van de toegangsbevoegdheden die men in een systeem heeft. Opmerkelijk is dat in het eerste geval een algemeen opzet volstaat en dat in het tweede geval een bijzonder opzet vereist is.

- Informaticasabotage: hierbij wordt opzettelijke schade aan data en schade aan systemen strafbaar gesteld.

1.2.3. Overzicht van de strafprocesrechtelijke wijzigingen

Op het gebied van het strafprocesrecht zijn deze nieuwe bevoegdheden van toepassing:

- Databeslag: de beslagregeling wordt uitgebreid tot elektronische data en bestanden, zodat niet steeds meer de materiële dragers moeten in beslag genomen worden.

- Netwerkzoeking: dit is een nieuwe vorm van zoeking die wordt geïntroduceerd. Bij deze zoeking verkrijgen de onderzoekers het recht om actief op een netwerk te gaan zoeken.

- Medewerkingsplicht: In bepaalde gevallen ontbreekt het de onderzoekers aan de nodige technische kennis. Door de medewerkingsplicht kunnen speurders een beroep doen op deskundigen die wel over de nodige specifieke technische bagage beschikken.

- Wijzigingen aan de tapmaatregel: de bestaande wettelijke regeling inzake het aftappen van telecommunicatie wordt gewijzigd. Het toepassingsgebied wordt uitgebreid. Tevens wordt een specifieke medewerkingsplicht ingevoerd voor de tapmaatregel.

1.2.4. Aanvulling van de Telecomwet[139]

Het derde deel van de Wet Informaticacriminaliteit voorziet in de bewaringsplicht van oproep- en identificatiegegevens voor operatoren en dienstverstrekkers.

In de hiernavolgende hoofdstukken wordt dieper ingegaan op de nieuwe strafbaarstellingen alsook op het nieuwe instrumentarium dat ter beschikking staat van de gerechtelijke diensten om informaticacriminaliteit op te sporen en te bestraffen. Ook staan we stil bij het derde deel van de Wet Informaticacriminaliteit, namelijk de aanvulling van de Telecomwet.

[139] Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991.

Hoofdstuk 2: Bespreking van de nieuwe incriminaties

2.1. Inleidende kritische beschouwingen

In het algemeen kan men enkele bemerkingen maken i.v.m. de nieuwe strafbaarstellingen die werden ingevoerd door de Wet Informaticacriminaliteit.

Poging van deze nieuwe misdrijven wordt steevast strafbaar gesteld. Enkel in het geval van sabotage, wordt de poging niet strafbaar gesteld. Ook wordt er voor recidive van informaticagebonden misdrijven steeds voorzien in een specifiek regime. Herhaling geeft aanleiding tot de verdubbeling van de straffen.

Een andere interessante bemerking is de vaststelling dat de wetgever bewust zo weinig mogelijk definities heeft gegeven van nieuwe begrippen in de wet zelf. Hiermee wou men vermijden dat bepaalde concepten en termen snel achterhaald zouden worden door de realiteit. De gehanteerde terminologie beoogt technologie-neutraal te zijn. In de voorbereidende werkzaamheden kan men wel een precisering terugvinden van de gehanteerde termen.[140]

De ruime begripsomschrijvingen heeft in een aantal gevallen voor kritiek gezorgd. De Raad van State stelde dat het legaliteitsbeginsel werd geschonden door de ruime omschrijvingen die werden gegeven aan de strafbare feiten.[141]

M.i. is een ruime omschrijving van de begrippen de enige juiste oplossing indien men ervoor wil zorgen dat nieuwe technologische evoluties in de toekomst ook onder de toepassing zullen vallen van de huidige Wet Informaticacriminaliteit. Het is immers niet ondenkbaar dat de technologische vooruitgang ook snel zal zorgen voor nieuwe types van delicten die zich zullen afspelen op het Internet. Indien de wetgever opteerde voor een strikte definiëring van het gehanteerde begrippenkader, dan zou het voor het Openbaar Ministerie, samen met de gerechtelijke opsporingsdiensten, niet evident zijn om nieuwe ICT-delicten onder de toepassing te laten vallen van de incriminaties die werden ingevoerd door de Wet Informaticacriminaliteit.

[140] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 12-13.
[141] LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 3-4.

2.2. Valsheid in informatica – art. 210bis Sw.

Art. 210 Sw. bestraft de gedraging van het vervalsen van juridisch relevante elektronische gegevens. De bestaande bepalingen van het Strafwetboek omtrent valsheid in geschrifte (art 193-197 Sw.) voldeden immers niet voor de strafbaarstelling van gedragingen waarbij elektronische gegevens die juridisch relevante informatie bevatten, vervalst worden.

Valsheid in informatica betreft bijvoorbeeld handelingen zoals het namaken of vervalsen van kredietkaarten en elektronisch opgemaakte contracten.

Het belangrijkste knelpunt is zonder twijfel de onzekerheid omtrent de kwalificatie van elektronische gegevens als geschrift. Data kunnen bijvoorbeeld ook spraak en beeld voorstellen, die als dusdanig niet onder de delictsomschrijving van schriftvervalsing vallen.[142]

Als elektronische gegevens door het gebruik van informatica gewijzigd worden en hierdoor ook de juridische draagwijdte verandert van de gegevens, dan kan een gevangenisstraf opgelegd worden van 6 maanden tot 5 jaar en/of een geldboete van 26 Euro tot 10.000 Euro. Bijzonder opzet is hierbij geen vereiste.

De juridische draagwijdte van de data dient gewijzigd te zijn, dit is een vereiste door de Wet gesteld. Een specifiek nadeel moet zich dus effectief gerealiseerd hebben. Of de data de facto een juridische draagwijdte hebben, is een feitenkwestie die door de rechter ten gronde moet worden beoordeeld.[143]

Poging tot het plegen van valsheid in informatica is strafbaar gesteld. In geval van recidive voorziet de Wet een streng regime. De reden hiervoor ligt in het feit dat dergelijke delicten op een vrij eenvoudige wijze kunnen gerealiseerd worden en vrij moeilijk op te sporen zijn.

2.3. Informaticabedrog – art. 504quater Sw.

De nieuwe incriminatie informaticabedrog stelt gegevensmanipulatie met het oogmerk voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel te verwerven, evenals de realisatie van dit oogmerk, strafbaar.

---

[142] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.

[143] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 13-14.

Vaak gebeurt het manipuleren van elektronische gegevens met het doel een onrechtmatig voordeel te bekomen. Verschillend met diefstal is dat men bij deze handeling geen zaken ontvreemdt maar deze op vrijwillige wijze laat overhandigen door het gebruik van bedrieglijke handelingen. Men kan daarbij denken aan het inbrengen van fictieve namen in een bestand of het wijzigen van bepaalde gegevens.

2.3.1. Informaticabedrog versus klassieke oplichting

De gedragingen die hoger geschetst werden, vertonen een nauw verband met de strafrechtelijke handeling van oplichting zoals deze omschreven is door de wetgever in art. 495 Sw. Bij oplichting zijn de wettelijke bestanddelen in de eerste plaats het doel om zich een zaak toe te eigenen die aan een ander toebehoort en vervolgens de afgifte van gelden, roerende goederen, verbintenissen, kwijtingen of schuldbevrijdingen. Bovendien moet deze afgifte veroorzaakt zijn door het gebruik van bedrieglijke middelen.

De rechtsleer is niet eenduidig m.b.t. de kwalificatie "oplichting" bij misdrijven waar de computer gebruikt wordt om zich een vermogensvoordeel toe te eigenen. De manipulatie van de computer heeft het zich doen afgeven van geld tot doel. Het feit dat deze afgifte geschiedt d.m.v. overschrijving van geld, levert geen moeilijkheid op. In de rechtspraak wordt namelijk de inschrijving van een som geld op de creditzijde van een rekening gelijkgesteld met het verkrijgen van een roerend goed. Het misdrijf van oplichting vereist dus geen materiële overhandiging. Het wijzigen of vervalsen van computergegevens kunnen dan als "listige kunstgrepen" beschouwd worden. Het spreekt voor zich dat de interpretatie door de rechter hierbij een belangrijke speelt. De toekomst zal dus ongetwijfeld meer duidelijkheid brengen.[144]

Het nieuwe art. 504quater Sw. bestraft diegene die voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwerft door elektronische gegevens in een informaticasysteem in te voeren, te wijzigen, te wissen of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem te wijzigen ("datamanipulatie"). Een bijzonder opzet (bedrog) is hierbij vereist.

De wetgever bepaalde de straffen als volgt: gevangenisstraf van 6 maanden tot 5 jaar en/of geldboete van 26 Euro tot 100.000 Euro. Poging wordt ook bestraft. Eveneens werd voorzien in een bijzonder regime voor herhaling.

[144] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.

In de Memorie van toelichting van het Wetsontwerp inzake Informaticacriminaliteit vinden we enkele voorbeelden terug die geviseerd worden door de nieuwe bepaling: het gebruik van een gestolen kredietkaart om geld uit een automatische biljettenverdeler te halen[145], het onrechtmatig overschrijden van het krediet van zijn eigen kredietkaart en het met winstbejag verduisteren van bestanden of programma's die men voor een welbepaald doel toevertrouwd heeft verkregen.[146]

2.3.2. Orange-zaak

In deze context kan ook een recent voorbeeld uit de prakijk vermeld worden. Op woensdag 7 maart 2001 raakte bekend dat telefoonoperator Orange[147] een grootschalige fraude met zijn "pre-pay"-kaarten had ontdekt. Malafide gebruikers waren erin geslaagd om door middel van het invoeren van een bijzondere code gratis te telefoneren. De code raakte op korte termijn sterk verspreid zodat er duchtig gebruik werd van gemaakt.[148]

Door het art. 504quater Sw. toe te passen op dit voorbeeld, kan men tot een aantal vaststellingen komen. De invoer van de code in het informaticasysteem van Orange valt onder het toepassingsgebied van art. 504 quater Sw. Bovendien kan al wie gebruik heeft gemaakt van deze code hiervoor bestraft worden. De personen die de code hebben doorgespeeld aan andere gebruikers, kunnen voor deze feiten bestraft worden. Het betreft een vermogensvoordeel voor derden. Al wie de code heeft trachten in te voeren maar hier echter niet is in gelukt omwille van de beperkte tijdspanne, is strafbaar. Poging van informaticabedrog werd immers ook strafbaar gesteld.

[145] Door een extensieve interpretatie door de rechtspraak werd deze handeling als diefstal door middel van valse sleutels gekwalificeerd. Het verdient aanbeveling om voor de vervolging ervan beroep te doen op het misdrijf "Informaticabedrog".
[146] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 14-15.
[147] Recent wijzigde de telecomoperator "Orange" de naam naar "Base".
[148] LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 26-27.

2.4. "Hacking" – art. 550bis Sw.

Eén van de belangrijkste artikels uit de Wet Informaticacriminaliteit is zonder twijfel art. 550 bis Sw. dat computerinbraak of "hacking" strafbaar stelt. Het door de nieuwe bepaling beschermde rechtsbelang, is op de eerste plaats de integriteit van het systeem. Dankzij dit artikel zal het niet meer nodig zijn dat de rechtspraak overgaat tot zeer gewaagde interpretaties om hacking te kunnen bestraffen.

2.4.1. De zaak "Redattack"[149]

In de Zaak "Redattack" werd de beklaagde ten laste gelegd met opzet kennis te hebben genomen van klantenbestanden van Internetprovider Skynet.[150] Ook was de hacker op de hoogte van een aantal betalingstransacties die uitgevoerd werden door klanten van Fortis Bank. Via verschillende media had "Redattack" deze gegevens wereldkundig gemaakt. De hacker bekende dat hij via de identificatiegegevens van een klant van Skynet alle klantinformatie had gekopieerd om vervolgens deze gegevens door te sturen naar een dertigtal bestemmelingen van de pers. Vervolgens zou hij deze informatie vernietigd hebben en deze nooit meer gebruikt hebben of medegedeeld hebben aan derden.

De beklaagde, Frans Devaere, werd veroordeeld op grond van art. 109 ter D, al. 1,3° van de Telecomwet.[151] De correctionele rechtbank te Gent oordeelde dat de beklaagde "vrijwillig", d.w.z. "wetens en willens" kennis heeft genomen van de geregistreerde klantenbestanden wetende dat hij niet beschikte over de toelating van de betrokken klanten. De beklaagde werd ook veroordeeld wegens het kenbaar maken aan derden van het paswoord van een Skynet-klant via verschillende media.[152]

Deze uitspraak illustreert welke kronkels de rechters dienden te gebruiken om een fenomeen als computerinbraak te bestraffen voordat er sprake was van de Wet Informaticacriminaliteit.

---

[149] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.
[150] LEFELON, P. en VAN AUDENAERDE, A., (1999/08/11) 'Internetpiraat kraakt Skynet' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=dss9908110011&trefwoord=redattack [10/04/2002]
[151] Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991.
[152] Corr. Gent, 11 december 2000, [WWW] Recht en Informatica, Universiteit Gent: http://allserv.rug.ac.be/~rdecorte/documenten/Rechtspraak/2000_12_11_Redattack.pdf [10/04/02]

2.4.2. Nieuw artikel 550bis Sw.

Inzake hacking wordt een onderscheid gemaakt tussen aantastingen van buiten het systeem ("externe hacking" : art. 550bis §1 Sw.) en aantastingen door gebruikers die bepaalde toegangsbevoegdheden hebben ("interne hacking door insiders" : art. 550bis §2 Sw.).

2.4.2.1. EXTERNE HACKING

Onder "externe hacking" kan men het elektronisch inbreken in een systeem begrijpen. In het geval iemand binnendringt in een netwerk waarbinnen hij geen enkele bevoegdheid heeft, volstaat een algemeen opzet als moreel element om deze handeling strafbaar te stellen. Voor wie onopzettelijk een netwerk binnendringt, is dezelfde straf voorzien indien men het netwerk niet onmiddellijk verlaat zodra men zich ervan bewust wordt dat men zich onrechtmatig in een netwerk bevindt. Men spreekt in dit laatste geval van "handhaven" in het netwerk.

De ratio legis voor de strafbaarstelling van externe hacking is dat de loutere transgressie door derden de veiligheid van een netwerk in gevaar brengt. Hacking moet dan ook beschouwd worden als een gevaarzettingsdelict dat als zodanig strafwaardig is, ongeacht de bijzondere kwaadwillige bedoelingen of de gerealiseerde effecten.[153]

De eis dat een beveiligingssysteem werd doorbroken, is niet als constitutief element voor de strafbaarstelling gehanteerd. Deze eis zou immers een aantal complicaties met zich zou hebben meegebracht. Men zou bijvoorbeeld een niveau van beveiliging moeten vastleggen.[154]

Externe hacking wordt bestraft met een gevangenisstraf van 3 maanden tot een jaar en/of een geldboete van 26 Euro tot 25.000 Euro. In geval van bedrieglijk opzet wordt dit 6 maanden tot 2 jaar en/of een geldboete van 26 Euro tot 25.000 Euro.

2.4.2.2. INTERNE HACKING

Met "interne hacking" wordt het overschrijden van de toegangsbevoegdheden die men heeft, bedoeld. De wetgever vereist hier een bijzonder opzet. De verklaring ligt in het feit dat wie zich in een netwerk bevindt waartoe hij bevoegd is, veel sneller die bevoegheid zal

[153] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 17-18.
[154] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.

overschijden. Om te vermijden dat alle vormen van overschrijding van bevoegdheden strafbaar zouden worden, heeft de wetgever ervoor gekozen om een bijzonder opzet als minimale strafbare drempel te voorzien.

Voorbereidende handelingen, poging, aanzetting en heling worden bij hacking afzonderlijk strafbaar gesteld. Aanzetting tot hacking wordt zelfs zwaarder bestraft dan de hacking zelf. De wetgever verklaart deze kronkel door het voorbeeld te geven van delinquente groeperingen die misbruik maken van naïeve computerfreaks om in te breken in computersystemen. De facto komt het er op neer dat de opdrachtgever strenger gestraft wordt dan de uitvoerder.[155]

Interne hacking wordt bestraft met een vrijheidsberovende straf van 6 maanden tot 2 jaar en/of een geldboete van 26 Euro tot 25.000 Euro.

2.4.2.3. "HACKERTOOLS"

De nieuwe wet voert een strafbaarstelling in voor een aantal handelingen die in sommige gevallen het eigenlijke hacken voorafgaan. Het *met bedrieglijk opzet of met het oogmerk om te schaden* opsporen, verzamelen, ter beschikking stellen, verspreiden of verhandelen van technische middelen om te hacken, wordt strafbaar gesteld ingevolge het art. 550bis §5 Sw.

Hierbij wordt in de eerste plaats de handel in 'hackertools'[156] en de toegangscodezwendel geviseerd. De wet vereist evenwel niet dat voor het ter beschikking stellen van deze technische middelen enige beloning zou voorzien zijn: het louter ter beschikking stellen om niet volstaat.

Om te vermijden dat de toepassing van dit artikel een hinderpaal zou kunnen vormen voor de vrije verspreiding van algemene informatie wordt een *bijzonder opzet* vereist[157]. Het zal bovendien aan de rechtspraak behoren om uit te maken of een eenvoudige verwijzing in een webpagina naar een vindplaats van dergelijke hackertools onder de strafbare gedraging valt.

De wetgever legt een straf op van 6 maanden tot 3 jaar en/of een geldboete van 26 Euro tot 100.000 Euro.

---

[155] LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 4-5.
[156] Een hackertool is software die speciaal werd ontwikkeld om onder meer codes te kraken of fouten in software te misbruiken en hackers aldus in staat te stellen zich een toegang tot informaticasystemen te verschaffen.
[157] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 17-18.

2.5. Informaticasabotage – art. 550quater Sw.

2.5.1. Sabotage van gegevens

Het nieuwe art. 550ter Sw. beoogt, net als het art. 550bis Sw. inzake "hacking", een tevoren bestaande lacune in het strafrecht in te vullen. Vernielingen en beschadigingen werden traditioneel in het strafrecht enkel in aanmerking genomen wanneer ze betrekking hadden op tastbare voorwerpen. Dit zou het geval geweest zijn wanneer hardware zou zijn getroffen. Door de nieuwe bepalingen wordt ook de vernieling of beschadiging, "*met het oogmerk om te schaden*", van gegevens strafbaar gesteld.

Een bijzonder opzet is dus vereist: hierdoor wordt vermeden dat de commercialisering van data of programma's waarvan een legitieme aanwending mogelijk is, maar die eventueel misbruikt zouden kunnen worden, in het algemeen zou worden verboden.[158]

Art. 550ter §1 Sw. viseert elke manipulatie van gegevens "*met het oogmerk om te schaden*". Hieronder wordt verstaan: het rechtstreeks of onrechtstreeks invoeren, wijzigen, wissen van gegevens in een informaticasysteem, of het veranderen met enig ander technologisch middel van de mogelijke aanwending van gegevens in een informaticasysteem. De wet voorziet een vrijheidsberovende straf van 6 maanden tot 3 jaar en/of een geldboete van 26 Euro tot 25.000 Euro. Indien de sabotage ook schade als gevolg heeft, voorziet de wetgever een gevangenisstraf van 6 maanden tot 5 jaar en/of een geldboete van 26 Euro tot 75.000 Euro.

2.5.2. Belemmering van de correcte werking van systemen

De wetgever koos er ook voor om de belemmering van de correcte werking van een informaticasysteem afzonderlijk strafbaar te stellen. De Memorie van Toelichting vermeldt in dit verband dat in de praktijk schade aan data en schade aan het computersysteem zelf vaak samen zullen voorkomen en technisch niet altijd strikt te scheiden zijn. Niettemin heeft de wetgever het wenselijk gevonden een juridisch onderscheid te maken tussen de gevolgen voor de data en voor een informaticasysteem.[159]

Gezien het belang dat informaticasystemen in onze samenleving innemen, wordt het belemmeren, geheel of gedeeltelijk, van de correcte werking van een informaticasysteem (art.

[158] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.
[159] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.

550ter §3 Sw.) zwaarder bestraft dan het louter berokkenen van schade aan data (art. 550ter §2 Sw.). De vrijheidsberovende straf werd bepaald op 1 jaar tot 5 jaar. Daarnaast kan een geldboete opgelegd worden van 26 Euro tot 100.000 Euro.

Uit een antwoord van de Minister op een vraag van een lid van de Commissie voor de Justitie van de Senaat in dit verband kan blijken dat het art. 550ter §3 Sw. ook van toepassing zou zijn op het massaal versturen van e-mails die het systeem van de geadresseerde blokkeren, waardoor de correcte werking van een computersysteem wordt verhinderd.[160]

2.5.3. Ontwikkeling en verspreiding van schadelijke gegevens

De nieuwe wet voorziet een strafbaarstelling inzake bepaalde handelingen die kwaadwillige manipulaties van gegevens en de gevolgen die daaruit voortvloeien voor informaticasystemen, kunnen voorafgaan. Hierbij is gedacht aan de ontwikkeling en de verspreiding van schadelijke gegevens en computerprogramma's zoals virussen (art. 550ter §4 Sw.).

Vele gevallen zijn bekend van virussen die op korte tijd wereldwijd schade toebrachten aan gegevens of zelfs aan het systeem zelf. Het beruchte "I love you"-virus beschadigde vooral geluids- en beelddocumenten. Het virus zelf werd maar actief zodra het aangehechte document aan de liefdesbrief-mail, met de boodschap "I Love You", werd geopend.[161]

De wetgever heeft een *bijzonder opzet* voorzien bij de strafbaarstelling van degene die gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, ontwerpt, ter beschikking stelt, verspreidt of verhandelt, terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of om, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren.[162] De wet voorziet een vrijheidsberovende straf van 1 jaar tot 5 jaar en/of een geldboete van 26 Euro tot 100.000 Euro.

[160] Verslag namens de Commissie voor de Justitie, *Belgische Senaat*, 28 juni 2000, 2 – 392/3, p 81 - 82.
[161] Boon, P., (200/05/05) 'Virus vermomt zich als liefdesbrief' [WWW]. De Standaard Online: http://www.standaard.be/nieuws/economie/detail.asp?articleID=DST05052000_045&Doctype=detail.asp [15/04/02]
[162] De vereiste van het bijzonder opzet dient te vermijden dat de commercialisering van data of programma's waarvan een legitieme aanwending mogelijk is, maar die evenwel ook misbruikt kunnen worden, in het algemeen zou worden verboden.

Hoofdstuk 3: Strafprocesrechtelijke implicaties

De Wet Informaticacriminaliteit brengt ook enkele wijzigingen teweeg op het vlak van het strafprocesrecht. Deze worden hieronder besproken.

3.1. Databeslag – art. 39bis Sv.

3.1.1. Kopiëren van bestanden

Art. 39bis Sv. zorgt voor een uitbreiding van de beslagregeling tot elektronische data en bestanden zodat niet meer steeds de materiële dragers in beslag moeten worden genomen. Er bestaat dus nu de mogelijkheid om enkel een kopie van de bestanden te maken op dragers van de Overheid (art. 39bis § 2 Sv.). Enkel in geval van dringendheid of om technische redenen[163] kunnen dragers worden gebruikt die ter beschikking staan van personen die gerechtigd zijn het informaticasysteem te gebruiken (art. 39bis § 4 Sv.).

3.1.2. Verhinderen van de toegang tot gegevens

Indien het kopiëren van data niet mogelijk blijkt omwille van technische redenen of wegens de omvang van de te kopiëren gegevens, dan wendt de procureur des Konings of de onderzoeksrechter passende technische middelen[164] aan om de toegang tot de gegevens te verhinderen en hun integriteit te waarborgen.[165]

3.1.3. Vernietiging van gegevens

Indien de Procureur des Konings van oordeel is dat de gegevens die worden aangetroffen, strijdig zijn met de openbare orde of de goede zeden, dan kan hij de vernietiging bevelen van deze gegevens.[166]

---

[163] Bijvoorbeeld wanneer de geschikte gegevensdragers niet aanwezig zijn voor de hardwareconfiguratie waarvan de gegevens dienen te worden onderzocht.
[164] De algemene formulering "passende technische middelen" werd doelbewust gekozen: gezien het vluchtige karakter van informaticagegevens, leek het de wetgever wenselijk om de specifieke maatregelen die de Procureur des Konings dient aan te wenden niet technisch te beschrijven. Deze formulering maakt het mogelijk dat de "passende middelen" de ontwikkeling van de technologie volgen.
[165] Dergelijke procedure betekent zoveel als de elektronische variant van de verzegeling .
[166] LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 6-7.

3.1.4. Bewaring door aanwending van gepaste technische middelen

Op de Procureur des Konings of de Onderzoeksrechter rust de verplichting om de integriteit en de vertrouwelijkheid van gegevens te waarborgen, door de aanwending van de passende technische middelen (art. 39bis § 6, 1e lid Sv.). Verder dienen "gepaste technische middelen" te worden aangewend voor de bewaring ter griffie van gegevens of van gegevens die samen met hun drager in beslag zijn genomen (art. 39bis § 6, 2e en 3e lid Sv.).

De notie "gepaste technische middelen" wordt in dit verband verder uitgewerkt in de Memorie van Toelichting : *"Het gaat om technische middelen, en derhalve is de aard daarvan afhankelijk van de stand van de technologie, evenals van de specifieke vereisten van de data. Deze middelen hebben als zodanig geen effect op de bewijswaarde van de data, maar betreffen de modaliteiten van de onttrekking of bewaring van de data, waardoor nodeloze bewijsbetwistingen voor de rechter kunnen worden voorkomen. Bovendien gaat het hier om een wettelijke vereiste met het oog op het beschermen van het bewijsmateriaal; deze bestaat zelfs niet in het gemeen recht, en werd ingevoegd omwille van de eigenheid van de geïnformatiseerde omgeving".*[167]

3.2. Netwerkzoeking – art. 88ter Sv.

Door invoeging van art. 88ter Sv. wordt een nieuwe wijze van zoeking geïntroduceerd die niet noodzakelijk gekoppeld is aan de huiszoeking.[168] Op deze manier wou men de onderzoekers de mogelijkheid gunnen om zoekingen uit te voeren op mobiele netwerken.

3.2.1. Hackende speurders?

Door de techniek "netwerkzoeking" krijgen speurders het recht om op actieve wijze een netwerk te doorzoeken op voorwaarde en inzoverre dat de persoon naar wie het onderzoek wordt gevoerd, gebruik mocht maken van het netwerk. De onderzoekers krijgen dus zelf *geen* toestemming om te hacken. Bovendien moet het gaan om een netwerk waartoe de verdachte een bijzondere toegang had. Men kan dus als speurder niet ongebreideld gaan zoeken op een open netwerk zoals het Internet.

[167] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 21-22.
[168] Verslag namens de Commissie, *Kamer van Volksvertegenwoordigers*, 19 oktober 2000, DOC 50 0213/011, p.8.

3.2.2. Grensoverschrijdende zoekingen: quid "hot pursuit"?

Kenmerkend voor informaticasystemen is dat ze meer en meer verbonden zijn in netwerken. Recente technologische evoluties zorgen er bovendien voor dat het aantal internationale netwerken snel toeneemt. Wanneer informaticasystemen zich op verschillende locaties bevinden, zijn derhalve meerdere bevelen tot huiszoeking of inbeslagneming vereist.

Het is duidelijk dat een dergelijke benadering problematisch is. Niet alleen bestaat het risico dat bij niet gelijktijdig optreden bewijsmateriaal verloren gaat, maar bovendien zal in veel gevallen niet a priori vastgesteld kunnen worden op welke plaatsen de zoeking moet plaatsvinden, welke bestanden relevant zijn, of waar de computers geografisch gesitueerd zijn.

Om hieraan te verhelpen bepaalt het nieuwe artikel de voorwaarden waarin de uitbreiding van de zoeking in een informaticasysteem naar elders gesitueerde systemen toegelaten is. Hierbij moet het gaan om onderling verbonden systemen.

Door de internationale verwevenheid van netwerken bestaat de kans dat er tijdens een netwerkzoeking bestanden geconsulteerd worden die zich in het buitenland situeren. De wetgever is zich hiervan bewust geweest, en heeft, in afwachting dat op internationaal vlak oplossingen worden gevonden inzake opsporingen en onderzoek in een IT-context, geopteerd voor een voorzichtige en pragmatische oplossing:

De wetgever stelt dat de grensoverschrijdende zoeking *niet* als regel kan worden aanvaard. Er kunnen immers ernstige problemen rijzen, wanneer de gerechtelijke overheden van een staat eenzijdig en welbewust een netwerkzoeking uitbreiden naar het buitenland zonder de bevoegde buitenlandse autoriteiten hierin te kennen. Indien voldoende tijd en kennis voorhanden is, moet de weg van de klassieke internationale rogatoire commissies worden gevolgd.[169]

Wanneer kunnen gegevens die resulteren uit grensoverschrijdende zoekingen toch gebruikt worden door de politiediensten? De wetgever was hier onduidelijk en onvolledig. Als de buitenlandse gegevens op een *toevallige* of *onopzettelijke* manier bekomen werden, sluit de wetgever deze gegevens niet *a priori* uit als bewijsmateriaal. Bovendien moet het optreden

[169] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.

van de politiediensten ter goeder trouw gebeurd zijn.[170] De Memorie van Toelichting schijnt nog een geval van *"hot pursuit"* te aanvaarden waarbij het nemen van voorlopige maatregelen toegelaten wordt in spoedeisende gevallen om de teloorgang van het bewijsmateriaal te vrijwaren: *"Men denke hier bijvoorbeeld aan het geval waar tijdens de zoeking wordt vastgesteld dat de relevante files zich op een welbepaalde plaats in het buitenland bevinden. Het stopzetten van de zoeking en het instellen van een internationale rogatoire commissie om ter plekke een huiszoeking te laten uitvoeren biedt de betrokkenen alle mogelijkheden om via de telecommunicatiekanalen ondertussen de data zelf te laten verdwijnen" .*[171]

Het spreekt voor zich dat deze regeling vatbaar is voor interpretatie. Hoe toont men immers aan dat gegevens "toevallig" of op een "onopzettelijke" manier bekomen werden? Deze regeling illustreert dat er geen consensus was m.b.t. deze materie bij de totstandkoming van de wet.

Art. 88ter, § 3, 2e lid van het Wetboek van Strafvordering bepaalt dat de gegevens die per toeval of onopzettelijk uit het buitenland werden bekomen, enkel worden gekopieerd, en dit om de teloorgang van het bewijsmateriaal te verhinderen. De toegang tot deze buitenlandse gegevens kan, in tegenstelling tot bij het gewone databeslag, niet worden verhinderd; evenmin kunnen ze worden geblokkeerd of gewist. De wetgever heeft in deze gevallen voorzien dat de bevoegde overheid van de betrokken Staat op de hoogte dient te worden gebracht. De ratio legis hiervan is dat de betrokken Staat een standpunt moet kunnen innemen m.b.t. het feit of er al dan niet een inbreuk op de rechtsorde werd gemaakt.

3.2.3. Rechtsmacht bij de afwikkeling van delicten gepleegd via Internet

De strafrechtelijke handhaving van delicten die gepleegd werden via het Internet, vergt een kordaat en snel optreden. Telecommunicatie houdt immers niet op aan de landsgrenzen. Eindeloos vertakte netwerken werken deze internationalisatie verder in de hand. De gebruikelijke rechtshulpprocedures zijn m.i. niet soepel en snel genoeg om adequaat te kunnen optreden. Er dient dus gezocht te worden naar betere oplossingen. De kronkels die de Belgische wetgever maakt m.b.t. "netwerkzoeking" illustreren deze nood.[172]

Bij misdrijven die gepleegd worden door het gebruik (of misbruik) van het Internet is in vele gevallen ook sprake van een opeenstapeling van verschillende rechtsmachten. Meerdere landen

[170] Verslag namens de Commissie voor de Justitie, *Belgisch Senaat*, 28 juni 2000, 2 – 392/3, p. 78.
[171] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 25-26.
[172] Zie hoger: 3.2.2. Grensoverschrijdende zoekingen: quid "hot pursuit".

hebben dus een aanknopingspunt om bepaalde feiten te kunnen vervolgen. Aangezien een strafbare handeling op Internet vaak rechtsgevolgen kan hebben in andere landen, hebben deze landen er belang bij om hun rechtsmacht te kunnen uitoefenen ten aanzien van deze delicten.

Het territorialiteitsbeginsel brengt de facto niet altijd soelaas. Zo kan men zich in bepaalde gevallen terecht de vraag stellen waar een bepaalde handeling werkelijk plaatsvindt. Zo groeit bij grote bedrijven meer en meer de trend om gebruik te maken van ingewikkelde, internationaal vertakte netwerkinfrastructuren. Gevoelige informatie wordt daarbij dikwijls bewaard op servers in verre landen. Dit brengt met zich mee dat onderzoekers die opsporingen verrichten in een computernetwerk vaak niet weten op welke plaats de informatie bewaard wordt waartoe ze zich de toegang hebben verschaft.

De gevolgen hiervan zijn niet te overzien. Speurders kunnen door het louter onderzoeken van netwerken een inbreuk plegen op de grondrechten van een andere staat. In de meeste gevallen is de derde lidstaat niet eens op de hoogte van de inbreuk waardoor ze geen waarborgen kan eisen. Dit toont m.i. in ieder geval aan dat de strafrechtelijke territorialiteit met de grootste omzichtigheid moet benaderd worden.

Toch durf ik te stellen dat het beginsel van de territorialiteit aan belang en kracht zal moeten inboeten. In ieder geval staat m.i. vast dat de principes inzake territorialiteit niet onverminderd kunnen blijven gelden. Het is immers absurd om zoekingen die plaatsvinden op netwerken te beperken tot het Belgisch grondgebied. De effectiviteit van deze zoekingen is immers quasi nihil, gezien bedrijven - niet altijd met bonafide bedoelingen- vaak informatie stockeren op buitenlandse servers.

Er ontstaat nl. in vele gevallen een soort samenloop van rechtsmacht. Dit vergt adequate strafrechtelijke samenwerkingsmodaliteiten.

Waar ligt dan eigenlijk de oplossing? Naar mijn mening moet met volle verwachting worden uitgekeken naar een harmonisatie van de regelgeving. Hierdoor zullen veel rechtsmachtproblemen kunnen vermeden worden. Interstatelijke verschillen zullen echter onvermijdelijk altijd blijven bestaan.

Men moet een afweging maken tussen de belangen van de nationale staat enerzijds en de baten die grensoverschrijdende zoekingen met zich meebrengen anderzijds. Het is van belang dat zoekingen in internationale context verbonden worden aan de naleving van strikte

voorwaarden. Deze moeten zorgen voor de rechtsbescherming van de integriteit en soevereiniteit van de nationale staten.

3.3. Medewerkingsplicht – art. 88quater Sv.

Het art. 88quater Sv. creëert de mogelijkheid om personen die het te onderzoeken informaticasysteem kennen of over een bijzondere expertise beschikken inzake bepaalde aspecten daarvan (bijvoorbeeld inzake beveiliging of cryptografie) te verplichten bijstand te verlenen aan de gerechtelijke overheden door mee te werken aan de bewijsgaring. De wetgever zag zich genoodzaakt deze bepaling in te voeren om een effectief onderzoek mogelijk te maken in een snel evoluerende hoogtechnologische context, waarbij de overheid vaak zelf niet over voldoende expertise beschikt of waar deskundigen weinig beschikbaar zijn. In dit opzicht worden verplichtingen opgelegd aan personen[173] om hun bijstand te verlenen.[174]

Men kan twee categorieën deskundigen onderscheiden, nl. diegenen met een bijzondere kennis van het informaticasysteem in kwestie en diegenen die om hun technische kennis gevraagd worden om het systeem te bedienen maar die geen specifieke band hebben met het informaticasysteem in kwestie. [175]

De verplichting om mee te werken kan niet opgelegd worden aan de verdachte zelf en diens naaste familieleden. Anderen riskeren zware bestraffen indien ze de medewerking weigeren. Dit kan ongetwijfeld tot moeilijke situaties aanleiding geven, gezien het bij de aanvang van een onderzoek niet steeds duidelijk is wie de mogelijke verdachten in de zaak kunnen zijn.

[173] De personen die in de beide gevallen kunnen worden gevorderd, worden in de wet niet nominatim omschreven. Het kan derhalve gaan om importeurs of verdelers van computers of software, dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt, beveiligingsspecialisten, enz.
[174] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 25-26.
[175] LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 6-7.

Hoofdstuk 4: Aanvulling van de Telecomwet

4.1. Inleidend

Het derde deel van de Wet Informaticacriminaliteit voorziet in de bewaringsplicht van oproep- en identificatiegegevens voor operatoren en dienstverstrekkers. De artt. 11, 12 en 13 van de Wet beogen een aanpassing van de modaliteiten van het regime van het gerechtelijk onderscheppen van telecommunicatie. In die zin werden aan de artt. 90ter, 90quater en 90 septies van het Wetboek van Strafvordering wijzigingen aangebracht. Tot op heden werden echter nog steeds geen uitvoeringsmaatregelen genomen door de koning.

4.2. Uitbreiding van de lijst misdrijven waar een tapmaatregel mogelijk is

In het art. 90ter Sv. wordt de bestaande lijst inzake het aftappen van telecommunicatie uitgebreid met de nieuwe misdrijven die door de Wet Informaticacriminaliteit worden ingevoerd. Het betreft valsheid in informatica (art. 210bis Sw.), informaticabedrog (art. 504quater Sw.), hacking (art. 550bis Sw.) en informaticasabotage (art. 550ter Sw.). De ratio legis hiervan is dat anders het opsporen van deze misdrijven waarbij in de praktijk veelal telecommunicatie wordt benut, sterk zou worden bemoeilijkt.[176]

4.3. Bijzondere medewerkingverplichting

De bijzondere medewerkingverplichting die is ingevoerd met het nieuwe art. 88quater Sv., wordt ook ingevoerd inzake het onderscheppen van telecommunicatie, en dit ten aanzien van personen waarvan de onderzoeksrechter vermoedt dat ze een bijzondere kennis hebben van de telecommunicatiedienst. Deze verplichting dient te worden onderscheiden van de medewerkingverplichting die berust op de operatoren van een communicatienetwerk of de verstrekker van een telecommunicatiedienst – art. 90quater §2 Sv.). De verplichting betreft immers zowel het verlenen van inlichtingen als het zelf toegankelijk maken van de telecommunicatie (art 90quater §4 Sv.).

Het onderscheid in strafmaat tussen de operatoren en verstrekkers van de telecommunicatiedienst bij de weigering tot medewerking (art. 90quater §2, 3e lid Sv.) en de

[176] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 28- 29.

nieuwe categorie van de tot medewerking verplichte personen (art. 90quater §4, 3e lid Sv.) wordt verklaard in de Memorie van Toelichting. Daarin wordt gesteld dat door de omstandigheid, de operatoren en dienstenverstrekkers de institutionele medespelers zijn van de overheid in de problematiek van interceptie. Hierdoor kan men van hen meer goodwill verwachten.[177]

4.4. Opname-, beveiligings-, vertalings- en bewaringstechnologieën[178]

In het art. 90septies Sv.werd een nieuw lid ingevoegd tussen het vierde en het vijfde lid. Deze nieuwe bepaling strekt ertoe de voorhanden zijnde beveiligings- en versleutelingstechnieken aan te wenden om de vertrouwelijkheid en de integriteit van het bekomen tapmateriaal (dat meer en meer digitaal zal worden) te waarborgen, met inbegrip van de bewaringsmodaliteiten op de griffie. Volgens de Memorie van Toelichting kan hierbij meer bepaald worden gedacht aan de mogelijkheden die de digitale handtekening biedt.

Naar de toekomst toe voorziet de nieuwe bepaling ook reeds de mogelijkheden inzake gedigitaliseerde transcriptie en vertaling.

4.5. Verplichtingen van de dienstenverstrekkers

In art. 109ter, E, van de Telecomwet[179] zijn door de Wet Informaticacriminaliteit een aantal wijzigingen aangebracht. Deze maken het mogelijk dat de verplichtingen kunnen worden gepreciseerd voor de telecomoperatoren en verstrekkers van telecommunicatiediensten inzake de registratie en bewaring van oproep- en identificatiegegevens van de gebruikers van telecommunicatiediensten. De ratio legis hiervan is het opvangen van de problemen die rijzen bij moderne vormen van telecommunicatie en bij nieuwe media, zoals het Internet, waarbij het eenvoudig is om op anonieme wijze gebruik te maken van de netwerken.

De Memorie van Toelichting vermeldt: *"In dit verband zullen de verstrekkers van telecommunicatiediensten structurele maatregelen moeten nemen om enerzijds de oproepgegevens (oorsprong, bestemming, lokalisatie duur, …) van telecommunicatie te kunnen achterhalen, en anderzijds de gebruikers die informatie aan het publiek aanbieden, te kunnen identificeren, en*

[177] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.
[178] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 29-30.
[179] Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991.

deze inlichtingen te bewaren. Het betreft derhalve zowel gegevens die betrekking hebben op privé-telecommunicatie als op openbare communicatie".[180]

4.5.1. De kwalificatie "oproepgegevens"

Het begrip "oproepgegevens" werd gebruikt omdat niet louter met de klassieke telefoonnummers wordt gewerkt. De wetgever wou ook Internetadresssen aan deze bepaling onderhevig maken. In eerste instantie worden de verbindingen tussen de gebruiker en de Internetproviders geviseerd. Toch kan het in bepaalde gevallen voor de magistraat nodig zijn om precies na te kunnen gaan welke Internetadressen werden bezocht.

4.5.2. Gegevens betreffende het Internetverkeer

4.5.2.1. INHOUD REGISTER

Het register behoort niet automatisch de gegevens te bevatten over de door de netwerkgebruiker geraadpleegde internetsites. Nochtans laat de bepaling toe dat de Koning maatregelen uitvaardigt om bijvoorbeeld Internetproviders te verplichten om bepaalde informatie te bewaren in uitzonderlijke gevallen en in functie van de technologie.[181]

4.5.2.2. TERMIJN

De termijn waarbinnen de oproepgegevens en de identificatiegegevens dienen te worden bewaard, mag nooit minder zijn dan 12 maanden. De bewaringsplicht voor de operatoren van telecommunicatienetwerken en de verstrekkers van de telecommunicatiediensten moet worden uitgevoerd binnen de grenzen van de Europese Unie. De nieuwe paragraaf 3 van het art. 109ter, E, voorziet de strafrechtelijke sancties bij het niet-nakomen van deze verplichtingen .

4.5.2.3. KRITISCHE NOOT

De bewaartermijn, die voor de operatoren een grote economische kost betekent, is het voorwerp geweest van veel lobbywerk, zowel van de kant van de operatoren als van de kant van de politiediensten. De politiediensten wensen een zo lang mogelijke termijn, zodat ze

[180] Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, Memorie van toelichting, 3 november 1999, 29-30.
[181] COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.

ondanks hun achterstand in hun opzoekingen toch nog tijdig de vereiste gegevens kunnen opvragen, terwijl de operatoren liever de termijn zo kort mogelijk houden om op deze manier de economische kost beperkt te houden.[182]

Van belang is te vermelden dat de bewaartermijn die wordt opgelegd, veel verder gaat dan wat in de andere Europese landen is voorzien. Slechts weinige landen hebben op dit ogenblik reeds een termijn geïncorporeerd in hun wetgeving. In de landen waar er wel sprake is van een bewaartermijn, zoals in Nederland en Duitsland, heeft men een termijn van 3 maanden ingevoerd. Deze werd met succes reeds toegepast.

Op Europees vlak merkt men een harmonisatiebeweging wat betreft de bewaartermijnen. In dit kader kan verwezen worden naar de "Aanbeveling 3/99 over de bewaring van verkeersgegevens door Internetdienstenaanbieders voor wetshandhavingsdoeleinden".[183] Deze aanbeveling werd uitgewerkt door de "Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens" en stelt een termijn voor van maximum 3 maanden. Hoewel de tekst werd uitgewerkt voor de aanbieders van Internetdiensten, is deze redenering vanzelfsprekend ook voor telecomoperatoren van belang.

Een andere reden die kan pleiten voor een verkorting van de bewaartermijn, houdt verband met de investeringskosten die operatoren zullen moeten dragen om te kunnen voldoen aan de gestelde eisen. De facto worden de gegevens in de praktijk momenteel slechts voor een periode van 3 tot 6 maanden bijgehouden. Een uitbreiding van deze termijn naar 12 maanden zal ongetwijfeld de kosten aanzienlijk de hoogte in jagen.

De praktijk zal m.i. moeten uitwijzen of de meerkost die de wettelijke bewaartermijn van 12 maanden met zich meebrengt, kan verantwoord worden vanuit het oogpunt van het forensisch onderzoek van deze bewaarde gegevens.

4.6. Korte evaluatie Wet Informaticacriminaliteit

Tot voor de inwerkingtreding van de Wet van 28 november 2000 was België één van de laatste landen van de Europese Unie waar nog geen specifieke regelgeving inzake informaticacriminaliteit uitgevaardigd was. De wettelijke bepalingen inzake de beteugeling van "cybercrime", kwamen tot stand in de context van de bewustwording van de ontwikkeling van

[182] LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 7-8.
[183] Working Party on the Protection of Individuals to the Processing of Personal Data, Recommendation No. 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, adopted on 7 september 1999, *Brussels*, 1999.

de informatietechnologie en van de steeds meer ingrijpende invloed die deze evolutie heeft op de wijze waarop de samenleving zich ontplooit. Deze invloed uit zich ook in het strafrecht. De ervaring leert dat nieuwe technologieën een criminaliteitsbevorderend potentieel in zich dragen.

De wetgever maakte van de strafrechtelijke bescherming van netwerken een prioriteit. Dit is niet verwonderlijk gezien zowel de overheid, bedrijven als particulieren steeds meer afhankelijk worden van de adequate werking van ingewikkelde netwerkstructuren. Computers zijn immers zelden nog van het type "stand alone".

De hoger geschetste "Bistel"-zaak[184], samen met de recente acties van de hacker "Redattack" hebben m.i. de creatie van de Wet Informaticacriminaliteit gewettigd. Het geavanceerde en snel wijzigende karakter van de informatietechnologie wordt immers niet altijd aangewend met bonafide bedoelingen. Dat de strafwetgeving terzake in het verleden onaangepast was, werd hierboven geschetst. De creatieve rechtspraak die herhaaldelijk aangewend werd in het nabije verleden, leidde ertoe dat men bepaalde individuen toch kon veroordelen. Wel zal iedere aandachtige toehoorder zich de vraag stellen of deze rechtspraak nog binnen de grenzen van het legaliteitsbeginsel kan gesitueerd worden. Met de nieuwe wet heeft men getracht om hieraan te remediëren.

Het is echter nog te vroeg om na te gaan of alle interpretatieproblemen van de baan zijn. De toekomst zal dit moeten uitwijzen. Wat de nieuwe zoekmogelijkheden betreft die in het Wetboek van Strafvordering ingelast werden, dient alleszins de nodige voorzichtigheid aan de dag gelegd te worden. Zoals hoger reeds werd geschetst[185], zal de netwerkzoeking mogelijks voor problemen zorgen. Omwille van het internationale karakter van het Internet, is de kans dat men tijdens netwerkzoekingen inbreuken pleegt op de soevereniteit van andere landen niet ondenkbaar.

[184] Zie daarvoor 2.1.2. De "Bistel"-zaak.
[185] Zie 3.2.3. Rechtsmacht bij delicten gepleegd via het Internet.

Hoofdstuk 5: Bestraffing van verwante misdrijven

5.1. Inleiding en verantwoording

In de voorgaande hoofdstukken van dit Deel III werd uitvoerig aandacht besteed aan enkele nieuwe strafbaarstellingen inzake informaticacriminaliteit. Ook kwamen enkele strafprocesrechtelijke nieuwigheden aan bod.

Toch zijn er nog enkele verwante misdrijven die niet uitdrukkelijk vermeld werden in de Belgische Wet Informaticacriminaliteit[186] maar die wel het voorwerp uitmaken van bestraffing. Deze misdrijven kwamen reeds aan bod in Deel II waar een typologie geschetst werd van enerzijds specifieke en a-specifieke vormen van informaticacriminaliteit en anderzijds "cybercrime". De nadruk in Deel II lag echter niet op de bestraffing van computercriminaliteit maar eerder op het geven van een overzicht van alle mogelijke vormen van "cybercrime".

In dit hoofdstuk wordt daarentegen wel in het bijzonder aandacht besteed aan de bestraffing van deze aanverwante misdrijven.

5.2. Bestraffing van pornografie

Men kan zich de vraag stellen of de huidige wetgeving voldoet om de verspreiding van illegale pornografie via het Internet en andere communicatiemiddelen te bestraffen. Hierbij kan men een onderscheid maken tussen pornografisch materiaal in het algemeen, kinderpornografie en reclame voor seksuele diensten.

5.2.1. DE VERSPREIDING VAN ONZEDELIJK MATERIAAL

Op dit moment wordt de verspreiding van pornografisch materiaal als openbare zedenschennis bestraft door artikel 383 Sw. Wanneer de openbare zedenschennis gebeurt in aanwezigheid van minderjarigen voorzien de artikelen 386 en 386bis Sw. in een strengere bestraffing. Artikel 383 Sw. bestraft onder meer het tentoonstellen, verkopen, verspreiden en het in voorraad hebben van liederen, vlugschriften, afbeeldingen of prenten, die strijdig zijn met de goede zeden.

[186] Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.*, 3 februari 2001.

Artikel 386 Sw. verzwaart de straffen als de misdrijven van artikel 383 tegenover minderjarigen worden gepleegd.

Met deze bepalingen stelt de wet elke vorm van openbare schennis van de goede zeden strafbaar, ongeacht of dit gebeurt door middel van gedrukte publicaties, prenten of afbeeldingen of via audiovisuele middelen. Bovendien stelt de wet geen bijzondere opzetvereiste: het wetens en willens verspreiden van zedenschendend materiaal volstaat.

Men kan er echter vanuit gaan dat de bepalingen van artikel 383 van de Strafwet perfect toepasbaar zijn op nieuwe vormen van pornografieverspreiding. Derhalve zal de persoon die via een computernetwerk pornografisch materiaal tentoonstelt of verspreidt dus strafbaar zijn, zelfs indien dit gratis gebeurt, zonder winstoogmerk. De verkoop van pornografisch materiaal wordt in elk geval strafbaar gesteld, ook wanneer dit via computernetwerken gebeurt.

Aangezien de wet een zekere openbaarheid vereist, lijkt het via elektronische post verzenden van pornografisch materiaal naar een correspondent niet onder de kwalificatie te vallen. Het gaat hier immers om privé – correspondentie. Evenmin is het louter bezitten van pornografisch materiaal op elektronische of optische bestanden strafbaar, tenzij deze met het oog op de handel of de verspreiding wordt bijgehouden.

Indien het pornografisch materiaal wordt vertoond aan minderjarigen voorzien de artikelen 386 en 386bis in een zwaardere bestraffing. Men kan zich afvragen of dit bij communicatie over computernetwerken niet altijd het geval is. Iedereen heeft immers toegang tot het Internet, ongeacht de leeftijd. Het feit dat een waarschuwing de plaatjes voorafgaat waarbij uitdrukkelijk vermeld wordt dat het gaat om materiaal dat niet geschikt is voor minderjarigen, doet in het Belgische recht niet ter zake.[187]

5.2.2. KINDERPORNOGRAFIE

Bij Wet van 13 april 1995[188] werd een artikel 383bis in het Strafwetboek ingevoegd waardoor kinderpornografie strafbaar wordt gesteld. Kinderpornografie onderscheidt zich van de gewone pornografie op grond van het criterium van de leeftijd van 16 jaar. Het is hierbij irrelevant of de minderjarigen daadwerkelijk betrokken zijn of dat het beeld deze leeftijd enkel zou oproepen.

[187] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.
[188] Wet van 13 april 1995 houdende bepalingen tot bestrijding van de mensenhandel en van de kinderpornografie, *B.S.*, 25 april 1995.

Niet alleen het tentoonstellen, verkopen, verhuren, verspreiden en overhandigen, maar tevens het bezit en het vervaardigen van kinderporno wordt strafbaar gesteld. De verspreiding van kinderpornografie via een computernetwerk zoals het posten van kinderpornografisch materiaal in een nieuwsgroep, kan dus gestraft worden op basis van de huidige wetgeving. Tevens valt het bezit op harde schijf of enig ander elektronisch of optisch medium onder de ruime bepalingen van deze wet.

5.2.3. RECLAME OP HET INTERNET VOOR SEKSUELE DIENSTEN

Op dit moment wordt de reclame voor seksuele diensten bestraft door artikel 380quinquies Sw.,ingevoegd bij Wet van 27 maart 1995[189]. Dit artikel is technologie – onafhankelijk geformuleerd en legt nergens de voorwaarde van de openbaarheid op. Bijgevolg is het perfect toepasbaar op alle vormen van reclame op het Internet.

De eerste paragraaf van artikel 380quinquies is gericht op de bestraffing van reclame voor een aanbod van seksuele diensten dat specifiek gericht is op minderjarigen, of dat gewag maakt van seksuele diensten aangeboden door minderjarigen.

De tweede paragraaf bestraft al wie reclame maakt voor seksuele diensten die worden verleend via één of ander telecommunicatiemiddel. Deze bepaling was oorspronkelijk ingevoegd ter bestraffing van reclame voor zgn. sekslijnen. Zij kan echter ook gebruikt worden ter bestraffing van reclame voor Internetseks. Het aanbieden van seksuele diensten op het Internet zelf, zoals live video en audio, lijkt niet strafbaar te zijn. De derde paragraaf bestraft vooral reclame voor zogenaamd sekstoerisme of reclame waarachter vrouwen – en kinderhandel schuilgaat.

5.3. Bestraffing van de aanranding van de eer of de goede naam van personen

Aanranding van de eer of de goede naam van personen is een vergrijp dat wordt bestraft door artikel 443-444 van het Strafwetboek. Door het gebruik van de nieuwe telecommunicatiemiddelen kan deze delictsvorm echter veel ingrijpender gevolgen hebben. Het is immers typisch aan het Internetgebruik dat een enorm grote gemeenschap kan bereikt worden zonder dat daarbij enige selectie van informatie gebeurt.

[189] Wet van 27 maart 1995 tot invoeging in het Strafwetboek van een artikel 380quinquies en tot opheffing van het artikel 380quater, tweede lid, van hetzelfde Wetboek, *B.S.*, 25 april 1995.

Artikel 443 Sw. bestraft het ten laste leggen van een bepaald feit aan een persoon, dat zijn eer kan krenken of hem aan de openbare verachting kan blootstellen, zonder dat het bewijs van dit feit kan of mag worden bewezen. Een bijzonder opzet (kwaadwillig) is vereist.

Artikel 444 Sw. voorziet in een strafverzwaring, wanner deze tenlasteleggingen gebeuren in openbare bijeenkomsten of plaatsen, in tegenwoordigheid van verscheidene personen, in tegenwoordigheid van de beledigde en voor getuigen, door geschriften, (al dan niet gedrukt), prenten of zinnebeelden, die aangeplakt, verspreid of verkocht, te koop geboden of openlijk tentoongesteld worden, of door geschriften, die niet openbaar gemaakt, maar aan verscheiden personen toegestuurd of meegedeeld worden.

Een strafbaarstelling van de aanranding van de eer of de goede naam van personen via moderne telecommunicatietechnieken lijkt mogelijk te zijn op basis van de huidige bepalingen van het strafrecht. Zo kan het plaatsen van lasterlijke berichten op een "bulletin board" beschouwd worden als een openbare bijeenkomst of plaats.[190]

Het uitwisselen van lasterlijke berichten via "Internet Relay Chat" (IRC) kan vallen onder de tweede omstandigheid namelijk "*in tegenwoordigheid van verschillende personen, in een plaats die niet openbaar is, maar toegankelijk voor een aantal personen die het recht hebben te vergaderen of ze te bezoeken*".

Lasterlijke of beledigende informatie die men op zijn persoonlijke homepage zet, lijkt te vallen onder de vierde omstandigheid: "*geschriften, al dan niet gedrukt, door prenten of zinnebeelden, die (…) openlijk tentoon gesteld worden*". Ook het verzenden van laster door het gebruik van verzendlijsten lijkt strafbaar. Deze kunnen immers gekwalificeerd worden als " *geschriften, die niet openbaar gemaakt, maar aan verscheidene personen toegestuurd of meegedeeld worden*".

Een ander fenomeen is het verzenden van "hate mail" waarbij een bepaalde persoon elektronische berichten krijgt met beledigende inhoud. Zulke gedragingen kunnen niet bestraft worden op basis van de voorafgaande artikelen omdat niet aan de voorwaarde van openbaarheid voldaan is. Artikel 561, 7° Sw. zou hier echter in een strafbaarstelling kunnen voorzien. Het zal nochtans moeilijk zijn om de misdrijven te vervolgen gezien er vaak gebruik wordt gemaakt van "anonymous remailers". Dit zijn computerprogramma's die alvorens het bericht door te zenden, de identificatiestrook van het elektronische bericht wegmaken. Ook

[190] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.

hanteren Internetgebruikers vaak een pseudoniem. Tenzij de internet service provider verplicht wordt de ware naam kenbaar te maken, is het niet mogelijk de identiteit van de dader te kennen.

5.4. Bestraffing van racistische uitingen en ontkenning van genocide

Computernetwerken worden als medium gehanteerd om racistisch of revisionistisch materiaal te verspreiden. De webpages bevatten daarbij informatie die verboden is in België op basis van de Anti – racismewet[191] en de Wet op de ontkenning van de genocide.[192]

5.4.1. RACISME EN XENOFOBIE

Uitingen en publicaties die aanzetten tot discriminatie en vreemdelingenhaat worden bestraft op basis van de Anti – racismewet. De wet stelt niet alleen verschillende vormen van racisme en discriminatie strafbaar, maar ook openbare uitingen van racisme, en de medewerking aan organisaties of groepen die in het openbaar aanzetten tot racisme. Niet alleen het openbaar ministerie of het slachtoffer, maar ook instellingen van openbaar nut en bepaalde verenigingen kunnen de strafvordering instellen.

Het in het openbaar beledigen van personen omwille van bepaalde kenmerken als afkomst, huidskleur of nationaliteit is niet strafbaar op basis van deze wet. De bepalingen omtrent de aanranding van de eer of de goede naam van personen (met name art.448 en 561, 7° Sw. m.b.t. beledigingen) voorzien evenwel reeds in een strafbaarstelling. Ook de verspreiding van racistisch materieel via audiovisuele media wordt op diverse manieren aan banden gelegd.

5.4.2. ONTKENNING VAN GENOCIDE

De Genocidewet[193] bestraft *"hij die onder eender welke omstandigheden, bepaald bij artikel 444 van het Strafwetboek, de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal – socialistische regime is gepleegd, ontkend,schromelijk minimaliseert, poogt te rechtvaardigen of*

[191] Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, *B.S.*, 8 augustus 1981. Deze Wet werd gewijzigd op 12 april 1994 (*B.S.*, 14 mei 1994) en 7 mei 1999 (*M.B.*, 25 juli 1999).
[192] Wet van 23 maart 1995 tot bestraffing van het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistische regime is gepleegd, *B.S.*, 30 maart 1995.
[193] Wet van 23 maart 1995 tot bestraffing van het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistische regime is gepleegd, *B.S.*, 30 maart 1995.

goedkeurt met een gevangenisstraf van acht dagen tot één jaar en met een geldboete van zesentwintig Euro tot vijfduizend Euro."

Problematisch evenwel, is dat de informatie zich meestal op een server bevindt die niet in België gelegen is maar in een land, zoals in de V.S., waar zulke uitingen volstrekt legaal zijn. In deze gevallen moet men zich de vraag stellen of degene die dit illegaal materiaal vanuit België beschikbaar maakt, gestraft kan worden. Men kan moeilijk aannemen dat het verzenden van illegaal materiaal vanuit België naar de server in het buitenland op zich een openbaarmaking is. De uitingen gebeuren dus niet onder de voorwaarden zoals bepaald in artikel 444 Sw.

5.5. Bestraffing van het aanzetten tot crimineel gedrag

Sinds geruime tijd is er via het Internet informatie verkrijgbaar over zaken die in onze maatschappij niet geaccepteerd worden. Zo vindt men bijvoorbeeld websites over het vervaardigen van springtuigen en het uitvoeren van aanslagen. Buiten de reeds besproken bepalingen omtrent onzedelijk gedrag, racisme en laster bestaat er momenteel geen specifieke wetgeving omtrent de verspreiding en/of het bezit van ongeoorloofd materiaal.

5.6. Bestraffing van gokken

In België is het uitbaten van een gokgelegenheid verboden, tenzij in expliciet benoemde plaatsen. Via het Internet is het echter mogelijk vanuit België te gokken in een of ander legaal of illegaal gokpaleis ergens op de wereld.

Een nieuwe Belgische Wet op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers werd op 30 december 1999 gepubliceerd in het Belgisch Staatsblad[194]. De wet huldigt een dubbel principe: enerzijds blijft de uitbating van de kansspelen verboden, anderzijds is het mogelijk een vergunning te bekomen om een kansspel uit te baten maar dit moet beschouwd worden als een voorrecht.

Vooreerst waagt de wet zich aan enkele positieve en negatieve definities. Opvallend hierbij is dat het begrip "kansspel" ruim wordt omschreven. Bij een verboden kansspel had volgens de vroegere rechtspraak van het Hof van Cassatie het toeval steeds de bovenhand op de

[194] Wet op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, *B.S.*, 30 december 1999.

lichamelijke of verstandelijke behendigheid. De huidige regeling stelt echter dat toeval zelfs een bijkomstig element mag zijn.[195]

Een belangrijk onderdeel van de wet voorziet in maatregelen ter bescherming van spelers en gokkers. Vooreerst verbiedt men aan bepaalde categorieën van personen de toegang tot de speelzalen of de deelname aan de spelen: personen jonger dan 21 jaar (casino's en lunaparken) of minderjarigen (drankgelegenheden), magistraten, notarissen, deurwaarders, leden van de politiediensten buiten de uitoefening van hun functies, …

Wie binnen het grondgebied van België de mogelijkheid biedt om online te gokken is strafbaar op basis van het huidige regime. Het gaat dan uiteraard niet om een casinogebouw. De persoon die via een website of via elektronische post een kansspel uitbaat, waarbij betaald wordt met echt geld, kan bestraft worden op basis van bestaande kansspelwetgeving. Helaas worden de meeste kansspelen op het Internet niet vanop het Belgisch grondgebied aangeboden. Tegen dit fenomeen staat de wetgever voorlopig zo goed als machteloos.

5.7. Bestraffing van namaking

Kwaadwillige of bedrieglijke inbreuken op het auteursrecht en de naburige rechten worden bestraft met geldboetes van 100 tot 100.000 Euro door de artikelen 80 en 81 van de Wet betreffende het auteursrecht en de naburige rechten van 30 juni 1994[196]. Dezelfde straffen gelden voor het verkopen, verhuren, te koop of te huur stellen, in voorraad hebben voor de verkoop of de verhuur of het in België invoeren voor commerciële doeleinden van voorwerpen waarvan men weet dat ze zijn nagemaakt.

In tegenstelling tot de nieuwe wet inzake informaticacriminaliteit[197], kunnen geen vrijheidsberovende straffen worden opgelegd. Wanneer het misdrijf van namaking echter plaatsvindt in een IT – context, zal het vaak samengaan met een nieuw informaticamisdrijf, zoals bijvoorbeeld de ongeoorloofde toegang tot een informaticasysteem.

[195] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.
[196] Wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, *B.S.*, 27 juli 1994.
[197] Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.*, 3 februari 2001.

Deel IV: Europese initiatieven

Hoofdstuk 1: Overzicht van internationale initiatieven

1.1. Inleiding en verantwoording

De informatie-infrastructuur is een cruciale schakel geworden in de ruggengraat van onze samenleving. Gebruikers moeten ervan kunnen uitgaan dat informatiediensten beschikbaar zijn en dat gegevens beschermd worden tegen toegang door onbevoegden. De technologie van de informatiemaatschappij kan worden gebruikt voor het plegen en vergemakkelijken van strafbare feiten.

Computercriminaliteit en de bestrijding ervan krijgt daarom steeds meer aandacht, ook in internationale fora. Dit leidde de laatste jaren tot verschillende initiatieven die uitgaan van uiteenlopende werkgroepen en internationale organisaties. Op verschillende niveaus is het besef gegroeid dat men de handen in elkaar moet slaan om op een adequate wijze alle mogelijke vormen van "cybercrime" te kunnen beteugelen.

☞ In deze eindverhandeling is het onmogelijk om een allesomvattend overzicht te presenteren van alle maatregelen en initiatieven die wereldwijd genomen werden om "cybercrime" in te dijken. Ik koos ervoor om in dit hoofdstuk een overzicht te geven van enkele initiatieven die door internationale organisaties werden genomen. Het is geenszins de bedoeling om een exhaustieve opsomming te geven. Toch wil ik de lezer erop wijzen dat op verschillende niveaus het fenomeen "cybercrime" bestudeerd wordt.

In het tweede en laatste hoofdstuk van dit deel, wordt aandacht besteed aan de initiatieven die door de Raad van Europa genomen werden om computercriminaliteit te bestrijden. De recente Cybercrime-Convention komt tevens aan bod in Hoofdstuk 2.

1.2. Nationale en internationale reacties

Computercriminaliteit speelt zich overal in "cyberspace" af en houdt niet op bij de conventionele landsgrenzen. Op nationaal niveau ontbreekt het m.i. vaak nog aan breed en internationaal geörienteerde antwoorden op nieuwe problemen zoals netwerkbeveiliging en computergerelateerde misdrijven. In de meeste landen zijn de reacties op informaticacriminaliteit immers nog te veel gericht op het nationale recht.

Ondanks de inspanningen van internationale en supranationale organisaties vertonen de nationale wetgevingen wereldwijd opmerkelijke verschillen en onduidelijkheden. Deze verschillen houden o.a. verband met de bepalingen inzake privacy-schendingen, de bevoegdheden van opsporingsdiensten en de jurisdictie ten aanzien van grensoverschrijdende incidenten.

Op internationaal niveau bestaat brede overeenstemming over het feit dat doeltreffend moet worden gereageerd tegen computercriminaliteit. Organisaties zoals de Verenigde Naties, de "Organisation for Economic Co-operation and Development", de G8, de Raad van Europa, de Europese Unie, Europol en ongetwijfeld nog andere, hebben in dit verband gemeenschappelijke objectieven en belangen. Ze hebben alle het fenomeen "cybercrime" uitvoerig bestudeerd. Daarnaast hebben ze instrumenten aangereikt die de ontwikkeling van een strikt wettelijk kader ter bestraffing van computercriminaliteit moeten bevorderen.

1.2.1. G8

De ministers van Justitie en Binnenlandse Zaken van de G8[198] hebben in hun bijeenkomst van 9-10 december 1997 een reeks beginselen en een 10-punten actieplan goedgekeurd om de zogenaamde "high-tech-criminaliteit" aan te pakken.[199] Dit plan werd door de G8-top in Birmingham van 8 mei 1998 bekrachtigd. De 10 punten luiden als volgt:[200]

1. *"There must be no safe havens for those who abuse information technologies.*
2. *Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.*
3. *Law enforcement personnel must be trained and equipped to address high-tech crimes.*
4. *Legal systems must protect the confidentiality, integrity and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.*
5. *Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.*
6. *Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.*
7. *Transborder electronic access by law enforcement to publicly available (open source) information does no require authorization from the State where the data resides.*
8. *Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.*
9. *To the extent practicable, information and telecommunication systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.*

[198] De G8-groep bestaat uit Frankrijk, Duitsland, Italië, Verenigd Koninkrijk, Verenigde Staten van Amerika, Canada, Japan en Rusland.
[199] Zie ook: VERMEULEN, G., *Wederzijdse rechtshulp in strafzaken in de Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de Lidstaten?*, Antwerpen, Maklu, 1999, 293-298.
[200] X., (1997/12/10) 'Meeting of Justice and Interior Ministers' [WWW] The Birmingham Summit : http://birmingham.g8summit.gov.uk/prebham/washington.1297.shtml [01/04/02]

10. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts."

Kort nadat het "I love you"-virus wereldwijd computers platlegde, hielden diplomaten uit de G8-landen (mei 2000) een conferentie over computercriminaliteit. Computerdeskundigen en lobbyisten hadden de hoop dat de verzamelde ministers in Parijs zouden praten over de oprichting van een internationaal politiekorps dat zich louter met de opsporing, en uiteindelijk ook de preventie van computercriminaliteit zou gaan bezighouden. De conferentiegangers bleken de ontmoeting in Parijs echter vooral te zien als een mogelijkheid elkaar advies te geven over hoe computercriminaliteit op nationaal niveau bestreden kan worden en over hoe nationale wetgeving op de nieuwe technologie kan worden aangepast.[201]

In oktober 2000 vond in Berlijn opnieuw een bijeenkomst plaats. Deze workshop bouwde voort op de resultaten uit de Parijse conferentie. Drie thema's stonden centraal: de lokalisering en identificatie van "cybercriminelen", preventie van "high-tech crime" en een betere samenwerking met het bedrijfsleven.[202]

Eind februari 2001 verzamelden de ministers van Justitie en Binnenlandse Zaken van de G8 zich in Milaan. Tijdens deze tweedaagse conferentie werd specifiek gewezen op het belang van de strijd tegen de seksuele uitbuiting van minderjarigen. Tevens werd de aandacht gevestigd op de eventuele implementatie van een "G8-database" die moet toelaten dat landen onderling op een snelle manier informatie kunnen uitwisselen over "cybercriminelen".[203]

Van 22 tot 24 mei 2001 organiseerde de G8 in Tokyo de "Government/Private Sector High level Meeting on High-tech Crime". Tijdens deze conferentie werd de aandacht nogmaals gevestigd op het belang van samenwerking van overheden met de private sector. Interstatelijke samenwerkingsverbanden volstaan niet om het hoofd te bieden aan computercriminaliteit. In werkgroepen wisselden vertegenwoordigers van overheden en private sector van gedachten over onderwerpen zoals de bewaring en opslag van elektronische data, de veiligheid van elektronische handel, de uitwisseling van informatie, enz.[204]

---

[201] KETELAAR, T., (2000/05/17) 'Cybercrime: kluif voor diplomaten' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Nieuws/2000/05/17/Med/02.html [01/04/02]

[202] Ministery of Foreign Affairs of Japan, (2000/10/26) 'The G8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace' [WWW]. G8 summit: http://www.mofa.go.jp/policy/economy/summit/2000/lyon.html [01/04/02]

[203] GOVERNMENT OF CANADA, (2001/02/27) 'G8 Justice and Interior Ministers' Meeting' [WWW]. http://www.g8.gc.ca/genoa/2001/Milan_Justice_Interior-e.asp [01/04/02]

[204] SICHERHEIT IM INTERNET (2001/05/24) 'Tokio G8 Workshop Press Release' [WWW]. http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=20&tdid=837&page=0 [01/04/02]

1.2.2. United Nations (UN)

De Verenigde Naties hebben verschillende onderzoeksgroepen die actief zijn rond het thema "cybercrime". In 1989 werden door de UN de "Guidelines on the Use of Computerised Personal Data Flow" aangenomen. Een jaar later volgden de richtlijnen met betrekking tot "personal data files". Ook werd onder impuls van de UN in 1994 werk gemaakt van een "*Manual on the prevention and control of computer-related crime*".[205]

Op initiatief van de Russische Federatie nam de Algemene Vergadering van de Verenigde Naties in december 1998 een resolutie aan over cybermisdaad, cyberterrorisme en cyberoorlog.[206] Resolutie 53/70 gaat in op de ontwikkeling van informatie en telecommunicatie in de context van internationale veiligheid. Zij nodigt lidstaten uit om de Algemene Secretaris te informeren over hun visies over het thema van informatieveiligheid en over internationale principes die de veiligheid van globale informatiesystemen kunnen waarborgen.

1.2.3. Organisation for Economic Co-operation and Development (OECD)

De OECD-groep telt een dertigtal landen die de principes van de vrije markteconomie en het democratisch regeren hoog in het vaandel dragen. Van 1983-1985 boog het "Ad hoc Committee on Computer Crime" zich over de mogelijkheid om een internationale harmonisatie van het strafrecht door te voeren voor het domein van de computergerelateerde economische criminaliteit. In 1985 deed dit comité aan de lidstaten de aanbeveling om te onderzoeken in welke mate economische computercriminaliteit dient gevat te worden in nationale regelgeving.[207]

In 1989 zette het OECD zijn werkzaamheden verder en werd er gewerkt rond de veiligheid en beveiliging van informatiesystemen. Drie jaar later nam de Raad van de OECD de "Recommendation Concerning Guidelines for the Security of Information Systems" aan.[208] Deze richtlijnen houden verband met de implementatie van minimale beveiligingsmaatregelen voor informatiesystemen.

---

[205] SIEBER, U., *Legal aspects of computer-related crime in the information society, Würzburg, 1998,* 152-153.
[206] UNITED NATIONS, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. GAOR, 53rd Sess., U.N. Doc. A/RES/53/70, *New York*, 1998.
[207] SIEBER, U., *Legal aspects of computer-related crime in the information society, Würzburg, 1998,* 157-158.
[208] OECD, *Recommendation of the Council concerning Guidelines for the Security of Information Systems*, adopted on 26 november 1992, C(92)188/FINAL, *Paris*, 1992.

1.2.4. Europese Unie

Op het niveau van de Europese Unie is tot voor kort voornamelijk wetgeving ontwikkeld in de vorm van maatregelen op het gebied van het auteursrecht, de bescherming van het fundamentele recht op privacy, de bescherming van persoonsgegevens, elektronische handel, elektronische handtekeningen en ook op het vlak van encryptie.

De belangrijkste aspecten die in de wetgeving inzake specifieke computercriminaliteit worden behandeld op EU-niveau of op het niveau van de lidstaten zijn:[209]

Inbreuken op de persoonlijke levenssfeer: verschillende landen hebben strafwetgeving ingevoerd tegen het onwettig verzamelen, opslaan, wijzigen, bekendmaken of verspreiden van persoonsgegevens. In de EU zijn enkele richtlijnen goedgekeurd ter onderlinge afstemming van de wetgeving inzake de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens.[210]

Delicten op het gebied van de inhoud: de EU stelt dat moet opgetreden worden tegen de verspreiding van (kinder)pornografie via het Internet. Ook racistische uitingen en het aanzetten tot geweld moet als onwettig beschouwd worden. De Raad van de E.U. keurde in dit verband een besluit goed ter bestrijding van kinderpornografie.[211]

Economische delicten, onbevoegde toegang en sabotage: in veel landen zijn wetten goedgekeurd waarin specifieke computercriminaliteit in de vorm van economische delicten wordt aangepakt. Ook nieuwe delicten die verband houden met de onbevoegde toegang tot computers en de verspreiding van virussen maakten reeds het voorwerp uit van wetgevende initiatieven.

Delicten op het gebied van de intellectuele eigendom: in dit verband kan gewezen worden op een aantal richtlijnen over de rechtsbescherming van computerprogramma's en van

[209] COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's*, De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden, COM (2000) 890 definitief, *Brussel*, 2001.
[210] EUROPEES PARLEMENT EN DE RAAD, Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Straatsburg*, 24 oktober 1995 en EUROPEES PARLEMENT EN DE RAAD, Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer, *Straatsburg*, 15 december 1997.
[211] RAAD VAN DE EUROPESE UNIE, Besluit van de Raad ter bestrijding van kinderpornografie op Internet, PB L 138 van 9.6.2000, *Brussel*, 29 mei 2000.

databanken.[212] Ook schendingen van het auteursrecht en de naburige rechten werden behandeld in een richtlijn.[213]

De laatste jaren werden echter ook een aantal belangrijke niet-wetgevende maatregelen genomen. Daaronder valt het "Actieplan tegen illegale en schadelijke inhoud op het Internet". In dit kader verleent de EU cofinanciering voor bewustmakingsacties en andere initiatieven die opgezet worden ter bescherming van minderjarigen en van de menselijke waardigheid in de informatiemaatschappij.

In het "Actieplan inzake georganiseerde misdaad", dat in mei 1997 door de JBZ-Raad werd goedgekeurd, werd de Commissie verzocht voor eind 1998 een studie naar computercriminaliteit te verrichten. Deze studie, de "COMCRIME-studie", werd door de Commissie in april 1998 ingediend bij de multidisciplinaire werkgroep van de Raad die zich bezighoudt met de bestrijding van georganiseerde criminaliteit.[214]

In januari 2001 vond te Gent de conferentie "Strategies of the EU and the US in combating transnational organized crime" plaats. Eén van de workshops was gewijd aan "cybercrime". In het verslag van deze werkgroep word gewezen op het belang van de afstemming van nationale regelgeving op de supranationale aanbevelingen en richtlijnen. Ook wordt gewaarschuwd voor het gevaar van tegenstrijdige wetgevende bepalingen ter beteugeling van "cybercrime".[215]

1.2.5. Europol

Europol richt zich als internationale organisatie op het bestrijden van grensoverschrijdende, georganiseerde criminaliteit. De organisatie heeft een ondersteunende rol ten behoeve van de politiediensten in de landen van de Europese Unie. Europol verzamelt en analyseert informatie over personen die (mogelijk) lid zijn van een criminele organisatie die internationaal opereert.

---

[212] EUROPEES PARLEMENT EN DE RAAD, Richtlijn 91/250/EEG betreffende de rechtsbescherming van computerprogramma's, *Straatsburg*, 14 mei 1991. en EUROPEES PARLEMENT EN DE RAAD, Richtlijn 96/9/EG betreffende de rechtsbescherming van databanken, *Straatsburg*, 11 maart 1996.

[213] EUROPEES PARLEMENT EN DE RAAD, Richtlijn 2001/29/EG betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, *Straatsburg*, 22 mei 2001.

[214] COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's*, De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden, COM (2000) 890 definitief, *Brussel*, 2001.

[215] Zie in dit verband: DE RUYVER, B., VERMEULEN, G. EN VANDERBEKEN, T., (eds.), *Strategies of the EU and the US in Combating Transnational Organized Crime*, Antwerpen, Maklu, 2002, 250 p.

Het huidige voorzitterschap van de EU is in handen van Spanje. Dit land pleit voor de oprichting van een waarnemingscentrum voor "hightechcriminaliteit" binnen Europol. Deze plannen zijn echter omstreden. Volgens Spanje zijn de Europese landen extreem kwetsbaar voor aanslagen op vitale infrastructuren zoals elektriciteitsvoorziening en communicatiesystemen.[216]

Om deze dreiging af te wenden moet er bij Europol een waarnemingscentrum voor hightechcriminaliteit komen. Dit centrum moet vroegtijdig bedreigingen van de vitale infrastructuur opsporen en tegenmaatregelen nemen. Ook zou deze instantie pro-actief het Internet kunnen monitoren. Daarnaast moet het waarnemingscentrum gaan fungeren als alarmcentrale. Er is immers op Europees niveau geen centraal punt waar bedrijven en overheden zich toe kunnen wenden.

Het Spaanse voorstel is met gemengde reacties ontvangen in de EU. Het voorstel is te vaag en legt veel verschillende activiteiten tegelijk bij één centrum, aldus een aantal lidstaten. Maar vooral de Europese Commissie keerde zich tegen de plannen.

Volgens de Commissie mag Europol zich alleen bemoeien met strafbare feiten op Internet. Zaken als netwerkintegriteit, de bescherming van netwerken tegen virussen of interceptie en privacybescherming vallen onder de sociaal-economische poot van de Europese Unie, waar de Europese Commissie de scepter zwaait. De Commissie is waarschijnlijk bang dat Europol, en in het verlengde daarvan de Europese justitieministers, een te grote rol gaan spelen op dit terrein, waardoor de Commissie een deel van haar macht kan kwijtraken. Omgekeerd vinden de justitieministers dat de Europese Commissie op het gebied van nieuwe technologieën te weinig oog heeft voor de belangen van de opsporingsautoriteiten.

[216] X., (2002/03/25) 'Europol krijgt waarnemingscentrum voor hightechcriminaliteit' [WWW]. Security.nl: http://www.security.nl/artikel.php3?id=2904 [01/04/02]

Hoofdstuk 2: Initiatieven van de Raad van Europa

2.1. Historische schets

2.1.1. "Recommendation No. R (89)"

Van 1985 tot 1989 boog het "Select Committee of Experts on Computer-Related Crime" van de Raad van Europa zich over de juridische problematiek rond computercriminaliteit. In 1989 werd in dit verband een rapport gepresenteerd. De werkzaamheden van deze groep hebben geleid tot "Recommendation No. R (89)".[217] Deze aanbeveling wil de lidstaten ertoe bewegen om bij de redactie van wetgevende initiatieven rekening te houden met de werkzaamheden van de Raad van Europa, meer bepaald het "Report on computer-related crime". In dit rapport wordt o.a. een minimumlijst geciteerd, die de lidstaten moeten helpen bij het strafbaar stellen van allerhande vormen van "cybercrime".

Op 8 september 1995 nam de Raad van Europa een aanbeveling aan inzake de opsporing van strafbare feiten in een geautomatiseerde omgeving. Deze aanbeveling dient gezien te worden als het vervolg op "Recommendation No. R (89)". Ze bestaat uit een aantal principes die de lidstaten van de Raad van Europa geacht worden in hun nationale wetgeving toe te passen. De principes formuleren een aantal nieuwe bevoegdheden voor justitie en politie en geven tevens aan hoe op dit punt de aanbevolen principes in de bestaande wetgeving worden ingepast.[218]

2.1.2. Aanloop naar het Cybercrime-Verdrag

De Raad van Europa richtte tevens twee "follow-up" comités op. Het "Committee of Experts on Procedural Law Problems Connected with Computer-related Crime" en anderzijds het "Committee of Experts on Crime in Cyberspace". Dit laatste comité kreeg als opdracht mee een verdrag uit te werken dat materieel- en formeelrechtelijke bepalingen zou bevatten m.b.t. criminaliteit die gepleegd wordt via het Internet of andere telecommunicatienetwerken. Ook diende dit Cybercrime-verdrag bepalingen te bevatten i.v.m. internationale samenwerking m.b.t. onderzoeken naar dergelijke misdrijven.

[217] COUNCIL OF EUROPE, *Computer-Related Crime*, Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989, Strasbourg, 1989. In dit verband kan ook verwezen worden naar: COUNCIL OF EUROPE, *Computer-Related Crime*, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg, 1990.
[218] VAN EECKE P., *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 90-91.

Teneinde een vlotte internationale samenwerking te bekomen, diende het Comité zich ook te buigen over aspecten als definities en sancties, en over de aansprakelijkheid van de diverse actoren in "cyberspace". Ook werden de mogelijkheden nagegaan inzake de grensoverschrijdende aanwending van dwangmiddelen in een technologische omgeving. Concreet dient men daarbij te denken aan de interceptie van telecommunicatieverkeer, elektronische bewaking van informatienetwerken, de zoeking en inbeslagneming in informaticaomgevingen, enz.[219]

Op 14 april 1997 presenteerde het "Committee of Experts on Crime in Cyberspace"[220], ook wel "PC-CY" genoemd, een "Green Paper on the protection of minors and human dignity in audiovisual and information services".[221] De redactieleden stellen in de inleiding dat twee belangrijke uitdagingen onderzocht worden in de "Green Paper". Het betreft enerzijds de bescherming van minderjarigen en anderzijds de vrijwaring van de menselijke waardigheid.

Het Comité diende uiterlijk eind 2000 een ontwerp van een verdrag aan de "Stuurgroep Strafrechtelijke Vraagstukken" van de Raad van Europa voor te leggen. Naast de grote Europese landen als Frankrijk, Duitsland en Engeland, werden niet-leden van de Raad nauw betrokken als waarnemer bij de werkzaamheden. De belangrijkste zijn de VS, Canada, Japan, Zuid-Afrika, de Europese Commissie, de OESO en de UNESCO. Daarnaast namen onafhankelijke wetenschappelijke experts aan de beraadslagingen deel.

In April 2000 werd een ontwerptekst van de Cybercrime-Conventie[222] vrijgegeven en gepubliceerd. Deze ongewone stap werd gezet zodat specialisten van over de hele wereld commentaar konden geven op de bepalingen van de ontwerptekst. Een jaar later werden experten uitgenodigd op een speciale hoorzitting.

Uiteindelijk werd de verdragstekst aangenomen door de Assemblée in april 2001. De ondertekening gebeurde door 26 lidstaten van de Raad van Europa te Boedapest op 23 november 2001.[223] Op 1 mei 2002 hadden reeds 33 staten het Verdrag ondertekend.[224] Voor de

[219] VERMEULEN, G., *Wederzijdse rechtshulp in strafzaken in de Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de Lidstaten?*, Antwerpen, Maklu, 1999, 293-298.
[220] Dit comité stond onder voorzitterschap van prof H.W.K. Kaspersen van het Instituut voor Informatica en Recht van de Vrije Universiteit te Amsterdam, Nederland.
[221] COUNCIL OF EUROPE, *Committee of Experts on Crime in Cyberspace*, Green Paper on the protection of minors and human dignity in audiovisual and information services, PC-CY (97) 20, Strasbourg, 14 april 1997.
[222] COUNCIL OF EUROPE, Convention on Cybercrime, ETS no. 185, Budapest, 2001.
[223] X., (2001/11/22) 'The road to the treaty' [WWW]. Cybercrime Convention: http://www.stopcybercrime.net/2_1_1.php [01/04/02]
[224] Voor de actuele stand van zaken kan ik verwijzen naar deze website: http://conventions.coe.int/.

inwerkingtreding van de Cybercrime-Conventie[225] zijn minstens vijf ratificaties vereist waarvan drie dienen te gebeuren door lidstaten van de Raad van Europa.

2.2. Bespreking van het Cybercrime-Verdrag

2.2.1. Objectieven

Een eerste objectief van dit verdrag is dat in alle Europese landen een gelijkaardige wetgeving wordt uitgevaardigd die toelaat specifieke inbreuken m.b.t. de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens en vervalsing, bedrog of oplichting met behulp van computers te bestraffen. Hetzelfde wordt overeengekomen voor niet-specifieke informaticamisdrijven, zoals deze die betrekking hebben op kinderpornografie of auteursrechtelijke inbreuken.

In de tweede plaats wil men via het verdrag bereiken dat in alle Europese landen de strafprocedure wordt aangepast aan het gebruik van informatica, zodat naast huiszoekingen ook opsporingen in bedrijfsnetwerken mogelijk worden. Een derde objectief is de bevordering van de internationale samenwerking. Daarom komen de deelnemende landen overeen dat ze onder bepaalde voorwaarden tot uitlevering van verdachten zullen overgaan. Ook worden een aantal vormen van wederzijdse samenwerking afgesproken met een contactpunt dat permanent bereikbaar moet zijn.[226]

2.2.2. Innovaties?

Het Cybercrime-Verdrag, waar vier jaar aan gewerkt is, verbiedt onder meer fraude, hacken en het bezitten, maken en verspreiden van kinderpornografie en virussen. Ook schending van het auteursrecht en merkenrecht wordt strafbaar gesteld. Het verdrag regelt ook dat rechtspersonen aansprakelijk kunnen worden gesteld voor schade die ontstaat door bijvoorbeeld hacken. Als een werknemer van een bedrijf aan het hacken slaat of als een bedrijf zijn systemen aantoonbaar onvoldoende heeft beveiligd waardoor een werknemer op een ander computernetwerk kan inbreken, moet de betreffende onderneming de schade betalen.

In veel landen die het verdrag ondertekenen zijn de meeste van de genoemde misdaden al strafbaar. Het verdrag is vooral bedoeld om bestaande wetgeving te harmoniseren en

[225] Het Cybercrime-Verdrag werd integraal opgenomen als Bijlage II.
[226] DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.

internationale samenwerking gemakkelijker te maken. Hoewel het verdrag zeer breed is, wordt over racisme en antisemitisme gezwegen.

2.2.3. Amerikaanse druk

Onder druk van de Verenigde Staten bevat het verdrag geen passage die racistische en antisemitische uitlatingen op Internet verbiedt. In de VS zijn racistische uitlatingen toegestaan omdat ze volgens de algemene consensus onder de vrijheid van meningsuiting vallen. Websites van neonazi-groeperingen en Holocaust-ontkenners zijn er legaal. Veel Europese rechtsextremisten hebben hun websites bij Amerikaanse bedrijven ondergebracht om aan strafrechtelijke vervolging in hun eigen land te ontkomen.

2.2.4. "First Additional Protocol to the Convention on Cybercrime"

Binnen afzienbare tijd komt er een protocol bij het Cybercrime-Verdrag voor landen die willen samenwerken om racisme en antisemitisme op Internet te bestrijden. In dit verband kan verwezen worden naar de zeer recente werkzaamheden van het "Committee of Experts on the Criminalisation of Acts of Racist of Xenophobic Nature committed through Computer Networks" (PC-RX).[227]

2.2.5. Kritische bemerkingen

Door racisme in een apart protocol op te nemen, kunnen de VS zich wel bij het Cybercrime-Verdrag aansluiten. De Raad van Europa is m.i. niet in staat geweest de Amerikanen haar wil op te leggen. Als de Amerikanen het verdrag niet zouden ondertekenen, zou het weinig waarde hebben, dacht men. Het is jammer dat de Europese landen niet beter hebben onderhandeld. Waarom deed de Raad van Europa niet beter haar best om de Amerikanen duidelijk te maken hoe men hier denkt over racisme en antisemitisme?

In de Europese Unie gaat men bovendien verder dan de Raad van Europa. Men deed immers een studie naar de wetgeving die in de verschillende lidstaten inzake informaticacriminaliteit werd uitgevaardigd. Op basis van deze analyse, onderzoekt men verschillende mogelijkheden die de EU kan nemen om computercriminaliteit te bestrijden.

[227] Zie in dit verband: COUNCIL OF EUROPE, *European Committee on Crime Problems*, Committee of Experts on the criminalisation of acts of a racist or xenophobic nature committed through computer systems, Public version N° 2, Strasbourg, 26 March 2002.

In de EU zal de onderlinge afstemming van de wetgeving verder gaan dan in het verdrag van de Raad van Europa. Internationale afstemming zal in deze laatste de facto tot een minimum beperkt blijven.

Deel V: Digitale recherche in België

Hoofdstuk 1: Federal Computer Crime Unit (FCCU)

1.1. Korte historische inleiding

De snelle evolutie in de informatica- en telecommunicatiesector heeft er ongetwijfeld mede toe bijgedragen dat er de laatste jaren een stijging waar te nemen is van allerlei vormen van zogenaamde *ICT-crime*. Om aan deze trend tegemoet te komen, werden er begin de jaren '90 in België gespecialiseerde eenheden in het leven geroepen om de informatica- en telecommunicatiecriminaliteit te bestrijden en om bijstand te leveren in het kader van gerechtelijke dossiers die ICT-onderzoek vergen.[228]

In 1992 zagen de *Computer Crime Units* (kortweg CCU) van de Gerechtelijke Politie het levenslicht. Drie jaar later, in 1995, voorzag ook de toenmalige Rijkswacht in de oprichting van een gespecialiseerde eenheid: het *Team voor Bijstand en Opsporingen in Geautomatiseerde Omgevingen*[229] (kortweg BOGO-team). In 1997 kreeg de Nationale Brigade van de Gerechtelijke Politie een *National Computer Crime Unit*.[230]

Deze gespecialiseerde teams ontsnapten echter evenmin aan de reorganisatie van de politiediensten op federaal niveau. Dit bracht met zich mee dat het *BOGO-team* van de Rijkswacht en de *National Computer Crime Unit* van de Gerechtelijke Politie samensmolten tot de *Federal Computer Crime Unit*. Naast deze FCCU blijven de regionale *Computer Crime Units* bestaan.

[228] COLLEGE VAN PROCUREURS-GENERAAL, *omzendbrief van 16 april 1999 betreffende de Ministeriële richtlijn van 16 maart 1999 tot regeling van de samenwerking, coördinatie en taakverdeling tussen de lokale politie en de federale politie inzake de opdrachten van gerechtelijke politie*, COL 6/99.
[229] BEIRENS, B., 'Op zoek naar criminele bits, digitaal rechercheren', *Politeia*, 1998, afl. 8, 9-12.
[230] SENNESAEL, V., 'National Computer Crime Unit: digitale flikken', *Computer Magazine*, 2000, afl. 6, 73-75; Zie ook: VANDEVINNE, D., 'Computer Crime Units: Belgische cyberpolitie', *Computer Magazine*, 2001, afl. 7, 10-12.

1.2. Situering en organisatie

De *Federal Computer Crime Unit* (FCCU) situeert zich op nationaal niveau binnen de *Directie voor de Bestrijding van Economische en Financiële Criminaliteit* (DJF). Op regionaal niveau vinden we de Computer Crime Units (CCU) terug. Deze zijn voorzien in de onderzoekscapaciteit van de Federale Recherche die op zijn beurt afhangt van de Gerechtelijke Dienst van het Arrondissement o.l.v. de gerechtelijk directeurs.[231]

1.3. Objectieven en taakomschrijving[232]

De FCCU moet er samen met de regionale CCU's voor zorgen dat politiediensten op een doeltreffende en snelle wijze bijgestaan worden in dossiers die verband houden met ICT-criminaliteit. Verder staat deze dienst in voor het uitstippelen van het beleid van zowel de FCCU als de regionale CCU's. Daarnaast worden ook nieuwe methoden en technieken ontwikkeld die moeten toelaten dat speurders op een meer efficiënte manier onderzoekingen kunnen uitvoeren.

Het takenpakket is echter ruimer. De FCCU voorziet in de opleiding en vorming van de personeelsleden, staat in voor het beheer van het nationaal en internationaal contactpunt en oefent functioneel toezicht uit op de werking van de CCU's. Verder wordt ook exclusieve bijstand geleverd aan bijzondere eenheden.

[231] BEIRENS. L., *Organisatie en werking van de Federal Computer Crime Unit en de regionale Computer Crime Units*. Brussel, april 2001, 1-2. (informatiefiche).
[232] BEIRENS. L., *Organisatie en werking van de Federal Computer Crime Unit en de regionale Computer Crime Units*. Brussel, april 2001, 3-4. (informatiefiche).

Hoofdstuk 2: Regionale Computer Crime Units (CCU)

2.1. Situering

In tegenstelling tot de FCCU die zich op nationaal niveau situeert, vinden we de CCU's op regionaal niveau terug. Ze zijn voorzien in de onderzoekscapaciteit van de Federale Recherche die op zijn beurt afhangt van de Gerechtelijke Dienst van het Arrondissement o.l.v. de gerechtelijk directeurs. De CCU's kennen een hoge graad van specialisatie.[233]

2.2. Taakomschrijving

De CCU's bezitten de nodige kennis om de (digitale) informatie die men vergaart in ICT-omgevingen om te zetten naar concreet, bruikbaar materiaal voor het parket en de politiediensten. Naast het leveren van de nodige bijstand aan onderzoekers zijn de CCU's actief in de bestrijding van zowat alle vormen van ICT-criminaliteit.

De taken zijn hoofdzakelijk operationeel van aard. Het betreft bijvoorbeeld het leveren van bijstand bij onderzoek in ICT-omgevingen, het uitvoeren van forensisch onderzoek van inbeslaggenomen ICT-materiaal, het verhoren van getuigen of verdachten in ICT-gebonden materies en de opsporing van verdachten of het volgen van sporen op internet.

2.3. Werking van de Computer Crime Units

Iedere CCU levert bijstand aan een onderzoekende eenheid die het dossier beheert. Bijstand voor ICT-onderzoek kan gevraagd worden door alle eenheden op verschillende manieren: per telefoon, fax of per nota. Vervolgens wordt een *proces-verbaal* opgesteld.

2.4. Voorwerp van onderzoek

Ieder systeem dat gegevensopslag, -verwerking of -overdracht van digitale informatie mogelijk maakt, komt in aanmerking voor forensisch onderzoek door de CCU's. Concreet gaat het daarbij om computers, netwerkomgevingen, allerlei kaartleesapparaten, prikklokken, mobiele telefoontoestellen, simkaarten, elektronische zakagenda's, enz.

[233] BEIRENS. L., *Organisatie en werking van de Federal Computer Crime Unit en de regionale Computer Crime Units*. Brussel, april 2001, 1-2. (informatiefiche).

Hoofdstuk 3: Centraal Gerechtelijk Meldpunt

3.1. Beheer

De Federal Computer Crime Unit beheert het *Centraal Gerechtelijk Meldpunt*. Op dit meldpunt kunnen alle vormen van criminaliteit die verband houden met het gebruik van internet worden gemeld. De verschillende Belgische *Internet Service Providers* (ISP) verzekeren door middel van hun portaalsite de kenbaarheid van het Centraal Gerechtelijk Meldpunt.[234]

Iedere internetgebruiker kan websites waarvan hij veronderstelt dat de inhoud ongeoorloofd is, rechtstreeks kenbaar maken via een e-mail (contact@gpj.be) of men kan gebruik maken van het standaardformulier op de website van de Federale Politie.[235] Deze is te bereiken op http://www.fedpol.be/.

Daarnaast kan men zich ook wenden tot zijn Internetprovider die op zijn beurt het centrale aanspreekpunt op de hoogte brengt. Indien de ongeoorloofde inhoud van kinderpornografische aard is, dan verbinden de ISP's er zich toe om de toegang tot de desbetreffende website te blokkeren.

3.2. Verwerking van meldingen

Het meldpunt oordeelt of de melding in acht dient genomen te worden op grond van de al dan niet geoorloofde inhoud van de feiten die gemeld worden. Als de feiten in aanmerking worden genomen, dan wordt het dossier doorgezonden voor verdere afhandeling naar het parket dat bevoegd is. Als de ongeoorloofde inhoud echter ondergebracht is bij buitenlandse internetproviders, dan wordt dit meegedeeld aan de vereniging van de ISP's van het betrokken land of bij gebreke daaraan, aan de betrokken ISP. Tevens wordt samengewerkt met Interpol.

[234] X., (1999/05/28) 'Samenwerkingsprotocol ter bestrijding van ongeoorloofd gedrag op het Internet' [WWW]. Internet Service Providers Association Belgium ISPA: http://www.ispa.be/nl/c040202.html [07/08/01]
[235] Opmerking: momenteel is het Centraal Gerechtelijk Meldpunt nog steeds ondergebracht op de website van de Gerechtelijke Politie. Deze is te bereiken op volgende url: http://www.gpj.be .

3.3. Aantal meldingen

Dagelijks ontvangt het Centraal Gerechtelijk Meldpunt een vijftigtal meldingen.[236] In 2000 werden 2359 meldingen onderzocht met bruikbare informatie. 343 meldingen bleken daarbij betrekking te hebben op criminele feiten. Van deze 343 meldingen waren er maar liefst 322 feiten gerelateerd aan kinderpornografie.

Het merendeel van de criminele feiten dient gesitueerd te worden buiten de Belgische landsgrenzen. Dit brengt met zich mee dat in 2000 vanuit het Centrale Gerechtelijke Meldpunt slechts een twintigtal feiten kenbaar werden gemaakt aan de Nationaal Magistraat. Voor de overige feiten werd Interpol ingelicht die op zijn beurt de berichten overmaakt naar de bevoegde overheid.

3.4. Evaluatie van de werking van het Centraal Gerechtelijk Meldpunt

De FCCU beheert het *Centraal Gerechtelijk Meldpunt*. Iedere internetgebruiker of Internet Service Provider kan websites waarvan verondersteld wordt dat de inhoud ongeoorloofd is, rechtstreeks kenbaar maken aan dit meldingspunt.

Momenteel wordt veel personeelscapaciteit opgeofferd aan het beheer van het meldpunt. Dit brengt met zich mee dat weinig tijd overblijft voor de speurders om actief aan digitale recherche te doen. Indien iemand vakantie neemt of ziek wordt, kan zelfs de verwerking van de nieuwe emailberichten die arriveren bij de FCCU in het gedrang komen. Nochtans verbindt het *Centraal Gerechtelijk Meldpunt* er zich toe om binnen de vierentwintig uur na ontvangst van een emailbericht een ontvangstmelding te versturen naar de internetgebruiker of de betrokken Internet Service Provider.[237]

Veel van de kostbare tijd gaat verloren bij het behandelen van emailberichten die geen bruikbare informatie bevatten. Zo ontvangt het meldpunt dagelijks berichten die besmet zijn met een virus, reclameberichten, valse meldingen, enz.

Sinds begin dit jaar kwamen ongeveer achtduizend meldingen toe op het verzamelpunt. Daarvan bleken slechts vijfduizend berichten bruikbare informatie te bevatten. Uit deze

[236] BEIRENS. L., *Organisatie en werking van de Federal Computer Crime Unit en de regionale Computer Crime Units*. Brussel, april 2001, 6-7. (informatiefiche).
[237] X., (1999/05/28) 'Samenwerkingsprotocol ter bestrijding van ongeoorloofd gedrag op het Internet' [WWW]. Internet Service Providers Association Belgium ISPA: http://www.ispa.be/nl/c040202.html [07/08/01]

vijfduizend berichten ging het slechts in vijfhonderd gevallen werkelijk om strafbare feiten. In slechts een half procent van deze gevallen hadden de strafbare feiten betrekking op misdrijven die in België gepleegd werden. De overige feiten werden gepleegd in het buitenland.[238]

Als men dus al een positieve melding ontvangt, dan blijkt het bijna altijd te gaan om misdrijven die een aanknopingspunt hebben in het buitenland. Hierdoor wordt vaak dubbel werk verricht: veel Internetgebruikers die informatie doorzenden naar het meldpunt sturen immers vaak ook een kopie van hun bericht naar de politiediensten van het betrokken land of zelfs de betrokken provider. Daardoor wordt de melding ook behandeld door opsporingsdiensten van andere landen.

Het komt er in veel gevallen op neer dat België het huiswerk opknapt van andere landen. Dit kan geenszins de bedoeling zijn van het Belgische meldpunt. Het Centraal Gerechtelijk Meldpunt kan onmogelijk de ambitie hebben om meldingen te verzamelen van strafbare feiten die wereldwijd werden gepleegd. Daarvoor zijn noch de middelen noch het personeel voorhanden. Tevens is het zo dat een positieve melding van strafbare feiten die in het buitenland werden gepleegd, geenszins een garantie geven op vervolging en bestraffing van de daders.

De handhaving van nationaal recht op Internet is in ieder geval geen eenvoudige zaak. Het Internet heeft een internationaal karakter terwijl jurisdicties gebonden zijn aan territoriale grenzen. Daarenboven is het vaak zeer moeilijk om te gaan vaststellen waar een handeling feitelijk heeft plaatsgevonden. Dit is te wijten aan het immateriële karakter van de informatie-uitwisseling die gebeurt via het World Wide Web.

In ieder geval is een betere internationale samenwerking nodig. Dit zal op zijn beurt positieve gevolgen hebben voor de handhaving van het strafrecht. Op die manier heeft men meer garanties om de identiteit van aansprakelijke personen te kunnen achterhalen. Het spreekt voor zich dat de Internetprovider hier een belangrijke rol speelt. Zijn medewerking zal immers vaak nodig zijn om de plegers van de strafbare feiten op te sporen.

[238] Gesprek met L. BEIRENS, diensthoofd Federal Computer Crime Unit, Brussel, 1 augustus 2001.

3.5. Territoriale werking van het recht en de internationale rechtsorde

In dit verband kan gewezen worden op de kwetsbare relatie die bestaat tussen de territoriale werking van het recht en de internationale rechtsorde. De nationale soevereiniteit van de betrokken staten komt bij deze afweging immers steeds in het gedrang.

In het strafrecht draait veel om de internationale strafrechtelijke samenwerking. In beginsel is de rechtsmacht van staten territoriaal begrensd. Daarom is het nodig dat voor het vergaren van gegevens in het buitenland, het betreffende delict ook in dat land strafbaar is gesteld. Deze dubbele incriminatie heeft ook repercussies voor de positieve meldingen die de politie ontvangt.

Stel dat men informatie ontvangt over een Amerikaanse site met afbeeldingen die strafbaar zijn volgens de geldende Belgische rechtsregels. Wanneer blijkt dat deze afbeeldingen volgens de Amerikaanse wetten niet strafbaar kunnen gesteld worden, dan kan men vanuit Belgisch oogpunt geen enkele actie ondernemen.

3.6. Europees meldpunt

Naar mijn mening moet werk gemaakt worden van een Europees meldingspunt waar alle meldingen kunnen ontvangen worden van strafbare handelingen die via het Internet op het grondgebied van een lidstaat gepleegd zijn. Op die manier kan veel tijd en personeelscapaciteit bespaard worden. Momenteel worden nl. veel dezelfde meldingen onderzocht door meerdere landen. Dit doet de werklast voor de politiediensten alleen maar toenemen.

Hoofdstuk 4: Enkele kritische beschouwingen

4.1. Personeelscapaciteit FCCU

4.1.1. Nieuwe bevoegdheden

Eén van de zwakke punten in de werking van de FCCU is zonder twijfel het gebrek aan personeel. In april 2001 bracht Minister van Justitie Marc Verwilghen een werkbezoek aan de FCCU. Reeds toen werd het tekort aan werkkrachten aangeklaagd door het management.[239] Anno 2002 is de situatie jammer genoeg quasi ongewijzigd gebleven. Dit blijkt o.a. uit de zeer recente parlementaire vraag die gesteld werd door senator Erika Thijs. Hierin werd nogmaals gewezen op de beperkte personeelsbezetting van de FCCU.[240]

Sinds de Wet Franchimont[241], die onder meer een wettelijke basis biedt voor de proactieve opsporing, beschikken de rechercheurs over een aantal nieuwe mogelijkheden zoals observatie. Bovendien zorgde de Wet Informaticacriminaliteit[242] voor de wettelijke regeling van een aantal nieuwe forensische onderzoekstechnieken. Politiediensten kunnen sinds deze wet beroep doen op nieuwe opsporingstechnieken zoals databeslag, medewerkingverplichting, netwerkzoeking en interceptie van communicatie. Het spreekt voor zich dat deze middelen in de praktijk slechts hun nut kunnen bewijzen indien voldoende personeel voorhanden is om de onderzoeken te voeren. In elk ander geval blijft de wet dode letter.

Bij een huiszoeking kan men geconfronteerd worden met situaties waarbij enorme hoeveelheden digitale informatie dienen onderzocht te worden.[243] In bepaalde gevallen is het daarbij onmogelijk om alle sporen te controleren door personeelsgebrek. Recent werd het tekort aan werkkrachten aan de kaak gesteld naar aanleiding van mogelijke aanvallen van cyberterrorisme en de Belgische reactie daarop.[244]

---

[239] PLA, (2001/04/21) 'Politie patrouilleert niet op het internet' in De Standaard Online [WWW]. De Standaard: http://www.destandaard.be/Archief/zoeken/DetailNew.asp?articleID=DST21042001_025 [15/10/01]

[240] Vraag om uitleg van mevrouw Erika Thijs aan de minister van Binnenlandse Zaken en aan de minister van Justitie over de FCCU, *Belgische Senaat*, 17 april 2002, nr. 2-197.

[241] Wet van 12 maart 1998 tot verbetering van de strafrechtspleging in het stadium van het opsporingsonderzoek en het gerechtelijk onderzoek, *B.S.*, 2 april 1998.

[242] Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.*, 3 februari 2001.

[243] De digitale opslagcapaciteit van computers wordt steeds groter waardoor ook steeds meer tijd nodig is om te zoeken naar criminele sporen.

[244] VANDERSMISSEN, M. (2001/10/05) 'Federal Computer Crime Unit: te weinig personeel en materieel' [WWW]. De Standaard: http://www.destandaard.be/Archief/zoeken/DetailNew.asp?articleID=DST05102001_029 [15/10/2001]

Men kan zich immers terecht de vraag stellen of de Belgische overheid beschikt over genoeg middelen om weerstand te kunnen bieden aan georganiseerde aanvallen van hackers. Momenteel heeft de FCCU echter nog geen personeelscapaciteit genoeg om op proactieve wijze cybercriminelen te gaan opsporen. Pas na een melding door een particulier of een vraag van een andere politiedienst gaat men tot de actie over.

Bij de FCCU zijn een veertiental personen werkzaam waaronder tien cyberagenten. Daarnaast zijn ook nog enkele burgers werkzaam bij deze dienst. Enkel de tien cyberagenten behoren tot het operationele kader.

4.1.2. De private sector lonkt…

Na de goedkeuring van het beleidsplan[245] dat door het diensthoofd werd voorgesteld, zal de personeelscapaciteit kunnen verdubbeld worden. Op dit moment zal zich m.i. echter een bijkomend probleem stellen. Het is immers niet evident om politieofficieren te vinden die beschikken over de nodige interesse en kennis in ICT-materies.

Tevens moet men bereid zijn om zich regelmatig bij te scholen door het volgen van vormingslessen maar ook door zelfstudie. Dit maakt het vinden van de geschikte kandidaten nog moeilijker. Bovendien zijn politiemensen doorgaans niet snel geneigd om hun vertrouwde werkomgeving bij de lokale politie te verlaten voor een job in Brussel.

Diensten die zich bezighouden met de opsporing van informaticacriminaliteit hebben nood aan ervaren informatici. Uit gesprekken[246] met het management van de FCCU blijkt dat de werving van gemotiveerde en ervaren informatici niet vanzelfsprekend is. Het wordt immers moeilijker om werknemers te motiveren zodat ze bij dezelfde werkgever blijven.

Daarnaast lonkt ook de privé-sector. De voorwaarden die van toepassing zijn op nieuwe werkkrachten die kiezen voor een job bij de overheid wegen niet altijd op tegen de voordelen die de ICT-sector biedt. Tevens kan men in de privé-sector vaak genieten van tal van extralegale voordelen die het geheel nog aantrekkelijker maken. Ook kiest men liever voor een job met normale werkuren dan voor de onregelmatige werkuren die vaak van toepassing zijn bij een politiedienst.

---

[245] BEIRENS, L., *Businessplan bijstand voor onderzoek in ICT, strijd tegen ICT-criminaliteit*. Brussel, januari 2001, 21 p. (businessplan).
[246] Gesprek met L. BEIRENS, diensthoofd Federal Computer Crime Unit, Brussel, 1 augustus 2001.

De laatste jaren merkt men ook op dat meer en meer internationale bedrijven die actief zijn in consultancy zogenaamde *forensic departments* opstarten. Meer en meer ondernemingen zien immers de noodzaak in om een 'securitypolitiek' uit te bouwen en doen daarbij beroep op bedrijven zoals Ernst & Young en KPMG. Het is voor bedrijven immers niet wenselijk dat i.g.v. diefstal onbevoegde personen toegang kunnen krijgen tot vertrouwelijke informatie.

Het spreekt voor zich dat deze consultingkantoren beschikken over gekwalificeerd en ervaren personeel bestaande uit informatici, ingenieurs, economen, juristen en criminologen. In deze branche krijgen IT-specialisten vaak interessante jobvoorwaarden waardoor weinigen zich nog geroepen voelen om als informaticus werkzaam te zijn bij de Federale Politie.

4.1.3. Conclusie

Concluderend kan gesteld worden dat de moeilijkheden waarmee men geconfronteerd wordt bij de werving van personeel de noodzaak van een mentaliteitswijziging aantonen. De bestaande voordelen waarvan universitair geschoolde politieambtenaren kunnen genieten, wegen in vele gevallen niet meer op tegen de legale en extralegale voorwaarden die van toepassing zijn in de private sector. Vooral informatici vinden meer hun gading in een job bij privé-bedrijven eerder dan bij de politie.

In de toekomst zullen de politionele overheden hier ongetwijfeld moeten aan tegemoet komen als men wil vermijden dat de meest ervaren werkkrachten massaal gaan kiezen voor een job in private ondernemingen. Recent nam de overheid in dit kader reeds een aantal initiatieven. Zo genoten informatici van een bijkomende premie om de extra werklast te compenseren die werd veroorzaakt door de overgang naar het jaar 2000.

4.2. Nood aan recent informaticamateriaal

Om op een efficiënte manier computercriminaliteit te kunnen opsporen heeft men nood aan aangepaste en recente onderzoeksapparatuur. Om de evoluties van de informaticasector te kunnen volgen zijn op regelmatige tijdstippen investeringen nodig. Dit staat buiten kijf. Toch is dit ook een kritiek punt bij de regionale CCU's en in mindere mate bij de FCCU.

Tot voor kort had men twee verschillende diensten -NCCU en BOGO-team- die elk beschikten over eigen budgetten en procedures voor de aankoop van nieuw materiaal. Op geen enkel moment bestond er een overleg tussen beide diensten voor de aanschaf van apparatuur. Dit is

eigenlijk niet verwonderlijk gezien het ging om twee aparte entiteiten, de ene gesitueerd onder de toenmalige Gerechtelijke Politie en de ander onder de toenmalige Rijkswacht.

In het kader van de algemene reorganisatie van de politiediensten werden beide diensten samengevoegd. Voortaan is er enkel nog sprake van de Federal Computer Crime Unit. Dit heeft repercussies voor het beheer van de investeringsbudgetten en voor de procedures die dienen gevolgd te worden bij de aankoop van nieuw materiaal:

Voortaan beschikt de FCCU over een budget dat beheerd wordt op centraal niveau. Op termijn zal deze keuze zijn nut ongetwijfeld bewijzen. Alle politiediensten die instaan voor de opsporing van computercriminaliteit zullen in de toekomst kunnen strijden met gelijke 'wapens'.

Een ander positief gevolg van het centraal beheer van de budgetten zal zijn dat vermeden wordt dat (nieuwe) ongelijkheden ontstaan bij de aanschaf van apparatuur. Iedere dienst die zich bezighoudt met de opsporing van ICT-crime zal immers voor de aanschaf van nieuwe hard- of software een aanvraag moeten indienen bij dezelfde directie. Deze laatste kan een kritische afweging maken van de concrete noden van de aanvrager. Naar mijn mening zal ook beter rekening kunnen gehouden worden met de interventies en werklast van elke CCU waardoor in sommige gevallen andere prioriteiten kunnen gelegd worden bij de aanschaf van materiaal.

4.3. Opleiding en vorming

Vorming is onontbeerlijk, zowel voor een werkgever als voor een werknemer. We leven nu eenmaal in een informatiemaatschappij waar kennis steeds evolueert en mensen zich voortdurend moeten bijscholen.

De FCCU en de regionale CCU's hebben als "onderneming" binnen de Federale Politie nood aan gekwalificeerd personeel dat beschikt over de nodige knowhow die nodig is om de job van 'ICT-investigator' naar behoren uit te oefenen. Tot voor kort waren echter noch de middelen noch het personeel voorhanden om een degelijke opleiding te garanderen voor alle leden van de ICT-recherche.

De beperkte budgetten die in het verleden voorzien waren voor de werking van de recherchediensten hebben gezorgd voor een gebrek aan personeel maar ook voor een tekort aan materiële middelen. Het onderdeel opleiding en vorming hangt hier nauw mee samen. Indien er weinig financiële middelen voorhanden zijn om een minimum aan personeelskader te

kunnen voorzien, dan is het allerminst verwonderlijk dat een lagere prioriteit wordt toegekend aan de vorming van speurders.

Speurders die werkzaam zijn bij een CCU zijn doorgaans mensen die een groot deel van hun vrije tijd opofferen aan computers en Internet. Veel van hun kennis van informatica in het algemeen en het Internet in het bijzonder hebben ze dus verworven door zelfstudie. Ook volgen regelmatig speurders bijkomende opleidingen om hun kennis te verfijnen. Deze vormingen financieren ze soms zelf. Eigenlijk is dit in een professionele werkomgeving quasi ondenkbaar maar toch realiteit.

Draadloze technologieën, elektronische handel, encryptie en cyberterrorisme zijn maar een paar van de complexe fenomenen waarmee men in de toekomst als rechercheur in toenemende mate zal geconfronteerd worden. Cybercrime wordt zelfs beschouwd als één van de grootste bedreigingen van de toekomst.[247] Het spreekt voor zich dat een adequate reactie op deze fenomenen enkel mogelijk kan zijn als men beschikt over professioneel opgeleide onderzoekers.

Enkele keren per jaar volgen een aantal leden van de FCCU en de CCU's cursussen die georganiseerd worden door Interpol en andere instanties. Dergelijke opleidingen zijn niet goedkoop. Bovendien zorgen de snelle technologische evoluties ervoor dat sommige cursussen snel verouderen. Het belangrijkste probleem dat zich stelt bij dit soort vorming is dat het gaat om specifieke en tijdsgebonden cursussen die een deelaspect behandelen van het hele ICT-gebeuren. Om specialist te worden zou men eigenlijk massa's opleidingen moeten volgen.

Een betere oplossing zou er in bestaan om te voorzien in een algemene basisopleiding die toegankelijk is voor *alle* personeelsleden die zich bezighouden met ICT-crime. Het is immers van groot belang dat alle rechercheurs kunnen beschikken over een ruime standaard aan basiskennis. Pas in tweede instantie moet men investeren in bijkomende specifieke opleidingen die buitenshuis ingericht worden door internationale organisaties.

[247] X., 'Cyber terrorism specialists gather in Chicago', *Crime and justice international*, 1998, afl. 20, 7-8.

Conclusie

De mogelijkheden om gegevens massaal en zeer snel wereldwijd te verspreiden, kunnen zowel voor legitieme als voor criminele doeleinden worden aangewend. In essentie bestaat er voor heel wat "traditionele" misdrijven een "elektronische" variant. Dit werd geïllustreerd door een uitgebreid overzicht te schetsen van allerhande vormen van computercriminaliteit en "cybercrime".

Het strafrecht in zijn huidige vorm vertoont weinig lacunes voor de bestrijding van een aantal inhoudsdelicten zoals pornografie, racisme en het aanzetten tot misdrijven. Voor enkele andere misdrijven was tot voor kort de strafbaarstelling in een ICT-omgeving minder duidelijk. De Belgische wetgever heeft hier op geanticipeerd met de Wet Informaticacriminaliteit. Hierin worden enkele nieuwe strafbaarstellingen opgenomen in de sfeer van computercriminaliteit.

De wetgever koos er bewust voor om zo weinig mogelijk definities te geven van nieuwe begrippen in de wet zelf. Deze keuze is m.i. de juiste geweest. Het is immers niet ondenkbaar dat nieuwe technologieën in de toekomst zullen zorgen voor andere types van delicten die zich ook afspelen op het Internet. Een te strikte definiëring zou het quasi onmogelijk maken om deze nieuwe misdrijven onder de toepassing te laten vallen van de Wet Informaticacriminaliteit.

Naast deze nieuwe incriminaties zijn er ook enkele strafprocesrechtelijke implicaties die moeten zorgen voor een adequate opsporing en bewijsvoering in ICT-omgevingen. In geïnformatiseerde omgevingen is er een bijzondere deskundigheid vereist om gegevens op te sporen die relevant zijn voor het strafonderzoek. De problematiek van de netwerkzoeking in computersystemen werd daarom wettelijk geregeld.

Door de internationale verwevenheid van computers bestaat de kans dat er tijdens een netwerkzoeking bestanden geconsulteerd worden die zich in het buitenland situeren. Deze bestanden kunnen als bewijsmateriaal gebruikt worden op voorwaarde dat de gegevens "toevallig" of "onopzettelijk" bekomen werden door de opsporingsdiensten. De wetgever regelde deze materie op een pragmatische maar vage manier die ongetwijfeld ruimte laat voor interpretatie.

Bij misdrijven die gepleegd worden door het gebruik (of misbruik) van het Internet is in vele gevallen sprake van een opeenstapeling van rechtsmachten. Gezien een strafbare handeling op Internet vaak rechtsgevolgen kan hebben in andere landen, hebben deze landen er belang bij om hun rechtsmacht te kunnen uitoefenen ten aanzien van deze delicten. Speurders kunnen door het louter onderzoeken van netwerken een inbreuk plegen op de grondrechten van andere staten. Dit toont aan dat de strafrechtelijke territorialiteit met de grootste omzichtigheid moet benaderd worden.

Toch is het onverstandig om zoekingen die plaatsvinden op netwerken te beperken tot het Belgisch grondgebied. De effectiviteit van deze zoekingen is immers quasi nihil, gezien particulieren en bedrijven vaak informatie bewaren op buitenlandse servers.

Naar mijn mening dient op internationaal niveau een afweging gemaakt te worden tussen de bescherming van de nationale belangen enerzijds en de baten die grensoverschrijdende onderzoekingen met zich meebrengen anderzijds. Het spreekt voor zich dat zoekingen die de eigen landsgrenzen overschrijden moeten gekoppeld worden aan strikte voorwaarden. Op deze manier kan de integriteit en soevereiniteit van de nationale staten gegarandeerd blijven.

In deze thesis werden ook enkele internationale initiatieven ter beteugeling van "cybercrime" belicht. Recent kwam de Europese "Cybercrime-Conventie" tot stand. Een belangrijk objectief van dit verdrag is dat in alle Europese landen een gelijkaardige wetgeving inzake computercriminaliteit wordt uitgevaardigd. Hoewel het verdrag zeer breed is, werd jammer genoeg over racisme en antisemitisme in alle talen gezwegen om de Amerikaanse steun niet te verliezen. Dit dient betreurd te worden.

Een laatste vaststelling of bemerking in deze eindconclusie houdt verband met de diensten die in België actief zijn in de strijd tegen "cybercrime". Tot op heden blijkt de Federal Computer Crime Unit nog steeds te kampen met een gebrek aan personeel.

Politiediensten kunnen sinds de Wet Informaticacriminaliteit beroep doen op nieuwe opsporingstechnieken zoals databeslag, medewerkingverplichting, netwerkzoeking en interceptie van communicatie. Het spreekt voor zich dat deze middelen in de praktijk slechts hun nut kunnen bewijzen indien voldoende personeel voorhanden is om deze technieken toe te passen. In elk ander geval blijft de wet dode letter.

Bibliografie

INTERNATIONALE REGELGEVING EN AANBEVELINGEN

- COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's*, de informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden, COM (2000) 890 definitief, *Brussel*, 2001.

- COUNCIL OF EUROPE, *Committee of Experts on Crime in Cyberspace*, Green Paper on the protection of minors and human dignity in audiovisual and information services, PC-CY (97) 20, *Strasbourg*, 14 april 1997.

- COUNCIL OF EUROPE, *Computer-Related Crime*, Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989, *Strasbourg*, 1989.

- COUNCIL OF EUROPE, *Computer-Related Crime*, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, *Strasbourg*, 1990.

- COUNCIL OF EUROPE, Convention on Cybercrime, ETS no. 185, Budapest, 2001.

- COUNCIL OF EUROPE, *European Committee on Crime Problems*, Committee of Experts on the criminalisation of acts of a racist or xenophobic nature committed through computer systems, Public version N° 2, Strasbourg, 26 March 2002.

- EUROPEES PARLEMENT EN DE RAAD, Richtlijn 91/250/EEG betreffende de rechtsbescherming van computerprogramma's, *Straatsburg*, 14 mei 1991.

- EUROPEES PARLEMENT EN DE RAAD, Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Straatsburg*, 24 oktober 1995.

- EUROPEES PARLEMENT EN DE RAAD, Richtlijn 96/9/EG betreffende de rechtsbescherming van databanken, *Straatsburg*, 11 maart 1996.

- EUROPEES PARLEMENT EN DE RAAD, Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer, *Straatsburg*, 15 december 1997.

- EUROPEES PARLEMENT EN DE RAAD, Richtlijn 2001/29/EG betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, *Straatsburg*, 22 mei 2001.

- OECD, Recommendation of the Council concerning Guidelines for the Security of Information Systems, adopted on 26 november 1992, C(92)188/FINAL, *Paris*, 1992.

- UNITED NATIONS, Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. GAOR, 53rd Sess., U.N. Doc. A/RES/53/70, *New York*, 1998.

- RAAD VAN DE EUROPESE UNIE, Besluit van de Raad ter bestrijding van kinderpornografie op Internet, PB L 138 van 9.6.2000, *Brussel*, 29 mei 2000.

- WORKING PARTY ON THE PROTECTION OF INDIVIDUALS TO THE PROCESSING OF PERSONAL DATA, Recommendation No. 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes adopted on 7 september 1999, *Brussels*, 1999.

WETTEN

- Wet van 19 juli 1930 tot oprichting van de Regie van Telegraaf en Telefoon, *B.S.*, 2 augustus 1930.

- Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, *B.S.*, 8 augustus 1981.

- Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.*, 27 maart 1991.

- Wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, *B.S.*, 27 juli 1994.

- Wet van 23 maart 1995 tot bestraffing van het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistische regime is gepleegd, *B.S.*, 30 maart 1995.

- Wet van 27 maart 1995 tot invoeging in het Strafwetboek van een artikel 380quinquies en tot opheffing van het artikel 380quater, tweede lid, van hetzelfde Wetboek, *B.S.*, 25 april 1995.

- Wet van 13 april 1995 houdende bepalingen tot bestrijding van de mensenhandel en van de kinderpornografie, *B.S.*, 25 april 1995.

- Wet van 12 maart 1998 tot verbetering van de strafrechtspleging in het stadium van het opsporingsonderzoek en het gerechtelijk onderzoek, *B.S.*, 2 april 1998.

- Wet op de kansspelen, de kansspelinrichtingen en de bescherming van de spelers, *B.S.*, 30 december 1999.

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

WETSONTWERPEN

- Wetsontwerp inzake Informaticacriminaliteit, *Parl. St.*, Kamer, nr. 213/001, 3 november 1999, 75 p.

COMMISSIEVERSLAGEN EN ANDERE PARLEMENTAIRE DOCUMENTEN

- Verslag namens de Commissie voor de Justitie, *Belgische Senaat*, 28 juni 2000, nr. 2 – 392/3.

- Verslag namens de Commissie, *Kamer van Volksvertegenwoordigers,* 19 oktober 2000, nr. 50 0213/011.

- Vraag om uitleg van mevrouw Erika Thijs aan de minister van Binnenlandse Zaken en aan de minister van Justitie over de FCCU, *Belgische Senaat*, 17 april 2002, nr. 2-197.

RECHTSPRAAK

- Rb. Brussel, 8 november 1990, *Computerrecht*, 1991, 31.

- Cass, 15 maart 1994, *Arr. Cass*, 245, noot G.VERMEULEN.

- Corr. Gent, 11 december 2000, [WWW] Recht en Informatica, Universiteit Gent: http://allserv.rug.ac.be/~rdecorte/documenten/Rechtspraak/2000_12_11_Redattack.pdf [10/04/02]

- Corr. Brussel, 15 januari 2002, [WWW] Centrum voor gelijkheid van kansen en racismebestrijding: http://www.antiracisme.be/nl/rechtspraak/vonnissen/2002/02-01-15_c_bsl.pdf [03/04/02]

MINISTERIELE OMZENDBRIEVEN EN RICHTLIJNEN

- COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn,* 16 maart 1999, omzendbrief *nr.* COL 6/1999.

- COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 31 mei 1999, omzendbrief nr. COL 12/1999.

- COLLEGE VAN PROCUREURS-GENERAAL, *Ministeriële richtlijn*, 14 februari 2002, omzendbrief nr. COL 01/2002.

HANDBOEKEN

- BONI, W.C., KOVACICH, G.L. en KENNEY, J.P., *I-Way Robbery: Crime on the Internet*, Woburn, Butterworth-Heineman, 1999, 240 p.

- BRUINSMA, G.J.N., VAN DE BUNT, H.G. en HAEN MARSHALL, I., Met het oog op de toekomst, verkenning naar de kennisvragen over misdaad en misdaadbestrijding in 2010, in AWT-Achtergrondstudies, TIMMERHUIS, V. (ed), 24, Den Haag, AWT, 2001, 71 p.

- CALCETAS-SANTOS, O., *Child pornography on the Internet*, in *Child abuse on the Internet, ending the silence*, ARNALDO C.A., (ed.), Paris, Unesco publishing, 2001, 220 p.

- COOLS M. en VANKEIRSBILCK K., *Handboek Security, beheersing van criminele risico's*, Diegem, Samsom, 1995, 800 p.

- DE RUYVER, B., VERMEULEN, G. EN VANDERBEKEN, T., (eds.), *Strategies of the EU and the US in Combating Transnational Organized Crime*, Antwerpen, Maklu, 2002, 250 p.

- DE VREESE, S., 'Belgische hooligans op het Internet' in *Handboek Politiediensten*, Diegem, Kluwer, 1999, 3500 p.

- DE ZEGHER, J., *Openbare zedenschennis*, in *APR-reeks*, Gent, Story-Scientia, 1973, 225 p.

- DUMORTIER, J., *Informatica-en telecommunicatierecht*, Leuven, ICRI, 1999, 214 p.

- FURNELL, S., *Cybercrime, Vandalizing the information society*, London, Addison-Wesley, 2002, 316 p.

- GRABOSKY, P.N. en SMITH, R.G., *Crime in the digital age: controlling telecommunications and cyberspace*, Sydney, Federation Press, 1998, 272 p.

- HAFNER, K. en LYON, M., *Where Wizards Stay Up Late: The Origins of the Internet*, New York, Simon & Schuster, 1998, 304 p.

- KASPERSEN, R., HOFMAN, A. en VERBEEK, J., 'Vertrouwelijkheid van e-mail', in *Nationaal Programma Informatietechnologie en Recht*, DE KROON, A. en SCHMIDT, A., (eds.), Deventer, Kluwer, 1999, 352 p.

- KASSENAAR, P., *Basiscursus Dreamweaver 4*, Schoonhoven, Academic Service, 2001, 277 p.

- KELLEHER, D. en MURRAY, K., *IT law in the European Union*, London, Sweet en Maxwell, 1999, 383 p.

- KÖHLER, M. en ARNDT., H.W., *Recht des Internet*, Heidelberg, Müller Verlag, 2000, 164 p.

- LAUREYS, T, *Informaticacriminaliteit*, Gent, Mys en Breesch, 2001, 117 p.

- MCLEAN, J.J., 'Homocide and child pornography' in *Handbook of Computer Crime Investigation*, CASEY, E., (eds.), London, Academic Press, 2002, 448 p.

- SIEBER, U., *Computerkriminalität und Strafrecht*, München, Heymans, 1980, 364 p.

- SIEBER, U., *The International Handbook on Computer Crime, Computer-Related Economic Crime and the Infringements of Privacy*, New York, Wiley & Sons, 1986, 290 p.

- SHIPLEY, T.G., 'Internet gambling investigations', in *Handbook of Computer Crime Investigation*, CASEY, E., (ed.), London, Academic Press, 2002, 448 p.

- SPRUYT, B., 'Computers op de strafbank', in *Informaticacriminaliteit,* DE SCHUTTER, B., (ed.), VII, Antwerpen, Kluwer, 1987, 777 p.

- SUTHERLAND, E., *White Collar Crime*, New York, Holt, Rinehart and Winston, 1949, 272 p.

- THOMAS, D. en LOADER B.D., Cybercrime: law enforcement, security and surveillance in the information age, London, Routledge, 2000, 300 p.

- VAN DEN WYNGAERT, C., *Strafrecht en strafprocesrecht in hoofdlijnen*, Boek 2, Antwerpen, Maklu, 1999, 543 p.

- VAN EECKE P., *Criminaliteit in Cyberspace*, Gent, Mys en Breesch, 1997, 121 p.

- VERMEULEN, G., *Wederzijdse rechtshulp in strafzaken in de Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de Lidstaten?*, Antwerpen, Maklu, 1999, 632 p.

- WELLS, L.E., 'Explaining crime in the year 2010' in *Crime and Justice in the Year 2010,* KLOFAS, J. en STOJKOVIC, S., (eds.), Belmont, CA Wadsworth, 1995, 320 p.

TIJDSCHRIFTEN

- BEIRENS, B., 'Op zoek naar criminele bits, digitaal rechercheren', *Politeia*, 1998, afl. 8, 9-12.

- BERKMOES, H., VAN DAELE, R., en DE BIE, B., 'Misdaad loont niet (meer?). De bijzondere verbeurdverklaring van vermogensvoordelen en de bestrijding van het witwassen in België', *Politeia*, 1994, 69-70.

- CAUBERGHE, L., 'Een harde noot voor krakers', *Computable*, 1991, afl. 2, 11-12.

- CLOUGH, B., 'Computer Crime', *Intersec*, 1997, 364-366.

- COLLIN, B.C., 'The future of cyberterrorism: the physical and virtual worlds converge', *Crime and justice international*, 1997, afl. 2, 14-18.

- DE DECKER, K., 'Het weerloze web', *Knack*, 2000, afl. 48, 92-95.

- DE SCHUTTER, B., 'Belgisch voorontwerp van wet inzake informaticacriminaliteit', *Computerrecht*, 1990, 208-210.

- DE SCHUTTER, B., 'Het Belgisch Bistel-syndroom', C*omputerrecht*, 1991, 164-166.

- DOMMERING, E.J., 'Het auteursrecht spoelt weg door het elektronische vergiet. Enige gedachten over de naderende crisis van het auteursrecht', *Computerrecht*, 1994, 109-110.

- DUMORTIER, J., VAN OUDENHOVE, B. en VAN EECKE, P., 'De nieuwe Belgische wetgeving inzake informaticacriminaliteit', *Vigiles*, 2001, 44-63.

- DUPONT, L., 'De wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden', *Panopticon*, 1981, 504-506.

- ERKELENS, C., 'Beteugeling van computercriminaliteit', *Panopticon,* 1985, 334-345.

- GOODMAN, M., 'Making computer crime count', *FBI Law Enforcement Bulletin*, 2001, afl. 8, 10-17.

- GOOSSENS, F., 'De wet inzake Informaticacriminaliteit', *Tijdschrift voor Wetgeving*, 2001, 94-99.

- KARTER, D. en KATZ, A., 'An emerging challenge for law enforcement', *FBI Law Enforcement Bulletin*, 1996, afl. 12, 1-8.

- NIEMEIJER, E. en NIJBOER, J., 'Informatisering van samenleving en criminaliteit', *Tijdschrift voor Criminologie*, 1999, 340-349.

- POLLITT, M.M., 'Cyberterrorism, fact or fancy?', *Computer Fraud and security*, 1998, afl. 2, 8-10.

- RIMM, M., 'Marketing pornography on the information superhigway', *Georgetown Law Journal*, 1995, 1849-1934.

- RINGENOLDUS, D.H., 'De computermisdadiger is de oude oplichter, schade door computerinbraken loopt de spuigaten uit', *Telecommagazine*, 1996, afl. 9, 12-18.

- SCHAAP, C.D., ROZEKRANS, R., VAN DUYNE, P.C., 'Geld witwassen. Een probleemverkenning van de opbrengstkant van op winst gerichte misdaad', *Tijdschrift voor de politie*, 1992, 107-111.

- SENNESAEL, V., 'National Computer Crime Unit: digitale flikken', *Computer Magazine*, 2000, afl. 6, 73-75.

- STOL, W.P., VAN TREECK, R.J. en VAN DER VEN A.E.B.M., 'Criminaliteit met ICT', *Modus*, 2000, afl. 4, 8-13.

- VANDEMEULEBROEKE O. en GAZAN, 'Traite des êtres humains, exploitation et abus sexuels. Les nouvelles lois des 27 mars et 13 avril 1995', *Revue de droit pénal*, 1995, 973-1077.

- VANDEVINNE, D., 'Computer Crime Units: Belgische cyberpolitie', *Computer Magazine*, 2001, afl. 7, 10-12.

- VERMEULEN, G., 'Kinderhandel, seksuele uitbuiting van kinderen, kinderporno en kindersekstoerisme', *Panopticon*, 2000, 201-207.

- VRIESDE, R., VAN OSS, J. en GELS, M., 'Criminaliteit op Internet, een eerste aanzet voor digitale surveillance en opsporing', *Algemeen Politieblad*, 1999, afl. 12, 8-10.

- VRIESDE, R., VAN OSS, J. en GELS, M., 'Criminaliteit op Internet, een overzicht van de verschijningsvorm', *Algemeen Politieblad*, 1999, afl. 13, 8-13.

- X., 'Cyber terrorism specialists gather in Chicago', *Crime and justice international*, 1998, afl. 20, 7-8.

INTERNETVERWIJZINGEN NAAR KRANTENARTIKELS

- ANP., (2001/11/15) 'Fraudenetwerk op web ontmanteld' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Nieuws/2001/04/14/Med/inhoud.html [15/ 11/01]

- BAEYENS, H., (2001/03/06) 'Het onveiligheidsgevoel op Internet' [WWW]. De Standaard Online: http://www.standaard.be/thema/multimedia/index.asp?doctype=detail.asp&ArticleID=DSM06032001_004 [24/12/01]

- BETTENS, B., (2001/02/20) 'Vlaamse kmo's hebben schrik voor e-commerce' [WWW]. De Standaard Online: http://www.standaard.be/thema/multimedia/index.asp?doctype=detail.asp &ArticleID=DSM20022001_004 [24/12/01]

- BOON, P., (2000/05/05) 'Virus vermomt zich als liefdesbrief' [WWW]. De Standaard Online: http://www.standaard.be/nieuws/economie/detail.asp?articleID=DST05052000_045&Doctype=detail.asp [15/04/02]

- CDR, (2000/03/25) 'E-mail stalker terroriseert gezin' [WWW]. De Standaard Online: http://www.destandaard.be/Archief/zoeken/DetailNew.asp?articleID=DST25032000_020&trefwoord=e%2Dmail [01/04/02]

- DE GRAEVE, F., (2001/11/23) 'On-line gokken in de lift' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DST23112001_013&trefwoord=virus [04/04/02]

- DJD., (2002/01/22) 'België beleefde breedband-explosie' [WWW]. De Standaard Online: http://www.standaard.be/Nieuws/Economie/index.asp?articleID=DEXA22012002_073&DocType=detail.asp [27/02/02]

- FDG, (2001/12/24) 'Geen bewondering voor virusschrijvers' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DST24122001_055&trefwoord=virus [04/04/02]

- KETELAAR, T., (2000/05/17) 'Cybercrime: kluif voor diplomaten' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Nieuws/2000/05/17/Med/02.html [01/04/02]

- LEFELON, P. en VAN AUDENAERDE, A., (1999/08/11) 'Internetpiraat kraakt Skynet' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=dss9908110011&trefwoord=redattack [10/04/02]

- PLA, (2001/04/21) 'Politie patrouilleert niet op het internet' in De Standaard Online [WWW]. De Standaard: http://www.destandaard.be/Archief/zoeken/DetailNew.asp?articleID= DST21042001_025 [15/10/01]

- STEKETEE, M., (2001/04/04) 'Nieuw Chinees militair zelfvertrouwen' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Nieuws/2001/04/04/Vp/05a.html [28/03/02]

- VANDERSMISSEN, M., (2001/10/05) 'Federal Computer Crime Unit: te weinig personeel en materieel' [WWW]. De Standaard Online: http://www.destandaard.be/Archief/zoeken/DetailNew.asp?articleID =DST05102001_029 [15/10/01] [28/03/02]

- VAN EECKE, P., (2002/02/18) 'Asmodeus, de webscalpeerder' [WWW]. De Standaard Online: http://www.standaard.be/Archief/zoeken/DetailNew.asp?articleID=DST18022002_124&trefwoord=asmodeus [01/04/02]

- VAN EECKE, P., (2001/11/12) 'Cyberstalking' in De Standaard Online [WWW]. De Standaard: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DST12112001_123&trefwoord=stalking [27/03/02]

- WUYTS, D., (2001/02/20) 'Hacken: wat is het en wat doe je eraan?' [WWW]. De Standaard Online: http://www.standby.be/Archief/zoeken/DetailNew.asp?articleID=DSM20022001_001&trefwoord=kredietkaart [02/04/02]

- X., (2002/01/26) 'Explosion des connexions' [WWW]. Le Soir en ligne: http://www.lesoir.com/articles/A_021981.asp [27/02/02]

- X., (1999/12/01) 'Hooligans met leger op Internet' [WWW]. NRC Handelsblad: http://www.nrc.nl/W2/Lab/EK2000/veiligheid/veilig991013wwwhool.html [20/03/02]

- Y.B., (2001/12/12) 'Minderjarige hackers lopen tegen de lamp' [WWW]. De Standaard Online: http://www.standaard.be/Archief/zoeken/DetailNew.asp?articleID=DST12122001_020&trefwoord=hackers [01/04/02]

ANDERE INTERNETREFERENTIES

- BENSCHOP, A., (2001/04/14) 'Wat is Usenet?' [WWW] Universiteit van Amsterdam, Social Science Information System: http://www.pscw.uva.nl/sociosite/about_usenet.html [22/12/01]

- CAMPBELL, T., (1998/03) 'The first e-mail message, who sent it and what it said' [WWW]. Pretext Magazine: http://www.pretext.com/mar98/features/story2.htm [08/12/01]

- CARABALLO, D. en LO, J., (2000/01/06) 'The IRC Prelude, what is IRC and how does it work?' [WWW]. IRC Help: http://www.irchelp.org/irchelp/new2irc.html [23/12/01]

- DNS BELGIË, (2001) 'De historiek van DNS' [WWW]. http://www.dns.be/nl/AboutUs/history.htm [06/03/02]

- GOVERNMENT OF CANADA, (2001/02/27) 'G8 Justice and Interior Ministers' Meeting' [WWW]. http://www.g8.gc.ca/genoa/2001/Milan_Justice_Interior-e.asp [01/04/02]

- ISPA, (2002/01/23) 'De Internetmarkt' [WWW]. Internet Service Providers Association: http://www.ispa.be/nl/d000200.html [27/02/02]

- JONES, J., (2001/07/23) 'Almost all e-mail users say Internet, e-mail have made lives better' [WWW]. The Gallup Organization: http://www.gallup.com/poll/releases/pr010723.asp [08/12/01]

- LUIIJF, E., (1999) 'Information warfare: de kwetsbaarheid van de samenleving' [WWW]. TNO Fysisch en Elektronisch Laboratorium: http://www.tno.nl/instit/fel/refs/pub99/io_war.html [28/03/02]

- MARCA, (1993/03/14) 'NCSA Mosaic for X 0.10 available' in comp.infosystems.gopher [news]. marca@ncsa.uiuc.edu [12/12/01]

- MINISTERIE VAN ECONOMISCHE ZAKEN, (2002/02/26) 'Communicatiemedia en Audiovisuele media' [WWW]. Nationaal Instituut voor de Statistiek: http://statbel.fgov.be/figures/d75_nl.asp#3 [27/02/02]

- MINISTERY OF FOREIGN AFFAIRS OF JAPAN, (2000/10/26) 'The G8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace' [WWW]. G8 summit: http://www.mofa.go.jp/policy/economy/summit/2000/lyon.html [01/04/02]

- OSTC, (1999) 'Wetgeving: inbraak' [WWW]. PISA, Providing Information About Internet Security Aspects: http://pisa.belnet.be/pisa/nl/juridisch/crack.htm [17/03/02]

- SICHERHEIT IM INTERNET (2001/05/24) 'Tokio G8 Workshop Press Release' [WWW]. http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=20&tdid=837&page=0 [01/04/02]

- TIMBL (1991/08/06) 'WorldWideWeb: Summary' in alt.hypertext [news]. timbl@info_.cern.ch [12/12/01]

- WUYTS, S. (2001/10/03) 'Dertig jaar elektronische post, bescheiden programma wordt killer-app' [WWW]. De Cursor: http://www.decursor.be/Nieuwsflash/index.html?330l02 [08/12/01]

- WUYTS, S., (s.d.) 'IRC: tien jaar wereldwijd babbelen' [WWW]. De Cursor: http://www.decursor.be/On-line/IRC/index.html [23/12/01]

- X., (1997//03/12) 'An overview of the World Wide Web' [WWW]. European Organisation for Nuclear Research: http://public.web.cern.ch/Public/ACHIEVEMENTS/WEB/Welcome.html [19/10/01]

- X., (s.d.) 'De strijd tegen piraterij' [WWW]. Business Software Alliance: http://www.bsa.org/belgium-dutch/antipiracy/imitatie.phtml [09/02/02]

- X., (2002/03/25) 'Europol krijgt waarnemingscentrum voor hightechcriminaliteit' [WWW]. Security.nl: http://www.security.nl/artikel.php3?id=2904 [01/04/02]

- X, (1999/07/02) 'Hacker Tool Targets Windows NT' [WWW]. PC World: http://www.pcworld.com/news/article.asp?aid=11662 [31/03/02]

- X., (1994/14/11) 'Mosaic Communications changes name to Netscape Communications Corporation' [WWW]. Netscape: http://home.netscape.com/newsref/pr/newsrelease5.html [19/10/01]

- X., (1997/12/10) 'Meeting of Justice and Interior Ministers' [WWW] The Birmingham Summit: http://birmingham.g8summit.gov.uk/prebham/washington.1297.shtml [01/04/02]

- X., (1999/05/28) 'Samenwerkingsprotocol ter bestrijding van ongeoorloofd gedrag op het Internet' [WWW]. Internet Service Providers Association Belgium ISPA: http://www.ispa.be/nl/c040202.html [07/08/01]

- X., (1994) 'The Anarchist Cookbook' [WWW]. The Little Bookstore: http://come.to/anarchy [27/03/02]

- X., (2001/11/22) 'The road to the treaty' [WWW]. Cybercrime Convention: http://www.stopcybercrime.net/2_1_1.php [01/04/02]

- X., (s.d.) 'Wat is FTP?' [WWW]. Surfnet: http://www.surfkit.nl/knowledge/ftp/home.html [23/12/01]

ANDERE DOCUMENTEN

- BEIRENS, L., Businessplan bijstand voor onderzoek in ICT, strijd tegen ICT-criminaliteit. Brussel, januari 2001, 21 p. (businessplan).

- BEIRENS. L., Organisatie en werking van de Federal Computer Crime Unit en de regionale Computer Crime Units, Brussel, april 2001, 11 p. (informatiefiche).

- COMPUTER SECURITY INSTITUTE, *Computer Crime and Security Survey*, 2001, 20 p. (onderzoeksrapport).

- CISCO SYSTEMS, Internet Revolutie zorgt voor omwenteling van de manier waarop we werken, leven, spelen en leren, Amsterdam, juni 1999. (persbericht).

- DE CANG, T., PITEUS, K. en VAN WASSENHOVE, I., *Kinderpornografie*, Gent, Academiejaar 2000-2001, 59 p. (scriptie in het kader van het vak Grondige Studie van het Strafrecht).

- DEMOTTE, G., *Elektronische handel*, Brussel, juli 2000, 11 p. (oriëntatienota Ministerie van Economische Zaken).

- DNS BELGIË, *liberalisering domeinnamen,* Leuven, september 2000. (persbericht).

- DROIT ET NOUVELLES TECHNOLOGIES, *La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique*, 2001, 28 p. (onderzoekspaper).

- INSITES CONSULTING, België telt 3,2 miljoen regelmatige Internetgebruikers, Gent, april 2002. (persbericht).

- INTERNET FRAUD COMPLAINT CENTER, *Six-month data trends report*, 2001, 14 p. (onderzoeksrapport).

- ISPA, *4de kwartaal van 2001: explosie breedband in België bevestigt trend van het hele jaar 2001*, Brussel, januari 2002. (persbericht).

- LOUVEAUX, S., *Le Spamming, état de la question*, CRID, Namur, oktober 2000, 7 p. (onderzoekspaper).

- MINISTERIE VAN VERKEER EN WATERSTAAT, *Kwetsbaarheid van het Internet*, Stratix Consulting Group, Schiphol, januari 2001, 224 p. (eindrapport).

- OGILVIE, E., 'Cyberstalking' in *Trends and Issues in Crime and Criminal Justice*, Australian Institute of Criminology, 2000, 6 p. (nieuwsbrief).

- PRICEWATERHOUSECOOPERS, *European Economic Crime Survey*, 2001, 18 p. (onderzoeksrapport).

- SABAM, *Het auteursrecht in de kijker*, 2001, 8 p. (brochure).

- VERENIGINGEN ZONDER WINSTOOGMERK, Statuten DNS België, *B.S.* 17 juni 1999 (bijlage), 5089-5091.

Bijlagen

Bijlage I: Wet van 28 november 2000 inzake Informaticacriminaliteit

LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

MINISTERE DE LA JUSTICE

F. 2001 — 298 [S − C − 2001/09035]

28 NOVEMBRE 2000. — Loi du 28 novembre 2000 relative à la criminalité informatique (1)

ALBERT II, Roi des Belges,

A tous, présents et à venir, Salut.

Les Chambres ont adopté et Nous sanctionnons ce qui suit :

CHAPITRE Ier. — *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE II. — *Dispositions complétant le Code pénal*

Art. 2. L'intitulé du chapitre IV, titre III, livre II du Code pénal, est remplacé par l'intitulé suivant :

« Des faux commis en écritures, en informatique et dans les dépêches télégraphiques. »

Art. 3. A l'article 193 du même Code, les mots « , en informatique » sont insérés entre les mots « en écritures » et les mots « ou dans les dépêches télégraphiques ».

Art. 4. Il est inséré dans le livre II, titre III, chapitre IV, du même Code une section II*bis*, rédigée comme suit :

« Section II*bis*. — Faux en informatique

Art. 210*bis*. § 1er. Celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 2. Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.

§ 3. La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cinquante mille francs ou d'une de ces peines seulement.

§ 4. Les peines prévues par les §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259*bis*, 314*bis*, 504*quater* ou au titre IX*bis*. »

Art. 5. Il est inséré dans le livre II, titre IX, chapitre II du même Code une section III*bis*, rédigée comme suit :

« Section III*bis*. — Fraude informatique

Art. 504*quater*. § 1er. Celui qui se procure, pour soi-même ou pour autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 2. La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cinquante mille francs ou d'une de ces peines seulement.

§ 3. Les peines prévues par les §§ 1er et 2 sont doublées si une infraction a l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis* ou au titre IX*bis*. »

MINISTERIE VAN JUSTITIE

N. 2001 — 298 [S − C − 2001/09035]

28 NOVEMBER 2000. — Wet van 28 november 2000 inzake informaticacriminaliteit (1)

ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamers hebben aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK I. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK II. — *Bepalingen tot aanvulling van het Strafwetboek*

Art. 2. Het opschrift van hoofdstuk IV, titel III, boek II van het Strafwetboek wordt vervangen als volgt :

« Valsheid in geschriften, in informatica en in telegrammen. »

Art. 3. In artikel 193 van hetzelfde Wetboek worden de woorden « geschriften of in telegrammen » vervangen door de woorden « geschriften, in informatica of in telegrammen ».

Art. 4. In boek II, titel III, hoofdstuk IV van hetzelfde Wetboek wordt een afdeling II*bis* ingevoegd, luidende :

« Afdeling II*bis*. — Valsheid in informatica

Art. 210*bis*. § 1. Hij die valsheid pleegt, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 2. Hij die, terwijl hij weet dat aldus verkregen gegevens vals zijn, hiervan gebruik maakt, wordt gestraft alsof hij de dader van de valsheid was.

§ 3. Poging tot het plegen van het misdrijf, bedoeld in § 1, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank of met een van die straffen alleen.

§ 4. De straffen bepaald in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 259*bis*, 314*bis*, 504*quater* of in titel IX*bis*. »

Art. 5. In boek II, titel IX, hoofdstuk II van hetzelfde Wetboek wordt een afdeling III*bis* ingevoegd, luidende :

« Afdeling III*bis*. — Informaticabedrog

Art. 504*quater*. § 1. Hij die, voor zichzelf of voor een ander, een bedrieglijk vermogensvoordeel verwerft, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 2. Poging tot het plegen van het misdrijf bedoeld in § 1 wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank, of met een van die straffen alleen.

§ 3. De straffen bepaald in de §§ 1 en 2 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis* of in titel IX*bis*. »

Art. 6. Il est inséré dans le livre II du même Code un titre IX*bis*, rédigé comme suit :

« Titre IX*bis*. — Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes.

Art. 550*bis*. § 1er. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§ 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d une de ces peines seulement.

§ 3. Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui :

1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique;

2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;

3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;

est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six francs belges à cinquante mille francs ou d'une de ces peines seulement.

§ 4. La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie des mêmes peines.

§ 5. Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1er à 4 peuvent être commises, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 6. Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent francs à deux cent mille francs ou d'une de ces peines seulement.

§ 7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 8. Les peines prévues par les §§ 1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*ter*.

Art. 550*ter*. § 1er. Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation possible de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.

§ 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à septante-cinq mille francs ou d'une de ces peines seulement.

§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

Art. 6. In boek II van hetzelfde Wetboek wordt een titel IX*bis* ingevoegd, luidende :

« Titel IX*bis*. — Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen.

Art. 550*bis*. § 1. Hij die, terwijl hij weet dat hij daar toe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van zesentwintig frank tot vijfentwintig duizend frank of met een van die straffen alleen.

Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, bedraagt de gevangenisstraf zes maanden tot twee jaar.

§ 2. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.

§ 3. Hij die zich in een van de gevallen bedoeld in de §§ 1 en 2 bevindt en :

1° hetzij de gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het informaticasysteem op enige manier overneemt;

2° hetzij enig gebruik maakt van een informaticasysteem van een derde of zich bedient van het informaticasysteem om toegang te verkrijgen tot een informaticasysteem van een derde;

3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die door middel van het informaticasysteem worden opgeslagen, verwerkt of overgedragen of aan een informaticasysteem van een derde of aan de gegevens die door middel van het laatstgenoemde informaticasysteem worden opgeslagen, verwerkt of overgedragen;

wordt gestraft met gevangenisstraf van een jaar tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank of met een van die straffen alleen.

§ 4. Poging tot het plegen van een van de misdrijven, bedoeld in §§ 1 en 2, wordt gestraft met dezelfde straffen.

§ 5. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem en waarmee de misdrijven, bedoeld in §§ 1 tot 4, gepleegd kunnen worden, opspoort, verzamelt, ter beschikking stelt, verspreidt of verhandelt, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 6. Hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven, bedoeld in §§ 1 tot 5, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van honderd frank tot tweehonderdduizend frank of met een van die straffen alleen.

§ 7 Hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 8. De straffen bepaald in de §§ 1 tot 7 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of 550*ter*.

Art. 550*ter*. § 1. Hij die, met het oogmerk om te schaden, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist, of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.

§ 2. Hij die, ten gevolge van het plegen van een misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot vijfenzeventigduizend frank of met een van die straffen alleen.

§ 3. Hij die, ten gevolge van het plegen van een van de misdrijven bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van zesentwintig f rank tot honderdduizend frank of met een van die straffen alleen.

§ 4. Celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des données stockées, traitées ou transmises par un système informatique, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis*. »

CHAPITRE III. — *Dispositions modifiant le Code d'instruction criminelle*

Art. 7. Il est inséré dans le Code d'instruction criminelle un article 39*bis*, rédigé comme suit :

« Art. 39*bis*. § 1er. Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28*sexies*, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.

§ 2. Lorsque le procureur du Roi découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

§ 3. Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

§ 4. Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

§ 5. Le procureur du Roi informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.

§ 6. Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents. »

§ 4. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, ontwerpt, ter beschikking stelt, verspreidt of verhandelt, terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 5. De straffen bepaald in de §§ 1 tot 4 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of 550*bis*. »

HOOFDSTUK III. — *Bepalingen tot wijziging van het Wetboek van strafvordering*

Art. 7. In het Wetboek van strafvordering wordt een artikel 39*bis* ingevoegd, luidende :

« Art. 39*bis*. § 1. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit wetboek inzake inbeslagneming, met inbegrip van artikel 28*sexies*, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem opgeslagen gegevens.

§ 2. Wanneer de procureur des Konings in een informaticasysteem opgeslagen gegevens aantreft die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

§ 3. Hij wendt bovendien de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om deze gegevens ontoegankelijk te maken.

Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.

§ 4. Wanneer de in § 2 vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt hij de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

§ 5. De procureur des Konings brengt de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking in het informaticasysteem en deelt hem een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk gemaakt of verwijderd.

§ 6. De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.

Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie.

Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informaticasysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen. »

Art. 8. Il est inséré dans le même Code un article 88*ter*, rédigé comme suit :

« Art. 88*ter*. § 1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :

— si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et

— si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

§ 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.

§ 3. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39*bis* s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.

§ 4. L'article 89*bis* est applicable à l'extension de la recherche dans un système informatique. »

Art. 9. Il est inséré dans le même Code un article 88*quater*, rédigé comme suit :

« Art. 88*quater*. § 1er. Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi.

§ 2. Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.

§ 3. Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

§ 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 5. L'Etat est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système. »

Art. 10. A l'article 89 du même Code, modifié par les lois des 10 juillet 1967 et 20 mai 1997, les mots « et 39 » sont remplacés par les mots « , 39 et 39*bis* ».

Art. 8. In hetzelfde Wetboek wordt een artikel 88*ter* ingevoegd, luidende :

« Art. 88*ter*. § 1. Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, kan deze zoeking worden uitgebreid naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt :

— indien deze uitbreiding noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

— indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.

§ 2. De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben.

§ 3. Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in artikel 39*bis*. De onderzoeksrechter brengt de verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

§ 4. Artikel 89*bis* is van toepassing op de uitbreiding van de zoeking in een informaticasysteem. »

Art. 9. In hetzelfde Wetboek wordt een artikel 88*quater* ingevoegd, luidende :

« Art. 88*quater*. § 1. De onderzoeksrechter, of in zijn opdracht een officier van gerechtelijke politie, hulpofficier van de procureur des Konings, kan personen van wie hij vermoedt dat ze een bijzondere kennis hebben van het informaticasysteem dat het voorwerp uitmaakt van de zoeking of van diensten om gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verstrekken over de werking ervan en over de wijze om er toegang toe te verkrijgen, of in een verstaanbare vorm toegang te verkrijgen tot de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De onderzoeksrechter vermeldt de omstandigheden eigen aan de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings.

§ 2. De onderzoeksrechter kan iedere geschikte persoon bevelen om zelf het informaticasysteem te bedienen of de ter zake dienende gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.

Het bevel bedoeld in het eerste lid kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.

§ 3. Hij die weigert de in §§1 en 2 gevorderde medewerking te verlenen of de zoeking in het informaticasysteem hindert, wordt gestraft met gevangenisstraf van zes maanden tot één jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.

§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. De Staat is burgerrechtelijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt. »

Art. 10. In artikel 89 van hetzelfde Wetboek, gewijzigd bij de wetten van 10 juli 1967 en 20 mei 1997, worden de woorden « en 39, » vervangen door de woorden « , 39 en 39*bis*, ».

Art. 11. A l'article 90*ter*, § 2, du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois des 7 avril 1995, 13 avril 1995, 10 juin 1998 et 10 janvier 1999, sont apportées les modifications suivantes :

A) le 1°*bis* est remplacé par les dispositions suivantes :

« 1°*bis*. A l'article 210*bis* du même Code;

1°*ter*. A l'article 259*bis* du même Code;

1°*quater*. A l'article 314*bis* du même Code;

1°*quinquies*. Aux articles 324*bis* et 324*ter* du même Code »;

B) il est inséré un 10°*bis*, rédigé comme suit :

« 10°*bis*. A l'article 504*quater* du même Code »;

C) il est inséré un 13°*bis*, rédigé comme suit :

« 13°*bis*. Aux articles 550*bis* et 550*ter* du même Code. »

Art. 12. L'article 90*quater* du même Code, inséré par la loi du 30 juin 1994 et modifié par la loi du 10 juin 1998, est complété par un § 4, rédigé comme suit :

« § 4. Le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.

Il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

Celui qui refuse de fournir la collaboration ordonnée conformément aux alinéas précédents, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est appelée à y prêter son concours technique, est liée par le secret de l'instruction. Toute violation du secret sera punie conformément à l'article 458 du Code pénal. »

Art. 13. A l'article 90*septies* du même Code, inséré par la loi du 30 juin 1994 et remplacé par la loi du 10 juin 1998, il est inséré entre le quatrième et le cinquième alinéa, un nouvel alinéa, rédigé comme suit :

« Les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée et, dans la mesure du possible, pour réaliser sa transcription ou sa traduction. La même règle vaut pour la conservation au greffe des enregistrements et de leur transcription ou de leur traduction et pour les mentions dans le registre spécial. Le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, ces moyens et le moment où ils remplacent la conservation sous pli scellé ou le registre spécial prévus aux alinéas 3 et 4. »

CHAPITRE IV. — *Disposition modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques*

Art. 14. A l'article 109*ter*, E, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, inséré par la loi du 21 décembre 1994, renuméroté par la loi du 19 décembre 1997 et remplacé par la loi du 10 juin 1998, sont apportées les modifications suivantes :

— 1° l'alinéa 1er du § 2 est complété comme suit :

« , ainsi que les obligations pour les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, dans les cas à déterminer par arrêté royal délibéré en Conseil des ministres et sur proposition du ministre de la Justice et du ministre qui a les Télécommunications et les Entreprises et Participations publiques dans ses attributions, les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications. Ce délai, qui ne peut jamais être inférieur à 12 mois, ainsi que les données d'appel et d'identification seront déterminés par arrêté royal délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée.

Art. 11. In artikel 90*ter*, § 2, van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 7 april 1995, 13 april 1995,10 juni 1998 en 10 januari 1999, worden de volgende wijzigingen aangebracht :

A) het 1°*bis* wordt vervangen door de volgende bepalingen :

« 1 °*bis*. Artikel 210*bis* van hetzelfde Wetboek;

1°*ter*. Artikel 259*bis* van hetzelfde Wetboek;

1°*quater*. Artikel 314*bis* van hetzelfde Wetboek;

1°*quinquies*. Artikelen 324*bis* en 324*ter* van hetzelfde Wetboek »;

B) er wordt een 10°*bis* ingevoegd, luidende :

« 10°*bis*. Artikel 504*quater* van hetzelfde Wetboek »;

C) er wordt een 13°*bis* ingevoegd, luidende :

« 13°*bis*. Artikelen 550*bis* en 550*ter* van hetzelfde Wetboek. »

Art. 12. In artikel 90*quater* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wet van 10 juni 1998, wordt een § 4 toegevoegd, luidende :

« § 4. De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van de telecommunicatiedienst waarop de bewakingsmaatregel betrekking heeft of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud van telecommunicatie die wordt of is overgebracht.

Hij kan personen bevelen om de inhoud van de telecommunicatie toegankelijk te maken in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.

Hij die weigert de overeenkomstig de vorige leden bevolen medewerking te verlenen, wordt gestraft met gevangenisstraf van zes maanden tot een jaar en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of die ertoe wordt geroepen zijn technische medewerking te verlenen, is gebonden door het geheim van het gerechtelijk onderzoek. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. »

Art. 13. In artikel 90*septies* van hetzelfde Wetboek ingevoegd bij de wet van 30 juni 1994 en vervangen bij de wet van 10 juni 1998, wordt tussen het vierde en het vijfde lid een nieuw lid ingevoegd, luidende :

« De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen, en voor zover mogelijk, de overschrijving of vertaling hiervan tot stand te brengen. Hetzelfde geldt voor de bewaring op de griffie van de opnamen en de overschrijving of vertaling hiervan en voor de vermeldingen in het bijzonder register. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, deze middelen en het ogenblik waarop ze de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en het vierde lid, vervangen. »

HOOFDSTUK IV. — *Bepaling tot wijziging van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven*

Art. 14. In artikel 109*ter*, E, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de wet van 21 december 1994, hernummerd bij de wet van 19 december 1997 en vervangen bij de wet van 10 juni 1998, worden de volgende wijzigingen aangebracht :

— 1° het eerste lid van § 2 wordt aangevuld als volgt :

« , evenals de verplichtingen voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten om de oproepgegevens van telecommunicatiemiddelen en de identificatiegegevens van gebruikers van telecommunicatiediensten te registreren en gedurende een bepaalde termijn te bewaren met het oog op de opsporing en vervolging van strafbare feiten, in de gevallen, te bepalen bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, Overheidsbedrijven en Participaties. Deze termijn, die nooit minder mag zijn dan 12 maanden, alsook de oproepgegevens en de identificatiegegevens worden bepaald bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Cette conservation imposée aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications doit s'effectuer à l'intérieur des limites du territoire de l'Union européenne. »;

— 2° l'article 109*ter*, E, est complété comme suit :

« § 3. Celui qui ne respecte pas les obligations prévues par le Roi en vertu des paragraphes précédents est puni d'un emprisonnement de trois mois à six mois et d'une amende de vingt-six francs à vingt mille francs ou d'une de ces peines seulement.

§ 4. Le Roi par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée prévoit les modalités et les moyens appropriés pour garantir la confidentialité et l'intégrité des données d'appels et d'identification visées au § 2. »

Promulguons la présente loi, ordonnons qu'elle soit revêtue du Sceau de l'Etat et publiée par le *Moniteur belge*.

Donné à Bruxelles, le 28 novembre 2000.

ALBERT

Par le Roi :

Le Ministre de la Justice,
M. VERWILGHEN

Scellé du Sceau de l'État :

Le Ministre de la Justice,
M. VERWILGHEN

Note

(1) Session 1999—2000.

Chambre des représentants.

Documents parlementaires. — Projet de loi, n° 50-213/1. — Amendements n^os^ 50-213/2 et 50-213/3. — Rapport de la commission, n° 50-213/4. — Texte adopté par la commission, n° 50-213/5. — Amendements, n° 50-213/6. — Texte adopté en séance plénière et transmis au Sénat, n° 50-213/7.

Annales parlementaires. — Discussion et adoption. Séance du 30 mars 2000.

Sénat.

Documents parlementaires. — Projet transmis par la Chambre des représentants, n° 2-392/1. — Amendements, n° 2-392/2. — Rapport de la commission, n° 2-392/3. — Texte adopté par la commission, n° 2-392/4. — Amendements, n^os^ 2-392/5 et 2-392/6. — Texte amendé en séance plénière et renvoyé à la Chambre des représentants, n° 2-392/7.

Annales parlementaires. — Discussion et adoption. Séance du 12 et 13 juillet 2000.

Chambre des représentants.

Documents parlementaires. — Projet amendé par le Sénat, n° 50-213/8. — Amendements, n°s 50-213/9 et 50-213/10. — Rapport de la commission, n° 50-213/11. — Texte adopté par la commission, n° 50-213/12. — Texte adopté en séance plénière et renvoyé au Sénat, n° 50-213/13.

Annales parlementaires. — Discussion et adoption. Séance du 26 octobre 2000.

Sénat.

Documents parlementaires. — Projet amendé par la Chambre des représentants, n° 2-392/8. — Rapport de la commission, n° 2-392/9. — Texte adopté par la commission, n° 2-392/10. — Décision de se rallier au projet réamendé par la Chambre, n° 2-392/11.

Annales parlementaires. — Discussion et adoption. Séance du 16 novembre 2000.

Deze bewaringsplicht voor de operatoren van de telecommunicatienetwerken en de verstrekkers van de telecommunicatiediensten moet worden uitgevoerd binnen de grenzen van de Europese Unie. »;

— 2° artikel 109*ter*, E, wordt als volgt aangevuld :

« § 3. Hij die de verplichtingen door de Koning krachtens de vorige paragrafen bepaald, niet nakomt, wordt gestraft met gevangenisstraf van drie maanden tot zes maanden en met geldboete van zesentwintig frank tot twintigduizend frank of met een van die straffen alleen.

§ 4. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer de modaliteiten en de middelen om de vertrouwelijkheid en de integriteit van de oproep- en identificatiegegevens bedoeld in § 2 te waarborgen. »

Kondigen deze wet af, bevelen dat zo met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 28 november 2000.

ALBERT

Van Koningswege :

De Minister van Justitie,
M. VERWILGHEN

Met 's Lands zegel gezegeld :

De Minister van Justitie,
M. VERWILGHEN

Nota

(1) Zitting 1999-2000.

Kamer van volksvertegenwoordigers.

Parlementaire bescheiden. — Wetsontwerp, nr. 50-213/1. — Amendementen nrs. 50-213/2 en 50-213/3. —Verslag van de commissie, nr. 50-213/4. —Tekst aangenomen door de commissie, nr. 50-213/5. — Amendementen, nr. 50-213/6. — Tekst aangenomen in plenaire vergadering en overgezonden aan de Senaat, nr. 50-213/7.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 30 maart 2000.

Senaat.

Parlementaire bescheiden. — Ontwerp overgezonden door de Kamer van volksvertegenwoordigers, nr. 2-392/1. — Amendementen, nr. 2-392/2. — Verslag van de commissie, nr. 2-392/3. — Tekst aangenomen door de commissie, nr. 2-392/4. — Amendementen, nrs. 2-392/5 en 2-392/6. — Tekst geamendeerd in plenaire vergadering en teruggezonden naar de Kamer van volksvertegenwoordigers, nr. 2-392/7.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 12 en 13 juli 2000.

Kamer van volksvertegenwoordigers.

Parlementaire bescheiden. — Ontwerp geamendeerd door de Senaat, nr. 50-213/8. — Amendementen, nrs. 50-213/9 en 50-213/10. — Verslag van de commissie, nr. 50-213/11. — Tekst aangenomen door de commissie, nr. 50-213/12. — Tekst aangenomen in plenaire vergadering en teruggezonden aan de Senaat, nr. 50-213/13.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 26 oktober 2000.

Senaat.

Parlementaire bescheiden. — Ontwerp geamendeerd door de Kamer van volksvertegenwoordigers, nr. 2-392/8. — Verslag van de commissie, nr. 2-392/9. — Tekst aangenomen door de commissie, nr. 2-392/10. — Beslissing om in te stemmen met het door de Kamer opnieuw geamendeerd ontwerp, nr. 2-392/11.

Parlementaire handelingen. — Bespreking en aanneming. Vergadering van 16 november 2000.

Bijlage II: Europese Cybercrime-Conventie

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

European Treaty Series - No. 18

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures

concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions
For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c "service provider" means:
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;
d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;
b offering or making available child pornography through a computer system;
c distributing or transmitting child pornography through a computer system;
d procuring child pornography through a computer system for oneself or for another person;
e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;
b a person appearing to be a minor engaged in sexually explicit conduct;
c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;
b an authority to take decisions on behalf of the legal person;
c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.

3
a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and
ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards
1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data
1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data
1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and
b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or
ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or
b on board a ship flying the flag of that Party; or
c on board an aircraft registered under the laws of that Party; or
d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;
b the preservation of data pursuant to Articles 29 and 30;
c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11,

paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;
b the deposit of any instrument of ratification, acceptance, approval or accession;
c any date of entry into force of this Convention in accordance with Articles 36 and 37;
d any declaration made under Article 40 or reservation made in accordance with Article 42;
e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.


84326 8734872724 89765287
71 0963 0
732 387 09838510
2876 236 0832