

Tien jaar wet informaticacriminaliteit

Jeff KEUSTERMANS
Advocaat
Gastdocent VUB en HUB

Tina DE MAERE
Advocaat

De wet van 28 november 2000 inzake informaticacriminaliteit bestaat tien jaar. Dit artikel bespreekt de belangrijkste evoluties van het afgelopen decennium. Voor het comfort van de lezer volgt deze tekst de indeling van het artikel dat eerder in dit tijdschrift verscheen.¹

I. Inleiding

Na inwerkingtreding van de wet van 28 november 2000 inzake informaticacriminaliteit² op 13 februari 2001, werd op 23 november 2001 de Overeenkomst van de Raad van Europa inzake informaticacriminaliteit, het zogenaamde Verdrag van Budapest (hierna: Cybercrime-Verdrag), ondertekend.³ Het Cybercrime-Verdrag vormt het eerste dwingende instrument van internationaal recht dat specifiek werd uitgewerkt om informaticacriminaliteit te bestrijden. Het voornaamste doel van het Cybercrime-Verdrag bestaat erin de constitutieve elementen van de misdrijven van het nationale materiële strafrecht, en de aanverwante bepalingen van dit recht op het vlak van informaticacriminaliteit, te harmoniseren. Daarnaast wordt een snel en efficiënt regime van internationale samenwerking uitgewerkt.⁴ In dit licht kent het Cybercrime-Verdrag ruime grensoverschrijdende opsporingsbevoegdheden toe aan justitie en politie. Voorts beoogt het Cybercrime-Verdrag dat alle verdragstaten voorzien in de bestraffing van informaticamisbruiken.⁵

Op 28 januari 2003 werd het aanvullend Protocol bij de Overeenkomst inzake informaticacriminaliteit betreffende de bestraffing van racistische en xenofobe feiten gepleegd met behulp van informaticasystemen opgemaakt te Straatsburg.⁶ Het aanvullend Protocol heeft twee objectieven: ten eerste wordt het materieel strafrecht ter bestrijding van racisme en xenofobie op internet geharmoniseerd, en ten tweede wordt de internationale samenwerking op dit gebied verbeterd.⁷

Opdat België zou voldoen aan de internationale verplichtingen neergelegd in het Cybercrime-Verdrag en het aanvullend Protocol waren een aantal wetsaanpassingen noodzakelijk.⁸ Deze kwamen er door de wet van 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550ter van het Strafwetboek,⁹ die in hoofdzaak resulteren in een uitbreiding van de bestraffing van informaticacriminaliteit. De wijzigingen houden voornamelijk verbeteringen in van de bestaande tekst die werden geformuleerd na raadpleging van de leden van

¹ J. KEUSTERMANS en F. MOLS, «De wet van 28 november 2000 inzake informaticacriminaliteit: een eerste overzicht», *RW* 2001-02, 721-732.

² Wet van 28 november 2000, *BS* 3 februari 2001, hierna: «Wet IC». Voor een volledig overzicht van deze materie en latere aanvullingen, zie: J. KEUSTERMANS, F. MOLS en T. DE MAERE, «Informaticacriminaliteit», in A. VANDEPLAS, P. ARNOU, S. VAN OVERBEKE en S. VANDROMME (red.), *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, 1-39.

³ Hierna: «Cybercrime-Verdrag», tekst gepubliceerd op de website van de Raad van Europa: www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en/asp.

⁴ *Parl.St.*, Kamer 2003-04, nr. 51-1284/001, p. 4.

⁵ Zie voor een verdere bespreking van deze internationale initiatieven: F. DE VILLENFAGNE en S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique», *AM* 2001-02, 61-63, met verwijzingen; P. DE HERT, «De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?», *T.Strafr.* 2001, p. 293-296, nrs. 14-18.

⁶ Tekst gepubliceerd op de website van de Raad van Europa: www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en/asp.

⁷ *Parl.St.* Kamer 2003-04, nr. 51-1284/001, p. 5.

⁸ *Ibid.*

⁹ Wet van 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550ter van het Strafwetboek, *BS* 12 september 2006 (in werking getreden op 22 september 2006), hierna: «wet van 15 mei 2006».

de *Federal Computer Crime Unit*, waardoor zij nauwelijks het voorwerp zijn geweest van discussie in het parlement.¹⁰

II. Terminologie

De wetgever heeft ervoor gezorgd dat de gebruikte terminologie technologie-neutraal is. Op deze manier tracht men te vermijden dat de begrippen al te snel achterhaald worden door de evolutie van de informaticatechnologie.¹¹

De twee in de Wet IC meest voorkomende begrippen «informaticasysteem» en «gegevens» (die enkel in de memorie van toelichting van de Wet IC en dus niet in de Wet IC zelf zijn omschreven) zijn ongewijzigd gebleven.

III. Materieel strafrecht

A. Valsheid in informatica

Wie de waarheid opzettelijk vervalst via datamanipulatie met betrekking tot juridisch relevante gegevens, maakt zich schuldig aan valsheid in informatica.¹²

1^o Juridisch relevante gegevens

Op 28 november 2005 oordeelde de Correctionele Rechterbank te Dendermonde dat het met bedrieglijk opzet of met het oogmerk te schaden aanmaken van een e-mailaccount op naam van een andere persoon en het verzenden van een e-mail via dit e-mailadres naar een derde persoon, manipulatie van juridisch relevante computergegevens inhoudt, die *in casu* strafbaar werd bevonden op basis van de artikelen 193 en 210bis Sw.¹³

¹⁰ B. DOCQUIR, «Loi du 15 mai 2006: nouvelles définitions des infractions en matière de criminalité informatique», *RDTI* 2006, 288; *Parl.St.* Kamer 2003-04, nr. 51-1284/001, p. 18-26.

¹¹ Deze wetgevingstechniek wordt algemeen toegepast sedert de Verenigde Staten er bewust voor opteeden om de definitie van een computerprogramma in art. 101 van de Computer Software Act van 1980 technologie-neutraal te definiëren.

¹² Art. 210bis Sw.: «Diegene die schuldig wordt geacht aan het misdrijf valsheid in informatica wordt gestraft met een gevangenisstraf van zes maanden tot vijf jaar en met een geldboete van 26 euro tot 100.000 euro of met een van die straffen alleen» (art. 210bis, § 1, Sw.). Een dergelijke zeer hoge geldboete komt eveneens voor in art. 11 van de wet van 30 juni 1994 betreffende de rechtsbescherming van computerprogramma's (van 100 tot 100.000 euro). Voor de strafbare poging en in geval van (bijzondere) herhaling zijn aangepaste straffen bepaald (art. 210bis, § 3 en § 4, Sw.).

¹³ Corr. Dendermonde 28 november 2005, *RABG* 2007, 427; zie ook: Corr. Dendermonde 14 mei 2007, *T.Strafr.* 2007, 403, noot E. BAEYENS.

2^o De vervalsing van de waarheid via datamanipulatie

Opdat er sprake is van valsheid in informatica, dient er een vervalsing van de waarheid plaats te vinden. Dit is de *conditio sine qua non*. Niet iedere vervalsing van de waarheid is echter strafbaar en kan worden gekwalificeerd als het misdrijf valsheid in informatica. Daartoe moet het gaan om een vervalsing op een door de wet omschreven wijze (art. 210bis, § 1, Sw.).

Voorbeelden van valsheid in informatica zijn: het vervalsen of namaken van kredietkaarten, het vervalsen van digitale contracten,¹⁴ het vervalsen van een elektronische handtekening en het gebruik van een vervalste protonkaart.

B. Informaticabedrog

Sinds de wetwijziging van 15 mei 2006 is het voldoende dat de betrokkene beoogt, met bedrieglijk opzet, een onrechtmatig economisch voordeel voor zichzelf of een ander te verwerven.^{15, 16} Voordien was het vereist dat de dader voor zichzelf of een ander effectief een bedrieglijk vermogensvoordeel verwierf via datamanipulatie om zich schuldig te maken aan informaticabedrog.¹⁷

1^o Het beogen een onrechtmatig economisch voordeel te verwerven

Aangezien er geen beperking wordt gesteld aan de aard van de zaken, kunnen alle economische bestanddelen rechtstreeks of onrechtstreeks het voorwerp van informaticabedrog vormen: ook immateriële goederen, onroerende goederen en dienstprestaties.¹⁸ Dit misdrijf heeft betrekking op de bedrieglijke manipulatie van gegevens met de bedoeling zichzelf of een ander te verrijken. Er kan worden gedacht aan:

¹⁴ I. DELBROUCK, «Informaticacriminaliteit», in *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, Antwerpen, Kluwer, 2010, I. 42/11.

¹⁵ Overeenkomstig art. 8 van het Cybercrime-Verdrag.

¹⁶ Art. 4 van de wet van 15 mei 2006 bepaalt: «In artikel 504quater, § 1, van hetzelfde Wetboek, ingevoegd bij de wet van 28 november 2000, worden de woorden «Hij die, voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwierft» vervangen door de woorden «Hij die, met bedrieglijk opzet, beoogt een onrechtmatig economisch voordeel voor zichzelf of voor een ander te verwerven».

¹⁷ Art. 504quater Sw. bepaalt: «Diegene die schuldig wordt bevonden aan het misdrijf informaticabedrog wordt gestraft met een gevangenisstraf van zes maanden tot vijf jaar en met een geldboete van 26 euro tot 100.000 euro of met een van die straffen alleen» (art. 504quater, § 1, Sw.). Voor de strafbare poging en in geval van (bijzondere) herhaling zijn aangepaste straffen bepaald (art. 504quater, § 2 en § 3, Sw.).

¹⁸ I. DELBROUCK, *o.c.*, in *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, I. 42/15.

- het gebruiken van een gestolen kredietkaart;
- het invoeren van programma-instructies, waardoor bepaalde verrichtingen een ander resultaat geven, om een onrechtmatig financieel voordeel te verkrijgen (een bankbediende voert afwijkende afrondingsregels voor de cijfers achter de komma in en leidt de opbrengst daarvan naar zijn eigen rekening);
- het met winstbejag verduisteren van bestanden die men enkel voor een welbepaald doel heeft toevertrouwd gekregen (een bediende op een boekhoudkantoor kopieert de aldaar gebruikte bestanden over de boekhouding van de klanten, waartoe hij uit hoofde van zijn tewerkstelling toegang heeft, en gaat vervolgens op zelfstandige basis het cliënteel van zijn vorige werkgever contacteren om hun boekhouding te voeren, met gebruikmaking van de gekopieerde bestanden¹⁹);
- het vervalsen van studieresultaten (een student dringt binnen in het informaticasysteem van zijn school en wijzigt zijn examenresultaten^{20, 21});
- het wijzigen van gegevens in een personeelsregistratiesysteem om zijn aanwezigheid te registreren en een alibi te creëren (het niet strafrechtelijk veroordeeld worden houdt een economisch voordeel in).

Informaticabedrog onderscheidt zich van het misdrijf «bedrog» in de zin van art. 496 Sw. doordat het doel van dit laatste misdrijf hoofdzakelijk erin bestaat om het vertrouwen van een natuurlijke persoon of rechtspersoon te schaden om zich een zaak toe te eigenen die aan een ander toebehoort. Het toepassingsgebied van informaticabedrog is daarentegen breder, omdat er sprake is van een misdrijf door de louter manipulatie van informaticagegevens zodra wordt aangetoond dat het verkregen of slechts gewilde economisch voordeel onrechtmatig is en dat dit gebeurde met bedrieglijk opzet.²²

Het beogen, met bedrieglijk opzet, een onrechtmatig economisch voordeel te verwerven voor zichzelf of voor een ander door middel van gegevensmanipulatie nader omschreven in art. 504*quater* Sw. is, sinds de inwerkingtreding ervan, een wanbedrijf, zodat het misdrijf niet meer onder de toepassing valt van art. 467, eerste lid, Sw. (een misdaad).²³ Volgens het Hof van Beroep te Brussel is de strafuitsluitingsgrond van

art. 462 Sw., gebaseerd op verwantschap of aanverwantschap, van toepassing op informaticabedrog.²⁴ Men kan zich afvragen of het Hof hier geen stap te verzet, omdat deze uitbreiding geen wettelijke basis heeft.²⁵

In een vonnis van 14 mei 2007 oordeelde de Correctionele Rechtbank te Dendermonde dat de verdachten zich schuldig hadden gemaakt aan informaticabedrog doordat zij bankkaarten kopieerden met aanwending van technische middelen, en de verkregen kopieën gebruikten met het doel zich gelden die aan een ander toebehoren toe te eigenen.²⁶ De feiten die aanleiding gaven tot dit vonnis, zijn de volgende. In diverse filialen van banken werden kaartlezers (deuropeners van *self-banks*) voorzien van een opzetstuk dat de magneetstrook van nietsvermoedende kaarthouders kopieerde. Een kleine camera, die gespoten was in dezelfde kleur als de bankautomaat en bovenaan in de geldverdelers verstopt zat, filmde de ingetikte pincodes. Vervolgens werden deze filmbeelden draadloos gezonden naar een videorecorder voorzien van minicassettes. Met gebruikmaking van de verkregen informaticagegevens werden ten slotte gelden afgehaald van de rekening van deze bankkaarthouders, telkens het maximum beschikbare bedrag per kaart juist vóór en juist na middernacht. De betrokkenen werden op grond van voormelde feiten tevens veroordeeld voor valsheid in informatica (*supra*) en hacking (*infra*).

Vóór de wetwijziging van 15 mei 2006 vereiste art. 504*quater* Sw. dat effectief een bedrieglijk vermogensvoordeel verworven werd opdat er sprake kon zijn van informaticabedrog: enkel indien de door de skimming²⁷ verkregen informaticagegevens vervolgens succesvol werden gebruikt om een bedrieglijk vermogensvoordeel te verwerven, kon dit als informaticabedrog worden bestempeld. De wet van 15 mei 2006 heeft dit vereiste geschrapt, zodat skimming sindsdien strafbaar is op grond van art. 504*quater* Sw. zodra de bedoeling bestaat om een onrechtmatig economisch voordeel te verwerven, zonder dat dit ook effectief lukt.²⁸

²⁴ Brussel 12 februari 2004, *Rev.dr.pén.* 2004, 748; in dezelfde zin: A. DE NAUW, *Inleiding tot het bijzonder strafrecht*, Mechelen, Kluwer, 2010, 379; I. DELBROUCK, o.c., in *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, I. 42/17.

²⁵ Het lijkt ons evenwel niet zo dat, omdat er plots technologie aan te pas komt, de uitbreiding van de toepassing van art. 462 Sw. zoals eerder in de rechtspraak en rechtsleer aanvaard (zie onder meer voetnoot 24) niet van toepassing zou zijn.

²⁶ Corr. Dendermonde 14 mei 2007, *T.Strafr.* 2007, 403.

²⁷ Onder het begrip «skimming» verstaat men het illegaal kopiëren van de gegevens van de magneetstrook van een betaalkaart.

²⁸ E. BAEYENS, «Informatica en recht: oude griffels – nieuwe leien», *T.Strafr.* 2007, 405.

¹⁹ Dit misdrijf maakt meestal ook valsheid in informatica (art. 210*bis*, § 1, Sw.) uit.

²⁰ Dit misdrijf maakt meestal ook computerinbraak (art. 550*bis*, § 1, Sw.) uit.

²¹ I. DELBROUCK, o.c., in *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, I. 42/15.

²² B. DOCQUIR, o.c., *RDTI* 2006, 291.

²³ Cass. 6 mei 2003, *Arr.Cass.* 2003, 1090; art. 504*quater* Sw. zoals na de wijziging door art. 4 van de wet van 15 mei 2006.

2^o Via datamanipulatie

Het Hof van Beroep te Antwerpen oordeelde op 10 september 2008 dat het gebruik maken met bedrieglijk opzet van andermans bankkaart met als doel zichzelf of een ander een onrechtmatig vermogensvoordeel te verschaffen informaticabedrog uitmaakt, ook al is de bankkaart op geen enkele wijze vervalst.²⁹

Om uit te maken of manipulatie van data al dan niet gerechtvaardigd is, zal men vaak moeten teruggrijpen naar het burgerlijk recht of het handelsrecht.³⁰ Nochtans dient men tevens rekening te houden met een zekere autonomie van het strafrecht.³¹

3^o Bijzonder opzet

Tot de wetwijziging van 15 mei 2006 diende het beoogde economisch voordeel bedrieglijk te zijn. Een vermogensvoordeel kan bezwaarlijk op zichzelf «bedrieglijk» zijn, zodat de wetgever wellicht bedoeld heeft dat de wijze waarop het vermogensvoordeel verworven wordt bedrieglijk moest zijn. In de tekst van het gewijzigde art. 504*quater* Sw. is geen sprake meer van een «bedrieglijk voordeel». De betrokkene dient met bedrieglijk opzet gehandeld te hebben; handelingen te goeder trouw zijn derhalve niet strafbaar.

C. Misdriften tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen

1^o Ongeoorloofde toegang tot een informaticasysteem

a) Externe «hacking»

Een buitenstaander die, terwijl hij weet dat hij daar niet toe gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, maakt zich schuldig aan computerinbraak.³² Externe hacking is een misdrijf dat vaak leidt tot publiciteit. Typische

²⁹ Antwerpen 10 september 2008, NC 2009, 328.

³⁰ Zie bv. de problematiek van toegelaten of verboden handelingen inzake software (J. KEUSTERMANS, «Auteursrecht. Recente evoluties in capita selecta», CABG 2009/2, 49); zie eveneens: B.J. KOOPS en J.E.J. PRINS, «Misbruik van technische hulpmiddelen: een beschouwing over te ver gaande regelingen in het Cybercrime-Verdrag en de Auteursrechtlijn», *Computerr.* 2004, 59-67; S. DUSOLLIER, *Droit d'auteur et protection des œuvres dans l'univers numérique*, Larcier, 2007, 619 p.; P. LAURENT, «Protection des programmes d'ordinateur», *RDTI* 2009, 57; zie ook: GrwH 12 november 2009, nr. 182/2009 (i.v.m. het ombouwen van Playstation consoles).

³¹ Zie hieromtrent: L. DUPONT, *Beginselen van strafrecht*, Leuven, Acco, 1997-98, 12-15.

voorbeelden betreffen de ReDaTack- en de Bistelzaak.³³

(i) Zich toegang verschaffen tot of zich handhaven in een informaticasysteem

Op 14 mei 2007 oordeelde de Correctionele Rechtbank te Dendermonde dat het ingeven in een terminal van een geïnformatiseerd banktransactiesysteem van frauduleus gekopieerde bankkaartgegevens een overtreding uitmaakt van art. 550*bis*, § 1, § 3, 1^o en 2^o, Sw.³⁴ Deze gedraging gebeurde volgens de rechtbank met het bedrieglijk opzet om in de geïnformatiseerde portefeuille van derden in te breken en gelden te debiteren en/of toe te eigenen.³⁵

De Correctionele Rechtbank te Brussel vonniste op 8 januari 2008 dat de werkgever die zich met welke intentie ook toegang verschaft tot de privécomputer van één van zijn werknemers, zich schuldig maakt aan computerinbraak, *a fortiori* indien de toegang tot deze computer wordt beschermd door een persoonlijk wachtwoord.³⁶

(ii) Algemeen opzet: terwijl men weet dat men daar niet toe gerechtigd is

De Correctionele Rechtbank te Hasselt oordeelde dat het feit dat een informaticasysteem niet beveiligd was, en dat een beklaagde aldus vrij het systeem kon binnendringen, impliceert dat er geen sprake was van kwaad opzet.³⁷ Het merendeel van de rechtspraak oordeelt evenwel dat de beklaagde strafbaar is van zodra hij willens en wetens in het informaticasysteem binnendrong.³⁸

³² Art. 550*bis*, § 1, Sw. bepaalt: «Externe «hacking» wordt bestraft met een gevangenisstraf van drie maanden tot één jaar en met een geldboete van 26 euro tot 25.000 euro of met een van deze straffen alleen. Wanneer het misdrijf wordt gepleegd met bedrieglijk opzet, bedraagt de gevangenisstraf zes maanden tot twee jaar».

³³ Corr. Brussel 8 november 1990, *JT* 1990, 11, noot: B. DE SCHUTTER, «Het Belgische Bistel-syndroom», *Computerr.* 1991, 164-166; J. SURMONT, «De Bistelzaak», *Computerr.* 1991, 43-44; Corr. Gent 11 december 2000, *AM* 2001, 157-161, noot B. MICHAUX.

³⁴ Corr. Dendermonde 14 mei 2007, *T.Strafr.* 2007, 403.

³⁵ E. BAEYENS, *o.c.*, *T.Strafr.* 2007, 406.

³⁶ Corr. Brussel 8 januari 2008, *JT* 2008, 337, noot A. LEROY.

³⁷ Corr. Hasselt 21 januari 2004, *Computerr.* 2004, 130, noot H. GRAUX; zie evenwel: J. KEUSTERMANS, F. MOLS en T. DE MAERE, *o.c.*, in A. VANDEPLAS, P. ARNOU, S. VAN OVERBEKE en S. VANDROMME (red.), *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, p. 21, nr. 48 in fine.

³⁸ Rb. Dendermonde 14 november 2008, *Computerr.* 2009, 74, noot L. DAUWE; Corr. Dendermonde 25 mei 2007, *TGR-TWVR* 2007, 351; zie ook: Corr. Eupen 15 december 2003, *Computerr.* 2004, 129, *RDTI* 2004, 61, noot O. LEROUX.

b) *Interne «hacking»*

Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, maakt zich schuldig aan interne «hacking».³⁹

Opdat er sprake kan zijn van interne «hacking» is, in tegenstelling tot bij externe «hacking», waarvoor een algemeen opzet volstaat, een bijzonder opzet vereist. In dit verband oordeelde het Grondwettelijk Hof in een arrest van 24 maart 2004 dat art. 550bis Sw. art. 10 en 11 van de Grondwet niet schendt doordat voor interne hacking (art. 550bis, § 2, Sw.) een bijzonder opzet vereist is, terwijl voor externe hacking (art. 550bis, § 1, Sw.) een algemeen opzet volstaat.⁴⁰

c) *Verzwarende omstandigheden (zowel voor interne als externe «hacking»)*

Een zwaardere straf wordt opgelegd in de volgende gevallen⁴¹;

- het overnemen van gegevens: bijvoorbeeld het stelen van industriële geheimen in het raam van bedrijfs-spionage⁴²;
- enig gebruikmaken van een informaticasysteem van een derde of het zich bedienen van een informaticasysteem om toegang te verkrijgen tot een informaticasysteem van een derde;
- het veroorzaken van schade aan het «gehackte» systeem, aan het systeem van derden of aan de gegevens in deze systemen, uit onvoorzichtigheid.⁴³ Daarbij dient te worden opgemerkt dat opzettelijke sabotage een apart (nieuw) misdrijf is en zwaarder bestraft wordt.⁴⁴

Deze drie gedragingen worden enkel als strafwaardig beschouwd indien zij tezelfdertijd als of na de «hacking» worden gepleegd. Door de ruime omschrijving van deze verzwarende omstandigheden, vooral van punt 2 («enig gebruik maken van»), bestaat het gevaar van de nagenoeg automatische toepassing ervan.⁴⁵

³⁹ Art. 550bis, § 2, Sw. bepaalt: «Hij die zich schuldig maakt aan interne «hacking» wordt gestraft met een gevangenisstraf van zes maanden tot twee jaar en met een geldboete van 26 euro tot 25.000 euro of met een van die straffen alleen».

⁴⁰ Arbitragehof nr. 51/2004, 24 maart 2004, BS 29 juni 2004, A.A. 2004, 619.

⁴¹ Een gevangenisstraf van een jaar tot drie jaar en een geldboete van 26 euro tot 50.000 euro of een van deze straffen alleen.

⁴² Corr. Hasselt 21 januari 2004, *Computerr.* 2004, 130, noot H. GRAUX.

⁴³ Corr. Hasselt 21 januari 2004, *Computerr.* 2004, 130, noot H. GRAUX; zie eveneens: Corr. Dendermonde 9 oktober 2002, *onuitg.*: de beklaagde die schade toebrengt aan de server van het bedrijf tot wiens informaticasysteem hij zich onrechtmatig toegang verschaft, maakt zich schuldig aan art. 550bis, § 1 en § 3, Sw.

⁴⁴ Art. 550ter Sw.

d) *Strafbare poging*

In 2002 oordeelde de Correctionele Rechtbank te Antwerpen dat hij die zich toegang tracht te verschaffen tot de buitenlijnen van PABX-telefooncentrales van niet nader geïdentificeerde buitenlandse bedrijven, met het bedrieglijke oogmerk telefoongesprekken op afstand te voeren op kosten van deze bedrijven, maar hierin niet slaagt alleen ten gevolge van omstandigheden buiten zijn wil, een overtreding van art. 550bis, § 1, eerste lid en § 4, Sw. begaat.⁴⁶

e) *Vorbereidingshandelingen («hackertools»)*

Voor bepaalde gedragingen die computerinbraak voorbereiden, wordt voorzien in een apart misdrijf. Het gaat om het bezit, de productie, de verkoop, het verkrijgen, de invoer, de verspreiding of terbeschikkingstelling van bepaalde middelen om te kunnen hacken.⁴⁷ Onder de vroegere wetsbepaling werd een bijzonder opzet, namelijk het bedrieglijk opzet of het oogmerk om te schaden, vereist om te vermijden dat deze bepaling een hinderpaal zou vormen voor de vrije verspreiding van informatie wat betreft beveiligingstechnieken.⁴⁸ De wet van 15 mei 2006 bepaalt dat deze gedragingen op onrechtmatige wijze dienen te gebeuren en schrapte aldus de bewoordingen «met bedrieglijk opzet of het oogmerk te schaden». Nochtans wordt in de rechtsleer verdedigd dat dit niet tot gevolg zal hebben dat deze voorbereidingshandelingen («hackertools») systematisch veroordeeld zullen worden.⁴⁹ Wij sluiten ons hierbij aan omdat het onrechtmatige karakter nog dient te worden bewezen. Naar onze mening zal dit bewijs evenwel gemakkelijker kunnen worden geleverd dan het vroegere vereiste bijzondere opzet.

Sedert 2006 werden art. 550bis, § 5, Sw. en art. 550ter, § 4, Sw. bovendien aangevuld met het begrip «instrumenten», zoals voorgeschreven door art. 6.1.a), 1), van het Cybercrime-Verdrag. Volgens de parlementaire voorbereiding bij voormelde wet dient onder «instrumenten» te worden verstaan: «middelen van toegang of andere werktuigen die ontworpen zijn om bijvoorbeeld gegevens te wijzigen of te vernietigen, of om binnen te dringen in de werking van systemen, zoals virusprogramma's, ofwel programma's die ont-

⁴⁵ B. DOCQUIR, *o.c.*, *RDTI* 2006, 293.

⁴⁶ Corr. Antwerpen 23 september 2002, *onuitg.*

⁴⁷ Art. 550bis, § 5, Sw.

⁴⁸ *Parl.St.* Kamer 1999-00, nr. 51-0213/001, p. 18.

⁴⁹ B. DOCQUIR, *o.c.*, *RDTI* 2006, 293.

worpen zijn om binnen te dringen in informaticasystemen».⁵⁰

f) Gevolghandelingen

Een gevolghandeling die strafbaar wordt gesteld, is het helen van de naar aanleiding van de «hacking» verkregen gegevens.⁵¹

Terecht werd opgemerkt dat deze bepaling een weerslag kan hebben op de persvrijheid.⁵²

Art. 6 van de wet van 7 april 2005 tot bescherming van de journalistieke bronnen⁵³ bepaalt dat de in de wet beschermde personen niet op grond van art. 505 Sw. (klassieke heling) kunnen worden vervolgd als zij hun recht uitoefenen om hun informatiebronnen te verzwijgen. Dat art. 550bis, § 7, Sw. niet is vermeld, lijkt een loutere vergetelheid van de wetgever. Het komt ons voor dat er geen reden is om de bescherming van het bronnengeheim van journalisten anders te behandelen wanneer de informatie wel of niet afkomstig is uit informaticasystemen. De wetgever had immers de bedoeling er zorg voor te dragen dat de Wet IC niet zou leiden tot een aantasting van de persvrijheid.⁵⁴

2° Ongeoorloofde datamanipulatie/sabotage

Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist, of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert, wordt bestraft met een gevangenisstraf van zes maanden tot drie jaar en met een geldboete van 26 euro tot 25.000 euro of met één van die straffen alleen.⁵⁵

Er is een strafverzwaring voorgeschreven indien er effectief schade is opgetreden aan gegevens of aan een informaticasysteem.⁵⁶

⁵⁰ *Parl.St.* Kamer 2003-04, nr. 51-1284/001, p. 6.

⁵¹ Art. 550bis, § 7, Sw.

⁵² P. DE HERT, *o.c.*, *T.Strafr.* 2001, p. 323, nr. 57.

⁵³ BS 27 april 2005, *err.* BS 13 mei 2005. Zie ook: B. DE SMET, «Beperkte draagwijdte van het journalistiek bronnengeheim», *RW* 2008-09, 1728; J. ENGLEBERT, «Les sources veilleront à ne laisser aucune trace...», *AM* 2008, 131; J. CEULEERS, «De journalistieke bronnen wettelijk beschermd», *RW* 2005-06, 48; E. BREWAEYS, «Informatiebronnen van journalisten», *NJW* 2005, 542; *Corr.* Dendermonde 3 november 2008, *AM* 2009, 455.

⁵⁴ Verklaring van de Minister opgenomen in het verslag namens de Commissie voor Justitie inzake het wetsontwerp informaticacriminaliteit, uitgebracht door de heer Verherstraeten, *Parl.St.* Kamer 1999-2000, nr. 0213/004, p. 28; P. DE HERT, *o.c.*, *T.Strafr.* 2001, p. 323, nr. 57.

⁵⁵ Art. 550ter, § 1, Sw.

Er is een verdubbeling van de straf in geval van herhaling van hetzelfde misdrijf of van de misdrijven bedoeld in art. 210bis Sw. (valsheid in informatica), art. 259bis Sw. (afluisteren, kennisnemen en opnemen van privécommunicatie en privételecommunicatie door een openbaar ambtenaar), art. 314bis Sw. (misdrijven betreffende het geheim van privécommunicatie en privételecommunicatie), art. 504quater Sw. (informaticabedrog) of art. 550bis Sw. (computerinbraak).⁵⁷

Sinds de wetwijziging van 15 mei 2006 is geen bijzonder opzet om te schaden meer vereist om te kunnen spreken van een schending van de integriteit van de informaticasystemen en van de door middel daarvan opgeslagen, verwerkte of overgedragen gegevens.⁵⁸

De wil om schade te berokkenen aan een derde is sedert de wetwijziging van 15 mei 2006 geen constitutief bestanddeel meer, maar vormt wel een verzwarende omstandigheid. Sedert de wet van 15 mei 2006 is de dader strafbaar indien hij zonder schadelijk oogmerk, maar wetende dat hij niet gerechtigd is wijzigingen aan te brengen, zulks toch gedaan heeft.⁵⁹

IV. Strafprocesrecht

Op het vlak van het strafprocesrecht vonden geen noemenswaardige evoluties plaats.⁶⁰

De wijzigingen in het Wetboek van Strafvordering die werden ingevoerd door de Wet IC vinden hun toepassing in de praktijk. Met betrekking tot netwerkzoeking⁶¹ oordeelde de Correctionele Rechtbank

⁵⁶ Art. 550ter, § 2, Sw. bepaalt: «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 een gevangenisstraf van zes maanden tot vijf jaar en met geldboete van 26 euro tot 75.000 euro of met een van die straffen alleen».

⁵⁷ Art. 550ter, § 5, Sw. bepaalt: «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 210bis, 259bis, 314bis, 504quater of 550bis».

⁵⁸ F. GOOSSENS, «Wijzigingen in het Belgisch Strafwetboek inzake informaticacriminaliteit», *TVW* 2006, 467.

⁵⁹ Art. 550ter, § 1, tweede lid, Sw.; I. DELBROUCK, *o.c.*, in *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, I, 42/21.

⁶⁰ Voor een algemeen overzicht, zie: J. KEUSTERMANS, F. MOLS en T. DE MAERE, *o.c.*, in A. VANDEPLAS, P. ARNOU, S. VAN OVERBEKE en S. VANDROMME (red.), *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, 30-38; P. VAN LINTHOUT en J. KERKHOFS, «Internetrecherche: informaticatop en netwerkzoeking, licht aan het eind van de tunnel», *T.Strafr.* 2008, 79-95; T. VERBIEST en E. WÉRY, *Le droit de l'internet et de la société de l'information*, Brussel, Larcier, 2001.

⁶¹ Art. 88ter Sv.

te Brussel op 10 januari 2008⁶² dat indien wordt gehandeld op basis van een geldig door de onderzoeksrechter afgeleverd huiszoekingsbevel, in het raam waarvan het noodzakelijk is om de zoeking uit te breiden naar een informaticasysteem dat zich op een andere plaats bevindt, de onderzoekers daartoe kunnen overgaan zonder bijkomende formaliteit, mits zij de voorwaarden naleven van art. 88ter, § 1 *in fine* en § 2, Sv. De onderzoeksgerechten en vonnisgerechten controleren of deze grenzen en voorwaarden werden gerespecteerd. De feiten die aanleiding gaven tot het vonnis waren de volgende. In het raam van een gerechtelijk onderzoek dat werd gevoerd door de onderzoeksrechter te Brussel en waarvoor door hem huiszoekingsbevelen werden afgeleverd, werden pc's in beslag genomen en «geëxploiteerd» (*sic*). Van de in verdenking gestelden was geweten dat zij gebruikmaakten van hotmailaccounts. De in verdenking gestelde weigerde het paswoord te geven en gaf bijgevolg geen toestemming tot exploitatie van zijn hotmailaccount. Bij de huiszoeking werd evenwel een document in beslag genomen waarop het paswoord werd vermeld van twee hotmailaccounts. De verbalisanten gingen vervolgens zonder meer over tot exploitatie en doorzoeking van de hotmailaccounts.

Uit de beoordeling in het vonnis blijkt dat de Correctionele Rechtbank de zoeking in het informaticasysteem koppelt aan de huiszoeking. De Correctionele Rechtbank oordeelde voorts dat in dit licht art. 88ter Sv. bepaalt dat, indien men in het raam van een huiszoeking genoodzaakt is om die zoeking uit te

breiden tot informaticasystemen die zich bevinden op een andere plaats dan de plaats waarvoor het huiszoekingsbevel is afgeleverd, zonder enige verdere formaliteit (d.i. een nieuw bevel van de onderzoeksrechter) de zoeking kan worden uitgebreid tot die informaticasystemen mits de voorwaarden van art. 88ter, § 1 *in fine* en § 2, Sv. worden nageleefd.

Door de rechtsleer⁶³ is – o.i. terecht – kritiek gekomen op bovenvermelde visie van de Correctionele Rechtbank te Brussel. De wetgever had geen soort «verlenging van de huiszoeking» op het oog, maar wenste wel degelijk een statuut *sui generis* te verlenen aan art. 88ter Sv. waarbij vooraf een beslissing en een beschikking van de onderzoeksrechter vereist zijn. Het tegendeel aanvaarden, zoals *in casu* in het vonnis van 10 januari 2008 door de Correctionele Rechtbank te Brussel, staat op gespannen voet met het recht op het privéleven.⁶⁴

V. Conclusie

Informaticacriminaliteit speelt zich af in een vluchtige, virtuele wereld die zonder moeite grensoverschrijdende gevolgen heeft. Dit vereist specifieke oplossingen. In de afgelopen tien jaren werden een aantal bezwaren opgelost door de wetgever en een aantal vragen beantwoord door de rechtspraak. Het toenemend aantal informaticamisdrijven staat garant voor een uitdagend volgend decennium.

⁶² Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, 149 (tegen dit vonnis werd hoger beroep ingesteld).

⁶³ P. VAN LINTHOUT en J. KERKHOFS, *o.c.*, *T.Strafr.* 2008, 79-95; zie ook: K.I. Gent 27 september 2007, *T.Strafr.* 2008, 129.

⁶⁴ Art. 8 E.V.R.M.