

**Recherches juridiques lausannoises**

Faculté de droit de l'Université de Lausanne

Editées par Hansjörg Peter, professeur à la Faculté de droit

**Jérémie Müller**

# **La cybercriminalité économique au sens étroit**

Analyse approfondie du droit suisse et aperçu  
de quelques droits étrangers

Schulthess § 2012  
ÉDITIONS ROMANDES

## Table des matières

<b>Table des abréviations</b> .....	<b>XVII</b>
<b>Bibliographie</b> .....	<b>XIX</b>
<b>Préambule 1</b>	
<b>Partie I : Les fondements</b> .....	<b>3</b>
<b>Chapitre I : Introduction</b> .....	<b>3</b>
<b>1. Les origines d'Internet</b> .....	<b>3</b>
<b>2. Historique de la lutte contre la cybercriminalité</b> .....	<b>4</b>
<b>2.1. Problématique</b> .....	<b>4</b>
<b>2.2. Au niveau national</b> .....	<b>4</b>
<b>2.2.1. SCOCI</b> .....	<b>5</b>
2.2.1.1. <i>Genèse et buts</i> .....	<b>5</b>
2.2.1.2. <i>Buts</i> .....	<b>6</b>
2.2.1.2.1. <i>Rechercher des contenus illicites sur Internet</i> .....	<b>6</b>
2.2.1.2.2. <i>Coordonner des procédures d'enquête</i> .....	<b>7</b>
2.2.1.2.3. <i>Analyser la criminalité sur Internet en Suisse</i> .....	<b>7</b>
<b>2.2.2. MELANI</b> .....	<b>7</b>
2.2.2.1. <i>Genèse et buts</i> .....	<b>7</b>
2.2.2.2. <i>Protection du cercle ouvert</i> .....	<b>7</b>
2.2.2.3. <i>Protection du cercle fermé</i> .....	<b>8</b>
<b>2.3. Au niveau international</b> .....	<b>8</b>
2.3.1. <i>Conseil de l'Europe</i> .....	<b>8</b>
2.3.2. <i>L'Union européenne</i> .....	<b>8</b>
2.3.3. <i>Organisation des Nations Unies</i> .....	<b>9</b>
2.3.4. <i>Organisation du Traité de l'Atlantique Nord</i> .....	<b>9</b>
2.3.5. <i>Interpol</i> .....	<b>9</b>
2.3.6. <i>Groupe des huit (G8)</i> .....	<b>10</b>
<b>3. Situation actuelle</b> .....	<b>11</b>
<b>Chapitre II : Définitions de la cybercriminalité économique</b> .....	<b>12</b>
<b>1. Définitions</b> .....	<b>12</b>
<b>1.1. La cybercriminalité</b> .....	<b>12</b>
1.1.1. <i>La cybercriminalité au sens étroit</i> .....	<b>12</b>
1.1.2. <i>La cybercriminalité au sens large</i> .....	<b>13</b>
<b>1.2. La criminalité économique</b> .....	<b>13</b>
<b>1.3. La cybercriminalité économique</b> .....	<b>13</b>
<b>2. Terminologie</b> .....	<b>14</b>
<b>Chapitre III : Le fonctionnement de l'informatique et d'Internet</b> .....	<b>15</b>
<b>1. Le système informatique</b> .....	<b>15</b>
<b>2. Les réseaux</b> .....	<b>17</b>
<b>2.1. Généralités</b> .....	<b>17</b>
<b>2.2. Internet : le réseau des réseaux</b> .....	<b>18</b>
2.2.1. <i>Le fonctionnement d'Internet</i> .....	<b>18</b>
2.2.2. <i>Résolution de noms</i> .....	<b>20</b>
2.2.3. <i>Le world wide web</i> .....	<b>20</b>
2.2.3.1. <i>La navigation</i> .....	<b>20</b>
2.2.3.2. <i>La recherche</i> .....	<b>21</b>
2.2.3.3. <i>Les sessions</i> .....	<b>21</b>
2.2.4. <i>Le courrier électronique</i> .....	<b>22</b>
2.2.5. <i>Le transfert de fichiers</i> .....	<b>22</b>
2.2.6. <i>Les fournisseurs d'accès Internet</i> .....	<b>22</b>
<b>2.3. La sécurité des réseaux</b> .....	<b>23</b>

2.3.1.	<i>La protection contre les attaques extérieures</i> .....	24
2.3.2.	<i>La protection contre les attaques intérieures</i> .....	26
2.3.2.1.	<i>Généralités</i> .....	26
2.3.2.2.	<i>Les différents types de logiciels malveillants</i> .....	27
2.3.2.3.	<i>Un remède : les antivirus et les antispywares</i> .....	28
2.3.3.	<i>Situation actuelle en matière de sécurité des réseaux</i> .....	28
<b>Chapitre IV : Bases légales</b> .....		<b>30</b>
1.	<b>Bases légales nationales</b> .....	<b>30</b>
1.1.	<b>Code pénal</b> .....	<b>30</b>
1.1.1.	<i>Les infractions propres à la criminalité informatique</i> .....	<b>30</b>
1.1.1.1.	<i>Genèse</i> .....	30
1.1.1.2.	<i>Arrêté fédéral portant approbation et mise en œuvre de la convention du Conseil de l'Europe sur la cybercriminalité</i> .....	30
1.1.1.3.	<i>Objets des infractions informatiques</i> .....	31
1.1.1.4.	<i>Les dispositions topiques du Code pénal</i> .....	32
1.1.1.4.1.	<i>La soustraction de données (art. 143 CP)</i> .....	32
1.1.1.4.2.	<i>L'accès indu à un système informatique (art. 143<sup>bis</sup> CP)</i> .....	34
1.1.1.4.3.	<i>La détérioration de données (art. 144<sup>bis</sup> CP)</i> .....	37
1.1.1.4.4.	<i>L'utilisation frauduleuse d'un ordinateur (art. 147 CP)</i> .....	38
1.1.1.5.	<i>Nature des infractions informatiques</i> .....	40
1.1.1.6.	<i>Nécessité d'adapter le Code pénal</i> .....	41
1.1.2.	<i>Les infractions économiques fréquemment liées à la criminalité informatique</i> .....	42
1.2.	<b>Droit pénal accessoire</b> .....	<b>42</b>
1.2.1.	<i>Loi sur les télécommunications</i> .....	42
1.2.2.	<i>Loi contre la concurrence déloyale</i> .....	43
2.	<b>Bases légales internationales</b> .....	<b>44</b>
2.1.	<b>Convention sur la cybercriminalité du 23 novembre 2001 (CCC)</b> .....	<b>44</b>
2.1.1.	<i>Genèse</i> .....	44
2.1.2.	<i>But</i> .....	44
2.1.3.	<i>Contenu</i> .....	45
2.1.3.1.	<i>Définitions</i> .....	45
2.1.3.1.1.	<i>Le système informatique</i> .....	45
2.1.3.1.2.	<i>Les données informatiques</i> .....	46
2.1.3.1.3.	<i>Le fournisseur de services</i> .....	46
2.1.3.1.4.	<i>Les données relatives au trafic</i> .....	46
2.1.3.2.	<i>Les différentes infractions</i> .....	47
2.1.3.2.1.	<i>Généralités</i> .....	47
2.1.3.2.2.	<i>Art. 2 CCC</i> .....	48
2.1.3.2.3.	<i>Art. 3 CCC</i> .....	49
2.1.3.2.4.	<i>Art. 4 CCC</i> .....	49
2.1.3.2.5.	<i>Art. 5 CCC</i> .....	50
2.1.3.2.6.	<i>Art. 6 CCC</i> .....	51
2.1.3.2.7.	<i>Art. 7 CCC</i> .....	52
2.1.3.2.8.	<i>Art. 8 CCC</i> .....	52
2.1.3.3.	<i>Droit procédural</i> .....	53
2.1.3.4.	<i>Compétence</i> .....	54
2.1.3.5.	<i>Coopération internationale</i> .....	55
2.2.	<b>Décision-cadre 2005/222/JAI du Conseil de l'Union européenne</b> .....	<b>55</b>
2.2.1.	<i>Genèse</i> .....	55
2.2.2.	<i>But</i> .....	55
2.2.3.	<i>Contenu</i> .....	56
2.3.	<b>Autres bases légales internationales</b> .....	<b>56</b>
3.	<b>Bases légales étrangères</b> .....	<b>57</b>
3.1.	<b>En Allemagne</b> .....	<b>57</b>
3.1.1.	<i>Historique</i> .....	57
3.1.2.	<i>Les dispositions topiques</i> .....	57
3.1.2.1.	<i>Ausspähen von Daten (§ 202a dStGB)</i> .....	57
3.1.2.2.	<i>Abfangen von Daten (§ 202b dStGB)</i> .....	58

3.1.2.3.	Vorbereitung des Ausspähen und Abfangen von Daten (§ 202c dStGB).....	58
3.1.2.4.	Computerbetrug (§ 263a dStGB).....	58
3.1.2.5.	Fälschung beweisrelevanter Daten (§ 269 dStGB) .....	59
3.1.2.6.	Datenveränderung (§ 303a dStGB).....	59
3.1.2.7.	Computersabotage (§ 303b dStGB).....	60
<b>3.2.</b>	<b>En Autriche</b> .....	<b>61</b>
3.2.1.	Historique.....	61
3.2.2.	Les dispositions topiques.....	61
3.2.2.1.	Widerrechtlicher Zugriff auf ein Computersystem (§ 118a öStGB) .....	61
3.2.2.2.	Missbräuchliches Abfangen von Daten (§ 119a öStGB) .....	62
3.2.2.3.	Datenbeschädigung (§ 126a öStGB) .....	62
3.2.2.4.	Störung der Funktionsfähigkeit eines Computersystems (§ 126b öStGB) .....	63
3.2.2.5.	Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c öStGB).....	63
3.2.2.6.	Betrügerischer Datenverarbeitungsmissbrauch (§ 148a öStGB).....	64
3.2.2.7.	Datenfälschung (§ 225a öStGB).....	65
<b>3.3.</b>	<b>En Italie</b> .....	<b>66</b>
3.3.1.	Historique.....	66
3.3.2.	Les dispositions topiques.....	67
3.3.2.1.	Falsita' in scrittura privata (art. 485 et 491 <sup>bis</sup> CPI) .....	67
3.3.2.2.	Accesso abusivo a un sistema informatico o telematico (art. 615 <sup>ter</sup> CPI) .....	67
3.3.2.3.	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 <sup>quater</sup> CPI).....	68
3.3.2.4.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 <sup>quater</sup> CPI) .....	68
3.3.2.5.	Danneggiamento di informazioni, dati e programmi informatici (art. 635 <sup>bis</sup> CPI) .....	69
3.3.2.6.	Danneggiamento di sistemi informatici o telematici (art. 635 <sup>quater</sup> CPI).....	69
3.3.2.7.	Frode informatica (art. 640 <sup>ter</sup> CPI) .....	70
<b>3.4.</b>	<b>En France</b> .....	<b>70</b>
3.4.1.	Historique.....	70
3.4.2.	Les dispositions topiques.....	71
3.4.2.1.	L'article 323-1 .....	71
3.4.2.2.	L' article 323-2 .....	72
3.4.2.3.	L' article 323-3 .....	73
3.4.2.4.	L' article 323-3-1 .....	73
<b>3.5.</b>	<b>En Angleterre</b> .....	<b>74</b>
3.5.1.	Historique.....	74
3.5.2.	Les dispositions topiques.....	74
3.5.2.1.	Unauthorised access to computer material (Section 1 Computer misuse Act) .....	74
3.5.2.2.	Unauthorised access with intent to commit or facilitate commission of further offences (Section 2 Computer misuse Act).....	75
3.5.2.3.	Unauthorised modification of computer material (Section 3 Computer misuse Act) .....	75
3.5.2.4.	Making, supplying or obtaining articles for use in offence under section 1 or 3 (Section 3A Computer misuse Act).....	76
<b>Partie II : La répression de la cybercriminalité économique.....</b>		<b>77</b>
<b>Chapitre I : Généralités.....</b>		<b>77</b>
1. Introduction.....		77
2. Méthodologie.....		77
<b>Chapitre II : Typologie des fraudes commises par voie électronique examinées</b>		
sous l'angle du droit suisse.....		79
1. Les fraudes nécessitant la participation de la victime ou d'un tiers .....		79
1.1. Les fraudes de type "phishing" .....		79
1.1.1. Définition.....		79
1.1.1.1. Description du mécanisme de base du "phishing".....		79
1.1.1.2. Évolution des méthodes de phishing.....		80
1.1.1.3. Problématique .....		81
1.1.2. Analyse du phishing "classique".....		81

1.1.2.1.	Qualifications juridiques .....	82
1.1.2.2.	Application de la partie générale .....	89
1.1.2.2.1.	Concours.....	89
1.1.2.2.2.	Degré de réalisation .....	89
1.1.2.2.3.	Participation.....	90
<b>1.1.3.</b>	<b>Analyse du phishing de type "man in the middle" (MitM).....</b>	<b>92</b>
1.1.3.1.	Qualifications juridiques .....	92
1.1.3.2.	Application de la partie générale .....	96
1.1.3.2.1.	Concours.....	96
1.1.3.2.2.	Degré de réalisation .....	96
1.1.3.2.3.	Participation.....	97
<b>1.1.4.</b>	<b>Analyse du phishing de type "man in the browser" (MitB).....</b>	<b>98</b>
1.1.4.1.	Qualifications juridiques .....	98
1.1.4.2.	Application de la partie générale .....	101
1.1.4.2.1.	Concours.....	101
1.1.4.2.2.	Degré de réalisation .....	102
1.1.4.2.3.	Participation.....	103
<b>1.1.5.</b>	<b>Illustrations .....</b>	<b>103</b>
1.1.5.1.	Les instituts financiers et le phishing.....	103
1.1.5.2.	RockPhish.....	103
1.1.5.3.	Koobface.....	104
<b>1.1.6.</b>	<b>Moyens de protection .....</b>	<b>104</b>
1.1.6.1.	Pistes techniques .....	104
1.1.6.2.	Pistes juridiques .....	105
<b>1.2.</b>	<b>Les fraudes de type extorsion.....</b>	<b>105</b>
<b>1.2.1.</b>	<b>Définition.....</b>	<b>105</b>
1.2.1.1.	Description du mécanisme de base.....	105
1.2.1.2.	Évolutions.....	106
1.2.1.3.	Problématique .....	106
<b>1.2.2.</b>	<b>Analyse de l'extorsion à l'attaque DDoS.....</b>	<b>107</b>
1.2.2.1.	Qualifications juridiques .....	107
1.2.2.2.	Application de la partie générale .....	108
1.2.2.2.1.	Degré de réalisation .....	108
1.2.2.2.2.	Participation.....	109
<b>1.2.3.</b>	<b>Analyse de l'extorsion au vol, à la dissimulation ou au cryptage de données.....</b>	<b>109</b>
1.2.3.1.	Qualifications juridiques .....	109
1.2.3.2.	Application de la partie générale .....	111
1.2.3.2.1.	Concours.....	111
1.2.3.2.2.	Degré de réalisation .....	112
1.2.3.2.3.	Participation.....	112
<b>1.2.4.</b>	<b>Illustrations .....</b>	<b>113</b>
1.2.4.1.	Zippo-A.....	113
1.2.4.2.	Ransom-A .....	113
<b>1.2.5.</b>	<b>Moyens de protection .....</b>	<b>113</b>
1.2.5.1.	Pistes techniques .....	113
1.2.5.2.	Pistes juridiques .....	114
<b>1.3.</b>	<b>Fraudes de type ventes aux enchères en ligne .....</b>	<b>114</b>
<b>1.3.1.</b>	<b>Définition.....</b>	<b>114</b>
1.3.1.1.	Description du mécanisme de base.....	114
1.3.1.2.	Évolution .....	115
1.3.1.3.	Problématique .....	116
<b>1.3.2.</b>	<b>Analyse des ventes aux enchères .....</b>	<b>116</b>
1.3.2.1.	Qualifications juridiques .....	116
1.3.2.2.	Application de la partie générale .....	120
1.3.2.2.1.	Concours.....	120
1.3.2.2.2.	Degrés de réalisation.....	120
1.3.2.2.3.	Participation.....	121
<b>1.3.3.</b>	<b>Illustrations .....</b>	<b>122</b>
1.3.3.1.	Achats à l'étranger .....	123
1.3.3.2.	eBay.....	123

1.3.4.	<b>Moyens de protection</b> .....	123
1.3.4.1.	Pistes techniques .....	123
1.3.4.2.	Pistes juridiques .....	124
1.4.	<b>Les fraudes de type transfert de valeurs patrimoniales</b> .....	124
1.4.1.	<b>Définition</b> .....	124
1.4.1.1.	Description du mécanisme de base.....	124
1.4.1.2.	Évolution .....	125
1.4.1.3.	Problématique .....	125
1.4.2.	<b>Analyse du transfert de valeurs patrimoniales</b> .....	125
1.4.2.1.	Qualifications juridiques .....	125
1.4.2.2.	Application de la partie générale .....	128
1.4.2.2.1.	Concours.....	128
1.4.2.2.2.	Degré de réalisation .....	128
1.4.2.2.3.	Participation .....	129
1.4.3.	<b>Illustration</b> .....	129
1.4.4.	<b>Moyens de protection</b> .....	130
2.	<b>Manipulations à l'insu de la victime</b> .....	132
2.1.	<b>Les fraudes de type drive by download</b> .....	132
2.1.1.	<b>Définition</b> .....	132
2.1.1.1.	Description du mécanisme de base.....	132
2.1.1.2.	Évolutions .....	133
2.1.1.3.	Problématique .....	133
2.1.2.	<b>Analyse de l'infection de systèmes informatiques</b> .....	134
2.1.2.1.	Qualifications juridiques .....	134
2.1.2.2.	Application de la partie générale .....	137
2.1.2.2.1.	Concours.....	137
2.1.2.2.2.	Degré de réalisation .....	138
2.1.2.2.3.	Participation .....	138
2.1.3.	<b>Illustrations</b> .....	140
2.1.3.1.	Le programme MPack .....	140
2.1.3.2.	Le cas de iFrameDollars.biz .....	141
2.1.3.3.	Infection des domaines.ch.....	141
2.1.4.	<b>Moyens de protection</b> .....	141
2.1.4.1.	Pistes techniques .....	141
2.1.4.2.	Pistes juridiques .....	142
2.2.	<b>Les fraudes de type réseau de zombies (bot-net)</b> .....	142
2.2.1.	<b>Définition</b> .....	142
2.2.1.1.	Description du mécanisme de base.....	142
2.2.1.2.	Évolution .....	145
2.2.1.3.	Problématique .....	145
2.2.2.	<b>Analyse des réseaux de zombies</b> .....	146
2.2.2.1.	Qualifications juridiques .....	146
2.2.2.2.	Application de la partie générale .....	151
2.2.2.2.1.	Concours.....	151
2.2.2.2.2.	Degré de réalisation .....	152
2.2.2.2.3.	Participation.....	153
2.2.3.	<b>Illustrations</b> .....	153
2.2.3.1.	Le ver Storm .....	154
2.2.3.2.	Arrestations de bot-herders .....	154
2.2.4.	<b>Moyens de protection</b> .....	154
2.2.4.1.	Pistes techniques .....	155
2.2.4.2.	Pistes juridiques .....	155
2.3.	<b>Les fraudes de type concurrence déloyale</b> .....	155
2.3.1.	<b>Définition</b> .....	155
2.3.1.1.	Description du mécanisme de base.....	155
2.3.1.2.	Évolution .....	157
2.3.1.3.	Problématique .....	158
2.3.2.	<b>Analyse des atteintes au système informatique</b> .....	158
2.3.2.1.	Qualifications juridiques .....	158

2.3.2.2.	<i>Application de la partie générale</i> .....	163
2.3.2.2.1.	<i>Concours</i> .....	163
2.3.2.2.2.	<i>Degré de réalisation</i> .....	163
2.3.2.2.3.	<i>Participation</i> .....	164
2.3.3.	<i>Analyse des actes de concurrence déloyale</i> .....	165
2.3.3.1.	<i>Qualifications juridiques</i> .....	165
2.3.3.2.	<i>Application de la partie générale</i> .....	168
2.3.3.2.1.	<i>Degré de réalisation</i> .....	168
2.3.3.2.2.	<i>Participation</i> .....	169
2.3.4.	<i>Illustrations</i> .....	169
2.3.4.1.	<i>Le cas heise.de</i> .....	170
2.3.4.2.	<i>Attaque contre l'Estonie</i> .....	170
2.3.5.	<i>Moyens de protection</i> .....	171
2.3.5.1.	<i>Pistes techniques</i> .....	171
2.3.5.2.	<i>Pistes juridiques</i> .....	171
2.4.	<i>Les fraudes de type espionnage industriel</i> .....	172
2.4.1.	<i>Définition</i> .....	172
2.4.1.1.	<i>Description du mécanisme de base</i> .....	172
2.4.1.2.	<i>Évolutions</i> .....	172
2.4.1.3.	<i>Problématique</i> .....	173
2.4.2.	<i>Analyse de l'espionnage industriel</i> .....	173
2.4.2.1.	<i>Qualifications juridiques</i> .....	173
2.4.2.2.	<i>Application de la partie générale</i> .....	176
2.4.2.2.1.	<i>Concours</i> .....	176
2.4.2.2.2.	<i>Degré de réalisation</i> .....	176
2.4.2.2.3.	<i>Participation</i> .....	177
2.4.3.	<i>Illustrations</i> .....	178
2.4.3.1.	<i>Espionnage industriel en Israël</i> .....	178
2.4.3.2.	<i>L'affaire Titan Rain</i> .....	178
2.4.3.3.	<i>Le cas twitter</i> .....	179
2.4.4.	<i>Moyens de protection</i> .....	179
2.4.4.1.	<i>Pistes techniques</i> .....	179
2.4.4.2.	<i>Pistes juridiques</i> .....	180
<b>Chapitre III : Solutions du droit international et de quelques droits étrangers..</b>		<b>181</b>
1.	<b>En droit international</b> .....	<b>181</b>
1.1.	<b>Les fraudes de type phishing</b> .....	<b>181</b>
1.1.1.	<b>Le phishing classique</b> .....	<b>181</b>
1.1.2.	<b>L'attaque de l'intermédiaire (MitM)</b> .....	<b>181</b>
1.1.3.	<b>L'attaque du navigateur (MitB)</b> .....	<b>182</b>
1.2.	<b>Les fraudes de type extorsion</b> .....	<b>183</b>
1.2.1.	<b>L'extorsion à l'attaque DDoS</b> .....	<b>183</b>
1.2.2.	<b>L'extorsion au vol, à la dissimulation ou au cryptage de données</b> .....	<b>183</b>
1.3.	<b>Les fraudes de type ventes aux enchères</b> .....	<b>184</b>
1.4.	<b>Les fraudes de type transfert d'argent</b> .....	<b>184</b>
1.5.	<b>Les fraudes de type drive by download</b> .....	<b>184</b>
1.6.	<b>Les fraudes de types réseau de zombies</b> .....	<b>185</b>
1.7.	<b>Les fraudes de type concurrence déloyale</b> .....	<b>185</b>
1.7.1.	<b>Les atteintes au système informatique</b> .....	<b>185</b>
1.7.2.	<b>Les actes de concurrence déloyale</b> .....	<b>186</b>
1.8.	<b>Les fraudes de type espionnage industriel</b> .....	<b>187</b>
2.	<b>En droits étrangers</b> .....	<b>188</b>
2.1.	<b>En droit allemand</b> .....	<b>188</b>
2.1.1.	<b>Les fraudes de type phishing</b> .....	<b>188</b>
2.1.1.1.	<b>Le phishing classique</b> .....	<b>188</b>
2.1.1.2.	<b>L'attaque de l'intermédiaire (MitM)</b> .....	<b>188</b>
2.1.1.3.	<b>L'attaque du navigateur (MitB)</b> .....	<b>189</b>
2.1.2.	<b>Les fraudes de type extorsion</b> .....	<b>189</b>
2.1.2.1.	<b>L'extorsion à l'attaque DDoS</b> .....	<b>189</b>

2.1.2.2.	<i>L'extorsion au vol, à la dissimulation ou au cryptage de données</i> .....	190
2.1.3.	<b>Les fraudes de type ventes aux enchères</b> .....	191
2.1.4.	<b>Les fraudes de type transfert d'argent</b> .....	191
2.1.5.	<b>Les fraudes de type drive by download</b> .....	192
2.1.6.	<b>Les fraudes de types réseau de zombies</b> .....	193
2.1.7.	<b>Les fraudes de type concurrence déloyale</b> .....	193
2.1.7.1.	<i>Les atteintes au système informatique</i> .....	193
2.1.7.2.	<i>Les actes de concurrence déloyale</i> .....	194
2.1.8.	<b>Les fraudes de type espionnage industriel</b> .....	195
2.2.	<b>En droit autrichien</b> .....	195
2.2.1.	<b>Les fraudes de type phishing</b> .....	195
2.2.1.1.	<i>Le phishing classique</i> .....	195
2.2.1.2.	<i>L'attaque de l'intermédiaire (MitM)</i> .....	196
2.2.1.3.	<i>L'attaque du navigateur (MitB)</i> .....	196
2.2.2.	<b>Les fraudes de type extorsion</b> .....	197
2.2.2.1.	<i>L'extorsion à l'attaque DDoS</i> .....	197
2.2.2.2.	<i>L'extorsion au vol, à la dissimulation ou au cryptage de données</i> .....	198
2.2.3.	<b>Les fraudes de type ventes aux enchères</b> .....	198
2.2.4.	<b>Les fraudes de type transfert d'argent</b> .....	199
2.2.5.	<b>Les fraudes de type drive by download</b> .....	199
2.2.6.	<b>Les fraudes de type réseau de zombies</b> .....	200
2.2.7.	<b>Les fraudes de type concurrence déloyale</b> .....	200
2.2.7.1.	<i>Les atteintes au système informatique</i> .....	200
2.2.7.2.	<i>Les actes de concurrence déloyale</i> .....	200
2.2.8.	<b>Les fraudes de type espionnage industriel</b> .....	201
2.3.	<b>En droit italien</b> .....	201
2.3.1.	<b>Les fraudes de type phishing</b> .....	201
2.3.1.1.	<i>Le phishing classique</i> .....	201
2.3.1.2.	<i>L'attaque de l'intermédiaire (MitM)</i> .....	202
2.3.1.3.	<i>L'attaque du navigateur (MitB)</i> .....	202
2.3.2.	<b>Les fraudes de type extorsion</b> .....	203
2.3.2.1.	<i>L'extorsion à l'attaque DDoS</i> .....	203
2.3.2.2.	<i>L'extorsion au vol, à la dissimulation ou au cryptage de données</i> .....	203
2.3.3.	<b>Les fraudes de type ventes aux enchères</b> .....	204
2.3.4.	<b>Les fraudes de type transfert d'argent</b> .....	204
2.3.5.	<b>Les fraudes de type drive by download</b> .....	205
2.3.6.	<b>Les fraudes de types réseau de zombies</b> .....	205
2.3.7.	<b>Les fraudes de type concurrence déloyale</b> .....	205
2.3.7.1.	<i>Les atteintes au système informatique</i> .....	205
2.3.7.2.	<i>Les actes de concurrence déloyale</i> .....	206
2.3.8.	<b>Les fraudes de type espionnage industriel</b> .....	206
2.4.	<b>En droit français</b> .....	207
2.4.1.	<b>Les fraudes de type phishing</b> .....	207
2.4.1.1.	<i>Le phishing classique</i> .....	207
2.4.1.2.	<i>L'attaque de l'intermédiaire (MitM)</i> .....	208
2.4.1.3.	<i>L'attaque du navigateur (MitB)</i> .....	208
2.4.2.	<b>Les fraudes de type extorsion</b> .....	209
2.4.2.1.	<i>L'extorsion à l'attaque DDoS</i> .....	209
2.4.2.2.	<i>L'extorsion au vol, à la dissimulation ou au cryptage de données</i> .....	209
2.4.3.	<b>Les fraudes de type ventes aux enchères</b> .....	210
2.4.4.	<b>Les fraudes de type transfert d'argent</b> .....	210
2.4.5.	<b>Les fraudes de type drive by download</b> .....	210
2.4.6.	<b>Les fraudes de type réseau de zombies</b> .....	211
2.4.7.	<b>Les fraudes de type concurrence déloyale</b> .....	211
2.4.7.1.	<i>Les atteintes au système informatique</i> .....	211
2.4.7.2.	<i>Les actes de concurrence déloyale</i> .....	211
2.4.8.	<b>Les fraudes de type espionnage industriel</b> .....	212
2.5.	<b>En droit anglais</b> .....	212
2.5.1.	<b>Les fraudes de type phishing</b> .....	212
2.5.1.1.	<i>Le phishing classique</i> .....	212

2.5.1.2.	<i>L'attaque de l'intermédiaire (MitM)</i> .....	213
2.5.1.3.	<i>L'attaque du navigateur (MitB)</i> .....	213
2.5.2.	<b>Les fraudes de type extorsion</b> .....	213
2.5.2.1.	<i>L'extorsion à l'attaque DDoS</i> .....	213
2.5.2.2.	<i>L'extorsion au vol, à la dissimulation ou au cryptage de données</i> .....	214
2.5.3.	<b>Les fraudes de type ventes aux enchères</b> .....	215
2.5.4.	<b>Les fraudes de type transfert d'argent</b> .....	215
2.5.5.	<b>Les fraudes de type drive by download</b> .....	216
2.5.6.	<b>Les fraudes de type réseau de zombies</b> .....	216
2.5.7.	<b>Les fraudes de type concurrence déloyale</b> .....	216
2.5.7.1.	<i>Les atteintes au système informatique</i> .....	216
2.5.7.2.	<i>Les actes de concurrence déloyale</i> .....	216
2.5.8.	<b>Les fraudes de type espionnage industriel</b> .....	217
<b>Partie III : La procédure</b> .....		<b>219</b>
<b>Chapitre I : For de poursuite et droit applicable</b> .....		<b>219</b>
1. <b>Les principes en matière de droit applicable</b> .....		219
1.1.	<b>Généralités</b> .....	219
1.2.	<b>Principe de la territorialité (art. 3 et 8 CP)</b> .....	220
1.2.1.	<i>Lieu où l'auteur a agi ou aurait dû agir</i> .....	220
1.2.2.	<i>Lieu où le résultat s'est produit ou aurait dû se produire</i> .....	220
1.2.2.1.	<i>Délits matériels et délits formels</i> .....	221
1.2.2.2.	<i>Évolution de la notion de résultat dans la jurisprudence fédérale</i> .....	221
1.2.2.3.	<i>La notion de résultat dans la doctrine</i> .....	222
1.3.	<b>Principe de protection de l'État (art. 4 CP)</b> .....	222
1.4.	<b>Principe d'universalité (art. 6 CP)</b> .....	223
1.5.	<b>Principe de la personnalité (art. 7 CP)</b> .....	223
2. <b>Les principes applicables en matière de for</b> .....		225
2.1.	<b>Généralités</b> .....	225
2.2.	<b>For du lieu de commission</b> .....	225
2.3.	<b>For du lieu de résultat de l'infraction</b> .....	225
2.4.	<b>For du lieu des premier actes d'instruction</b> .....	225
2.5.	<b>For en cas de pluralité d'infractions</b> .....	226
3. <b>Essai d'application des règles de droit applicable et de for au cas particulier du cyberspace</b> .....		227
3.1.	<b>Essai d'application au principe de territorialité</b> .....	227
3.1.1.	<i>Lieu où l'auteur a agi ou aurait dû agir</i> .....	227
3.1.2.	<i>Lieu où le résultat s'est produit ou aurait dû se produire</i> .....	228
3.1.3.	<b>Deux cas particuliers</b> .....	230
3.1.3.1.	<i>Les actes préparatoires</i> .....	230
3.1.3.2.	<i>Les actes de participation</i> .....	231
3.2.	<b>Essai d'application au principe de protection de l'État</b> .....	232
3.3.	<b>Essai d'application au principe d'universalité</b> .....	232
3.4.	<b>Essai d'application au principe de personnalité</b> .....	233
4. <b>Règles de conflit ?</b> .....		234
4.1.	<b>Conflit positif</b> .....	234
4.2.	<b>Conflit négatif</b> .....	234
<b>Chapitre II : Qualité pour agir</b> .....		<b>235</b>
1. <b>Généralités</b> .....		235
1.1.	<b>La partie plaignante (demanderesse au pénal)</b> .....	235
1.2.	<b>La partie plaignante (demanderesse au civil)</b> .....	235
2. <b>Les différents cas de figure</b> .....		236
2.1.	<b>Fraudes de type phishing</b> .....	236
2.1.1.	<i>Phishing classique</i> .....	236
2.1.2.	<i>Man in the Middle</i> .....	237

2.1.3.	<i>Man in the Browser</i> .....	237
2.2.	<i>Fraudes de type extorsion</i> .....	238
2.2.1.	<i>Extorsion à l'attaque DDoS</i> .....	238
2.2.2.	<i>Extorsion au vol, au cryptage ou à la dissimulation de données</i> .....	239
2.3.	<i>Fraudes de type ventes aux enchères</i> .....	239
2.4.	<i>Fraudes de type transfert d'argent</i> .....	240
2.5.	<i>Fraudes de type drive-by-download</i> .....	240
2.6.	<i>Fraudes de type réseaux de zombies</i> .....	241
2.7.	<i>Fraudes destinées à nuire à un concurrent</i> .....	241
2.7.1.	<i>Les atteintes au système informatique</i> .....	241
2.7.2.	<i>Les actes de concurrence déloyale</i> .....	242
2.8.	<i>Fraudes de type espionnage industriel</i> .....	242
<b>Partie IV : Quelles solutions pour demain ?</b> .....		<b>245</b>
<b>Chapitre I : Prévention générale</b> .....		<b>246</b>
1.	<i>Dans le domaine de l'information</i> .....	246
2.	<i>Dans le domaine juridique</i> .....	247
2.1.	<i>Moyens nécessaires à la découverte de l'infraction et de son auteur</i> .....	247
2.2.	<i>Collaboration internationale</i> .....	248
2.3.	<i>Nouvelle réglementation</i> .....	249
2.4.	<i>Une "police" internationale pour surveiller Internet</i> .....	250
2.5.	<i>Vers une cybercour de Justice ?</i> .....	251
3.	<i>Dans le domaine technique</i> .....	252
3.1.	<i>Collaboration avec le secteur privé</i> .....	252
3.2.	<i>Lutte contre le spam</i> .....	252
3.3.	<i>Protection accrue des réseaux</i> .....	253
<b>Chapitre II : Prévention spéciale</b> .....		<b>255</b>
1.	<i>Une nouvelle mesure ?</i> .....	255
2.	<i>Reconversion professionnelle</i> .....	256
<b>Partie V : Conclusion</b> .....		<b>257</b>
<b>Annexes 259</b>		
1.	<i>Bases légales suisses</i> .....	259
1.1.	<i>Code pénal suisse</i> .....	259
1.2.	<i>Loi sur la concurrence déloyale</i> .....	264
2.	<i>Bases légales internationales</i> .....	266
2.1.	<i>Convention sur la cybercriminalité</i> .....	266
2.2.	<i>Décision-cadre 2005/222/JAI du Conseil de l'Union européenne du 24 février 2005</i> .....	291
2.3.	<i>Convention du Conseil de l'Europe relative au blanchiment du 16 mai 2005</i> .....	299
2.4.	<i>Résolution 1565 (2007) de l'Assemblée parlementaire du Conseil de l'Europe</i> .....	301
3.	<i>Bases légales nationales</i> .....	304
3.1.	<i>Normes topiques en droit allemand</i> .....	304
3.1.1.	<i>Deutsches Strafgesetzbuch (dStGB)</i> .....	304
3.1.2.	<i>Gesetz gegen den unlauteren Wettbewerb (dUWG)</i> .....	309
3.1.3.	<i>Telemediengesetz (dTMG)</i> .....	312
3.2.	<i>Normes topiques en droit autrichien</i> .....	313
3.2.1.	<i>Österreichisches Strafgesetzbuch (öStGB)</i> .....	313
3.2.2.	<i>Unlauterer-Wettbewerbs-Gesetz (öUWG)</i> .....	318
3.2.3.	<i>Telekommunikationsgesetz (öTKG)</i> .....	319
3.3.	<i>Normes topiques en droit italien</i> .....	321
3.3.1.	<i>Codice penale italiano (CPI)</i> .....	321
3.3.2.	<i>Codice civile italiano (CCI)</i> .....	327

Table des matières

3.4. Normes topiques en droit français..... 329

3.4.1. Code pénal français (CPF)..... 329

3.4.2. Code des postes et communications électroniques..... 333

3.5. Normes topiques en droit anglais ..... 334

3.5.1. Computer Misuse Act 1990 (modifié par le Police and Justice Act 2006)..... 334

3.5.2. Forgery and counterfeiting Act 1981 ..... 337

3.5.3. Theft Act 1968 ..... 338

3.5.4. Fraud Act 2006..... 338

3.5.5. Proceeds of Crime Act 2002..... 339

3.5.6. Privacy and electronic communications regulations 2003 ..... 342

3.5.7. Trade Marks Act 1994..... 343

3.5.8. Defamation Act 1952..... 344

Glossaire ..... 345

Table des concordances des arrêts cités ..... 349

**Index..... 351**