

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

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

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
Chapitre IV : Bases légales		30
1. Bases légales nationales		30
1.1. Code pénal		30
1.1.1. Les infractions propres à la criminalité informatique		30
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^{bis} CP)</i>	34
1.1.1.4.3.	<i>La détérioration de données (art. 144^{bis} 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. Droit pénal accessoire		42
1.2.1.	<i>Loi sur les télécommunications</i>	42
1.2.2.	<i>Loi contre la concurrence déloyale</i>	43
2. Bases légales internationales		44
2.1. Convention sur la cybercriminalité du 23 novembre 2001 (CCC)		44
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. Décision-cadre 2005/222/JAI du Conseil de l'Union européenne		55
2.2.1.	<i>Genèse</i>	55
2.2.2.	<i>But</i>	55
2.2.3.	<i>Contenu</i>	56
2.3. Autres bases légales internationales		56
3. Bases légales étrangères		57
3.1. En Allemagne		57
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
3.2.	En Autriche	61
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
3.3.	En Italie	66
3.3.1.	Historique.....	66
3.3.2.	Les dispositions topiques.....	67
3.3.2.1.	Falsita' in scrittura privata (art. 485 et 491 ^{bis} CPI).....	67
3.3.2.2.	Accesso abusivo a un sistema informatico o telematico (art. 615 ^{ter} CPI).....	67
3.3.2.3.	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 ^{quater} CPI).....	68
3.3.2.4.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 ^{quater} CPI).....	68
3.3.2.5.	Danneggiamento di informazioni, dati e programmi informatici (art. 635 ^{bis} CPI).....	69
3.3.2.6.	Danneggiamento di sistemi informatici o telematici (art. 635 ^{quater} CPI).....	69
3.3.2.7.	Frode informatica (art. 640 ^{ter} CPI).....	70
3.4.	En France	70
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
3.5.	En Angleterre	74
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
Partie II : La répression de la cybercriminalité économique		77
Chapitre I : Généralités		77
1. Introduction.....		77
2. Méthodologie.....		77
Chapitre II : Typologie des fraudes commises par voie électronique examinées 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
1.1.3.	Analyse du phishing de type "man in the middle" (MitM).....	92
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
1.1.4.	Analyse du phishing de type "man in the browser" (MitB).....	98
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
1.1.5.	Illustrations	103
1.1.5.1.	Les instituts financiers et le phishing.....	103
1.1.5.2.	RockPhish.....	103
1.1.5.3.	Koobface.....	104
1.1.6.	Moyens de protection	104
1.1.6.1.	Pistes techniques	104
1.1.6.2.	Pistes juridiques	105
1.2.	Les fraudes de type extorsion.....	105
1.2.1.	Définition.....	105
1.2.1.1.	Description du mécanisme de base.....	105
1.2.1.2.	Évolutions.....	106
1.2.1.3.	Problématique	106
1.2.2.	Analyse de l'extorsion à l'attaque DDoS.....	107
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
1.2.3.	Analyse de l'extorsion au vol, à la dissimulation ou au cryptage de données.....	109
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
1.2.4.	Illustrations	113
1.2.4.1.	Zippo-A.....	113
1.2.4.2.	Ransom-A	113
1.2.5.	Moyens de protection	113
1.2.5.1.	Pistes techniques	113
1.2.5.2.	Pistes juridiques	114
1.3.	Fraudes de type ventes aux enchères en ligne	114
1.3.1.	Définition.....	114
1.3.1.1.	Description du mécanisme de base.....	114
1.3.1.2.	Évolution	115
1.3.1.3.	Problématique	116
1.3.2.	Analyse des ventes aux enchères	116
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
1.3.3.	Illustrations	122
1.3.3.1.	Achats à l'étranger	123
1.3.3.2.	eBay.....	123

1.3.4.	Moyens de protection	123
1.3.4.1.	Pistes techniques	123
1.3.4.2.	Pistes juridiques	124
1.4.	Les fraudes de type transfert de valeurs patrimoniales	124
1.4.1.	Définition	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.	Analyse du transfert de valeurs patrimoniales	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.	Illustration	129
1.4.4.	Moyens de protection	130
2.	Manipulations à l'insu de la victime	132
2.1.	Les fraudes de type drive by download	132
2.1.1.	Définition	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.	Analyse de l'infection de systèmes informatiques	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.	Illustrations	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.	Moyens de protection	141
2.1.4.1.	Pistes techniques	141
2.1.4.2.	Pistes juridiques	142
2.2.	Les fraudes de type réseau de zombies (bot-net)	142
2.2.1.	Définition	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.	Analyse des réseaux de zombies	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.	Illustrations	153
2.2.3.1.	Le ver Storm	154
2.2.3.2.	Arrestations de bot-herders	154
2.2.4.	Moyens de protection	154
2.2.4.1.	Pistes techniques	155
2.2.4.2.	Pistes juridiques	155
2.3.	Les fraudes de type concurrence déloyale	155
2.3.1.	Définition	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.	Analyse des atteintes au système informatique	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
Chapitre III : Solutions du droit international et de quelques droits étrangers..		181
1.	En droit international	181
1.1.	Les fraudes de type phishing	181
1.1.1.	Le phishing classique	181
1.1.2.	L'attaque de l'intermédiaire (MitM)	181
1.1.3.	L'attaque du navigateur (MitB)	182
1.2.	Les fraudes de type extorsion	183
1.2.1.	L'extorsion à l'attaque DDoS	183
1.2.2.	L'extorsion au vol, à la dissimulation ou au cryptage de données	183
1.3.	Les fraudes de type ventes aux enchères	184
1.4.	Les fraudes de type transfert d'argent	184
1.5.	Les fraudes de type drive by download	184
1.6.	Les fraudes de types réseau de zombies	185
1.7.	Les fraudes de type concurrence déloyale	185
1.7.1.	Les atteintes au système informatique	185
1.7.2.	Les actes de concurrence déloyale	186
1.8.	Les fraudes de type espionnage industriel	187
2.	En droits étrangers	188
2.1.	En droit allemand	188
2.1.1.	Les fraudes de type phishing	188
2.1.1.1.	Le phishing classique	188
2.1.1.2.	L'attaque de l'intermédiaire (MitM)	188
2.1.1.3.	L'attaque du navigateur (MitB)	189
2.1.2.	Les fraudes de type extorsion	189
2.1.2.1.	L'extorsion à l'attaque DDoS	189

2.1.2.2.	<i>L'extorsion au vol, à la dissimulation ou au cryptage de données</i>	190
2.1.3.	Les fraudes de type ventes aux enchères	191
2.1.4.	Les fraudes de type transfert d'argent	191
2.1.5.	Les fraudes de type drive by download	192
2.1.6.	Les fraudes de types réseau de zombies	193
2.1.7.	Les fraudes de type concurrence déloyale	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.	Les fraudes de type espionnage industriel	195
2.2.	En droit autrichien	195
2.2.1.	Les fraudes de type phishing	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.	Les fraudes de type extorsion	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.	Les fraudes de type ventes aux enchères	198
2.2.4.	Les fraudes de type transfert d'argent	199
2.2.5.	Les fraudes de type drive by download	199
2.2.6.	Les fraudes de type réseau de zombies	200
2.2.7.	Les fraudes de type concurrence déloyale	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.	Les fraudes de type espionnage industriel	201
2.3.	En droit italien	201
2.3.1.	Les fraudes de type phishing	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.	Les fraudes de type extorsion	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.	Les fraudes de type ventes aux enchères	204
2.3.4.	Les fraudes de type transfert d'argent	204
2.3.5.	Les fraudes de type drive by download	205
2.3.6.	Les fraudes de types réseau de zombies	205
2.3.7.	Les fraudes de type concurrence déloyale	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.	Les fraudes de type espionnage industriel	206
2.4.	En droit français	207
2.4.1.	Les fraudes de type phishing	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.	Les fraudes de type extorsion	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.	Les fraudes de type ventes aux enchères	210
2.4.4.	Les fraudes de type transfert d'argent	210
2.4.5.	Les fraudes de type drive by download	210
2.4.6.	Les fraudes de type réseau de zombies	211
2.4.7.	Les fraudes de type concurrence déloyale	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.	Les fraudes de type espionnage industriel	212
2.5.	En droit anglais	212
2.5.1.	Les fraudes de type phishing	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.	Les fraudes de type extorsion	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.	Les fraudes de type ventes aux enchères	215
2.5.4.	Les fraudes de type transfert d'argent	215
2.5.5.	Les fraudes de type drive by download	216
2.5.6.	Les fraudes de type réseau de zombies	216
2.5.7.	Les fraudes de type concurrence déloyale	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.	Les fraudes de type espionnage industriel	217
Partie III : La procédure		219
Chapitre I : For de poursuite et droit applicable		219
1. Les principes en matière de droit applicable		219
1.1.	Généralités	219
1.2.	Principe de la territorialité (art. 3 et 8 CP)	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.	Principe de protection de l'État (art. 4 CP)	222
1.4.	Principe d'universalité (art. 6 CP)	223
1.5.	Principe de la personnalité (art. 7 CP)	223
2. Les principes applicables en matière de for		225
2.1.	Généralités	225
2.2.	For du lieu de commission	225
2.3.	For du lieu de résultat de l'infraction	225
2.4.	For du lieu des premier actes d'instruction	225
2.5.	For en cas de pluralité d'infractions	226
3. Essai d'application des règles de droit applicable et de for au cas particulier du cyberspace		227
3.1.	Essai d'application au principe de territorialité	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.	Deux cas particuliers	230
3.1.3.1.	<i>Les actes préparatoires</i>	230
3.1.3.2.	<i>Les actes de participation</i>	231
3.2.	Essai d'application au principe de protection de l'État	232
3.3.	Essai d'application au principe d'universalité	232
3.4.	Essai d'application au principe de personnalité	233
4. Règles de conflit ?		234
4.1.	Conflit positif	234
4.2.	Conflit négatif	234
Chapitre II : Qualité pour agir		235
1. Généralités		235
1.1.	La partie plaignante (demanderesse au pénal)	235
1.2.	La partie plaignante (demanderesse au civil)	235
2. Les différents cas de figure		236
2.1.	Fraudes de type phishing	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
Partie IV : Quelles solutions pour demain ?		245
Chapitre I : Prévention générale		246
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
Chapitre II : Prévention spéciale		255
1.	<i>Une nouvelle mesure ?</i>	255
2.	<i>Reconversion professionnelle</i>	256
Partie V : Conclusion		257
Annexes 259		
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