

Myriam QUÉMÉNER

Joël FERRY

Cybercriminalité

Défi mondial et réponses

Préface de Yves CHARPENEL



1460 D

ECONOMICA

Table des matières

Introduction	1
PREMIÈRE PARTIE	
CONNAÎTRE LE CONTEXTE DE LA CYBERCRIMINALITE	7
Chapitre I. Internet et révolution numérique	9
I. L'origine du concept de l'Internet	9
II. Les échanges sur les réseaux numériques	11
Comment accéder à Internet ?.....	11
Le protocole TCP/IP (Transmission Control Protocol).....	15
Le serveur Proxy	18
III. Vers la convergence des instruments de communication	19
Chapitre II. Services et dérivés sur les réseaux numériques	23
I. Les prestations d'Internet	23
Le web.....	23
Le courrier électronique	25
Internet Relay Chat (IRC).....	26
La messagerie instantanée	27
Le forum de discussion.....	28
Le file transfert protocol (FTP)	29
Le blog	30
Quels outils pour la cybercriminalité ?.....	31

Chapitre III. Acteurs sur les réseaux numériques	36
I. Les internautes citoyens	36
II. Les prestataires des réseaux numériques	40
III. Les autres acteurs	50
Les autorités indépendantes	51
<i>La commission nationale de l'informatique et des libertés</i> (CNIL)	51
<i>L'autorité de régulation des communications électroniques et</i> <i>des Postes (ACERP)</i>	51
<i>La Direction du développement des médias (DDM)</i>	53
<i>Le Conseil Stratégique des technologies de l'Information</i> <i>(CSTI)</i>	53
<i>La Mission pour l'Economie Numérique (MEN)</i>	53
Les CERTs	54
<i>Le Secrétariat général de la défense nationale (SGDN)</i>	54
<i>La direction générale de la modernisation de l'Etat (DGME)</i> .	55
<i>Le ministère de l'éducation nationale</i>	55
<i>La délégation aux usages de l'Internet</i>	55
<i>Le Forum des Droits sur l'Internet</i>	56
IV. Les internautes délinquants	57

DEUXIEME PARTIE

CERNER LES FORMES DE CYBERCRIMINALITE	63
--	----

Chapitre I. Les technologies numériques, objets de la cybercriminalité	65
I. Informatique et protection des libertés	66
La nature des données à préserver	67
Les principes essentiels de la loi du 6 janvier 1978	68
L'intervention de la CNIL	74
II. Atteintes aux systèmes automatisés de données	78
III. Cryptologie et cybercriminalité	84
L'évolution de la cryptologie	86
Les mesures pénales et administratives compensatoires à la libération de la cryptologie	88
Les mesures organisationnelles	90
Chapitre II – Les technologies numériques, moyens de la cybercriminalité	95

I. Terrorisme et atteintes aux intérêts des Etats	95
II. Atteintes aux droits des personnes	105
Vol de données et usurpation d'identité.....	106
Atteintes aux documents numérisés	107
Atteintes à l'image des personnes	111
Diffusion d'images violentes sur Internet : le happy slapping	112
III. Atteintes aux personnes	115
Cybercriminalité et affaires criminelles	115
Exploitation sexuelle, proxénétisme et traite des êtres humains	118
Et à l'étranger ?	120
IV. Atteintes aux droits de propriété intellectuelle	123
Contrefaçon de marques.....	123
Contrefaçon de produits.....	128
Téléchargement illicite et droit d'auteur	131
V. Atteintes aux biens	138
I. Spamming, phishing et appât du gain	138
Le spamming.....	138
Le Phishing.....	143
II. Aspects spécifiques de la délinquance financière	148
III. Fraude à la carte bancaire	151
Les jeux en ligne	155
La réglementation des jeux de hasard	156
Les cybers casinos	157
La réglementation des loteries.....	159
La réglementation des paris hippiques	159
Chapitre III. Les technologies numériques, support de la cybercriminalité	166
I. Atteintes sexuelles aux mineurs	166
Protection des mineurs face aux contenus préjudiciables	168
Protection des mineurs face à la pédo-pornographie	168
II. Racisme, antisémitisme, xénophobie en ligne	181
III. Infractions « de presse »	186
Les incriminations	187
Blog et droit de la presse.....	190

IV. <i>Risques de dérives sectaires en ligne</i>	195
--	-----

TROISIEME PARTIE

LUTTER CONTRE LA CYBERCRIMINALITE	201
Chapitre I. Les ressources dédiées à la cybercriminalité	203
I. Les organes de coopération policière au plan international	203
Interpol	203
Europol.....	205
Le système d'information Schengen.....	207
II. Les services nationaux d'enquête	210
L'OCLCTIC : Une structure interministérielle.....	210
<i>Des services spécifiques à chaque institution</i>	212
La police nationale	212
La gendarmerie nationale.....	214
Le service technique de recherches judiciaires et de documentation (STRJD)	215
L'institut de recherche criminelle de la gendarmerie nationale (IRCGN)	216
La douane	216
III. Les organes judiciaires et de coordination	217
Les juridictions interrégionales spécialisées (JIRS)	217
Eurojust.....	217
Le Réseau judiciaire Européen (RJE)	219
Les magistrats de liaison, acteurs de l'amélioration de la coopération judiciaire.....	219
L'Office européen de lutte antifraude (OLAF)	220
Chapitre II. Des outils procéduraux adaptés à la cybercriminalité	222
I. Problématique de la compétence territoriale	222
II. Problématique des preuves	227
La recherche de la preuve numérique	227
La conservation des données contre le déperissement des preuves	229
III. Evolution des moyens d'investigation	234
Les interceptions de communications	234

Saisies de données, perquisitions à distance.....	237
Les réquisitions télématiques	239
Les infiltrations	239
La mise au clair de données chiffrées	240
Chapitre III. Evolution des instruments juridiques internationaux	242
I. L'action de l'Union européenne.....	242
II. La démarche de sensibilisation des Nations Unies	246
La législation relevant du premier pilier régissant le com- merce électronique	244
La législation relevant du troisième pilier régissant le droit des réseaux numériques	244
III. L'action de l'Organisation de coopération et de développement économique (OCDE)	247
IV. L'action du G 8.....	248
V. L'action contraignante du Conseil de l'Europe.....	249
La convention du conseil de l'Europe sur la Cybercriminalité	250
Application sur le plan international :.....	253
VI. Eléments de droit comparé	258
Etats-Unis	258
Canada.....	259
Royaume-Uni	259
Allemagne	260
Conclusion	261
Glossaire.....	265
Bibliographie sélective	273