

TABLE DES MATIERES

PREFACE ET REMERCIEMENTS.....	3
-------------------------------	---

I. INTRODUCTION : L'EMERGENCE D'UNE NOUVELLE MENACE.....	5
---	---

II. LE PHENOMENE DE LA DELINQUANCE INFORMATIQUE	7
---	---

A. Les délits économiques liés à l'informatique	7
1. La fraude par manipulation informatique	7
a) L'objet de la "fraude informatique" ou escroquerie.....	8
b) Modes opératoires : les méthodes de manipulation	10
c) Les délinquants	17
2. Espionnage informatique et piratage de logiciel.....	18
a) L'objet de l'espionnage	18
b) Modes opératoires	19
c) Les délinquants	21
3. Sabotage informatique	22
a) L'objet du sabotage.....	22
b) Modes opératoires	22
c) Les délinquants	25
4. Vol de services.....	26
5. Accès non autorisé au système informatique et "Hacking"	27
6. L'ordinateur instrument de commission de délits commerciaux traditionnels	28
B. Les atteintes informatiques à la vie privée.....	29
1. Utilisation de données incorrectes	30
a) Manipulation et effacement de données personnelles par des personnes non autorisées	30
b) Collecte, traitement et divulgation de données incorrectes par leur détenteur légitime	31
2. Collecte et stockage illicites de données correctes	32
a) Techniques illicites d'obtention de données	32
b) Contenu illicite des données stockées	32
3. Divulgation illégale et utilisation illicite de données	33
a) Données personnelles couvertes par les dispositions traditionnelles sur le secret.....	33
b) Données personnelles non secrètes.....	34

4.	Violations des formalités prévues par les lois sur la protection de la vie privée.....	35
C.	Autres abus et questions de définition	36
1.	Délits contre l'Etat et les Intérêts Politiques	36
2.	Extension des délits contre l'intégrité de la personne.....	36
3.	Questions de définition.....	37
III.	ETENDUE, IMPACT ET FUTUR DEVELOPPEMENT DE LA DELINQUANCE INFORMATIQUE.....	39
A.	L'étendue du phénomène de la délinquance informatique	39
1.	Le nombre des cas connus. Un recensement des études internationales sur la délinquance informatique	39
2.	Le problème du "chiffre noir"	44
B.	Montant des dommages.....	45
C.	Futurs développements	48
D.	Nécessité d'une Recherche Criminologique Internationale.....	49
IV.	LES PROBLEMES JURIDIQUES SOULEVES PAR LA DELINQUANCE INFORMATIQUE.....	51
A.	Les délits économiques liés à l'informatique	51
1.	Escroquerie par manipulation d'ordinateur	53
a)	<i>Problèmes de droit traditionnel</i>	53
1)	Vol et détournement de fonds	53
2)	Escroquerie.....	54
3)	Escroquerie par carte de crédit	56
4)	Abus de confiance	56
5)	Faux en écriture et infractions connexes	57
6)	Résumé et conclusion	58
b)	<i>Les nouvelles lois</i>	59
1)	La Loi Suédoise sur les Données de 1973.....	59
2)	La législation américaine de 1976 à 1985.....	59
3)	Réforme législative au Royaume Uni, en particulier la loi de 1981 sur le Faux et la Contrefaçon.....	63
4)	La législation australienne de 1983 à 1985	64
5)	La Loi Canadienne de 1985 Amendant le Code Pénal.....	66
6)	La loi danoise de 1985 sur la "Data Kriminalitet".....	67
7)	"Seconde Loi Allemande de 1986 pour la Prévention des Délits Economiques"	67

8)	La loi autrichienne de 1987.....	68
9)	La loi française de 1988.....	68
c)	<i>Projets et propositions de lois</i>	69
1)	Amendements en Suisse et Grèce.....	69
2)	Amendements dans les pays nordiques.....	70
3)	Les solutions adoptées au Portugal.....	71
d)	<i>Analyse comparative des projets d'amendement</i>	72
e)	<i>Suggestions de politique législative</i>	73
2.	Espionnage informatique, piratage de programmes et copie de "puces".....	74
a)	<i>La protection de l'ensemble des données stockées dans les systèmes informatiques</i>	75
1)	Le droit de propriété traditionnel.....	75
2)	Secrets d'affaires et droit de la concurrence.....	80
—	La situation juridique actuelle.....	80
—	Propositions de réforme.....	83
—	Evaluation et suggestions de politique législative.....	85
3)	Protection de certains types d'information et de certaines relations juridiques.....	86
—	Protection de certains types d'information.....	86
—	Protection de certaines relations juridiques.....	87
4)	La protection pénale générale des données stockées par informatique.....	89
5)	Protection par le droit des contrats.....	89
b)	<i>Protection renforcée des programmes d'ordinateur</i>	90
1)	Le droit des brevets.....	92
2)	Le droit de la propriété intellectuelle.....	94
—	L'applicabilité du droit d'auteur.....	94
—	L'étendue de la protection par le droit d'auteur.....	102
—	La nécessité d'une révision du Droit Pénal.....	105
3)	Protection particulière des programmes d'ordinateur.....	107
c)	<i>Protection Particulière des Circuits Intégrés</i>	109
1)	Protection par les règles de droit traditionnelles.....	110
2)	Nouvelles lois, propositions et projets de loi et leur coordination internationale.....	111
3.	Sabotage informatique.....	114
a)	<i>Problèmes de droit traditionnel</i>	114
b)	<i>Nouvelles lois, projets et propositions de lois</i>	116
c)	<i>Suggestions de politique législative</i>	119
4.	L'utilisation non autorisée d'ordinateurs.....	119
a)	<i>Les problèmes de droit traditionnel</i>	119
b)	<i>Nouvelles lois, projets et propositions de lois</i>	121
c)	<i>Suggestions de politique législative</i>	124
5.	L'accès non autorisé (Protection de l'Intégrité des Systèmes Informatiques).....	125
a)	<i>La situation juridique en vigueur</i>	126
b)	<i>Lois nouvelles, propositions et projets de réforme</i>	127
c)	<i>Evaluation et suggestions de politique législative</i>	130

6.	Fraude fiscale et infractions douanières.....	131
a)	<i>Fraude fiscale "traditionnelle" assistée par ordinateur.....</i>	131
b)	<i>Pratiques comptables nationales et évaluation nationale des logiciels.....</i>	132
c)	<i>Problèmes fiscaux et douaniers posés par les flux transfrontières de données.....</i>	133
d)	<i>Recommandations de politique législative.....</i>	134
7.	Conclusion : les Recommandations du Groupe de Travail de l'O.C.D.E.	134
B.	Les atteintes informatiques à la vie privée.....	135
1.	Le cadre international.....	136
a)	<i>Les lignes directrices de l'O.C.D.E.</i>	137
b)	<i>La Convention du Conseil de l'Europe</i>	138
c)	<i>Les résolutions et recommandations des Communautés Européennes.....</i>	139
2.	Les concepts généraux des législations nationales.....	140
a)	<i>Les législations en vigueur</i>	140
b)	<i>Analyse comparative</i>	144
3.	Concepts pénaux et violation des Lois sur la Vie Privée.....	147
a)	<i>Les différents champs d'application.....</i>	148
b)	<i>Nature des délits</i>	148
1)	<i>Violations matérielles des droits à la vie privée</i>	149
2)	<i>Violations des exigences formelles des lois</i>	152
3)	<i>Violation des Droits à l'Information de l'Individu.....</i>	154
4)	<i>Négligence dans l'application des mesures de sécurité.....</i>	154
c)	<i>Résumé et conclusions.....</i>	155
4.	Suggestion d'Actions	155
C.	Problèmes de procédure.....	157
1.	Administration de la preuve par enregistrement informatique.....	158
a)	<i>Différences entre les pays de droit de tradition germano-romaniste et les pays de common law.....</i>	158
b)	<i>Nouvelles lois et projets de loi dans les pays de common law.....</i>	159
c)	<i>Coopération Internationale, en particulier en droit de procédure civile.....</i>	161
2.	Problèmes procéduraux dans les cas internationaux de délinquance informatique.....	162
D.	Nécessité du développement du droit comparé et de la coopération internationale.....	163

V. LES MESURES DE SECURITE QUE DOIVENT PRENDRE LES UTILISATEURS D'ORDINATEUR.....	165
A. Les buts et l'étendue des mesures de sécurité.....	165
1. Les buts à atteindre.....	165
2. Les menaces visées.....	166
B. L'élaboration d'une stratégie de sécurité.....	166
1. La nécessité d'une prise de conscience des risques et de l'organisation d'un groupe de travail.....	166
2. Détermination des mesures de protection à mettre en oeuvre.....	167
a) <i>Identification des biens</i>	167
b) <i>Evaluation du risque</i>	168
c) <i>Sélection des mesures de protection</i>	169
3. Contrôle du système et mise en place de contre-mesures.....	170
a) <i>Les tactiques organisationnelles utilisées par les délinquants</i>	170
b) <i>Les tactiques utilisées par les délinquants en matière de programmation de système et d'application</i>	171
c) <i>Les tactiques utilisées par les délinquants en matière de programmation de système</i>	172
d) <i>Ecoutes téléphoniques et autres méthodes "techniques"</i>	173
4. La mise en place, le contrôle et la mise à jour du système de sécurité.....	174
C. Les principaux éléments d'un système de sécurité efficace.....	175
1. Les mesures de sécurité personnelles et éducatives.....	175
a) <i>Les contrôles</i>	176
b) <i>Motivation, éducation et codes d'éthique</i>	177
2. Les mesures de sécurité physique.....	177
a) <i>La conception architecturale</i>	178
b) <i>Les matériaux et équipements des bâtiments</i>	178
3. Les mesures de sécurité organisationnelles et techniques.....	179
a) <i>Les mesures générales de contrôle</i>	179
b) <i>Les contrôles spéciaux de l'input</i>	182
c) <i>Les contrôles spéciaux des communications</i>	182
d) <i>Les contrôles spéciaux du traitement</i>	183
e) <i>Les contrôles spéciaux du stockage des données</i>	184
f) <i>Les contrôles spéciaux des sorties</i>	185
g) <i>La protection spéciale des programmes sous licence</i>	186
4. Le contrôle interne.....	187
5. Assurance contre la délinquance informatique.....	188
6. La formulation des contrats.....	189
7. Les procédures et actions juridiques en cas de suspicion et de pertes.....	190
D. Les aspects internationaux.....	192

VI. LA POURSUITE JUDICIAIRE DE LA DELINQUANCE INFORMATIQUE.....	193
A. Difficultés de détection	193
1. Le déguisement du délit.....	193
2. Les indices cachés	194
3. L'invisibilité de la preuve.....	194
4. L'encodage de la preuve	195
5. L'effacement de la preuve	196
6. Le grand nombre de données.....	196
7. L'inexpérience des enquêteurs	197
8. Incertitudes juridiques et frontières nationales	197
B. Les mesures à prendre	198
1. Formation spéciale des enquêteurs dans plusieurs pays	198
2. Le contenu de la formation sur la détection de la délinquance informatique.....	200
 VII. CONCLUSION : NECESSITE DE RECHERCHES SUPPLEMENTAIRES, D'INITIATIVES ET DE COOPERATION INTERNATIONALES	203
 ANNEXE 1	
ELEMENTS DE BIBLIOGRAPHIE INTERNATIONALE.....	205
Une compilation des principales études sur la délinquance informatique effectuées en Australie, en Autriche, en Belgique, au Canada, au Danemark, en République Fédérale d'Allemagne, en Finlande, en France, en Italie, au Japon, au Luxembourg, aux Pays-Bas, en Norvège, en Suède, en Suisse, au Royaume Uni, aux Etats-Unis et à l'initiative d'organisations internationales.	
 ANNEXE 2	
CORPUS IURIS INTERNATIONAL DES TEXTES SUR LA DELINQUANCE INFORMATIQUE	219
Une compilation des lois, projets et propositions de lois sur la délinquance informatique en Australie, en Autriche, au Canada, au Danemark, en Finlande, en France, en République Fédérale d'Allemagne, en Italie, au Japon, au Luxembourg, aux Pays-Bas, en Norvège, en Suisse, au Royaume Uni et aux Etats-Unis.	